NISZ

Nemzeti Infokommunikációs Szolgáltató Zrt.

Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott minősített tanúsítványszolgáltatásokhoz (BSZ-DÁP-TAN)

Verziószám	1.4
OID	0.2.216.1.200.1100.100.42.3.1.38
Hatályba lépés dátuma	2025.02.05.
Dokumentum besorolása	nyilvános
Jóváhagyó	Adorján István

Adorján István

Digitálisan aláírta: Adorján István
Dátum: 2025.02.04 09:37:19 +01'00'

Változáskövetés

verzió	módosítás dátuma	a változás leírása	készítette	ellenőrizte	jóváhagyta
0.1	2024.07.08	első változat	NISZ Zrt. Polysys Kft. ACPM Zrt.	Kővári-Szabó Zoltán Nagy Benjámin	-
0.2	2024.07.15	észrevételeket beépítő, a tárolt kulcsos szolgáltatást kihagyó (különálló dokumentumba szervező) változat	ACPM Zrt.	Kővári-Szabó Zoltán Nagy Benjámin	-
0.3	2024.07.22	DÁP szolgáltató beépítése	ACPM Zrt.	Kővári-Szabó Zoltán Nagy Benjámin	-
0.4	2024.07.30	Felügyeleti szervnek benyújtott előzetes változat	ACPM Zrt.	Kővári-Szabó Zoltán Nagy Benjámin	-
0.5	2024.11.04.	Továbbfejlesztett változat	Kővári-Szabó Zoltán	Nagy Benjámin ACPM Zrt.	-
0.6	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	2024.12.11	A megfelelőségértékelési eljáráson tett észrevételek alkalmazása.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.2	2024.12.17	Hatálybalépés dátumának módosítása.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.3	2025.01.28	• A visszavonáskezelésre vonatkozó rendelkezésreállási követelménynek való megfeleléssel történő 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. (továbbiakban, mint Kormányzati Hitelesítés Szolgáltató vagy Szolgáltató) Bizalmi Szolgáltatási Szabályzata, amely a Digitális Állampolgárság Program keretében megvalósított elektronikus aláírás funkcióhoz szükséges minősített tanúsítványszolgáltatás nyújtására és igénybevételére vonatkozik.

A Szolgáltató a fenti tárgykörben az alábbi szolgáltatást nyújtja:

> A Digitális Állampolgárság Program (DÁP) keretében az állampolgárok, mint természetes személyek számára elektronikus aláírás célú EU minősített tanúsítvány kibocsátása, ezen tanúsítványokhoz kapcsolódóan visszavonási és tanúsítvány állapot információk biztosítása (a továbbiakban DÁP-TAN szolgáltatás)

A DÁP-TAN szolgáltatás a {J1} eIDAS 3. cikk 16. pont a) alpontjának megfelelő alábbi bizalmi szolgáltatásnak felel meg:

> *elektronikus aláírások tanúsítványainak kibocsátása*

Jelen bizalmi *szolgáltatási szabályzat* a DÁP-TAN szolgáltatás eljárásrendi és működési szabályait tartalmazza.

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

1.1 Áttekintés

A szolgáltatási szabályzat célja, hogy összefoglalja mindazokat az információkat, melyeket a Szolgáltató Szolgáltatásaival 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, a kibocsátott tanúsítványok, tanúsítvány visszavonási listák, valós idejű tanúsítvány-állapot válaszok 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 kibocsátott minősített tanúsítványokhoz"; OID: 0.2.216.1.200.1100.100.42.3.1.36 (BR-DÁP-TAN).

Jelen bizalmi szolgáltatási szabályzat az {Sz13} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában – a szükséges, Szolgáltatóra 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-TAN 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 a Digitális Állampolgárság Program keretében nyújtott minősített tanúsítványszolgáltatáshoz”

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

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

Jelen BSZ-DÁP-TAN tartalmazza a BR-DÁP-TAN bizalmi szolgáltatási rend hatálya alatt kiadott tanúsítványok kibocsátására és felhasználására vonatkozó részletes szabályokat.

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

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

1.2.2 A dokumentum azonosítása

A BSZ-DÁP-TAN a DÁP tv. 8. § 43. pontja szerinti *szolgáltatási szabályzat*, mely a DÁP-TAN szolgáltatás eljárásrendi és működési szabályait tartalmazza és amely egyúttal az ETSI EN 319 401 szerinti ún. *„trust service practice statement”*-nek és az ETSI EN 319 411-1 szerinti ún. *„certification practice statement”*-nek tekintendő.

1.2.3 Hitelesítési rendek

A BR-DÁP-TAN bizalmi szolgáltatási rend (OID: 0.2.216.1.200.1100.100.42.3.1.36) megfelel az {Sz3} EN 319 411-2 szabvány 5.5.1 fejezetében definiált `QCP-n-qscd` (OID: 0.4.0.194112.1.2) hitelesítési rendnek.

Szolgáltató az Aláírók tanúsítványának `certificatePolicy` kiterjesztésében mind a saját (BR-DÁP-TAN) mind pedig a szabványos (`QCP-n-qscd`) hitelesítési rend OID-ját is feltünteti.

1.3 PKI közösség

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

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

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

1.3.1 Hitelesítő szervezet

A hitelesítő szervezet a Szolgáltató központi szervezete, amely a hitelesítőközpontokból, a szolgáltatás-támogató informatikai rendszerek erőforrásaiból, az ezt körül vevő biztonságos fizikai

környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Jelen szolgáltatási szabályzat szempontjából feladatai közé tartozik a tanúsítvány igénylések feldolgozása, tanúsítványok kibocsátása, tanúsítványok visszavonása, valamint a kibocsátott tanúsítványokra vonatkozóan visszavonási információk szolgáltatása.

Jelen bizalmi BSZ-DÁP-TAN hatálya alatt Szolgáltató kizárólag az állampolgárok részére, a Digitális Állampolgárság Program keretében bocsát ki tanúsítványokat.

Gyökér-hitelesítőközpont

A Szolgáltató ECC alapú gyökér-hitelesítőközpontja P-384-es görbét alkalmazó ECC kulcsával és SHA384 algoritmus felhasználásával szolgáltatói tanúsítványokat bocsát ki a produktív hitelesítőközpontok részére.

A gyökér-hitelesítőközpont főbb adatai a következők.

Subject (alany): CN=GovCA Főtanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=GovCA Főtanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

A gyökértanúsítvány SHA1 lenyomata:
49:47:e8:6b:02:1f:f2:e3:94:b3:dd:d4:fd:0f:da:65:78:e6:49:7f

A gyökértanúsítvány SHA256 lenyomata:
B1:ED:0B:29:D0:54:2B:2A:13:71:D9:66:F5:8E:42:0B:9E:BD:9C:A1:9F:B9:B2:AF:81:E6:DE:1E:99:D5:E0:8A

Produktív hitelesítőközpont

A Szolgáltató produktív hitelesítőközpontja P-384-es görbét alkalmazó ECC kulcsával és SHA384 algoritmus felhasználásával végtanúsítványokat bocsát ki az Aláírók részére.

A produktív hitelesítőközpont tanúsítványának főbb adatai a következők.

Subject (alany): organizationIdentifier=VATHU-10585560, CN=Digitális Állampolgárság Tanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=GovCA Főtanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

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 igazolja az Aláírók személyazonosságát.

1.3.3 Előfizetők

A DÁP-TAN szolgáltatás előfizetői Magyarország azon állampolgárai, akik a Szolgáltatótól a DÁP keretalkalmazáson keresztül a jelen BSZ-DÁP-TAN szerint tanúsítványt igényelnek és az {D1} ÁSZF-DÁP elfogadásával Szolgáltatási Szerződést kötnek a Szolgáltatóval a DÁP-TAN és DÁP-TK szolgáltatások igénybevételére. Mivel az Aláíró a jelen 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 Szolgáltató kizárólag a Digitális Állampolgárság Program keretében, Magyarország azon állampolgárai részére biztosít szolgáltatást, akik megfelelnek a 4.1.1 pontban foglaltaknak.

Az Aláíró felelősségét és kötelezettségeit a 9.6.3 fejezet írja le.

1.3.4 Érintett Felek

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

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

Az Érintett Felek felelősségét a 9.6.4 fejezet írja le.

1.3.5 Egyéb felek

1.3.5.1 Felügyeleti Szerv

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

1.3.5.2 Kiberbiztonsági Felügyelet

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

1.4 A tanúsítvány alkalmazhatósága

A BSZ-DÁP-TAN hatálya alatt kibocsátott tanúsítvány az {J1} eIDAS - szerinti minősített tanúsítvány,

az {Sz4} EN 319 412-1 szabvány 3.1 fejezetében az „EU minősített tanúsítványra” vonatkozó követelményeknek megfelelően.

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

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

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

Teszttanúsítványok

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

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

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

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

1.4.1 Engedélyezett tanúsítvány használat

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

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

1.4.2 Tiltott tanúsítvány használat

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

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

1.5 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 és egyéb szabályzatai tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek eredményeit megfelelő módosításokkal alkalmazza az érintett dokumentumokban.

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

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

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

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

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

1.6 Fogalmak, rövidítések és hivatkozások

1.6.1 Fogalmak

alany: A Szolgáltató által kiadott tanúsítványban azonosított entitás, aki a tanúsítványban szereplő nyilvános kulcsnak (elektronikus aláírás érvényesítési adat) megfelelő magánkulcsot (elektronikus aláírás létrehozásához használt adat) birtokolja.
Jelen bizalmi szolgáltatási szabályzat szerint az Alany az állampolgár.

aláíró: elektronikus aláírás létrehozó természetes személy.
Jelen bizalmi szolgáltatási szabályzat szerint az Aláíró az állampolgár.

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

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

bizalmi felügyelet: lásd „felügyeleti szerv”.

bizalmi 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 az a) pont alatti szolgáltatás, azzal, hogy a Szolgáltató jelen BSZ-DÁP-TAN keretében kizárólag elektronikus aláírások tanúsítványainak

kibocsátását végzi.

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

bizalmi szolgáltatási rend: olyan szabálygyűjtemény, amelyben egy bizalmi szolgáltató igénybe vevő vagy más személy valamely bizalmi szolgáltatás használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára.

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

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

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

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

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

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

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

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

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

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

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

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

elektronikus aláírás minősített tanúsítványa: olyan elektronikus aláírás céljára használt tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel a {J1} eIDAS I.

mellékletében megállapított követelményeknek.

elektronikus aláírás érvényesítés: az elektronikusan aláírt elektronikus dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a bizalmi szolgáltató által közzétett elektronikus aláírás érvényesítési adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával.

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

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

elektronikus azonosító eszköz: olyan fizikai és/vagy nem fizikai egység, amely személyazonosító adatokat tartalmaz, és amelyet online szolgáltatások, vagy adott esetben offline szolgáltatások céljából történő hitelesítésre használnak.

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

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

elektronikus bélyegző minősített tanúsítványa: elektronikus bélyegző olyan tanúsítványa, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel a {J1} eIDAS III. mellékletében megállapított követelményeknek.

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

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

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

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

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

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

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

érintett fél: az a természetes személy vagy jogi személy, aki/amely az elektronikusan aláírt, és/vagy elektronikusan időbélyegzett dokumentum fogadója, és az adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az elektronikus aláírás és/vagy az elektronikus időbélyegző hitelességének ellenőrzésekor.

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

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

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

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 visszavonás igényléséhez szükséges azonosítását elvégző folyamat.

felügyeleti szerv: az adott tagállamban kijelölt felügyeleti szerv (Magyarországon a Nemzeti Média- és Hírközlési Hatóság), amely a bizalmi szolgáltatók felügyeletét végzi, melynek keretében előzetes és utólagos felügyeleti tevékenységek révén ellenőrzi, hogy a szolgáltatók és az általuk nyújtott szolgáltatások eleget tesznek a jogszabályban megállapított követelményeknek.

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

a) kizárólag az aláíróhoz köthető;
b) alkalmas az aláíró azonosítására;
c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozták létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

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

a) kizárólag a bélyegző létrehozójához kötött;

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

gyökér-hitelesítőközpont (ROOT CA, vagy Főtanúsítvány kiadó): az elsőnek létrehozott, fizikailag is működő hitelesítőközpont, amely az alárendelt másodlagos (produktív) hitelesítőközpontokat hitelesíti.

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

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

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

időbélyegző: lásd „elektronikus időbélyegző”.

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

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

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

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

Kiberbiztonsági Felügyelet: az adott tagállamban kijelölt felügyeleti szerv (Magyarországon a Szabályozott Tevékenységek Felügyeleti Hatósága).

kompromittálódás: az az eset, amikor a magánkulcs (elektronikus aláírás létrehozásához használt adat vagy elektronikus bélyegző létrehozásához használt adat) használatára arra nem jogosított személy képessé válik vagy azokat megismeri.

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

kriptográfiai modul (Hardware Security Module - HSM): olyan hardver alapú biztonságos eszköz, amely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására.

lenyomat: olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti a következő feltételeket:

- a képzett lenyomat egyértelműen származtatható az elektronikus dokumentumból;
- a képzett lenyomatból az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés;
- a képzett lenyomat alapján az elvárható biztonsági szinten belül nem lehetséges olyan elektronikus dokumentum utólagos létrehozatala, melyre alkalmazva a lenyomatképző eljárást, annak eredményeképp az adott lenyomat keletkezik.

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 (megfelelőségértékelési tevékenységeket – beleértve a kalibrálást, vizsgálatot, tanúsítást és ellenőrzést – végző) szervezet, amelyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére, vagy az európai digitális személyiadat-tárcák vagy az elektronikus azonosító eszközök tanúsításának elvégzésére.

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

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

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

minősített elektronikus aláírás létrehozó eszköz: olyan elektronikus aláírás létrehozó eszköz, amely megfelel a {J1} eIDAS II. mellékletben megállapított követelményeknek, rövidítése: QSCD (Qualified Signature Creation Device).
Korábbi elnevezése: biztonságos aláírás-létrehozó eszköz (BALE).

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.

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

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

regisztrációs adatok: azon információk, adatok összessége, amelyeket a Szolgáltató a tanúsítványkiadás érdekében az Aláíróról begyűjt.

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

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.

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.

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

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

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

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

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

tanúsítvány: az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a weboldal-hitelesítő tanúsítvány, valamint mindazon, a bizalmi szolgáltatás keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a tanúsítványra vonatkozó érvényesítési adatot és a tanúsítvány használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen.

tanúsítvány visszavonási lista (Certificate Revocation List - CRL): valamely okból visszavont vagy felfüggesztett, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a bizalmi szolgáltató bocsát ki és hitelesít.

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

távoli minősített elektronikus aláírás létrehozó eszköz: az aláíró nevében valamely minősített bizalmi szolgáltató által a {J1} eIDAS 29a. cikkével összhangban kezelt, minősített elektronikus aláírás létrehozó eszköz.

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

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

1.6.2 Rövidítések

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

DÁP-TK		Szolgáltató BSZ-DÁP-TK szerinti szolgáltatása
HSM	Hardware Security Module	hardver biztonsági modul, kriptográfiai modul
NTP	Network Time Protocol	időforrás protokoll
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
PDS-DÁP	Public Disclosure Statement	Szolgáltatási Kivonat a Digitális Állampolgárság Program keretében biztosított bizalmi szolgáltatásokhoz
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
QSCD	Qualified Signature Creation Device	minősített elektronikus aláírás létrehozó eszköz
RA	Registration Authority	regisztrációs szervezet
UTC	Coordinated Universal Time	koordinált univerzális idő

1.6.3 Hivatkozások

1.6.3.1 Jogszabályi hivatkozások

{J1} Az Európai Parlament és a Tanács (EU) 910/2014 rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (eIDAS)

{J2} 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (DÁP tv.)

{J3} 2013. évi V. törvény a Polgári Törvénykönyvről

{J4} 2016. évi CXXX. törvény a polgári perrendtartásról

{J5} 24/2016. (VI.30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

{J6} 679/2016/EU Európai Parlament és Tanács rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (GDPR)

{J8} 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)

{J9} 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetébenalkalmazandó konkrét védelmi intézkedésekről

{J10} Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS2 irányelv)

{J11} A Bizottság (EU) 2024/2690 végrehajtási rendelete a 2022/2555 irányelvnek (NIS2 irányelv) a kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményei, valamint a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, online keresőprogramok vagy közösségimédia-szolgáltatási platformok szolgáltatói és a bizalmi szolgáltatók tekintetében jelentősnek minősülő biztonsági események eseteinek további pontosítása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

1.6.3.2 Szabványok és műszaki-technikai hivatkozások

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

		Providers
{Sz2}	EN 319 411-1 V1.4.1 (2023-10)	Policy and security requirements for Trust Service Providers issuing certificates
{Sz3}	EN 319 411-2 V2.5.1 (2023-10)	Policy and security requirements for Trust Service Providers issuing EU qualified certificates
{Sz4}	EN 319 412-1 V1.5.1 (2023-09)	Certificate Profiles; Part 1: Overview and common data structures
{Sz5}	EN 319 412-2 V2.3.1 (2023-09)	Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons
{Sz6}	EN 319 412-5 V2.4.1 (2023-09)	Certificate Profiles; Part 5: QCStatements
{Sz7}	ETSI TS 119 312 V1.4.3 (2023-08)	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
{Sz8}	ITU-T X.520 (10/19)	Information technology - Open Systems Interconnection - The Directory: Selected attribute types
{Sz9}	ITU-T X.509 (10/19)	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework
{Sz10}	ISO/IEC 15408-1-5:2022	ISO/IEC 15408 (parts 1 to 5): Information Information security, cybersecurity and privacy protection – Evaluation criteria for IT security
{Sz11}	ISO/IEC 19790:2012	ISO/IEC 19790: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz13}	RFC 3647 (November 2003)	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
{Sz14}	RFC 3739 (March 2004)	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
{Sz15}	RFC 4514 (June 2006)	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz16}	RFC 5280 (May 2008)	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz17}	RFC 6818 (January 2013)	Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
{Sz18}	RFC 6960 (June 2013)	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP

1.6.3.3 Hivatkozott dokumentumok

{D1}	ÁSZF-DÁP	Általános Szerződési Feltételek a NISZ Zrt. Digitális Állampolgárság Programhoz kapcsolódó hitelesítés szolgáltatásaihoz
{D3}		NISZ Zrt. Szervezeti és Működési Szabályzata
{D4}		Adatkezelési tájékoztató a DÁP eAlárás szolgáltatáshoz
{D5}		NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája

{D6}		GovCA biztonsági szabályzat
{D7}		NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}		DÁP eAláírás tanúsítványprofilok
{D9}	BR-DÁP-TAN	Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz
{D10}	BSZ-DÁP-TK	Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszköz kezelése minősített bizalmi szolgáltatáshoz

2 KÖZZÉTÉTEL ÉS ADATTÁRAK

2.1 Tanúsítványtár

A Szolgáltató gondoskodik arról, hogy az általa kibocsátott szolgáltatói tanúsítványok visszavonási állapotára vonatkozó információk, valamint az egyéb közérdekű szolgáltatói információk az Aláírók és az Érintett Felek részére folyamatosan rendelkezésre álljanak. A Szolgáltató ezen információk elérhetőségét az év minden napján, napi 24 órában, éves szinten 99,9 %-os rendelkezésre állással biztosítja, úgy, hogy a kiesés nem lépheti túl esetenként a 3 órás időtartamot.

A Szolgáltató továbbá gondoskodik arról, hogy a kibocsátott tanúsítványokat tartalmazó nyilvántartása a saját, DÁP-TAN és DÁP-TK szolgáltatást megvalósító informatikai rendszere és a DÁP szolgáltató számára folyamatosan rendelkezésre álljon, az év minden napján, napi 24 órában, éves szinten 99,9 %-os rendelkezésre állással, úgy, hogy egy eseti kiesés nem lépheti túl a 3 órás időtartamot. Szolgáltató az Aláírók és az Érintett felek számára közvetlenül nem teszi elérhetővé a kibocsátott tanúsítványokat tartalmazó nyilvántartását.

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

2.2 Szolgáltatói információ közzététele

A Szolgáltató a szolgáltatói tanúsítványokat, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokat (BR-DÁP-TAN, BSZ-DÁP-TAN, ÁSZF-DÁP, PDS-DÁP) internetes honlapján (https://hiteles.gov.hu) teszi közzé.

A Szolgáltató a végfelhasználói tanúsítványokat belső tanúsítványtárában tárolja, a kiadott tanúsítványt az Aláíró számára a DÁP keretalkalmazáson keresztül rendelkezésre bocsátja, úgy, hogy az a tanúsítvány visszavonásáig vagy érvényessége lejártáig bármikor letölthető.

A Szolgáltató a szolgáltatói tanúsítványokkal kapcsolatos visszavonási állapot információkat CRL és OCSP formájában is biztosítja.

A Szolgáltató a végfelhasználói tanúsítványokkal kapcsolatos visszavonási állapot információkat OCSP formájában biztosítja.

A visszavonási állapot információk közzétételével kapcsolatos információkat a 4.10 fejezet tartalmazza.

2.3 A közzététel gyakorisága

Szolgáltató a szolgáltatói tanúsítványokat azok kibocsátását követő 24 órán belül teszi közzé.

Szolgáltató a tanúsítványokkal kapcsolatos szabályzatokat (BR-DÁP-TAN, BSZ-DÁP-TAN, ÁSZF-DÁP, PDS-DÁP) azok változása esetén közzé teszi legalább 30 nappal a változás hatályba lépését megelőzően.

Szolgáltató a szolgáltatói tanúsítványokra vonatkozó CRL-t legalább 24 óránként frissíti, azaz két egymást követő CRL kibocsátási között idő nem haladja meg a 24 órát. Amennyiben egy szolgáltatói tanúsítvány állapota megváltozik, a Szolgáltató a változást követően haladéktalanul, de legfeljebb egy órán belül új CRL-t állít elő és tesz közzé.

Szolgáltató az OCSP szolgáltatása keretében minden OCSP kérésre friss választ állít elő és ad vissza.

2.4 Hozzáférés-ellenőrzések

A Szolgáltató olvasás céljára korlátozás nélküli hozzáférést biztosít a szolgáltatói tanúsítványokhoz, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos nyilvános szabályzatokhoz (BR-DÁP-TAN, BSZ-DÁP-TAN, ÁSZF-DÁP, PDS-DÁP), a tanúsítványokkal kapcsolatos visszavonási információkhoz.

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

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

3 AZONOSÍTÁS ÉS HITELESÍTÉS

3.1 Elnevezések

3.1.1 Nevek típusa

A tanúsítványban szereplő nevek megadása megfelel az {Sz8} ITU-T X.520 ajánlásnak.
A tanúsítvány `Issuer` mezőjében szereplő név az alábbi {Sz8} ITU-T X.520 szerinti attribútumokat tartalmazza:

- `countryName`;
- `organizationName`;
- `organizationIdentifier;`
- `commonName`.

Az `Issuer` mező a fentieken kívül más attribútumokat nem tartalmaz.

A tanúsítvány `Subject` mezőjében szereplő név az alábbi {Sz8} ITU-T X.520 szerinti attribútumokat tartalmazza:

- `countryName`;
- `givenName`;
- `surName`;
- `serialNumber`;
- `commonName`.

A `Subject` mező fentieken túl más attribútumokat nem tartalmaz.

3.1.2 Nevek jelentése

A tanúsítvány `Issuer` mezőjében szereplő attribútumok jelentése megegyezik az {Sz8} ITU-T X.520 szerintivel. Ezen túl, az `organizationIdentifier` attribútum a Szolgáltató adószámát tartalmazza, tartalma és jelentése megfelel az {Sz4} EN 319 412-1 5.1.4 fejezetében megadottaknak.

A tanúsítvány `Subject` mezőjében szereplő attribútumok jelentése megegyezik az {Sz8} ITU-T X.520 szerintivel. Ezen túl, az alábbi szabályok érvényesek:

- `countryName`: "HU"
- `surname`: betű szerint azonosan megegyezik a személyazonosító okmányba foglalt viselt vezetéknévvel, amely egy vagy több családi nevet és "DR." jelzést tartalmazhat, egymástól szóköz karakterrel elválasztva
- `givenName`: betű szerint azonosan megegyezik a személyazonosító okmányba foglalt viselt utónévvel, amely egy vagy több keresztnevet és "DR." jelzést tartalmazhat, egymástól szóköz karakterrel elválasztva.
- `serialNumber`: a DÁP azonosítót tartalmazza.
- `commonName`: a `surname` és `givenName` egymás után fűzése, egymástól szóköz karakterrel elválasztva

3.1.3 Előfizetők névtelensége és álnév használata

Az Aláírók névtelensége és álnév használata nem megengedett.

3.1.4 Különféle név formák megjelenítési szabályai

A tanúsítványba foglalt megkülönböztető nevek (Distinguished Name) ASN.1 szintaxisa az {Sz16}

RFC 5280 szerinti, megjelenítési szabályait az {Sz15} RFC 4514 adja meg.

3.1.5 A nevek egyedisége

A tanúsítvány tulajdonosa megkülönböztető nevének (Distinguished Name) egyediségét Szolgáltató úgy biztosítja, hogy a `Subject` mezőbe befoglalja az Aláíró DÁP azonosítóját.

3.1.6 Márkanevek elismerése, hitelesítése és szerepe

Szolgáltató nem foglalja be a tanúsítványba azokat a védjegyeket vagy márkaneveket, melyekkel Aláíró esetleg rendelkezik.

3.2 Kezdeti azonosítás

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

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

A Szolgáltató az Aláíró kezdeti azonosítását, hitelesítését és jogosultságának ellenőrzését a DÁP szolgáltató, mint külső fél által végzett, a {J2} DÁP tv. 63. § szerinti személyazonosításra alapozva végzi, úgy, hogy annak eredményét a DÁP szolgáltató a tanúsítványkérelemmel együtt, általa hitelesítve küldi meg a Szolgáltató felé, majd a Szolgáltató az ennek keretében átadott adatok hitelességét ellenőrzi a DÁP szolgáltató elektronikus bélyegzőjének érvényesítésével (lásd még: 4.2.1).

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

3.2.1 A magánkulcs birtoklásának bizonyítása

Az Aláíró számára a tanúsítványhoz tartozó magánkulcsot a Szolgáltató saját szervezetén belül maga generálja QSCD minősítésű kriptográfiai eszközben. Ez az eszköz állítja össze a produktív hitelesítőközpont felé a tanúsítványkérelmet, saját infrastrukturális magánkulcsával, elektronikus aláírással hitelesítve annak tartalmát, egyúttal bizonyítva, hogy a kapcsolódó magánkulcsot az Aláíró birtokolja.

A kérelmek, illetve kérések az eszközben valósulnak meg, azt el nem hagyják és a szükséges rendszerelemek egyazon zárt rendszert képezik.

3.2.2 A szervezeti azonosság hitelesítése

A tanúsítvány az állampolgárok, mint természetes személyek számára kerül kibocsátásra és magánszemélyi minőségben kerül felhasználásra, így semmilyen szervezeti azonosság nem kerül vizsgálatra és hitelesítésre.

3.2.3 A személyazonosság hitelesítése

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

(2) bekezdését.

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

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

3.2.4 Előfizető nem ellenőrzött adatai

Nincs nem ellenőrzött adat.

3.2.5 Jogosultság ellenőrzése

Az Aláíró jogosultságának ellenőrzését, azaz, hogy jogosult-e a Szolgáltatótól tanúsítványt igényelni (lásd 4.1.1) a DÁP szolgáltató a {J2} DÁP tv. szabályai szerint ellenőrzi, bírálja el, a 3.2.3 pont szerinti személyazonosítás részeként. Sikeres személyazonosítás esetén az Aláíró Szolgáltatás igénybevételére való jogosultságát a Szolgáltató igazoltnak tekinti.

3.2.6 Együttműködési kritériumok

A Szolgáltató a Szolgáltatások nyújtása során nem működik együtt más bizalmi szolgáltatóval.

3.3 Azonosítás és hitelesítés kulcscsere esetén

A Szolgáltató nem nyújt kulcscsere szolgáltatást.

3.3.1 Azonosítás és hitelesítés érvényes tanúsítvány esetén

Nincs kikötés.

3.3.2 Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Nincs kikötés.

3.4 Azonosítás és hitelesítés visszavonási kérelem esetén

3.4.1 Visszavonás DÁP keretalkalmazáson keresztül

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

- a DÁP keretalkalmazás elindítása saját mobileszközén és visszavonási funkció kiválasztása;

- az azonosításhoz szükséges adat megadása a DÁP keretalkalmazásban.

A Szolgáltató szempontjából az Aláíró felhasználóazonosítását a DÁP szolgáltató, mint külső fél végzi, a 3.2 fejezet szerinti személyazonosításra építve.

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

3.4.2 Visszavonás webes felületen keresztül

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

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

A Szolgáltató szempontjából az Aláíró felhasználóazonosítását a DÁP szolgáltató, mint külső fél végzi, a 3.2 fejezet szerinti személyazonosítás keretében ellenőrzött adatokra építve.

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

4 A TANÚSÍTVÁNYOK ÉLETCIKLUSA

A tanúsítványok teljes életciklus folyamatát a Szolgáltató működteti.

4.1 Tanúsítványigénylés

4.1.1 Ki nyújthat be tanúsítványigénylést

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

4.1.2 Igénylési folyamat és felelősségek

A tanúsítványigénylés folyamata röviden a következő:

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

4.1.2.1 Tájékoztatás/tájékozódás

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

- az elektronikus aláírás használati lehetőségeiről és jogszabályi feltételeiről;
- az aláírás létrehozásához használt adat (magánkulcs) használatával kapcsolatos intézkedésekről;
- az aláírás létrehozásához használt adat védelméhez szükséges biztonsági intézkedésekről;
- az aláíró és az aláírást ellenőrizni kívánó felek felelősségéről, kötelezettségeiről;
- tanúsítványok visszavonásának lehetőségéről;
- tanúsítványok kibocsátásának körülményeiről;
- a tanúsítvány érvényességéről, érvényességi idejének lejártáról;
- a szolgáltatási szabályzat tartalmáról és elérhetőségéről;
- a tanúsítvánnyal kapcsolatos, a tanúsítványban meghatározott tárgybeli, időbeli, földrajzi vagy egyéb korlátozásokról;
- a szolgáltatói nyilvános kulcsról, valamint annak elérhetőségéről;
- arról, hogy a szolgáltatás igénybe vétele díjmentes;
- arról, hogy a szolgáltatás minősített bizalmi szolgáltatásnak minősül;
- a panaszok benyújtására, a jogviták rendezésére vonatkozó szabályokról.

4.1.2.2 Regisztráció

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

4.1.2.3 Szolgáltatási szerződés megkötése

Az Igénylő a DÁP keretalkalmazás által vezérelt folyamatban egy külön interakciót kívánó megerősítéssel igazolja a megadott adatok valódiságát, majd elfogadja az {D1} ÁSZF-DÁP tartalmát és ezen keresztül létrejön a Szolgáltatási Szerződés.

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

4.1.2.4 Tanúsítványkérelem előállítása

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

Az igénylés elküldése előtt a DÁP keretalkalmazás egy üzenethitelesítő kulcspárt generál, melynek nyilvános kulcsát továbbítja mind a Szolgáltatónak, mind pedig a DÁP szolgáltatónak. Szolgáltató az üzenethitelesítő nyilvános kulcsot a megfelelő aláíróhoz rendelve rögzíti a szolgáltatást megvalósító saját informatikai rendszerében. A későbbiekben a DÁP keretalkalmazás az üzenethitelesítő kulcspár magánkulcsával hitelesíti üzenetét mind a Szolgáltató, mind a DÁP szolgáltató felé – a jelen DÁP-TAN szolgáltatás és a DÁP-TK szolgáltatás keretén belül egyaránt.

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

A Szolgáltató a DÁP szolgáltatótól kizárólag legalább minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzővel hitelesített üzenetet fogad el.

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

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

4.2 Tanúsítványigénylés feldolgozása

4.2.1 Azonosítási és hitelesítési műveletek

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

- a Szolgáltató a DÁP szolgáltatót az üzenetet védő legalább minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegző érvényesítésével azonosítja és hitelesíti;
- az elektronikus bélyegző tanúsítványában szerepel a DÁP szolgáltató egyedi azonosítója;
- a DÁP szolgáltató üzenetében legalább az alábbiak szerepelnek
    - az Aláíró tanúsítványba foglalandó adatai,
    - annak ténye, hogy a tanúsítványba foglalandó adatokat és a személyazonosságot a DÁP szolgáltató a 3.2.3 pont szerint ellenőrizte,
    - tanúsítvány igénylésére vonatkozó üzenet,
    - a DÁP szolgáltatót igazoló legalább fokozott biztonságú elektronikus bélyegző.

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

4.2.2 Tanúsítványigénylés elfogadása vagy visszautasítása

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

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

4.2.3 Tanúsítványigénylés feldolgozás időtartama

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

4.3 Tanúsítvány kibocsátás

4.3.1 Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek

Szolgáltató ellenőrzi és hosszú távú érvényesítésre alkalmas formára egészíti ki a kulcsgenerálási kérelmet is jelentő tanúsítványkérelem DÁP szolgáltatót igazoló elektronikus bélyegzőjét, majd tárolja azt belső nyilvántartásaiban.

A Szolgáltató saját informatikai rendszerében a 6.1.1.2 fejezetben leírtak szerint megvalósítja az igényelt kulcspár generálását a DÁP-HSM modulban. A generált magánkulcs nem hagyja el a DÁP-HSM modult.

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

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

4.3.2 Előfizető értesítése a tanúsítvány kibocsátásról

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

4.4 Tanúsítványelfogadás

4.4.1 Tanúsítvány Előfizető általi elfogadása

A tanúsítványba kerülő adatokat az Aláíró a tanúsítvány kibocsátása előtt, a tanúsítványigénylési folyamatban (lásd 4.1.2) előzetesen visszaigazolja a Szolgáltató felé a DÁP keretalkalmazáson keresztül.

Aláíró a tanúsítványba került adatait a DÁP keretalkalmazás tanúsítványmegtekintő és -letöltő funkciójával tekintheti meg. Aláírónak a tanúsítványa kibocsátásáról szóló értesítő kézhez vétele

után haladéktalanul ellenőriznie kell a tanúsítványba került adatainak a helyességét.

Amennyiben az Aláíró a kiállított tanúsítványba került adataiban eltérést talál, azt a tanúsítvány haladéktalan visszavonásával kell kezelnie, a 4.9 fejezetekben leírtak szerint.

4.4.2 Tanúsítvány közzététele

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

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

4.4.3 További felek értesítése a tanúsítvány kibocsátásáról

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

4.5 A kulcspár és a tanúsítvány használata

4.5.1 Az Előfizető magánkulcs és tanúsítvány használata

Aláíró csak azt követően használhatja a magánkulcsot és a tanúsítványt, hogy a tanúsítványban foglalt adatok helyességéről meggyőződött (lásd 4.4.1).

Aláíró csak az 1.4.1 fejezetben ismertetett célokra és módon használhatja a magánkulcsot és a tanúsítványt.

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

4.5.2 Az Érintett Felek nyilvános kulcs- és tanúsítvány használata

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

- a tanúsítványok, valamint az elektronikus aláírások ellenőrzését olyan megbízható alkalmazással végezze, amely megfelel a jelen szolgáltatási szabályzat 1.6.3.1 fejezetében felsorolt jogszabályoknak és amely képes az 1.6.3.2 fejezetben megadott műszaki szabványok támogatására és azokat helyesen valósítja meg;
- az előző pontban említett aláírás ellenőrző alkalmazást megbízható, vírusmentes környezetben használja, továbbá az aláírás ellenőrző alkalmazás beállítási lehetőségei helyesen legyenek konfigurálva;
- a tanúsítványokat csak olyan alkalmazásokban fogadja el, melyek összhangban vannak a tanúsítvány "kulcshasználat" (`KeyUsage`) és "kiterjesztett kulcshasználat" (`ExtendedKeyUsage`) kiterjesztésének tartalmával;
- végezze el a tanúsítványra az {Sz16} RFC 5280 6. fejezetében leírt tanúsítási útvonal felépítést és érvényesítést, valamint visszavonás ellenőrzést, a tanúsítványt, illetve az ezen alapuló elektronikus aláírást csak ezen ellenőrzések pozitív eredménye esetén fogadja el;
- vegyen figyelembe minden korlátozást, amely a tanúsítványban vagy a tanúsítvány által hivatkozott szabályzatokban szerepel;

- vegye figyelembe a szolgáltatói felelősségvállalás maximális értékét, mivel az ezen összeghatárt meghaladó ügyletekben létrehozott és aláírt elektronikus dokumentumokból származó esetleges károkért való felelősségét a Szolgáltató korlátozza.

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

4.6 Tanúsítványok megújítása

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

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

Lejárt vagy lejárófélben lévő tanúsítvány esetén új kulcs és új tanúsítvány igénylésével lehet a szolgáltatást fenntartani, a 4.1 alfejezetben leírt módon.

A lejárt, vagy visszavont tanúsítványokat és hozzájuk tartozó magánkulcsokat a Szolgáltató megsemmisíti, a 6.2.10 fejezetben leírtak szerint.

4.6.1 Tanúsítvány megújítás körülményei

Nincs kikötés.

4.6.2 Ki kérelmezhet tanúsítvány megújítást

Nincs kikötés.

4.6.3 Tanúsítvány megújítási kérelmek feldolgozása

Nincs kikötés.

4.6.4 Az Előfizető értesítése a megújított tanúsítvány kibocsátásáról

Nincs kikötés.

4.6.5 Tanúsítvány Előfizető általi elfogadása

Nincs kikötés.

4.6.6 Megújított tanúsítvány közzététele

Nincs kikötés.

4.6.7 További felek értesítése tanúsítvány megújításról

Nincs kikötés.

4.7 Kulcscsere

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

tartalmazó, új tanúsítványba foglalja.

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

4.7.1 Kulcscsere körülményei

Nincs kikötés.

4.7.2 Ki kérelmezhet kulcscserét

Nincs kikötés.

4.7.3 Kulcscsere kérelmek feldolgozása

Nincs kikötés.

4.7.4 Előfizető értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.7.5 Új tanúsítvány Előfizető általi elfogadása

Nincs kikötés.

4.7.6 Új tanúsítvány közzététele

Nincs kikötés.

4.7.7 További felek értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.8 Tanúsítványmódosítás

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

A Szolgáltató nem nyújt a fentiek szerinti, szabványos tanúsítványmódosítási szolgáltatást.
Az Aláírónak a meglevő tanúsítványában foglalt adatok módosulása esetén azt vissza kell vonnia (lásd 4.9) és új tanúsítványt kell igényelnie (lásd 4.1).

4.8.1 Tanúsítvány-módosítás körülményei

Nincs kikötés.

4.8.2 Ki kérelmezhet tanúsítvány-módosítást

Nincs kikötés.

4.8.3 Tanúsítvány-módosítási kérelmek feldolgozása

Nincs kikötés.

4.8.4 Előfizető értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.8.5 Módosított tanúsítvány Előfizető általi elfogadása

Nincs kikötés.

4.8.6 Módosított tanúsítvány közzététele

Nincs kikötés.

4.8.7 További felek értesítése a módosított tanúsítvány kibocsátásáról

Nincs kikötés.

4.9 Tanúsítvány visszavonás és felfüggesztés

A Szolgáltató felfüggesztési szolgáltatást nem nyújt.

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

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

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

4.9.1 Visszavonás körülményei

Szolgáltató visszavonja a tanúsítványt, ha:

- az Aláíró ezt kéri, mert:
  - nem kívánja a továbbiakban használni a DÁP keretalkalmazás elektronikus aláírás funkcióját; vagy
  - fennáll az a lehetőség vagy gyanú, hogy a DÁP keretalkalmazás elektronikus aláírás funkciójával illetéktelen személy visszaél; vagy
  - adatváltozás miatt.
- a DÁP szolgáltató ezt kezdeményezi, mert:
  - az Aláíró DÁP felhasználói profilja inaktív;
  - az Aláíró a DÁP szolgáltatónak jelezte, hogy a magánkulcsához tartozó mobiltelefonját elvesztette, eltulajdonították vagy használhatatlanná vált;
  - az Aláíró újratelepíti a DÁP keretalkalmazást;

- Aláíró új tanúsítványt igényel ugyanazon mobil eszközre, melyhez kapcsolódóan érvényes tanúsítvánnyal rendelkezik;
- a Szolgáltató a Szolgáltatásokkal kapcsolatos rendellenességről szerez tudomást;
- a Szolgáltató tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, illetve a BR-DÁP-TAN-nak, amely hatálya alatt a tanúsítvány kibocsátásra került, vagy a tanúsítványt jogellenesen használták, vagy az elektronikus aláírás létrehozásához használt magánkulcsot aktivizáló adat nem az Aláíró kizárólagos birtokában van;
- a Felügyeleti Szerv jogerős és végrehajtható határozatában elrendeli a visszavonást;
- a visszavonást jogszabály kötelezővé teszi;
- a Szolgáltató befejezi a jelen BSZ-DÁP-TAN szerinti tevékenységét;
- a tanúsítvány formátuma vagy műszaki tartalma (pl. kriptográfiai algoritmus vagy kulcsméret már nem biztonságos) elfogadhatatlan kockázatot jelent az Érintett Felek részére;
- a tanúsítványban felhasznált kriptográfiai algoritmus, kulcshossz, azok paraméterei már nem biztosítják az Aláíró és a nyilvános kulcs hiteles összekapcsolását a tanúsítvány érvényességének hátralevő időszakára.

4.9.2 Ki kezdeményezheti a visszavonást?

Visszavonást kezdeményezhet, a 4.9.1 fejezetben megjelölt esetekben:

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

4.9.3 Visszavonási kérelemre vonatkozó eljárás

4.9.3.1 Visszavonás DÁP keretalkalmazáson keresztül

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

- DÁP keretalkalmazás elindítása saját mobil eszközön;
- tanúsítványvisszavonási funkció indítása a DÁP keretalkalmazásban;
- azonosítási és hitelesítési műveletek elvégzése a 3.4.1 szerint;
- a tanúsítvány adattartamának ellenőrzése a DÁP keretalkalmazásban;
- a visszavonási igény rögzítése.

A sikeresen rögzített visszavonási igényt a DÁP keretalkalmazás üzenethitelesítő kulcsával hitelesítve továbbítja a DÁP szolgáltatónak, aki saját, legalább minősített tanúsítványon alapuló fokozott biztonságú bélyegzőjével hitelesítve küldi tovább a Szolgáltató informatikai rendszere felé, mely a visszavonási kérés azonosítását és hitelesítését automatikusan végrehajtja a 3.4.1-ben foglaltak szerint, majd sikeres azonosítás és hitelesítés után szintén automatikusan végrehajtja a tanúsítvány visszavonását, azaz rögzíti a tanúsítványt a visszavont tanúsítványok nyilvántartásában. A tanúsítvány visszavont tanúsítványok nyilvántartásában való rögzítését követően a Szolgáltató informatikai rendszere saját, legalább minősített tanúsítványon alapuló fokozott biztonságú bélyegzőjével hitelesítve visszaigazolást küld a DÁP szolgáltatón keresztül az Aláíró részére a tanúsítvány visszavonásáról. A Szolgáltató visszaigazolását a DÁP szolgáltató e-mailbe foglalva az Aláíró DÁP profil aktiválása előtt ellenőrzött e-mail címére küldi ki.

4.9.3.2 Visszavonás webes felületen

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

- a DÁP portál megfelelő menüpontjának megnyitása böngészőben;
- azonosítási és hitelesítési műveletek elvégzése a 3.4.2 szerint;
- a visszavonási igény rögzítése.

A sikeresen rögzített visszavonási igényt a DÁP szolgáltató saját, legalább minősített tanúsítványon alapuló fokozott biztonságú bélyegzőjével hitelesítve küldi tovább a Szolgáltató informatikai rendszere felé, mely a visszavonási kérés azonosítását és hitelesítését automatikusan végrehajtja a 3.4.1-ben foglaltak szerint, majd sikeres azonosítás és hitelesítés után szintén automatikusan végrehajtja a tanúsítvány visszavonását, azaz rögzíti a tanúsítványt a visszavont tanúsítványok nyilvántartásában. A tanúsítvány visszavont tanúsítványok nyilvántartásában való rögzítését követően a Szolgáltató informatikai rendszere saját, legalább minősített tanúsítványon alapuló fokozott biztonságú bélyegzőjével hitelesítve visszaigazolást küld a DÁP szolgáltatón keresztül az Aláíró részére a tanúsítvány visszavonásáról. A Szolgáltató visszaigazolását a DÁP szolgáltató e-mailbe foglalva az Aláíró DÁP profil aktiválása előtt ellenőrzött e-mail címére küldi ki.

4.9.4 Kivárási idő visszavonási kérelem esetén

Szolgáltató nem alkalmaz kivárási időt a visszavonási kérelmek teljesítése során.

4.9.5 Visszavonási kérelem feldolgozásának időbelisége

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

A Szolgáltató a visszavonási igények kezelését éves szinten az alábbi rendelkezésreállással biztosítja:

- DÁP keretalkalmazáson keresztül: 97%;
- DÁP portálon keresztül: 99,9%.

4.9.6 Visszavonás ellenőrzésének ajánlása az Érintett Felek számára

Az Érintett Feleknek a tanúsítvány és az ahhoz felépített tanúsítványlánc minden elemének visszavonási állapotát javasolt ellenőriznie a tanúsítványból megállapított vagy a 4.10.1 fejezetben megadott elérhetőségekről.

4.9.7 CRL kibocsátási gyakoriság

A végfelhasználói tanúsítványokra Szolgáltató nem biztosít CRL kibocsátást.

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

4.9.8 CRL előállítása és közzététele között leghosszabb idő

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

4.9.9 OCSP szolgáltatás biztosítása

Szolgáltató a végfelhasználói és szolgáltatói tanúsítványokhoz OCSP szolgáltatást nyújt, a 4.10 fejezetben ismertetett elérhetőségen, működési jellemzőkkel és rendelkezésre állással.

4.9.10 OCSP alapú visszavonás ellenőrzés követelményei

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

4.9.11 Visszavonási állapotközlés más formái

Szolgáltató nem alkalmaz egyéb visszavonási állapotközlési formát.

4.9.12 Különleges követelmények a kulcs kompromittálódása esetére

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

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

4.9.13 Felfüggesztés körülményei

A Szolgáltató nem nyújt felfüggesztési szolgáltatást.

4.9.14 Ki kérelmezhet felfüggesztést

Nincs kikötés.

4.9.15 Felfüggesztésre vonatkozó eljárás

Nincs kikötés.

4.9.16 A felfüggesztés megengedett időtartama

Nincs kikötés.

4.10 Visszavonási állapot szolgáltatások

4.10.1 Működési jellemzők

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

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

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

CRL

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

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

A CRL minden esetben tartalmazza a következő kibocsátás időpontját (`nextUpdate`). A záró CRL (az adott hitelesítőközpont által kiadott utolsó CRL) esetén a `nextUpdate` mező tartalma a „99991231235959Z" {Sz16} RFC 5280 szerinti speciális időpont. Szolgáltató biztosítja, hogy az új CRL kibocsátása a `nextUpdate` mezőben jelzett időpont előtt minden esetben megtörténik

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

- kulcs átállás (5.6 fejezet) miatt; vagy
- a szolgáltatói magánkulcs kompromittálódása (5.7.3 fejezet) miatt; vagy
- a szolgáltatói tevékenység megszüntetése (5.8 fejezet) miatt.

A Szolgáltató csak azt követően bocsátja ki a záró CRL-t, miután minden, az adott hitelesítőközpont által kibocsátott tanúsítvány lejárt vagy azok visszavonását elvégezte. Szolgáltató (illetve a szolgáltatási tevékenység megszüntetése esetén a szolgáltatás átvevő bizalmi szolgáltató, lásd 5.8 fejezet) a záró CRL kibocsátását követő 10 évig biztosítja a záró CRL elérhetőségét.

Szolgáltató a CRL aláírásához ugyanazt a szolgáltatói magánkulcsot használja, melyet a kérdéses tanúsítvány aláírására használt.

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

OCSP

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

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

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

Az OCSP kérésekre vonatkozó szabályok a következők:

- a Nonce (Single Request Extension) használata nem kötelező, de erősen javasolt,
- kritikusnak jelölt kiterjesztést nem szabad használni, az ilyen kéréseket a kiszolgáló MALFORMED hiba válasszal (Responder Error: malformedRequest) elutasítja.

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

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

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

- kulcs átállás (5.6 fejezet) miatt; vagy
- a szolgáltatói magánkulcs kompromittálódása (5.7.3 fejezet) miatt; vagy
- a szolgáltatói tevékenység megszüntetése (5.8 fejezet) miatt.

A Szolgáltató csak azt követően bocsátja ki a záró OCSP-t, miután minden, az adott hitelesítőközpont által kibocsátott tanúsítvány lejárt vagy azok visszavonását elvégezte. Szolgáltató (illetve a szolgáltatási tevékenység megszüntetése esetén a szolgáltatás átvevő bizalmi szolgáltató,

lásd 5.8 fejezet) a záró OCSP kibocsátását követő 10 évig biztosítja az OCSP válasz elérhetőségét. A záró OCSP (az adott hitelesítőközponthoz kapcsolódóan kiadott utolsó OCSP válasz) esetén a `nextUpdate` mező tartalma a „99991231235959Z” {Sz16} RFC 5280 szerinti speciális időpont.

Végfelhasználói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége:

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

Szolgáltatói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége:

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

4.10.2 Szolgáltatás rendelkezésre állása

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

4.10.3 Opcionális lehetőségek

Nincs kikötés.

4.11 Az előfizetés vége

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

4.12 Kulcsletét és visszaállítás

Szolgáltató nem nyújt kulcsletét és visszaállítás szolgáltatást.

4.12.1 Kulcsletét és visszaállítás szabályai

Nincs kikötés.

4.12.2 Rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Nincs kikötés.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

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.
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. Ez a szabályzat biztonsági okokból nem nyilvános. A Szolgáltató informatikai rendszerei vonatkozásában a Szolgáltató {D6} biztonsági szabályzata 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.
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.
Szolgáltató gondoskodik arról, hogy eszközei és információi a megfelelő szintű védelemben részesüljenek. Szolgáltató valamennyi informatikai értékéről leltárt vezet, ezek védelmi követelményeit az elvégzett kockázatelemzéssel összhangban osztályokba sorolja és minősíti.
Szolgáltató a tanúsítványok előállításában, a visszavonási információk menedzsmentjében 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 objektumaiban 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 belépés naplózásra kerül;
- a géptermekbe saját jogon csak a bizalmi szerepkört betöltő, erre feljogosított munkatárs léphet be, azonosítást követően;
- önálló jogosultsággal nem rendelkező személy csak indokolt és engedélyezett esetben, a

szükséges időtartamig tartózkodhat a géptermekben megfelelő jogosultságú, bizalmi munkakört betöltő kísérő személy állandó felügyelete mellett;
- az eszközök aktivizáló adatai (jelszavak, PIN kódok stb.) a géptermen belül sem tárolhatók nyílt formában;
- jogosulatlan személy jelenlétében:
  - a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják;
  - a bejelentkezett terminálok nem maradnak felügyelet nélkül;
  - nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet;
- a gépterem elhagyásakor ellenőrzésre kerül:
  - minden eszköz és berendezés megfelelően biztonságos üzemállapotban van;
  - minden terminálon megtörtént a kijelentkezés;
  - a fizikai tároló eszközök megfelelően elzárásra kerültek;
  - a fizikai védelmet biztosító rendszerek és berendezések megfelelően működnek.

5.1.3 Áramellátás és légkondicionálás

A 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.

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

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

5.1.5 Tűzmegelőzés és tűzvédelem

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

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

5.1.7 Selejt kezelése és megsemmisítése

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

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. 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 stb.) 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

Szolgáltató 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;
f) regisztrációs felelős: a végfelhasználói tanúsítványok előállításának, kibocsátásának jóváhagyásáért, az életciklus menedzsment tevékenységek és adminisztráció szabályszerű végzéséért felelős személy;
g) visszavonás felelős: a végtanúsítványok visszavonásának jóváhagyásáért felelős személy.*

* A vonatkozó jogszabály ({J5} 84/2012. (IV. 21.) Korm. rendelet) a visszavonás felelős feladatkörét a regisztrációs felelős tevékenységi körébe tartozóan rögzíti.

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:

- szolgáltatói kulcspár létrehozása;
- szolgáltatói magánkulcs mentése és visszaállítása;
- szolgáltatói magánkulcs aktiválása;
- szolgáltatói magánkulcs megsemmisítése;
- végfelhasználói (aláírói) kulcspár előállítására 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 bizalmi munkakörökhöz tartozó fiókok esetében erős azonosítási, hitelesítési és engedélyezési eljárásokat kell alkalmazni.
- Tervezett időközönként felül kell vizsgálni a bizalmi munkakörökhöz tartozó, különösen a rendszerüzemeltető és rendszeradminisztrátor 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

A 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, a regisztrációs felelős, 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 és szakképesítéssel igazolni tudja.

A Szolgáltató informatikai rendszeréért általánosan felelős vezető kinevezéséhez 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 regisztrációs felelős esetén középfokú végzettség és legalább fél 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.

Szolgáltató ellenőrzi a felvételi eljárásban benyújtott önéletrajzban megadott, releváns információkat.

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

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;
- szolgáltatói tanúsítványok életciklusával kapcsolatos minden esemény;
- végfelhasználói tanúsítványok életciklusával kapcsolatos minden esemény, beleértve a tanúsítvány kérelmek benyújtása és teljesítése, a visszavonási kérelmek benyújtása és az annak eredményeképpen végzett tevékenység 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

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 a 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 a 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. A 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, mely segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek

jogosulatlan hozzáférést eredményezhetnek vagy hatással lehetnek a tanúsítvány kibocsátási folyamatra, a tanúsítványban tárolandó adatok megmásítását, módosítását, sérülését vagy megsemmisülését eredményezhetik, a Szolgáltató által tárolt végfelhasználói magánkulcsok módosítását, sérülését, megsemmisülését vagy jogosulatlan aktiválását eredményezhetik.

A sebezhetőség vizsgálathoz kapcsolódóan a 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, 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

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:

- tanúsítványok igénylésével, regisztrációval kapcsolatos minden adat vagy irat, különösen a Szolgáltatási Szerződés, Aláíró által aláírt nyilatkozatok és átvételi elismervények;
- tanúsítványokkal 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

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 Szolgáltató legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel, valamint minősített időbélyegzővel látja el.

5.5.4 Archívum mentési eljárásai

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

A Szolgáltató a végfelhasználói tanúsítványok aláírására használt kulcspárhoz tartozó szolgáltatói tanúsítvány lejárata előtt új szolgáltatói tanúsítványt bocsát ki - és azt a 2.2 és 2.3 fejezetekben leírt módon közzé teszi -, kellő időben ahhoz, hogy a bizalmi szolgáltatás megszakítás nélkül üzemeljen, a kiadott végtanúsítványok érvényességének lejáratát figyelembe véve.

Amennyiben új szolgáltatói kulcspár és tanúsítvány előállítása szükséges, Szolgáltató ezt olyan módon teszi meg, hogy az átállás az Aláírók és Érintett Felek számára a lehető legkisebb kényelmetlenséget jelentse:

- a kulcs átállást követően kibocsátott tanúsítványokat kizárólag csak az új szolgáltatói kulcs felhasználásával írja alá;
- a régi szolgáltató kulcspárból a nyilvános kulcsot és a szolgáltatói tanúsítványt megőrzi a legutoljára kibocsátott tanúsítvány érvényességének lejártát követő két évig vagy a kulcs átállástól számított tíz évig, amely időtartam a hosszabb;

A Szolgáltató a tervezett kulcsátállást megelőzően legalább 30 nappal értesíti a Felügyeleti Szervet és vele egyeztet a szükséges feladatokról.

Amennyiben az Aláíró tárolt magánkulcsának algoritmusa, paraméterei vagy kulcshossza tekintetében olyan hirtelen elavulás következik be, amely miatt a tárolt kulcshoz tartozó tanúsítvány érvényességének lejárata előtt visszavonásra került, Aláírónak új kulcspárt kell igényelnie.

5.7 Helyreállítás rendkívüli üzemi 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. A rendkívüli üzemeltetési helyzet bekövetkezése esetén a visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását megelőzi.

A visszavonási nyilvántartások, a kibocsátott tanúsítványokat tartalmazó nyilvántartás és a visszavonás kezelési szolgáltatás 3 órát meghaladó kiesése esetén a Szolgáltató haladéktalanul, de legkésőbb az esetről való értesüléstől számított 24 órán belül értesíti a Felügyelet Szervet.

Egyéb incidens esetén – amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra – a 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 {J6} GDPR 51. cikke szerinti illetékes hatóságnak.

A bekövetkezett incidens kiértékelése alapján a 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 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 Szolgáltató kialakította és fenntartja azt a tartalék CA rendszert, mely a rendkívüli üzemeltetési helyzetben képes a nyilvános szabályzatok elérhetőségét, a visszavonás kezelési szolgáltatások teljes értékű működését, a szolgáltatói tanúsítványokra vonatkozó CRL-ek közzétételét biztosítani.

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 Szolgáltató magánkulcsának kompromittálódása esetén követendő eljárás

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

- visszavonja az összes érintett tanúsítványt;
- záró CRL-t (4.10.1) bocsájt ki;
- megszünteti az érintett magánkulcs használatát;
- értesíti a Felügyeleti Szervet;
- értesíti a DÁP szolgáltatót;
- intézkedik valamennyi érintett fél értesítéséről;
- új szolgáltatói kulcspárokat és tanúsítványokat hoz létre.

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 a 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 a 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. Különösképpen gondoskodik a tanúsítvány

visszavonási kezelés és közzététel szolgáltatások folyamatos fenntartásáról.

- A megszüntetés előtt legalább 90 nappal korábban:
    - értesíti a Felügyeleti Szervet, és internetes honlapján tájékoztatja az felhasználói közösség tagjait;
    - beszünteti az új Szolgáltatás igénylések fogadását;
    - beszünteti a kulcspárok generálását, tanúsítványok előállítását és kibocsátását;
    - 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:
    - visszavonja az összes végfelhasználói tanúsítványt és kibocsájtja a záró OCSP-t;
    - leállítja a visszavonás kezelés szolgáltatást;
    - visszavonja az érintett szolgáltató tanúsítványokat és kibocsájtja a záró CRL-t;
    - a szolgáltatói magánkulcsokat és azok mentéseit olyan módon semmisíti meg, hogy azok használata a továbbiakban már nem lehetséges;
    - beszünteti a tanúsítványok és visszavonási állapot információk közzétételét (mind a CRL publikációt, mind az OCSP szolgáltatást) és gondoskodik arról, hogy ezzel egyidejűleg a visszavonási információk az átvevő szolgáltatónál elérhetővé váljanak;
    - 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 tanúsítványok és visszavonási listák aláírására használt kulcspárokat fizikailag védett környezetben, az erre szolgáló HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, más személy jelenlétének kizárásával generálja. A Szolgáltató a tanúsítványok hitelesítésére használt kulcspárok előállítását dokumentált „kulcsceremónia" eljárás szerint végzi, melyről a vonatkozó szabványkövetelményeknek megfelelő jegyzőkönyv készül. 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 szigorúan védett környezetben, emberi beavatkozás nélkül, az erre szolgáló DÁP-HSM modulban, kizárólag bizalmi munkakört betöltő személyek részvételével állítja elő. 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

A Szolgáltató az Aláíró magánkulcsát - annak teljes életciklusa során - abban a DÁP-HSM modulban tárolja, melyben a kulcspár előállítás megtörtént. Következésképpen magánkulcsok tulajdonoshoz történő külön eljuttatása nem szükséges és nem is 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 hitelesítőközpont - között kerül sor.

A DÁP-HSM az általa generált végfelhasználói kulcspár nyilvános kulcs részét PKCS#10 formátumnak megfelelő, a nyilvános kulcshoz tartozó magánkulccsal létrehozott digitális aláírással hitelesített tanúsítványkérelmekben juttatja el a produktív hitelesítőközpontnak.

A produktív hitelesítőközpont a tanúsítványba foglalandó nyilvános kulcsot csak akkor fogadja el, ha sikeresen ellenőrizte az alábbiakat:

- a tanúsítványkérelem a QSCD tanúsítással rendelkező DÁP-HSM modultól érkezett;
- a tanúsítványkérelem sértetlenül érkezett meg;
- a tanúsítványkérelem a benne szereplő nyilvános kulcs magánkulcs párjával került aláírásra.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

A Szolgáltató a tanúsítványok és visszavonási listák aláírására használt nyilvános kulcsait a szolgáltatói tanúsítványban teszi közzé a 2.2 fejezetben leírtak szerint. A szolgáltatói tanúsítvány elérhetősége minden esetben szerepel a kérdéses tanúsítvány `AuthorityInformationAccess` kiterjesztésében.

Az Aláírók számára a Szolgáltató a nyilvános kulcsait a DÁP keretalkalmazáson keresztül letölthetővé teszi.

Az Érintett Feleknek a szolgáltatói tanúsítványokra az {Sz16} RFC 5280 6. fejezetében leírt tanúsítási útvonal felépítést és érvényesítést javasolt elvégezniük az érintett nyilvános kulcs használata előtt.

6.1.5 Kulcsméretek

Szolgáltató Szolgáltatásai nyújtása során az {Sz7} ETSI TS 119 312 szabvány mindenkor hatályos verziója szerint megbízható szabványos algoritmusokat, paramétereket és kulcshosszakat használ.

6.1.5.1 Hitelesítőközpont kulcsméretek

Szolgáltató a minősített tanúsítvány kibocsátás Szolgáltatás nyújtása során az alábbi algoritmus készleteket és kulcshosszakat használja:

hitelesítőközpont	algoritmus azonosító	görbe
"Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató"	ecdsaWithSHA384	secp384r1
"Minősített Állampolgári Tanúsítványkiadó"	ecdsaWithSHA384	secp384r1
OCSP válaszadó	ecdsaWithSHA384	secp384r1

6.1.5.2 Aláírói kulcs méretek

Szolgáltató a minősített tanúsítvány kibocsátás Szolgáltatás nyújtása során az alábbi algoritmus készlettel és kulcshosszal generálja az aláírói kulcspárokat:

végfelhasználó	algoritmus azonosító	görbe
”DÁP aláíró tanúsítvány"	ecdsaWithSHA384	secp384r1

6.1.5.3 A kulcs méretek figyelemmel kísérése

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 Szolgáltató betartja a HSM modul tanúsítási jelentésében foglalt előírásokat is.

Szolgáltató az Aláírók kulcsainak generálását szigorúan védett, biztonságos környezetben és eljárásokkal végzi, melynek során betartja a QSCD tanúsítási jelentésében foglalt előírásokat is.

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

A szolgáltatói magánkulcsok használati célja kizárólag tanúsítványok és visszavonási listák aláírása.

Az OCSP válaszadó magánkulcsának használati célja kizárólag OCSP válaszok aláírása.

Az Aláírók számára kibocsátott végfelhasználói tanúsítványokhoz kapcsolódó magánkulcs kizárólag minősített elektronikus aláírás létrehozására használható.

Szolgáltató a tanúsítványokban a `KeyUsage` és `ExtendedKeyUsage` kiterjesztésekben az {Sz9} ITU-T X.509 v3 szabványnak megfelelően jelzi a kulcs használat célját.

	kiterjesztés		kiterjesztés	
	kritikus?	KeyUsage	kritikus?	ExtendedKeyUsage
CA tanúsítványa	igen	`KeyCertSign` `CRLSign`	-	-
OCSP válaszadó tanúsítványa	igen	`NonRepudiation` `DigitalSignature`	nem	`OCSPSigning`
Aláíró tanúsítványa	igen	`NonRepudiation`	nem	`DocumentSigning`

6.2 Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1 Kriptográfiai modul szabványok és szabályozások

Szolgáltató a szolgáltatói magánkulcsok előállítására, tárolására és használatára olyan kriptográfiai modult alkalmaz, amely olyan megbízható rendszer, amelynek értékelése az {Sz10} 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 kezdeményezésére az aláírói magánkulcsokat (kulcspárokat) olyan DÁP-HSM modulban állítja elő, 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.

Amennyiben a QSCD tanúsítása megszűnik (lejár), a Szolgáltató visszavonja az összes olyan tanúsítványt, amelyhez tartozó magánkulcs az adott QSCD-n került kiadásra és érvényessége még nem járt le a tanúsítás megszűnésének időpontjában.

A DÁP-TAN szolgáltatás keretében alkalmazott QSCD eszköz tanúsítottságáról a Szolgáltató weboldalán ad tájékoztatást.

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

A Szolgáltató a hitelesítőközpontokban alkalmazza a több szereplős "n-ből m" ellenőrzést a gyökér hitelesítőközpont kulcsgondozási funkcióinak aktiválásánál.

A 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 a hitelesítőközpontok magánkulcsait nem teszi letétbe semmilyen célból.

A Szolgáltató nem nyújt az Aláírók számára magánkulcs letét szolgáltatást.

6.2.4 Magánkulcs visszaállítása

A hitelesítőközpontok szolgáltatói magánkulcsai biztonsági okokból mentésre kerülnek (lásd 6.2.5 fejezet). A mentés titkosított formában, speciális eszközök alkalmazásával történik. Szolgáltató a hitelesítőközpontok magánkulcsait rendkívüli üzemi helyzetek esetén a titkosított mentésből visszaállíthatja, hasonlóan szigorú fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a magánkulcs előállítása eredetileg történt.

Szolgáltató az előfizetői kulcspárokat a 6.2.5 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 hitelesítőközpontok szolgáltatói magánkulcsai, valamint a Szolgáltatások nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok biztonsági okokból mentésre kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik. Szolgáltató a hitelesítőközpontok magánkulcsait rendkívüli üzemi helyzetek esetén a titkosított mentésből visszaállíthatja, hasonlóan szigorú fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a magánkulcs előállítása eredetileg történt.

Szolgáltató az előfizetői kulcspárokról a Szolgáltató 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.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

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

A Szolgáltató az aláírói (végfelhasználói) magánkulcsokat 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 a Szolgáltató a 6.2.4 fejezet szerint végzi a magánkulcs bejuttatását a kriptográfiai modulba.

6.2.7 Magánkulcs kriptográfiai modulban történő tárolásának módja

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

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

6.2.8 Magánkulcs aktiválásának módja

A hitelesítőközpontok magánkulcsainak aktiválását a Szolgáltató a HSM modul gyártói dokumentációjában előírtak szerint végzi el.

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

Az Aláíró a Szolgáltató által tárolt magánkulcsának távoli aktiválását az erre szolgáló aktiváló adat DÁP keretalkalmazáson keresztüli megadásával végzi, {D10} BSZ-DÁP-TK 6.2.8 pontjában foglaltak szerint.

6.2.9 Magánkulcs aktív állapotának megszüntetési módja

A szolgáltatói kulcsok deaktiválásának módját a Szolgáltató belső szabályzata részletezi.

Az aláírói (végfelhasználói) tanúsítványok magánkulcsát Szolgáltató minden egyedi vagy kötegelt aláírási műveletet követően azonnal és automatikusan deaktiválja.

6.2.10 Magánkulcs megsemmisítésének módja

A Szolgáltató a szolgáltatói és a végfelhasználói magánkulcsokat visszaállíthatatlan módon megsemmisíti, amikor használatuk már nem szükséges vagy a kapcsolódó tanúsítvány lejárt vagy 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.

Végfelhasználói tanúsítvány érvényességének lejárata vagy visszavonása esetén az Aláíró magánkulcsa a DÁP-HSM modulban visszaállíthatatlan módon megsemmisítésre kerül.

A magánkulcs visszavonhatatlan megsemmisítése azt is garantálja, 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

Az elektronikus aláírás érvényesítési adatot (a nyilvános kulcsot) a tanúsítvány tartalmazza. Szolgáltató minden általa kibocsátott tanúsítványt archivál és az érvényesség lejártától számított tíz évig, illetve a tanúsítványhoz kapcsolódó elektronikus aláírás létrehozásához használt adat (magánkulcs) felhasználásával létrehozott elektronikus aláírással kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőriz. Az archiválás biztonsági okokból két példányban (redundáns rendszer alkalmazásával) történik. A megőrzési kötelezettségnek Szolgáltató minősített archiválás szolgáltató igénybe vételével is eleget tehet.

6.3.2 Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

A kulcspár felhasználás időtartama azonos a nyilvános kulcs hitelességét igazoló tanúsítvány

érvényességi idejével.

"Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató"	25 év
"Minősített Állampolgári Tanúsítványkiadó"	20 év
OCSP válaszadó	legfeljebb 32 nap
Aláírói tanúsítvány	3 év

A Szolgáltató úgy biztosítja, hogy az előfizetői tanúsítvány érvényességi időszakának lejárata minden esetben korábbi legyen, mint a hitelesítéséhez használt szolgáltatói tanúsítvány lejáratának időpontja, hogy kellő időben végrehajtja az 5.6 fejezetben leírt kulcs átállást.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

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

Az aláírói (végfelhasználói) magánkulcsokat aktivizáló adatok előállítását és cseréjét a DÁP keretalkalmazás felhasználói útmutatójában előírtak szerint kell végezni.

6.4.2 Aktivizáló adatok védelme

A hitelesítőközpontok magánkulcsát aktivizáló adatokat a Szolgáltató alkalmazottai biztonságosan, technikai és szervezési intézkedésekkel védve kezelik, jelszavakat csak titkosított formában tárolnak.

Az aláírói (végfelhasználói) magánkulcsokat aktivizáló adatok kizárólagos birtoklását és védelmét az Aláírónak kell biztosítania. A Szolgáltató azt biztosítja, hogy a DÁP-HSM modulban az előfizetői magánkulcshoz kapcsolódó aktivizáló adat kizárólag csak az Aláíró sikeres azonosítását és hitelesítését követően legyen használható.

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, {Sz2} EN 319 411-1 és {Sz3} EN 319 411-2 szabványoknak a nyilvános kulcsú tanúsítványokat kibocsátó, minősített bizalmi szolgáltatás nyújtására vonatkozó, informatikai biztonsági műszaki követelményeiben határozza meg.

Ezek alapján a Szolgáltató olyan megbízható informatikai rendszert (beleértve a redundáns kiépítést) és technikákat alakított ki és üzemeltetett, 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 {J9} 7/2024. (VI. 24.) MK rendelet 1. mellékletében felsorolt szempontok szerint biztonsági osztályba sorolta. Szolgáltató - a {J8} Kiberbiztonsági tv. 16 §. (1) bekezdése alapján - kétévente a biztonsági osztályba sorolástól függő védelmi intézkedések teljesülésére kiberbiztonsági auditot is végeztetni fog, 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.

A fentiek megfelelnek a {J10} NIS2 rendelet és a kapcsolódó {J11} 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. A belső {D6} GovCA Biztonsági szabályzat figyelembe veszi az {Sz3} EN 319 411-2 szabvány 6.5.6 fejezetében előírt követelményeket.

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

6.7 Hálózatbiztonsági óvintézkedések

A hálózati védelmi intézkedéseket a Szolgáltató {D6} biztonsági szabályzatában meghatározott követelményeknek megfelelően valósítja meg, melyek figyelembe veszik az {Sz3} EN 319 411-2 szabvány 6.5.7 fejezetében leírt követelményeket is.

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

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

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

7.1.1 Verziószám

A tanúsítványok verziószáma: V3.

7.1.2 Tanúsítvány kiterjesztések

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

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

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

7.1.3 Algoritmus azonosítók

A tanúsítványok aláírásához alkalmazott algoritmus azonosító az alábbi:

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

7.1.4 Név formák

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

7.1.5 Név megszorítások

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

7.1.6 Hitelesítési rend objektumazonosító

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

7.1.7 Szabályzati megszorítások kiterjesztés használata

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

7.1.8 Szabályzat minősítők szintaktikája és szemantikája

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

7.1.9 A kritikus hitelesítési rendek (Certificate Policies) kiterjesztés feldolgozása

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

7.2 CRL profil

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

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

7.2.1 Verziószám

A visszavonási listák verziószáma: V2.

7.2.2 CRL és CRL bejegyzés kiterjesztések

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

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

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

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

7.3 OCSP profil

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

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

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

7.3.1 Verziószám

Az OCSP válaszok verziószáma: V1.

7.3.2 OCSP kiterjesztések

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

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

`Nonce`	az OCSP kérésben megadott, visszajátszásos támadások megelőzésére szolgáló véletlenszám (csak akkor, ha a kérés tartalmazta azt)
`ArchiveCutoff`	jelzi, hogy a Szolgáltató a tanúsítvány lejárata után is biztosítja a visszavonási státuszt, a 4.10.1 fejezetben megadott időtartamig.

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

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

8 MEGFELELŐSÉGVIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

Jelen szolgáltatási szabályzat tartalmazza az összes, a természetes személyek számára kibocsátott minősített tanúsítványokkal kapcsolatos szolgáltatások során teljesíteni szükséges követelményt, melyeket a különösen az alábbi nemzetközi szabványok határoznak meg:

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

8.1 Vizsgálatok gyakorisága és körülményei

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

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 {J8} 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 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 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 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 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 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

9.1.1 Tanúsítvány kibocsátás díja

A Szolgáltató a tanúsítvány kibocsátásáért díjat nem számít fel.

9.1.2 Tanúsítványhozzáférés díja

A Szolgáltató a közzétett tanúsítványok eléréséért nem számít fel díjat.

9.1.3 Visszavonási és állapot információ hozzáférés díja

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

9.1.4 Egyéb szolgáltatások díja

Nincs kikötés.

9.1.5 Visszatérítési szabályzat

Visszatérítéssel kapcsolatos rendelkezéseket a Szolgáltató nem állapít meg.

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

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

9.2.3 Felelősségbiztosítás vagy garancia végfelhasználók számára

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.

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

9.4.3 Bizalmasként nem kezelendő személyes adatok

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

9.4.4 Személyes adatok védelmének felelőssége

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

9.4.5 Személyes adatok felhasználásának elfogadása

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

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

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

9.4.7 Egyéb, felfedést eredményező körülmények

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

9.5 Szellemi tulajdonjogok

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

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

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

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. A Szolgáltató sajátjaként felel a Közreműködő Felek vagy egyéb alvállalkozók által a Szolgáltatások nyújtása során okozott kárért.

A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért, az Aláíróval az ÁSZF elfogadásával létrejött Szolgáltatási Szerződésben és a 9.8 fejezetben foglalt korlátozásokkal kártérítést fizet.

A Szolgáltató nem felel:

- az Érintett Felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért;
- az Érintett Felek vagy mások által kibocsátott szabályzatokért.

Szolgáltató kötelezettsége

Szolgáltató azzal, hogy jelen szolgáltatási szabályzat hatálya alatt kibocsát egy aláírói tanúsítványt, 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

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

9.6.3 Aláíró felelőssége és helytállása

9.6.3.1 Aláíró jogai

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

9.6.3.2 Aláíró felelőssége

- Aláíró felelős a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért.

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

9.6.3.3 Aláíró kötelezettsége

- Aláíró köteles a Szolgáltatások igénybe vétele előtt jelen szolgáltatási szabályzatot megismerni.
- Aláíró köteles tudomásul venni, hogy Szolgáltató a tanúsítványt a jelen szabályzatban leírt módon és eljárásokkal bocsátja ki.
- Aláíró köteles a Szolgáltatások igénybe vételéhez szükséges adatokat hiánytalanul és a valóságnak megfelelően szolgáltatni.
- Aláíró köteles tudomásul venni, hogy a számára kibocsátott tanúsítványban a jogszabályokban előírt adatok befoglalásra kerülnek.
- Aláíró köteles a tanúsítványba foglalt bármely adata megváltozása esetén haladéktalanul kérni a tanúsítvány visszavonását.
- Aláíró kötelezettsége, hogy a tanúsítványt és a kapcsolódó magánkulcsot, csak jogszabályokban megengedett és nem tiltott célra, valamint a szabályzatokban és hivatkozott dokumentumokban foglaltaknak megfelelően használja.
- Aláíró köteles biztosítani, hogy a Szolgáltatások igénybe vételéhez szükséges - saját hatáskörébe tartozó - adatokhoz és eszközökhöz illetéktelen személyek ne férhessenek hozzá.
- Aláíró köteles Szolgáltatót haladéktalanul írásban értesíteni, amennyiben valamely a Szolgáltatásokban kiadott tanúsítvánnyal vagy azon alapuló elektronikus aláírással kapcsolatban jogvita indul.
- Aláíró haladéktalanul köteles a magánkulcs nem jogszerű használatának vagy kompromittálódásának gyanúja esetén a tanúsítvány visszavonását kérni.
- Aláíró köteles tudomásul venni, hogy Szolgáltató jogosult a tanúsítványt visszavonni, amennyiben Aláíró a Szolgáltatási Szerződést megszegi vagy Szolgáltató tudomására jut, hogy a tanúsítványt illegális tevékenységhez használták.
- Aláíró köteles tudomásul venni, hogy Szolgáltató a tanúsítványt a Felügyeleti Szerv erre vonatkozó határozata esetén visszavonja.

9.6.4 Érintett Felek felelőssége és helytállása

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

- a szolgáltatási szabályzatban foglalt követelmények és előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- a tanúsítvány felhasználására vonatkozó valamennyi korlátozás figyelembe vétele, amely a tanúsítványban vagy a szolgáltatási szabályzatban szerepel

- a tőle elvárható magatartás tanúsítása a tanúsítvány ellenőrzésekor.

Szolgáltató kizárja a felelősségét (9.8 fejezet) amennyiben az Érintett Fél a tanúsítvány vagy az azon alapuló 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

A Szolgáltató kizárja felelősségét, amennyiben:

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

9.8 Felelősség korlátozása

A Szolgáltató korlátozza a kártérítési felelősségét:

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

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

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

9.9 Kártérítések

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

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 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 - az {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 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

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