NISZ

Nemzeti Infokommunikációs Szolgáltató Zrt.

Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz (BR-DÁP-TAN)

Verziószám	1.5
OID	0.2.216.1.200.1100.100.42.3.1.36
Hatályba lépés dátuma	2025.04.16.
Dokumentum besorolása	nyilvános
Jóváhagyó	Adorján István

Adorján István

Digitálisan aláírta:
Adorján István
Dátum: 2025.03.15
10:12:25 +01'00'

Változáskövetés

verzió	módosítás dátuma	a változás leírása	készítette	ellenőrizte	jóváhagyta
0.1	2024.07.29	első változat	NISZ Zrt. Polysys Kft. ACPM Zrt.		
0.2	2024.07.30	visszajelzéseket beépítő, hatóságnak benyújtott változat	ACPM Zrt.	Kővári-Szabó Zoltán	-
0.3	2024.11.06	Továbbfejlesztett változat	Kővári-Szabó Zoltán	Nagy Benjámin ACPM Zrt.	-
1.0	2024.11.29	Első jóváhagyott verzió	Kővári-Szabó Zoltán	Nagy Benjámin ACPM Zrt.	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 követelménnyel 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 tovább pontosítások	Nagy Benjámin Gál Ferenc	Kővári-Szabó Zoltán	Adorján István
1.5	2025.03.14	OCSP szolgáltatásra vonatkozó pontosítás.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István

Tartalomjegyzék

1 BEVEZETÉS

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban, mint Kormányzati Hitelesítés Szolgáltató vagy Szolgáltató) Bizalmi Szolgáltatási Rendje, 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 rend 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

Jelen bizalmi szolgáltatási rend egy olyan szabálygyűjtemény, amely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára, valamint rögzíti azokat a követelményeket, melyeket a Szolgáltatónak a Szolgáltatások nyújtása során teljesítenie kell.

Jelen bizalmi szolgáltatási rend az {Sz13} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában – a szükséges, Szolgáltatóra specifikus eltérésektől eltekintve – szigorúan követi annak előírásait.

Jelen bizalmi szolgáltatási rend előírja az állampolgárok, mint természetes személyek számára kibocsátott minősített tanúsítványokkal kapcsolatos, a Szolgáltatások nyújtása során teljesíteni szükséges összes követelményt, melyeket 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}

Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a NISZ Zrt. "Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz" (BSZ-DÁP-TAN) {D5} dokumentum tartalmazza.

Jelen bizalmi szolgáltatási rendnek megfelelően kibocsátott tanúsítványok az {Sz4} EN 319 412-1 szabvány 3.1 fejezetében meghatározott "EU minősített tanúsítványok", és tartalmazzák jelen dokumentum objektum azonosítóját, mely alapján az érintett felek képesek meghatározni az adott

tanúsítvány alkalmazhatóságát és megbízhatóságát.

Jelen bizalmi szolgáltatási rend megfelel a {J1} eIDAS rendeletben megállapított - minősített bizalmi szolgáltatásra vonatkozó - követelményeknek, és a hatálya alatt nyújtott szolgáltatás EU minősített bizalmi szolgáltatásnak minősül.

1.2 Dokumentum neve és azonosítása

1.2.1 A dokumentum neve

Jelen bizalmi szolgáltatási rend teljes neve: NISZ Zrt. "Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz".

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

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

A jelen BR-DÁP hatálya alatt kiadott tanúsítványok kibocsátására és felhasználására vonatkozó részletes szabályokat a {D5} BSZ-DÁP-TAN szolgáltatási szabályzat tartalmazza.

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

Jelen BR-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 BR-DÁP-TAN a DÁP tv. 8. § 5. pontja szerinti *bizalmi szolgáltatási rend*, mely a DÁP-TAN szolgáltatásra vonatkozó feltételeket és biztonsági követelményeket tartalmazó szabálygyűjtemény és amely egyúttal az ETSI EN 319 401 szerinti ún. *„trust service policy”*-nek és az ETSI EN 319 411-1 szerinti ún. *„certification policy”*-nek tekintendő.

1.2.3 Hitelesítési rendek

A BR-DÁP-TAN bizalmi szolgáltatási rend 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.

1.3 PKI közösség

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

- Szolgáltató: a jelen bizalmi szolgáltatási rendnek 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 dokumentumban 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 rend szempontjából feladatai közé tartozik a tanúsítvány igénylések feldolgozása, tanúsítványok kibocsátása, tanúsítványok visszavonása, valamint a kibocsátott tanúsítványokra vonatkozóan visszavonási információk szolgáltatása.

Jelen bizalmi szolgáltatási rend hatálya alatt Szolgáltató kizárólag az állampolgárok részére, a Digitális Állampolgárság Program keretében bocsát ki tanúsítványokat.

Gyökér-hitelesítőközpont

A Szolgáltató elsőnek létrehozott, fizikailag is működő hitelesítőközpontja, amely az alárendelt másodlagos (produktív) hitelesítőközpontokat hitelesíti.

Produktív hitelesítőközpont

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

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

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 BR-DÁP-TAN szerint tanúsítványt igényelnek a {D5} BSZ-DÁP-TAN-ban foglaltak szerint.

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 ellenőrzéséhez, a tanúsítvány érvényességének megállapításához minden esetben javasolt igénybe vennie a Szolgáltató visszavonási információt szolgáltató Szolgáltatásait (OCSP).

Az Érintett Felek felelősségét a 9.6.4 fejezet írja le.

1.3.5 Egyéb felek

1.3.5.1 Felügyeleti Szerv

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

1.3.5.2 Kiberbiztonsági Felügyelet

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

1.4 A tanúsítvány alkalmazhatósága

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

A jelen BR-DÁP-TAN hatálya alatt kibocsátott tanúsítványok minősített elektronikus aláírást létrehozó eszköz alkalmazását megkövetelő, minősített tanúsítványok, így a kapcsolódó magánkulccsal együtt minősített elektronikus aláírás létrehozására, illetve ellenőrzésére használhatók.

A Szolgáltató a jelen BR-DÁP-TAN szerint kibocsátott tanúsítványokhoz kapcsolódó magánkulcsokat minősített elektronikus aláírást létrehozó eszközben generálja és tárolja, azok teljes életciklusában.

A minősített elektronikus aláírás joghatását a {J3} DÁP tv 54. § határozza meg. E szerint a BR-DÁP-TAN hatálya alatt kibocsátott tanúsítvány felhasználásával létrehozott elektronikus aláírás minősített elektronikus aláírás, mely teljes bizonyító erejű magánokirat és közokirat létrehozására alkalmas.

Teszt tanúsítványok

A Szolgáltató az éles szolgáltatást nyújtó gyökérhitelesítőközpont hierarchiájában kizárólag saját rendszerének tesztelése céljából bocsát ki teszttanúsítványokat a {D5} BSZ-DÁP-TAN-ban foglaltak szerint.

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

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

1.4.1 Engedélyezett tanúsítvány használat

A kibocsátott tanúsítványokhoz kapcsolódó magánkulcsok kizárólag elektronikus aláírás

létrehozására használhatók.

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

A Szolgáltató területi, pénzügyi stb. korlátozásokat szabhat a szolgáltatási szabályzatban, melyeket a kibocsátott tanúsítványban fel kell tüntetni.

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 Szolgáltatónak szervezetén belül Szabályozási Csoportot kell működtetnie, amely többek között jelen bizalmi szolgáltatási rend karbantartásáért is felelős.

1.5.2 Kapcsolat

Szolgáltató adatai:

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

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

1.5.3 A szolgáltatási rend alkalmasságának meghatározása

A Szolgáltató legalább évente egyszer megvizsgálja a bizalmi szolgáltatási rend, illetve a bizalmi szolgáltatási szabályzat tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek eredményeit változtatási igényként figyelembe veszi.

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

1.5.4 A szolgáltatási rend jóváhagyásának eljárása

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

1.6 Fogalmak, rövidítések és hivatkozások

1.6.1 Fogalmak

alany: A Szolgáltató által kiadott tanúsítványban azonosított entitás, aki a tanúsítványban szereplő nyilvános kulcsnak (elektronikus aláírást érvényesítő adat) megfelelő magánkulcsot (elektronikus aláírás létrehozásához használt adat) birtokolja. Jelen hitelesítési rend szerint az Alany az állampolgár.

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

aláírás érvényesítő adat: olyan egyedi adat, amelyet az elektronikus aláírt dokumentumot megismerő személy (vagy eszköz) az elektronikus aláírás ellenőrzésére 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 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 aláírást 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 hitelesítési rend szerinti bizalmi szolgáltatás az a) pont alatti szolgáltatás, azzal, hogy a Szolgáltató jelen DÁP-TAN szolgáltatás 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.

bizalmi szolgáltatási szabályzat: a bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási és egyéb működési szabályokról, a szolgáltatási rendben meghatározott követelmények teljesítésének módjáról.

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

biztonságos környezet: olyan fizikai környezet, mely védett illetéktelen hozzáféréstől, és bizonyos mértékig tűz, víz 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 {J3} 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 érvényesítő adat: lásd „Aláírás érvényesítő adat”.

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

elektronikus aláírás célú tanúsítvány: olyan elektronikus igazolás, amely az elektronikus aláírást érvényesítő adatokat egy természetes személyhez kapcsolja és igazolja legalább az érintett személy nevét vagy álnevét.

elektronikus aláírás célú minősített tanúsítvány: 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 hardver- és/vagy szoftvereszköz, amely a személyazonosító adatokat tartalmazza, és amelyet online szolgáltatások céljából történő azonosításra használnak.

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

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 rend 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 {J3} 1999/93/EK direktíva vagy a {J1} eIDAS rendelet közül azzal

összhangban kibocsátott minősített tanúsítvány, amely hatályos a tanúsítvány kibocsátásának időpontjában.

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 sorozata (így különösen azon tanúsítványok, tanúsítványokkal kapcsolatos információk, érvényesítési adatok, a tanúsítvány állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató érvényesítési adatára és annak visszavonási állapotára vonatkozó információk), melyek alapján megállapítható, hogy az elektronikus dokumentumon elhelyezett elektronikus aláírás, elektronikus bélyegző vagy elektronikus időbélyegző, valamint az azokhoz kapcsolódó tanúsítványok az elektronikus aláírás, elektronikus bélyegző vagy elektronikus 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 rendben): 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.

kiberbiztonsági felügyelet: az adott tagállamban kijelölt felügyeleti szerv (Magyarországon a Szabályozott Tevékenységek Felügyeleti Hatósága), amely azon vállalatok, szervezetek – köztük a bizalmi szolgáltatók – kiberbiztonsági felügyeletét végzi, amelyek a társadalom és a gazdaság működése szempontjából alapvető szolgáltatásokat, illetve a digitalizáció fejlődése miatt nélkülözhetetlen infrastrukturális szolgáltatásokat nyújtanak.

fokozott biztonságú elektronikus aláírás: olyan elektronikus aláírás, amely megfelel a {J1} eIDAS 26. cikkben 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. cikkben 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.

hitelesítési szabályzat (Certificate Policy Statement - CPS): olyan bizalmi szolgáltatási szabályzat, 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 vagy amely elektronikus azonosítást, európai digitális személyiadat-tárcát vagy más elektronikus azonosító eszközt, vagy bizalmi szolgáltatást vesz igénybe.

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

Kiberbiztonsági Felügyelet: az adott tagállamban kijelölt felügyeleti szerv (Magyarországon a Szabályozott Tevékenységek Felügyeleti Hatósága), amely azon vállalatok, szervezetek – köztük a bizalmi szolgáltatók – kiberbiztonsági felügyeletét végzi, amelyek a társadalom és a gazdaság működése szempontjából alapvető szolgáltatásokat, illetve a digitalizáció fejlődése miatt nélkülözhetetlen infrastrukturális szolgáltatásokat nyújtanak.

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

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

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

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

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

magánkulcs aktiválása: az a folyamat, melynek során a jogosult - különféle azonosító elemek (pl. jelszó, PIN kód megadásával - engedélyezi, hogy az elektronikus aláírást 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 aláírást létrehozó eszközön tárolt magánkulcs üzemszerű működésre megszüntetésre kerül.

megfelelőségértékelő szervezet: a {J2} 765/2008/EU 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 aláírást létrehozó eszközzel állítottak elő, és amely elektronikus aláírás célú minősített tanúsítványon alapul.

minősített elektronikus aláírás létrehozó eszköz: olyan elektronikus aláírást 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 (publikus) 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 adat: egy természetes vagy jogi személy, vagy egy másik természetes személyt vagy egy jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő, az uniós vagy a nemzeti joggal összhangban kibocsátott adatok.

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

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;

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.

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 aláírást 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.

visszavonási jelszó: az elektronikus aláíró tanúsítvány ügyfél kérelmére történő visszavonásához szükséges kód.

1.6.2 Rövidítések

ÁSZF-DÁP	Általános Szerződési Feltételek a DÁP eAláírás szolgáltatáshoz
BR-DÁP-TAN	Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz
BSZ-DÁP-TAN	Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz
BR-DÁP-TK	Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében nyújtott

		elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszköz kezelése minősített bizalmi szolgáltatáshoz
CA	Certification Authority	hitelesítő szervezet
CP	Certificate Policy	szolgáltatási rend
CPS	Certificate Practice Statement	hitelesítési szolgáltatási szabályzat
CRL	Certification Revocation List	tanúsítvány visszavonási lista
DÁP		digitális állampolgárság
DÁP-TK		Szolgáltató {D6} BR-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 aláírást 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}	765/2008/EU Európai Parlament és Tanács rendelete a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről
{J3}	2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (DÁP tv.)
{J4}	24/2016. (VI.30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
{J5}	679/2016/EU Európai Parlament és Tanács rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (GDPR)
{J7}	2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
{J8}	7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetébenalkalmazandó konkrét védelmi intézkedésekről
{J9}	Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS2 irányelv)

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

1.6.3.2 Szabványok és műszaki-technikai hivatkozások

{Sz1}	EN 319 401 V3.1.1 (2024-06)	General policy requirements for Trust Service Providers
{Sz2}	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 4514 (June 2006)	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz15}	RFC 5280 (May 2008)	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz16}	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}		Adatkezelési tájékoztató a DÁP eAláírás szolgáltatáshoz
{D5}	BSZ-DÁP-TAN	Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz
{D6}	BR-DÁP-TK	Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszköz kezelése minősített bizalmi szolgáltatáshoz

2 KÖZZÉTÉTEL ÉS ADATTÁRAK

2.1 Tanúsítványtár

A Szolgáltatónak gondoskodnia kell arról, hogy az általa kibocsátott szolgáltatói tanúsítványok, a tanúsítványok visszavonási állapotára vonatkozó információk, valamint az egyéb közérdekű szolgáltatói információk az Aláírók és az Érintett Felek részére folyamatosan, napi 24 órában, heti hét napban rendelkezésre álljanak. A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy az információk elérhetetlensége ne haladhassa meg a jogszabályokban és a {D5} BSZ-DÁP-TAN-ban meghatározott időtartamot.

A Szolgáltatónak továbbá gondoskodnia kell arról, hogy a kibocsátott tanúsítványokat tartalmazó nyilvántartása a saját, DÁP-TAN és DÁP-TK szolgáltatást megvalósító informatikai rendszere és a DÁP szolgáltató számára folyamatosan, napi 24 órában, heti hét napban rendelkezésre álljon. A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy a nyilvántartás elérhetetlensége ne haladhassa meg a jogszabályokban és a {D5} BSZ-DÁP-TAN-ban meghatározott időtartamot.

2.2 Szolgáltatói információ közzététele

A Szolgáltatónak a szolgáltatói tanúsítványokat, valamint a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokat (BR-DÁP-TAN, BSZ-DÁP-TAN, ÁSZF-DÁP, PDS-DÁP) internetes honlapján közzé kell tennie.

A Szolgáltatónak a végfelhasználói tanúsítványokat belső tanúsítványtárában kell tárolnia, a kiadott tanúsítványt az Aláíró számára rendelkezésre kell bocsátania a {D5} BSZ-DÁP-TAN-ban meghatározottak szerint.

A Szolgáltatónak a szolgáltatói tanúsítványokkal kapcsolatos visszavonási állapot információkat CRL és OCSP formájában is biztosítania kell.

A Szolgáltatónak a végfelhasználói tanúsítványokkal kapcsolatos visszavonási állapot információkat OCSP formájában kell biztosítania.

2.3 A közzététel gyakorisága

A Szolgáltatónak a szolgáltatói tanúsítványokat azok kibocsátását követő 24 órán belül közzé kell tennie.

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

A Szolgáltatónak a szolgáltatói tanúsítványokra vonatkozó CRL-t legalább 24 óránként frissítenie kell, azaz két egymást követő CRL kibocsátási között idő nem haladja meg a 24 órát. Amennyiben egy szolgáltatói tanúsítvány állapota megváltozik, a Szolgáltatónak a változást követően haladéktalanul, de legfeljebb egy órán belül új CRL-t kell előállítania és közzé tennie.

A Szolgáltatónak az OCSP szolgáltatása keretében minden OCSP kérésre friss választ kell előállítania és visszaadnia.

2.4 Hozzáférés-ellenőrzések

A Szolgáltatónak olvasás céljára korlátozás nélküli hozzáférést kell biztosítania 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 Szolgáltatónak biztonsági intézkedésekkel és eljárási szabályokkal gondoskodnia kell az információk jogosulatlan megváltoztatása, törlése, sérülése és megsemmisülése elleni védelemről.

3 AZONOSÍTÁS ÉS HITELESÍTÉS

3.1 Elnevezések

3.1.1 Nevek típusa

A tanúsítványokban szereplő nevek megadása meg kell, hogy feleljen az {Sz8} ITU-T X.520 ajánlásnak.

A tanúsítvány `Issuer` mezőjében szereplő név legalább az alábbi, {Sz8} ITU-T X.520 szerinti attribútumokat kell, hogy tartalmazza:

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

Az `Issuer` mező fentieken túl további attribútumokat is tartalmazhat.

A tanúsítvány `Subject` mezőjében szereplő névnek tartalmaznia kell az alábbi, {Sz8} ITU-T X.520 szerinti attribútumokat:

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

A `Subject` mező fentieken túl további név elemeket is tartalmazhat, azonban nem tartalmazhat álnevet (`pseudonym`).

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, további szabályok a {D5} BSZ-DÁP-TAN-ban találhatók.

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 {Sz15} RFC 5280 szerinti, megjelenítési szabályait az {SZ14} 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

Szolgáltatónak az Aláíró kezdeti azonosítását, hitelesítését és jogosultságának ellenőrzését a DÁP szolgáltató, mint külső fél által végzett, a {J2} DÁP tv. 63. § szerinti személyazonosításra alapozva kell végeznie, a {D5} BSZ-DÁP-TAN-ban leírt módon.

Szolgáltatónak biztosítania kell, hogy a DÁP szolgáltató által végzett személyazonosítás és annak jelen BR-DÁP-TAN szerinti tanúsítványok kibocsátásához történő felhasználása teljesítse az {J1} eIDAS rendelet 24. cikk (1a) bekezdés c) pontja szerinti ún. magas megbízhatósági szintű azonosításra vonatkozó követelményeket és ezt megfelelőségértékelő szervezet igazolja.

A Szolgáltatónak a közte és DÁP szolgáltató, mint közreműködő fél között lévő jogviszonyt külön megállapodásban kell rendeznie, 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.
Következésképpen a Szolgáltatónak nem kell szervezeti azonosságot vizsgálnia, hitelesítenie.

3.2.3 A személyazonosság hitelesítése

Az Aláíró személyazonosságának hitelesítését a DÁP szolgáltató végzi a {D5} BSZ-DÁP-TAN-ban leírtak szerint.

3.2.4 Előfizető nem ellenőrzött adatai

Nincs kikötés.

3.2.5 Jogosultság ellenőrzése

A 3.2.3 pont szerinti személyazonosítás sikeressége esetén az Aláíró Szolgáltatás igénybevételére való jogosultságát a Szolgáltatónak igazoltnak kell tekintenie.

3.2.6 Együttműködési kritériumok

Szolgáltató a Szolgáltatások nyújtása során nem működhet együtt más bizalmi szolgáltatókkal.

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

Az Aláíró visszavonási kérelem azonosításához szükséges felhasználóazonosítását a DÁP szolgáltató mint külső fél végzi a {D5} BSZ-DÁP-TAN-ban foglaltak szerint.

Szolgáltatónak a {D5} BSZ-DÁP-TAN-ban foglaltak szerint meg kell győződnie a DÁP szolgáltató által továbbított visszavonási kérés hitelességéről és sértetlenségéről.

4 A TANÚSÍTVÁNYOK ÉLETCIKLUSA

A tanúsítványok teljes életciklus folyamatát a Szolgáltatónak kell működtetnie.

4.1 Tanúsítványigénylés

4.1.1 Ki nyújthat be tanúsítványigénylést

A Szolgáltatónak biztosítania kell a tanúsítványigénylés lehetőségét a {D5} BSZ-DÁP-TAN szerinti feltételeknek megfelelő személyeknek.

4.1.2 Igénylési folyamat és felelősségek

Tanúsítvány a DÁP keretalkalmazás megfelelő funkciójával igényelhető a {D5} BSZ-DÁP-TAN-ban foglaltak szerint.

A folyamatot és az ezzel kapcsolatos felelősségeket a Szolgáltatónak a {D5} BSZ-DÁP-TAN-ban kell részleteznie.

4.2 Tanúsítványigénylés feldolgozása

4.2.1 Azonosítási és hitelesítési műveletek

A Szolgáltató kizárólag a DÁP szolgáltatótól érkezett tanúsítványkérelmet fogadhat el, melyek hitelességét és sértetlenségét a {D5} BSZ-DÁP-TAN-ban foglaltak szerint kell ellenőriznie. Ennek során:

- a DÁP szolgáltatót az üzenetet védő elektronikus bélyegző érvényesítésével azonosítania és hitelesítenie kell,
- a DÁP szolgáltató üzenetében szereplő, Aláíróra vonatkozó adatokat hitelesnek kell elfogadnia.

4.2.2 Tanúsítványigénylés elfogadása vagy visszautasítása

A Szolgáltatónak el kell fogadnia a sikeresen azonosított DÁP keretalkalmazástól származó hitelesített tanúsítványkérelmet.

A Szolgáltatónak vissza kell utasítania a tanúsítványkérelmet, ha az nem egy DÁP keretalkalmazástól származik, vagy ha a tanúsítványkérelem hitelesítése sikertelen.

4.2.3 Tanúsítványigénylés feldolgozás időtartama

A Szolgáltatónak a szolgáltatási szabályzatban kell megadnia a tanúsítványkérelem feldolgozására vállalt időtartamot.

4.3 Tanúsítvány kibocsátás

4.3.1 Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek

A Szolgáltatónak a tanúsítványkibocsátás során az alábbi műveleteket kell elvégeznie:

- A 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 **Hiba! A hivatkozási forrás nem található.** f ejezetben 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

Szolgáltatónak a DÁP szolgáltató közvetítésével értesítenie kell az Aláírót a tanúsítvány kibocsátásáról.

4.4 Tanúsítványelfogadás

4.4.1 Tanúsítvány Előfizető általi elfogadása

A tanúsítványelfogadás módját Szolgáltatónak a {D5} BSZ-DÁP-TAN-ban kell ismertetnie.

4.4.2 Tanúsítvány közzététele

Nincs kikötés.

4.4.3 További felek értesítése a tanúsítvány kibocsátásáról

Szolgáltatónak a tanúsítvány kibocsátásáról automatizált elektronikus úton értesítenie kell a DÁP szolgáltatót is.

4.5 A kulcspár és a tanúsítvány használata

4.5.1 Az Előfizető magánkulcs- és tanúsítvány használata

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

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

Az 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 bizalmi szolgáltatási rend hatálya alatt kibocsátott tanúsítványon alapuló elektronikus aláírás elfogadása során szükséges, hogy az Érintett Fél megfelelő körültekintéssel járjon el.

Az erre vonatkozó követelményeket a {D5} BSZ-DÁP-TAN részletezi.

4.6 Tanúsítványok megújítása

A Szolgáltató nem nyújt tanúsítvány megújítási szolgáltatást.

Az Aláírónak lejárt vagy lejárófélben lévő tanúsítvány esetén új tanúsítványt kell igényelnie, a 4.1 fejezetben leírt módon.

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

A Szolgáltató nem nyújt tanúsítvány 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

A Szolgáltató nem nyújt tanúsítványmódosítás szolgáltatást.

Az Aláírónak a meglevő tanúsítványában foglalt adatok módosulása esetén új tanúsítványt kell igényelnie, a 4.1 fejezetben leírt módon.

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. A visszavonási kérelem elfogadásától, 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

A Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell a visszavonáshoz vezető körülményeket.

4.9.2 Ki kezdeményezheti a visszavonást

Visszavonást kezdeményezhet:

- az Aláíró;
- a Szolgáltató.

4.9.3 Visszavonási kérelemre vonatkozó eljárás

A Szolgáltatónak ellenőriznie kell a visszavonást kérelmező azonosságát és jogosultságát, valamint ellenőriznie kell a visszavonási kérelemben foglalt adatokat. Ha az ellenőrzések sikeresek, a Szolgáltatónak el kell végeznie a tanúsítvány visszavonását és a megváltozott visszavonási állapot információt közzé kell tennie, valamint értesítenie kell az Aláírót a tanúsítvány visszavonásáról.

A tanúsítvány visszamenőleges visszavonása nem megengedett, és az sem, hogy a kérelmező egy jövőbeni visszavonási időpontot jelöljön meg a kérelemben.

A Szolgáltató az egyszer már visszavont tanúsítvány érvényességét nem állíthatja vissza érvényesre.

Szolgáltatónak a {D5} BSZ-DÁP-TAN-ban tájékoztatást kell adnia arról, hogy az arra jogosultak hogyan kezdeményezhetik tanúsítvány visszavonását.

4.9.4 Kivárási idő visszavonási kérelem esetén

A Szolgáltató nem alkalmaz kivárási időt a visszavonási kérelmek teljesítése során.

4.9.5 Visszavonási kérelem feldolgozásának időbelisége

A Szolgáltatónak a benyújtott visszavonási kérelmet haladéktalanul, minden más típusú tevékenysége (így különösen tanúsítvány előállítása vagy kibocsátás) előtt fel kell dolgoznia.

A Szolgáltatónak a visszavonási igények kezelését éves szinten 99,9%-os rendelkezésreállással kell biztosítania.

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 szolgáltatási szabályzatban megadott elérhetőségekről letöltött CRL vagy megkért OCSP válasz alapján.

4.9.7 CRL kibocsátási gyakoriság

A Szolgáltató a végfelhasználói tanúsítványokra nem biztosít CRL kibocsátást.

A Szolgáltatónak a szolgáltatási szabályzatban meg kell határoznia a szolgáltatói tanúsítványokra vonatkozó CRL kibocsátásának gyakoriságát.

4.9.8 CRL előállítása és közzététele között leghosszabb idő

A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia azt a maximális időtartamot, melyen belül a szolgáltatói tanúsítványokra vonatkozó CRL-t az előállítását követően közzéteszi.

4.9.9 OCSP szolgáltatás biztosítása

A Szolgáltatónak mind a végfelhasználói, mind a szolgáltatói tanúsítványok visszavonási állapotának megállapításához OCSP szolgáltatást kell nyújtania.

4.9.10 OCSP alapú visszavonás ellenőrzés követelményei

A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia az OCSP alapú visszavonás ellenőrzésével kapcsolatban az Érintett Felek számára fontos figyelmeztetéseket.

4.9.11 Visszavonási állapotközlés más formái

Nincs kikötés.

4.9.12 Különleges követelmények a kulcs kompromittálódása esetére

A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy a szolgáltatói magánkulcsának kompromittálódása esetén az eseményről az Aláírókat és az Érintett Feleket értesítse.

A produktív hitelesítőközpont magánkulcsának kompromittálódása esetén a Szolgáltatónak képesnek kell lennie az összes érintett végfelhasználói tanúsítvány visszavonására és az érintett CRL-nek 24 órán belüli kibocsátására és közzétételére, majd ezt követően, az adott szolgáltatói tanúsítvány visszavonására és az érintett CRL-nek 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

A Szolgáltatónak a szolgáltatói tanúsítványokhoz kapcsolódó visszavonási információkat mind CRL, mind OCSP formájában szolgáltatnia kell. A Szolgáltatónak biztosítania kell, hogy a visszavonási állapot információ változása mind a CRL, mind az OCSP szolgáltatásban azonosan, konzisztens módon megjelenjen, figyelembe véve az egyes szolgáltatásokban eltérő frissítési időket is.

A Szolgáltatónak a végfelhasználói tanúsítványokhoz kapcsolódó visszavonási információkat OCSP formájában szolgáltatnia kell.

CRL

A Szolgáltató által kibocsátott CRL-nek meg kell felelnie a {Sz15} RFC 5280 szabványnak.

A CRL-nek tartalmaznia kell minden olyan visszavont tanúsítványt, melyek érvényessége a CRL kibocsátásának időpontjában nem járt még le.

A CRL-nek tartalmaznia a következő kibocsátás időpontját (`nextUpdate`). A záró CRL (az adott hitelesítőközpont által kiadott utolsó CRL) esetén a `nextUpdate` mező tartalma a „99991231235959Z” RFC 5280 {Sz9} szerinti speciális időpont. A Szolgáltatónak biztosítania kell, hogy az új CRL kibocsátása a `nextUpdate` mezőben jelzett időpont előtt minden esetben megtörténjen.

A Szolgáltatónak záró CRL-t kell kibocsátania, amikor egy adott hitelesítőközpont működtetését megszünteti:

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

A Szolgáltató csak azt követően bocsáthatja ki a záró CRL-t, miután minden, az adott hitelesítőközpont által kibocsátott tanúsítvány lejárt vagy azok visszavonását elvégezte.
Szolgáltatónak (illetve a szolgáltatási tevékenység megszüntetése esetén a szolgáltatást átvevő bizalmi szolgáltatónak, lásd 5.8 fejezet) a záró CRL kibocsátását követő 10 évig biztosítania kell a záró CRL elérhetőségét.
A Szolgáltatónak a CRL aláírásához ugyanazt a szolgáltatói magánkulcsot kell használnia, melyet a kérdéses tanúsítvány aláírására használt.

A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a szolgáltatói tanúsítványokra vonatkozó CRL elérhetőségét.

OCSP

A Szolgáltató által biztosított OCSP szolgáltatásnak meg kell felelnie az {Sz16} RFC 6960 szabványnak.

Az OCSP szolgáltatást a Szolgáltatónak az {Sz16} RFC 6960 2.2 fejezetében meghatározott "Authorized Responder" elvnek megfelelően kell működtetnie.

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

A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia az OCSP kérésekre vonatkozó szabályokat.

Az OCSP szolgáltatás keretében a Szolgáltatónak biztosítania kell a visszavonási információt a tanúsítvány lejáratát követően is, az érintett hitelesítőközpont működtetési időtartamában.

A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a szolgáltatói és a végfelhasználói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetőségét.

4.10.2 Szolgáltatás rendelkezésre állása

A szolgáltatói tanúsítványokra vonatkozó CRL-nek, illetve az OCSP szolgáltatásnak az év minden napján, napi 24 órában elérhetőnek kell lennie, 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

A {D5} BSZ-DÁP-TAN-ban meghatározva.

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

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

5.1 Fizikai óvintézkedések

5.1.1 Telephelyek elhelyezése és szerkezeti felépítése

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

5.1.2 Fizikai hozzáférés

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

Ehhez biztosítania kell, az alábbiakat:

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

5.1.3 Áramellátás és légkondicionálás

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

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

- tartós áramszünet esetére saját áramellátó berendezés biztosítja - üzemanyag utántöltéssel - tetszőlegesen hosszú időtartamig az áramellátást.

A Szolgáltatónak a gépteremben olyan légkondicionáló berendezést kell alkalmaznia, mely biztosítja az alábbiakat:

- az operátorok biztonságos munkavégzéséhez szükséges mennyiségű oxigén biztosított;
- a levegő nedvességtartalma nem haladja meg az informatikai rendszerek által megkívánt szintet;
- hűtés történik a szükséges üzemeltetési hőmérséklet biztosítására, az eszközök és berendezések túlhevülésének megakadályozására.

5.1.4 Beázás és elárasztás veszélyeztetettség

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

5.1.5 Tűzmegelőzés és tűzvédelem

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

5.1.6 Adathordozók tárolása

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

5.1.7 Selejt kezelése és megsemmisítése

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

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

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

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

5.2 Eljárásbeli előírások

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

5.2.1 Bizalmi munkakörök

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

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

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

A Szolgáltatónak a szolgáltatási szabályzatában meg kell határoznia, hogy mely műveletek végezhetők csak kettős ellenőrzés mellett, egyéb meghatározott feltételek biztosításával.

A szolgáltatási szabályzatában az alábbi elvárást mindenképp meg kell fogalmazni:
Csak védett környezetben, legalább kettő, bizalmi munkakört betöltő munkatárs egyidejű fizikai jelenlétében végezhetők el az alábbi műveletek:

- gyökér szolgáltató tanúsítvány kibocsájtása;
- tanúsítványok aláírására használt szolgáltatói kulcspár létrehozása;
- szolgáltatói kulcspár biztonságos kriptográfiai eszközben történő telepítése és helyreállítása;
- szolgáltatói aláírás célú magánkulcs mentése, tárolása és visszaállítása.

5.2.3 Az egyes szerepkörökben elvárt azonosítás és hitelesítés

A bizalmi munkaköröket betöltő személyek azonosítását és hitelesítését erős PKI eljárásokkal kell végezni, mielőtt a Szolgáltatások nyújtásában érintett kritikus informatikai rendszerekhez hozzáférhetnének.

A Szolgáltatónak a „legkisebb jogosultságok” elvét alkalmazva kell adminisztrálnia a bizalmi munkaköröket betöltő személyek felhasználói hozzáférési képességeit, különösen a {D5} BSZ-DÁP-TAN-ban meghatározottak biztosításával.

5.2.4 Egymást kizáró munkakörök

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

A Szolgáltatónak biztosítania kell, hogy a bizalmi munkakörök vonatkozásában:

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

5.3 Személyzetre vonatkozó előírások

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

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

5.3.2 Biztonsági háttér ellenőrzés eljárásai

A Szolgáltató olyan alkalmazottakat foglalkoztathat, akik:

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, ami a büntetlenséget befolyásolhatja (a büntetlen előéletet három hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni);
- nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkoztatástól eltiltás hatálya alatt.

5.3.3 Képzési követelmények

A Szolgáltató csak olyan személyeket foglalkoztathat, akik az adott munkakör vagy szerepkör ellátásához szükséges mértékben elsajátították:

- a PKI elméleti alapjait;
- Szolgáltató informatikai rendszerének sajátosságait és kezelésének módját;
- a szerepkör ellátáshoz szükséges speciális ismereteket;
- Szolgáltató nyilvános és belső szabályzataiban meghatározott folyamatokat és eljárásokat;
- az egyes tevékenységek jogi következményeit;
- az alkalmazandó biztonsági szabályokat.

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

5.3.4 Továbbképzési gyakoriságok és követelmények

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

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

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Nincs kikötés.

5.3.6 Felhatalmazás nélküli tevékenységek büntető következményei

A Szolgáltatónak a munkavállalóval kötendő munkaszerződésben vagy külső munkatárssal kötött megbízási szerződésben szabályoznia kell a 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 foglalkoztathat.

Az egyéb feladatok ellátására, vállalkozási vagy megbízásos szerződés keretében a beszállítóval

vagy közreműködő féllel Szolgáltatónak írásos megállapodást kell kötnie.

5.3.8 A személyzet számára biztosított dokumentációk

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

5.4 A biztonsági naplózás folyamatai

5.4.1 Naplózott esemény típusok

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

5.4.2 Naplóállomány feldolgozásának gyakorisága

A Szolgáltatónak biztosítania kell a naplóállományok rendszeres ellenőrzését és kiértékelését.

5.4.3 Naplóállomány megőrzési időtartama

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

5.4.4 Naplóállomány védelme

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

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

5.4.5 Naplóállomány mentési folyamatai

A naplóállományokról rendszeres mentést kell készíteni.

5.4.6 Naplózás gyűjtési rendszere

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

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

5.4.7 Rendellenes eseményeket kiváltó alanyok értesítése

Nincs kikötés.

5.4.8 Sebezhetőség értékelések

A Szolgáltatónak rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot és behatolás tesztet kell végeznie, mely segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek jogosulatlan hozzáférést eredményezhetnek vagy hatással lehetnek a tanúsítvány kibocsátási folyamatra, a tanúsítványban tárolandó adatok megmásítását, módosítását, sérülését vagy megsemmisülését eredményezhetik.

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

5.5 Adatok archiválása

5.5.1 A tárolt adatok típusai

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

Ehhez legalább a {D5} BSZ-DÁP-TAN-ban meghatározott információkat tárolja.

5.5.2 Archívum megőrzési időtartama

A Szolgáltató az 5.5.1 fejezetben meghatározott archivált adatokat köteles megőrizni:

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

5.5.3 Archívum védelme

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

5.5.4 Archívum mentési eljárásai

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

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

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

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

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

elektronikus aláírások, bélyegzők és időbélyegzők hitelességének fenntartásáról.

5.5.6 Archívum gyűjtési rendszere

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

5.5.7 Archívum hozzáférés és ellenőrzés eljárásai

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

5.6 Kulcsátállás

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

Amennyiben új szolgáltatói kulcspár és tanúsítvány előállítása szükséges, a Szolgáltatónak ezt olyan módon kell kiviteleznie, hogy az átállás az Aláírók és az Érintett Felek számára a lehető legkisebb kényelmetlenséget jelentse és megfeleljen a vonatkozó jogszabályi és szabványi követelményeknek.

5.7 Helyreállítás rendkívüli üzemeltetési helyzetek esetén

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

A visszavonási nyilvántartások, a kibocsátott tanúsítványokat tartalmazó nyilvántartás és a visszavonás kezelési szolgáltatás 3 órát meghaladó kiesése esetén a Szolgáltatónak haladéktalanul értesítenie kell a Felügyeleti Szervet.

Egyéb incidens esetén - amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra -, az esetről való értesüléstől számított 24 órán belül értesíteni kell az Érintett Feleket, valamint jelenteni kell az incidenst a Felügyeleti Szervnek.

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

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

A Szolgáltatónak rendelkeznie kell üzletmenet folytonossági tervvel.

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

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

A rendkívüli üzemeltetési helyzetben a Szolgáltatónak a lehető legrövidebb időn belül tájékoztatást kell közzé tennie internetes honlapján, valamint - lehetőség szerint - elektronikus levélben kell értesítenie azokat a személyeket, akiket az esemény érint.

5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

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

5.7.3 Szolgáltató magánkulcsának kompromittálódása esetén követendő eljárás

A Szolgáltató magánkulcsának kompromittálódása esetén haladéktalanul meg kell tennie az alábbi 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 Szolgáltatónak rendelkeznie kell tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.

5.8 A szolgáltatási tevékenység megszüntetése

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

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

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

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

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

A Szolgáltatónak a tanúsítványok és visszavonási listák aláírására használandó kulcspárokat fizikailag védett környezetben, kriptográfiai modulban (HSM) kell előállítania. A kriptográfiai modulnak meg kell felelnie a 6.2.1 fejezet szerinti követelményeknek. A tanúsítványok hitelesítésére használt kulcspárok előállítását dokumentált „kulcsceremónia" eljárás szerint kell végezni, melyről a vonatkozó szabvány követelményeinek megfelelő tartalmú jegyzőkönyvet kell felvenni. A Szolgáltató magánkulcsainak teljes életciklusuk alatt a kriptográfiai modulban kell maradniuk.

A Szolgáltatónak az Aláíró kulcspárját fizikailag védett környezetben, QSCD tanúsítással rendelkező kriptográfiai modulban (DÁP-HSM) kell előállítania. A kriptográfiai modulnak meg kell felelnie a 6.2.1 fejezet szerinti követelményeknek. Az Aláírók magánkulcsainak teljes életciklusuk alatt a kriptográfiai modulban kell maradniuk.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

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

6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A hitelesítőközpont a tanúsítványba foglalandó nyilvános kulcsokat csak az azonosított és feljogosított, kulcspárt előállító kriptográfiai modultól fogadhat el, annak szolgáltatói kulcsával előállított elektronikus bélyegző hitelesítése mellett.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

A Szolgáltatónak biztosítania kell, hogy a Szolgáltató nyilvános kulcsa a kicserélésen alapuló támadás (substitution attack) ellen védett módon legyen eljuttatva az Érintett Felekhez.

6.1.5 Kulcs méretek

A Szolgáltatónak a Szolgáltatások nyújtása során - mind a szolgáltatói, mind a végfelhasználói kulcsok tekintetében - az {Sz7} ETSI TS 119 312 szabvány mindenkor hatályos verziója szerint megbízható szabványos algoritmusokat, paramétereket és kulcshosszakat kell használnia.

6.1.6 A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

A szolgáltatói kulcspárokat a 6.1.1 fejezet szerint védett környezetben és tanúsított HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétét kizárva kell előállítani.

Az aláírói (végfelhasználói) kulcspárok előállítását a 6.1.1 fejezet szerint védett környezetben és QSCD tanúsított DÁP-HSM modulban kell végrehajtani, olyan eljárások mellett, melyek megfelelnek a QSCD tanúsítási jelentésében foglalt előírásoknak is.

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

A Szolgáltatónak a tanúsítványokban a `KeyUsage` és `ExtendedKeyUsage` kiterjesztésekben az {Sz11} ITU-T X.509 v3 szabványnak megfelelően kell jeleznie a kulcs használat célját.

6.2 Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1 Kriptográfiai modul szabványok és szabályozások

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

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

Amennyiben a QSCD tanúsítása megszűnik (lejár), a Szolgáltatónak vissza kell vonnia az összes olyan végtanúsítványt, amely az adott QSCD-n került kiadásra és érvényessége még nem járt le a tanúsítás megszűnésének időpontjában.

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

Nincs előírás.

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 Szolgáltató a hitelesítőközpontok magánkulcsait és az aláírói (végfelhasználói) magánkulcsokat rendkívüli üzemeltetési helyzetek esetén a titkosított mentésből visszaállíthatja, hasonlóan szigorú fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a magánkulcs előállítása eredetileg történt.

6.2.5 Magánkulcs mentése

A hitelesítőközpontok szolgáltatói és aláírói (végfelhasználói) magánkulcsait biztonsági okokból menteni kell. A mentést titkosított formában, speciális eszközök alkalmazásával kell megvalósítani.

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 üzemeltetési helyzet során szükséges, akkor a Szolgáltató a 6.2.4 fejezet szerint végzi a magánkulcs bejuttatását a kriptográfiai modulba.

A Szolgáltató az aláírói (végfelhasználói) magánkulcsokat a 6.1.1 fejezetben leírtak szerint QSCD tanúsított kriptográfiai modulban (DÁP-HSM) állítja elő, és azok teljes életciklusuk alatt a kriptográfiai modulban maradnak. Amennyiben a magánkulcs visszaállítása rendkívüli üzemeltetési 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 kriptográfiai modulban (DÁP-HSM) kerülnek tárolásra.

6.2.8 Magánkulcs aktiválásának módja

A hitelesítőközpontok magánkulcsainak aktiválását a Szolgáltatónak a HSM modul gyártói dokumentációjában előírtak szerint kell végeznie.

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

6.2.9 Magánkulcs aktív állapotának megszüntetési módja

A szolgáltatói kulcsok deaktiválásának módját a Szolgáltatónak dokumentáltan szabályoznia kell.

Az aláírói (végfelhasználói) tanúsítványok magánkulcsát Szolgáltatónak minden egyedi vagy kötegelt aláírási műveletet követően azonnal és automatikusan deaktiválnia kell.

6.2.10 Magánkulcs megsemmisítésének módja

A Szolgáltatónak a hitelesítőközpontok magánkulcsát visszaállíthatatlan módon meg kell semmisítenie, amikor használatuk már nem szükséges vagy a kapcsolódó tanúsítvány lejárt vagy visszavonásra került. A magánkulcs és az aktiválásához szükséges minden adat megsemmisítését olyan módon kell végezni, hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkezhető vagy levezethető.

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

6.2.11 Kriptográfiai modul értékelése

Lásd a 6.2.1 fejezetben.

6.3 Kulcspár gondozás egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

A Szolgáltató köteles minden általa kibocsátott tanúsítvánnyal hitelesített nyilvános kulcsot a tanúsítványba foglalva archiválni és az érvényesség lejártától számított tíz évig megőrizni.

6.3.2 Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

A kulcspár felhasználás időtartama azonos a nyilvános kulcs hitelességét igazoló tanúsítvány érvényességi idejével, melyet Szolgáltatónak a {D5} BSZ-DÁP-TAN-ban szabályoznia kell.

A Szolgáltatónak biztosítania kell, hogy az előfizetői tanúsítvány érvényességi időszakának lejárata minden esetben korábbi legyen, mint a hitelesítéséhez használt szolgáltatói tanúsítvány lejáratának időpontja.

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 telepítését a DÁP keretalkalmazás felhasználói útmutatójában előírtak szerint kell előállítani és telepíteni.

6.4.2 Aktivizáló adatok védelme

A hitelesítőközpontok magánkulcsát aktivizáló adatokat a Szolgáltató alkalmazottainak biztonságosan, technikai és szervezési intézkedésekkel védve kell kezelniük, jelszavakat csak titkosított formában tárolhatnak.

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

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.

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

6.5.2 Informatikai biztonsági értékelés

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

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

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

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

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

6.6.2 Biztonságkezelési óvintézkedések

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

6.6.3 Életciklus biztonsági óvintézkedések

A Szolgáltatónak belső szabályzatban meghatározott rendszeres időközönként el kell végeznie a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

6.7 Hálózatbiztonsági óvintézkedések

A hálózati védelmi intézkedéseket a Szolgáltató belső biztonsági szabályzatában meghatározott követelményeknek megfelelően kell megvalósítani, figyelembe véve az {Sz3} EN 319 411-2 szabvány 6.5.7 fejezetében leírt követelményeket is.

6.8 Időforrások

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

7 TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

7.1 Tanúsítvány profil

A Szolgáltató által kiadott tanúsítványoknak meg kell felelniük az {Sz8} RFC 5280 és az {Sz4} EN 319 412-1, {Sz5} EN 319 412-2, {Sz6} EN 319 412-5 műszaki szabványoknak, valamint a vonatkozó jogszabályi előírásoknak.

A tanúsítvány profilokat a Szolgáltatónak a {D5} BSZ-DÁP-TAN-ban meghatározott módon dokumentálnia kell.

7.1.1 Verziószám

A tanúsítványok verziószáma: V3.

7.1.2 Tanúsítvány kiterjesztések

A tanúsítványokban alkalmazott kiterjesztéseknek mindenben követniük kell az {Sz8} 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.

A Szolgáltatónak az Aláírók tanúsítványaiban alkalmaznia kell a minősített tanúsítványokra vonatkozó nyilatkozatokat tartalmazó szabványos kiterjesztéseket, nem kritikusnak megjelölve (`qcStatements`).

7.1.3 Algoritmus azonosítók

A szolgáltatási szabályzatban meghatározva.

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 tüntethet fel.

7.1.6 Hitelesítési rend objektumazonosító

A Szolgáltatónak a tanúsítványokban fel kell tüntetnie a hitelesítési rend objektumazonosítóját.

7.1.7 Szabályzati megszorítások kiterjesztés használata

Nincs előírás.

7.1.8 Szabályzat minősítők szintaktikája és szemantikája

Nincs előírás.

7.1.9 A kritikus hitelesítési rendek (Certificate Policies) kiterjesztés feldolgozása

Nincs előírás.

7.2 CRL profil

A Szolgáltató által kiadott visszavonási listáknak meg kell felelniük az {Sz8} RFC 5280 műszaki szabványnak.

A CRL profilokat a Szolgáltatónak a {D5} BSZ-DÁP-TAN-ban meghatározott módon dokumentálnia kell.

7.2.1 Verziószám

A visszavonási listák verziószáma: V2.

7.2.2 CRL és CRL bejegyzés kiterjesztések

Nincs előírás.

7.3 OCSP profil

A Szolgáltató által biztosított OCSP szolgáltatásnak meg kell felelnie az {Sz12} RFC 6960 műszaki szabványnak.

Az OCSP profilokat a Szolgáltatónak a {D5} BSZ-DÁP-TAN-ban meghatározott módon dokumentálnia kell.

7.3.1 Verziószám

Az OCSP válaszok verziószáma: V1.

7.3.2 OCSP kiterjesztések

Nincs előírás.

8 MEGFELELŐSÉGVIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

Jelen bizalmi szolgáltatási rend előírja az összes, állampolgárok, mint 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 {Sz2}
- EN 319 411-2: Policy and security 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 gyakoriságának és körülményeinek meg kell felelniük a hatályos jogszabályi előírásoknak.

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

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

8.2 Auditor azonosítása és képesítése

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

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

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

A megfelelőségértékelési vizsgálatot a Szolgáltató olyan, a {J2} 765/2008/EU rendelet 2. cikkének 13. pontjában meghatározott megfelelőségértékelő szervezettel végezteti el, melyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére.

A kiberbiztonsági auditot Szolgáltató olyan auditorral végezteti el, amely szerepel az SZTFH által nyilvántartott auditor listán, és amely jogosult a Szolgáltató elektronikus információs rendszerének

biztonsági osztálya szerinti auditálásra.

8.3 Auditor függetlensége

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

8.4 Audit során vizsgált területek

A megfelelőségértékelés az alábbi területeket fedi le:

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

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

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

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

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

8.5 Hiányosságok esetén végrehajtandó tevékenységek

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

A Felügyeleti Szerv (hatóság) által végzett rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltatónak a hatósággal megállapodott határidőn belül meg kell szüntetnie a hatályos jogszabályok alapján és a hatóságtól kapott információk és ajánlások figyelembe vételével.

8.6 Eredmény kommunikációja

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

9 EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1 Díjak

A díjazással kapcsolatos információkat a {D5} BSZ-DÁP-TAN szolgáltatási szabályzat tartalmazza.

9.2 Anyagi felelősség

A Szolgáltatónak az anyagi felelősség mértékéről, illetve annak korlátairól a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban rendelkeznie kell.

9.2.1 Biztosítási fedezet

A Szolgáltatónak felelősségbiztosítással kell rendelkeznie, mely egyaránt kiterjed az elektronikus aláírással, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, valamint a Bizalmi Felügyeletnél felmerült jogszabály szerinti költségekre, és amely fedezetet biztosít az összes károsultnak okozott kárra, a {D5} BSZ-DÁP-TAN-ban foglaltaknak megfelelően.

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

9.2.2 További követelmények

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

9.2.3 Felelősségbiztosítás vagy garancia végfelhasználók számára

Nincs kikötés.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

A Szolgáltatónak a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban meg kell határoznia a bizalmasan kezelendő információk körét.

9.3.2 Bizalmasnak nem tekintett információk köre

Nincs kikötés.

9.3.3 Bizalmas információk védelmének felelőssége

A Szolgáltatónak meg kell védenie a bizalmas információkat.

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

9.4 Személyes adatok védelme

9.4.1 Adatvédelem

A Szolgáltatónak rendelkeznie kell adatvédelmi szabályozással, valamint a Szolgáltatásokra vonatkozó adatvédelmi tájékoztatóval {D3}, melyeknek összhangban kell lenniük a nemzetközi és hazai vonatkozó jogszabályokkal. Szolgáltatónak az adatvédelmi tájékoztatót {D4} elérhetővé kell tennie internetes honlapján.

9.4.2 Bizalmasként kezelendő személyes adatok

A Szolgáltató csak az Aláíró kifejezett hozzájárulásával gyűjthet személyes adatot és csak olyan mértékben, ami a tanúsítvány kiállításához, valamint Aláíró tájékoztatásához, személyazonosságának megállapításához szükséges.

A Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

- az Aláíró minden adatát.

9.4.3 Bizalmasként nem kezelendő személyes adatok

Szolgáltató nem bizalmasként kezelendő személyes adatnak tekinti a tanúsítványhoz kapcsolódó státusz információkat, beleértve a tanúsítvány esetleges visszavonásának okát és időpontját is.

9.4.4 Személyes adatok védelmének felelőssége

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

9.4.5 Személyes adatok felhasználásának elfogadása

Az Aláírónak a {D1} ÁSZF-DÁP elfogadásával tudomásul kell vennie a tanúsítvány kiállításához és a szerződés megkötéséhez szükséges adatok Szolgáltató által történő nyilvántartásba vételét, kezelését és tárolását.

9.4.6 Felfedés hatósági vagy polgári peres eljárás keretében

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

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

9.4.7 Egyéb, felfedést eredményező körülmények

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

9.5 Szellemi tulajdonjogok

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

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

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 Szolgáltató felelőssége és helytállása

A Szolgáltató felel a jelen bizalmi szolgáltatási rendben és a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban, valamint a {D1} ÁSZF-DÁP-ban megfogalmazott valamennyi kötelezettség maradéktalan betartásáért, még akkor is, ha a Szolgáltatások nyújtásához kapcsolódó egyes feladatokat a Közreműködő Felek vagy egyéb alvállalkozók végzik.

9.6.2 A regisztrációs szervezet felelőssége

A Szolgáltató regisztrációs szervezetének felelőssége a tanúsítványkibocsátások megfelelőségének időszakos, {D5} BSZ-DÁP-TAN szerinti ellenőrzése.

9.6.3 Aláíró felelőssége és helytállása

Az Aláíró jogait, felelősségeit és kötelezettségeit a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban meg kell határozni.

9.6.4 Érintett Felek felelőssége és helytállása

Az Érintett Felek felelősségeit és helytállását a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban meg kell határozni.

9.6.5 Egyéb felek felelőssége és helytállása

Nincs kikötés.

9.7 Helytállás érvénytelenségi köre

A helytállás érvénytelenségi körét a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban meg kell határozni.

9.8 Felelősség korlátozása

A Szolgáltató a {D5} BSZ-DÁP-TAN-ban foglaltak szerint korlátozhatja a kártérítési felelősségét.

9.9 Kártérítések

A kártérítésekről a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban kell rendelkezni.

9.10 Hatályosság és megszűnés

9.10.1 Hatályosság

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

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

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

9.10.2 Megszűnés

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

9.10.3 Megszűnés után is hatályban maradó rendelkezések

A megszűnés után is hatályban maradó rendelkezéseket a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban meg kell határozni.

9.11 Egyéni hirdetmények és kommunikáció a részvevőkkel

A {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban rendelkezni kell a felek és részvevők között kommunikáció joghatást kiváltó módjairól.

9.12 Módosítások

9.12.1 Módosítás eljárása

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

9.12.2 Értesítés módszere és időtartama

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

9.12.3 OID megváltozását előidéző körülmények

A bizalmi szolgáltatási rend OID-ja nem változik.

9.13 Vitás kérdések rendezése

A {D5} BSZ-DÁP-TAN szolgáltatási szabályzat 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 köteles végezni.

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Nincs kikötés.

9.16.2 Átruházás

Nincs kikötés.

9.16.3 Részleges érvénytelenség

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

9.16.4 Igényérvényesítés

A {D5} BSZ-DÁP-TAN szolgáltatási szabályzat tartalmazza.

9.16.5 Force Majeure (Vis maior)

A {D5} BSZ-DÁP-TAN szolgáltatási szabályzat tartalmazza.

9.17 Egyéb rendelkezések

9.17.1 Hozzáférhetőség a fogyatékossággal élő személyek számára

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