NISZ

Nemzeti Infokommunikációs Szolgáltató Zrt.

Bizalmi Szolgáltatási Szabályzat
a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz
(BSZ-ESZIG)

Verziószám	2.0
OID	0.2.216.1.200.1100.100.42.3.1.12.2
Hatályba lépés dátuma	2020.01.13.
Dokumentum besorolása	nyilvános

© Copyright NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. – Minden jog fenntartva

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
1.0	2015.11.27	Hatóságnak benyújtott változat nyilvántartásba vételhez	Polysys Kft.	dr. Sandl Judit Kővári Ferenc	Ferencz Attila
1.1	2016.01.07	Hatóság észrevételei alapján módosított változat	Polysys Kft.	dr. Sandl Judit Kővári Ferenc	Ferencz Attila
1.2	2016.04.27	eSZIG tároló elemének BALE tanúsítása miatt módosított változat	Polysys Kft.	dr. Sandl Judit Kővári Ferenc	Ferencz Attila
1.3	2016.08.01.	On-line tanúsítványigénylés kapcsán tett módosítások	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.4[1]	2016.12.29	eIDAS megfelelőségértékelésre átdolgozott változat	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.5[2]	2017.04.28	Megfelelőségértékelő szervezet észrevételei alapján módosított változat. On-line rendelkezések törlése.	Polysys Kft. Kővári Ferenc	Kővári Ferenc	Ferencz Attila
1.6	2017.05.31	NMHH észrevétele alapján módosított változat	Papp Eszter	Kővári Ferenc	Ferencz Attila
1.7	2018.11.30.	Tanúsítvány érvényességi idő módosítása 2 évről 1 évre	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.8	2019.04.08	MALE/QSCD tanúsítás megújítása	Kővári Ferenc	Joláthy Dániel	Ferencz Attila
1.9	2019.03.14	EN szabványok változásainak követése, egyéb frissítések	Polysys Kft.	Kővári Ferenc	Ferencz Attila
2.0	2020.02.13	Tranzakciós limit módosítása	Joláthy Dániel	Kővári Ferenc	Ferencz Attila

---

[1] Nem lépett hatályba.

[2] Nem lépett hatályba

Tartalomjegyzék

1 BEVEZETÉS

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban, mint Kormányzati Hitelesítés Szolgáltató vagy Szolgáltató) Bizalmi Szolgáltatási Szabályzata, amely a tároló elemmel rendelkező személyazonosító igazolvány (továbbiakban: eSzemélyi) elektronikus aláírás funkciójához szükséges minősített tanúsítvánnyal kapcsolatos bizalmi szolgáltatására vonatkozik (továbbiakban: BSZ-ESZIG).

A Szolgáltató a fenti tárgykörben az alábbi szolgáltatás-elemeket nyújtja:

a) az állampolgárok, mint természetes személyek számára elektronikus aláírás célú EU minősített tanúsítvány kibocsátása, ezen tanúsítványokhoz kapcsolódóan visszavonási és tanúsítvány állapot információk biztosítása;

b) elektronikus aláírás létrehozásához használt adatnak (magánkulcsnak) az Aláíró nevében történő előállítása az eSzemélyi tároló elemén.

Jelen bizalmi szolgáltatási szabályzat a NISZ Zrt. - mint minősített bizalmi szolgáltató - fenti szolgáltatás-elemeire (továbbiakban együttesen Szolgáltatások) vonatkozó eljárásrendi és működési szabályait tartalmazza.

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

1.1 Áttekintés

A szolgáltatási szabályzat célja, hogy összefoglalja mindazokat az információkat, melyeket a Szolgáltató Szolgáltatásaival kapcsolatba kerülő feleknek ismerni szükséges vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát és annak megítélését a Szolgáltatásokat igénybe vevők számára, hogy az ismertetett szolgáltatási gyakorlat, a kibocsátott tanúsítványok, tanúsítvány visszavonási listák, valós idejű tanúsítvány-állapot válaszok mennyiben felelnek meg az elvárásaiknak.

Jelen szolgáltatási szabályzat a "Bizalmi Szolgáltatási Rend a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz" (BR-ESZIG) hatálya alá tartozó Szolgáltatásokra vonatkozik.

Jelen dokumentum, valamint a 1.6.3 fejezetben hivatkozott jogszabályok, szabványok és műszaki specifikációk, továbbá a Szolgáltató 1.6.3.3 fejezetben felsorolt nyilvános dokumentumainak megismerése után a tanúsítványok, tanúsítvány visszavonási listák, valós idejű tanúsítvány-állapot válaszok használói és elfogadói egyértelműen meg tudják állapítani azok kezelésének módját, az általuk garantált biztonság mértékét, valamint a rájuk vonatkozó technikai, üzleti és pénzügyi garanciákat és jogi felelősségvállalásokat.

Jelen szolgáltatási szabályzat az {Sz7} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában szigorúan követi annak előírásait. Az ott meghatározott felépítés szigorú megtartása érdekében azok a fejezetek is szerepelnek a dokumentumban, melyeknél nincs követelmény előírva; ezekben a fejezetekben a "Nincs kikötés" szöveg szerepel.

Szolgáltató az eSzemélyi elektronikus aláírás funkciójához kapcsolódó szolgáltatásait a Felügyeleti Szervnek 2015.11.30.-án jelentette be. A bizalmi felügyelet erre vonatkozó nyilvántartásának elérhetősége: http://webpub-ext.nmhh.hu/esign2016/index.jsp

1.2 Dokumentum neve és azonosítása

Jelen szolgáltatási szabályzat teljes neve: NISZ Zrt. "Bizalmi Szolgáltatási Szabályzat a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz".

A szolgáltatási szabályzat rövid neve: BSZ-ESZIG.

A szolgáltatási szabályzat objektum azonosítója és verziószáma a címlapon található.

Jelen BSZ-ESZIG tartalmazza a BR-ESZIG bizalmi szolgáltatási rend hatálya alatt kiadott tanúsítványok kibocsátására és felhasználására vonatkozó részletes szabályokat. A szolgáltatási szabályzat hatályba lépését és hatályának megszűnését a 9.10 fejezet tartalmazza.

Jelen BSZ-ESZIG-nek csak a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával ellátott változata tekinthető hitelesnek.

1.2.1 Hitelesítési rendek

A BR-ESZIG 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 Szabályzat keretei között nyújtott Szolgáltatásokat alkalmazó közösség az alábbi felekből áll:

- Szolgáltató: a jelen szolgáltatási szabályzat hatálya alatt tanúsítványokat kibocsátó hitelesítés-szolgáltató, amely a tanúsítványok kibocsátásával és menedzsmentjével kapcsolatos műszaki tevékenységeket végzi;
- Közreműködő Felek: a Szolgáltatóval szerződéses kapcsolatban álló vagy jogszabályban meghatározott, a Szolgáltatások nyújtásában közreműködő Regisztrációs és Kártyakibocsátó Szervezet;
- Végfelhasználók: a tanúsítványokat igénylő állampolgárok (Aláírók);
- Érintett Felek: a tanúsítványokon alapuló elektronikus aláírásokat fogadó harmadik felek;
- és Egyéb Felek, azon felek, melyek a fenti szerepkörök egyikébe sem sorolhatók.

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

1.3.1 Hitelesítő szervezet

A hitelesítő szervezet a Szolgáltató központi szervezete, amely a hitelesítő központokból, a szolgáltatás-támogató informatikai rendszerek erőforrásaiból, az ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladatai közé tartozik a tanúsítvány igénylések feldolgozása, tanúsítványok kibocsátása, tanúsítványok megújítása, tanúsítványok visszavonása, továbbá a kibocsátott tanúsítványokra vonatkozóan a visszavonási információk szolgáltatása CRL és OCSP formájában.

Jelen szolgáltatási szabályzat hatálya alatt Szolgáltató kizárólag az állampolgárok részére, az elektronikus személyazonosító igazolványokhoz kapcsolódóan bocsát ki tanúsítványokat. Az aláírás létrehozó eszköz az eSzemélyi tároló elemének elektronikus aláírás funkciót megvalósító része.

Szolgáltató - az email-ben küldött értesítéseket kivéve - az állampolgárokkal közvetlen kapcsolatot nem tart, Aláírók a Regisztrációs Szervezet közreműködésével vehetik igénybe a tanúsítvány kibocsátásra és visszavonás kezelésre irányuló szolgáltatásokat.

Gyökér hitelesítő központ

A Szolgáltató saját gyökér hitelesítő központja RSA 4096 bites kulcsával és SHA256 algoritmus felhasználásával szolgáltatói tanúsítványokat bocsát ki a Szolgáltató produktív hitelesítő központjai részére. A Szolgáltató gyökér tanúsítványának főbb adatai a következők.

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

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

A gyökér tanúsítvány SHA1 lenyomata:
FF:B7:E0:8F:66:E1:D0:C2:58:2F:02:45:C4:97:02:92:A4:6E:88:03
A gyökér tanúsítvány SHA256 lenyomata:
C2:15:73:09:D9:AE:E1:7B:F3:4F:4D:F5:E8:8D:BA:EB:A5:7E:03:61:EB:81:4C:BC:23:9F:4D:54:D3:29:A3:8D

Produktív hitelesítő központ

A Szolgáltató produktív hitelesítő központja RSA 4096 bites kulcsával és SHA256 algoritmus felhasználásával végtanúsítványokat bocsát ki az Aláírók részére. A Szolgáltató produktív hitelesítő központja tanúsítványának főbb adatai a következők.

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

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

Telefonos Ügyfélszolgálat (Kormányzati Ügyfélvonal – 1818)

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

Hitelesítési Rend és Szabályozási Csoport

A Hitelesítési Rend és 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.

1.3.2 Regisztrációs Szervezet és Kártyakibocsátó Szervezet

1.3.2.1 Regisztrációs Szervezet

Regisztrációs Szervezet: a {J6} SzigR. 11. § (1) bekezdésben megjelölt *eljáró hatóság*, amely az általa működtetett helyszínekből, valamint az ott dolgozó személyzetből áll. A Regisztrációs Szervezet a Kártyakibocsátó Szervezet által erre a célra kifejlesztett és üzemeltetett informatikai rendszereket és eszközöket használja.

A Regisztrációs Szervezet a Szolgáltatások nyújtásában Közreműködő Fél, feladata a tanúsítványok kibocsátására és visszavonására irányuló igénylésekkel kapcsolatos adminisztratív és operatív tevékenységek ellátása, különösen a tanúsítványok alanyainak azonosítása, adataik rögzítése, ügyfélszolgálati tevékenységek ellátása.

Regisztrációs Irodák

A Regisztrációs Szervezet Regisztrációs Irodákat tart fenn minden olyan helyen, ahol az állampolgár állandó személyazonosító igazolványt igényelhet, azaz az okmányirodákban és kormányablakokban.

A Regisztrációs Szervezet tartja a közvetlen kapcsolatot Aláírókkal, miközben azok Szolgáltatótól tanúsítványt igényelnek, vagy a tanúsítvány visszavonását kérik. A tanúsítvány kibocsátása folyamat során kapcsolatba lép a Kártyakibocsátó Szervezettel és azzal együttműködve intézkedik az eSzemélyi gyártásáról, a tároló eleme elektronikus aláírás létrehozó részének megszemélyesítéséről, a tanúsítványigénylésnek összeállításáról és Szolgáltatónak való megküldéséről, a kiadott tanúsítványnak az eSzemélyi-re felírásáról. A tanúsítvány visszavonási folyamat során a Regisztrációs Szervezet fogadja Aláíró tanúsítványának visszavonására irányuló kérelmét, továbbítja azt a Szolgáltatónak, aki elvégzi a tanúsítvány visszavonását.

A Regisztrációs Szervezet Szolgáltatóval és a Kártyakibocsátó Szervezettel PKI autentikációval és titkosítással védett biztonságos csatornán, elektronikus bélyegzővel hitelesített üzenetek formájában tartja a kapcsolatot.

A Regisztrációs Szervezet felelősségét és kötelezettségeit a 9.6.2.1 fejezet írja le.

1.3.2.2 Kártyakibocsátó Szervezet

Kártyakibocsátó Szervezet: a Szolgáltatóval szerződéses kapcsolatban álló, {J6} SzigR. 2. § szerinti *nyilvántartást kezelő szerv*, az állandó személyazonosító igazolvány (eSzemélyi) kibocsátója, és az általa működtetett helyszínek és informatikai rendszerek hardver és szoftver összetevőiből, az ezeket körül vevő biztonságos fizikai környezetből, valamint az üzemeltetést ellátó személyzetből áll.

A Kártyakibocsátó Szervezet a Szolgáltatások nyújtásában Közreműködő Fél, feladata az eSzemélyi gyártásakor vagy utólag az Aláírók kulcspárjainak generálása, visszavonási jelszavak generálása, PUK és PIN kódok előállítása és kártyához rendelése, a Regisztrációs Szervezettől kapott adatokkal a kártya megszemélyesítése (a tároló elemre a polgár {J5} Nytv.-ben meghatározott adatainak felírása), tanúsítványkérelmek eljuttatása Szolgáltatónak, a kiadott tanúsítvány felírása, valamint a visszavonási kérelmek továbbítása Szolgáltatónak.

Az aláírói kulcspárok előállítását végző Kártyakibocsátó Szervezet megfelel a {J8} NekR. által előírt műszaki, technológiai, biztonsági előírásoknak és követelményeknek, valamint teljesíti a minősített elektronikus aláírást létrehozó eszköz - QSCD – (korábbi elnevezése: biztonságos aláírás-létrehozó eszköz) tanúsítási jelentésében foglalt előírásokat.

A Kártyakibocsátó Szervezet felelősségét és kötelezettségeit a 9.6.2.2 fejezet írja le.

1.3.3 Előfizetők

Előfizető: az állampolgár (Aláíró), aki a tároló elemmel rendelkező személyazonosító igazolványa elektronikus aláírás funkcióját használni kívánja és Szolgáltatási Szerződést köt a Szolgáltatóval a Szolgáltatások igénybe vételére. Aláíró csak a saját nevére szóló tanúsítványt igényelhet, így jelen dokumentum fogalomrendszerében az Előfizető és az Aláíró személye azonos.

Aláíró kizárólagosan birtokolja az eSzemélyi-t és így az annak tároló elemén levő aláírói kulcspárokat.

Az Aláíró felelősségét és kötelezettségeit a 9.6.3 fejezet írja le.

1.3.4 Érintett Felek

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

Szolgáltatóval.

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

Az Érintett Felek felelősségét a 9.6.4 fejezet írja le.

1.3.5 Egyéb felek

1.3.5.1 Postai Szolgáltató

A {J6} SzigR. 56. § (4) bekezdésének b) pontja szerinti egyetemes postai szolgáltató (továbbiakban Postai Szolgáltató) a Kártyakibocsátó Szervezettel kötött szerződés alapján végzi az eSzemélyi, rajta a tároló elemén elhelyezett tanúsítvány és a kapcsolódó elektronikus aláírás létrehozásához használt adat kézbesítését, abban az esetben, ha az állampolgár az eSzemélyi átvételére a postai utat jelölte meg.

1.3.5.2 Felügyeleti Szerv

A jogszabályokban megjelölt Felügyeleti Szerv biztosítja a Szolgáltató 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.

1.4 A tanúsítvány alkalmazhatósága

A BR-ESZIG hatálya alatt kibocsátott tanúsítvány a kibocsátás időpontjában hatályos jogszabály - {J4} Eat. vagy {J1} eIDAS - szerinti minősített tanúsítvány, az {Sz4} EN 319 412-1 szabvány 3.1 fejezetében az „EU minősített tanúsítványra” vonatkozó követelményeknek megfelelően.

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

A minősített elektronikus aláírás joghatását a {J10} polgári perrendtartásról szóló törvény 325. § határozza meg. E szerint a BR-ESZIG hatálya alatt kibocsátott tanúsítvány felhasználásával létrehozott elektronikus aláírással hitelesített elektronikus dokumentum teljes bizonyító erejű magánokirat.

A Szolgáltató által kibocsátott tanúsítványok (illetve az ehhez kapcsolódó kulcspárok) felhasználhatók minden olyan számítástechnikai alkalmazásban, melyek támogatják a PKI technológián alapuló elektronikus aláírás létrehozási és érvényesítési funkciókat.

Teszt tanúsítványok

A Szolgáltató - egyrészt saját rendszerének tesztelése céljából, másrészt azért, hogy harmadik felek a Szolgáltatásokat kipróbálhassák - teszt tanúsítványokat is kibocsát. A Szolgáltató semmilyen felelősséget nem vállal a teszt tanúsítványok kibocsátásáért, felhasználásukért, a hozzájuk kapcsolódó szolgáltatások rendelkezésre állásáért.

Szolgáltató az éles szolgáltatást nyújtó gyökér hitelesítő központ hierarchiájában nem bocsát ki teszt tanúsítványt. A teszt tanúsítványok a külön az erre a célra létesített teszt gyökér hitelesítő központ hierarchiájában kerülnek kiadásra.

A teszt tanúsítványok megjelölése olyan módon történik, hogy a tanúsítványban feltüntetett hitelesítési rend objektumazonosító: 0.2.216.1.200.1100.100.42.3.999.

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 jelen szabályzat hatálya alatt kibocsátott tanúsítványon alapuló elektronikus aláírással az egy alkalommal vállalható kötelezettség mértéke (tranzakciós limit): 50 000 000 (ötven millió) Forint.

A fentieken túl, kibocsátott tanúsítványok csak a {D1} Általános Szerződési Feltételekben, illetve a {D2} Szolgáltatási Szerződésben rögzített feltételekkel használhatók fel.

A tranzakciós limit a tanúsítványban is rögzítésre kerül. A tanúsítvány elfogadása, a feltüntetett használati információktól eltérő, bármely módú felhasználása az Aláíró és az Érintett Fél egyéni felelőssége és kockázata.

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.

Az eSzemélyi-hez kiadott tanúsítványt (illetve a kapcsolódó magánkulcsot) Aláíró csak magáncélra használhatja fel; ezek használata bármilyen üzleti, munkahelyi vagy egyéb szakmai tevékenység céljából nem megengedett.

1.5 Szabályzat adminisztráció

1.5.1 Szabályzatot karbantartó szerv

A Szolgáltató szervezetén belül Hitelesítési Rend és Szabályozási Csoportot működtet, amely jelen szabályzat karbantartásáért felelős.

1.5.2 Kapcsolat

Az Érintett Felek Szolgáltatóval a kapcsolatot elsősorban a Telefonos Ügyfélszolgálat, másodsorban a Regisztrációs Irodák útján vehetik fel.

Telefonos Ügyfélszolgálat:

Telefon:	1818 Kormányzati Ügyfélvonal, külföldről: +36 1 550-1858
Email:	ekozig@1818.hu
Postacím:	NISZ Zrt. Kormányzati Ügyfélvonal, 1389 Budapest, Pf. 133.

Regisztrációs Irodák:

A http://www.nyilvantarto.hu/hu/oik honlap tartalmazza az elérhetőségeiket és a nyitvatartási időket.

Illetékes fogyasztóvédelmi felügyelőség:

Budapest Főváros Kormányhivatala, Fogyasztóvédelmi Főosztály
Cím: 1052. Budapest, Városház u. 7.
Telefon: +36 1 450 2598
Email: fogyved_kmf_budapest@bfkh.gov.hu

A Szolgáltatással kapcsolatos kifogások és panaszok bejelentésének helye és módja

a) telefonon vagy email-ben a Kormányzati Ügyfélvonalra
b) írásban a Telefonos Ügyfélszolgálat postacímére

Illetékes békéltető testület

Budapesti Békéltető Testület
Cím: 1016 Budapest, Krisztina krt. 99. III, em.310.
Levelezési cím: 1253 Budapest, Pf.:20.
Telefon: +36 1 488 2131
Email: bekelteto.testulet@bkik.hu

Szolgáltató adatai:

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
Cégjegyzék szám: 01-10-041633
Székhely: 1081 Budapest, Csokonai u. 3.
Levelezési cím: 1389 Budapest, Pf.: 133.
Telefon: +36 1 459 4200
Fax: +36 1 303 1000
Email: eSZIG@hiteles.gov.hu
URL: http://hiteles.gov.hu

1.5.3 BR/BSZ alkalmasságának meghatározása

A Szolgáltató legalább évente egyszer megvizsgálja a bizalmi szolgáltatási rend, illetve a 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 Hitelesítési Rend és Szabályozási Csoport gyűjti, a módosításokat legalább évente egyszer elvégzi, majd ellenőrzésre és jóváhagyásra előterjeszti.

1.5.4 BR/BSZ jóváhagyásának eljárása

Az ellenőrzésre, illetve jóváhagyásra a Szolgáltató belső szervezete, illetve a Szolgáltatásokért felelős vezetője rendelkezik hatáskörrel és felelősséggel.

A jóváhagyás előtt a Szolgáltató megvizsgálja a szolgáltatási szabályzat bizalmi szolgáltatási rendnek való megfelelését.

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

A szolgáltatási szabályzat új verziója mindig új verziószámmal kerül elfogadásra.

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

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

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

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

1.6 Fogalmak, rövidítések és hivatkozások

1.6.1 Fogalmak

Alany: A Szolgáltató által kiadott tanúsítványban azonosított entitás, aki/amely a tanúsítványban szereplő nyilvános kulcsnak (elektronikus aláírást érvényesítő adat) megfelelő magánkulcsot (elektronikus aláírás létrehozásához használt adat) birtokolja.

Aláíró: elektronikus aláírást létrehozó természetes személy

Aláírást érvényesítő adat vagy **Elektronikus aláírást 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 vagy **Elektronikus aláírás létrehozásához használt adat**: olyan egyedi adat, amelyet az aláíró elektronikus aláírás létrehozásához használ. Jellemzően kriptográfiai magánkulcs, korábbi elnevezése: aláírás-létrehozó adat.

Aláírást létrehozó eszköz vagy **Elektronikus aláírást létrehozó eszköz**: elektronikus aláírás létrehozásához használt, konfigurált hardver- vagy szoftvereszköz. Korábbi elnevezése: aláírás-létrehozó eszköz.

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, elektronikus bélyegzők, vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése vagy érvényesítése; vagy
b) weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy
c) elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése

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

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

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

Biztonságos környezet: olyan fizikai környezet, mely védett illetéktelen hozzáféréstől, és bizonyos mértékig tűz, víz és egyéb katasztrófaeseményektől, egyéb erőszakos behatásoktól

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

Elektronikus aláírást érvényesítő adat: lásd „Aláírást 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 ellenőrzése: 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 aláírást érvényesítő adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával

Elektronikus aláírás felhasználása: elektronikus adat elektronikus aláírással történő ellátása, illetve az elektronikus aláírás ellenőrzése

Elektronikus aláírási termék: olyan szoftver vagy hardver, illetve más elektronikus aláírás alkalmazáshoz kapcsolódó összetevő, amely elektronikus aláírással kapcsolatos bizalmi szolgáltatások nyújtásához, így különösen elektronikus aláírások, elektronikus bélyegzők, illetőleg elektronikus időbélyegző létrehozásához vagy érvényesítéséhez használható

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

Elektronikus bélyegző létrehozásához használt adatok: olyan egyedi adatok, melyeket az elektronikus bélyegző létrehozója elektronikus bélyegző létrehozásához használ (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 vagy **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

Email cím: az Aláíró a Szolgáltatási Szerződés megkötésekor kötelezően meg kell adjon egy email címet. Ez elsődlegesen a Szolgáltató általi kapcsolattartásra szolgál („értesítési email cím”); emellett ez a cím befoglalásra kerül a tanúsítványba is, ha ezt Aláíró kérte. Ha a későbbiekben Aláíró email címe megváltozik (azaz lesz egy új email címe is), és az új címre szeretné megkapni a Szolgáltató értesítéseit, de ezzel együtt a tanúsítványba foglalt email címe nem változott meg (azaz nem szűnt meg, azt továbbra is használja), akkor a két email cím eltér egymástól.

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

eSzemélyi: A {J5} Nytv. 29. § (1) bekezdésében meghatározott, tároló elemmel ellátott, állandó személyazonosító igazolvány (elektronikuskártya), amely alkalmas az ügyfél elektronikus úton történő közhiteles azonosítására, a polgár kérelmére elektronikus aláírás létrehozására, valamint a polgár a törvényben megjelölt esetekben gyakorolhatja vele a külföldre utazás jogát. A polgár kérelmére tároló eleme tartalmazza az elektronikus aláírás létrehozásához használt adatot és az ahhoz tartozó elektronikus aláírást érvényesítő adatot hitelesítő, elektronikus aláírás célú tanúsítványt.

EU minősített tanúsítvány: a {J2} 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: olyan folyamat, amelynek keretében ellenőrzik és igazolják, hogy az elektronikus aláírás vagy elektronikus bélyegző érvényes

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 (végfelhasználó): olyan entitás, aki/amely a Szolgáltatások keretében előállított kulcsokat és tanúsítványokat és/vagy időbélyegeket rendeltetésüknek megfelelően használja

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

Fokozott biztonságú elektronikus aláírás: olyan elektronikus aláírás, amely megfelel a {J1} eIDAS 26. 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 későbbi változása kimutatható.

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 kimutatható.

Gyökér hitelesítő központ (ROOT CA, vagy Főtanúsítvány kiadó): az elsőnek létrehozott, fizikailag is működő hitelesítő központ, amely az alája rendelt másodlagos (produktív) hitelesítő központokat 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

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

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

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

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 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott szervezet, amelyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére

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

PIN kód: az eSzemélyi tároló eleméhez rendelt, az elektronikus aláírás funkció használatához szükséges, az aláíró hozzáférési jogosultságát ellenőrző adat. Jelen szabályzat a PIN kód alatt minden esetben az elektronikus aláíráshoz tartozó PIN kódot (nem az állandó személyazonosító igazolványhoz tartozó PIN kódot) érti. Ha az állampolgár az eSzemélyi igénylésekor tanúsítványt is igényel, akkor személyesen veszi át a PIN kódot (és visszavonási jelszót) tartalmazó borítékot. A borítékban átvett PIN kód úgynevezett aktiváló (transzport) PIN kód, amely szükséges az elektronikus aláíráshoz tartozó PIN kód létrehozásához.

PUK kód: az eSzemélyi tároló eleméhez rendelt, a személyazonosító igazolványhoz tartozó PIN kód és az elektronikus aláíráshoz tartozó PIN sikertelen megadása után használható feloldó adat. A PUK kódot is tartalmazó borítékot az állampolgár személyesen veszi át az eSzemélyi igénylésekor.

Regisztrációs szervezet: a Szolgáltató és a vele szerződéses alapon vagy jogszabályban meghatározott együttműködő társaságok azon szervezeti egységei, amelyek az állampolgárok adatainak regisztrációját, ellenőrzését, az igénylő személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a hitelesítő szervezethez történő továbbítását, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el

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 jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő adat

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, illetve az archiváláshoz használ

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

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

Tanúsítvány: elektronikus aláírás célú tanúsítvány rövidített megnevezése

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

Visszavonási jelszó: az elektronikus aláíró tanúsítvány ügyfél kérelmére történő visszavonásához szükséges kód. Az állampolgár a visszavonási jelszót az eSzemélyi igénylésekor személyesen, lezárt borítékban veszi át.

1.6.2 Rövidítések

CA	Certification Authority	hitelesítő szervezet

CRL	Certification Revocation List	tanúsítvány visszavonási lista
CP	Certificate Policy	hitelesítési rend
CPS	Certificate Practice Statement	hitelesítési szolgáltatási szabályzat
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
NEK		Nemzeti Egységes Kártyarendszer
NTP	Network Time Protocol	időforrás protokoll
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} 910/2014/EU Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (továbbiakban eIDAS)

{J2} 1999/93/EK Európai Parlament és a Tanács irányelve az elektronikus aláírásra vonatkozó közösségi keretfeltételekről*

{J3} 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (továbbiakban E-ügyintézési tv.)

{J4} 2001. évi XXXV. törvény az elektronikus aláírásról (továbbiakban Eat.)*

{J5} 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról (Nytv.)

{J6} 414/2015. (XII.23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól (SzigR.)

{J7} 2014. évi LXXXIII. törvény az elektronikuskártya-kibocsátási keretrendszerről (Nektv.)

{J8} 53/2015. (IX.24.) BM rendelet az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény végrehajtásához szükséges kapcsolódási, műszaki, technológiai, biztonsági előírásokról, követelményekről és a hitelesítési rendről (NekR.)

{J9} 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről*

{J10} 2016. évi CXXX. törvény a polgári perrendtartásról

{J11} 2013. évi V. törvény a Polgári Törvénykönyvről

{J12} 24/2016. (VI.30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

{J13} 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 (továbbiakban: GDPR)

* Hatályon kívül helyezett jogszabály

1.6.3.2 *Szabványok és műszaki-technikai hivatkozások*

{Sz1}	EN 319 401	General policy requirements for Trust Service Providers
{Sz2}	EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates
{Sz3}	EN 319 411-2	Policy and security requirements for Trust Service Providers issuing EU qualified certificates
{Sz4}	EN 319 412-1	Certificate Profiles; Part 1: Overview and common data structures
{Sz5}	EN 319 412-2	Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons
{Sz6}	EN 319 412-5	Certificate Profiles; Part 5: QCStatements
{Sz7}	RFC 3647	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
{Sz8}	RFC 5280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz9}	ITU-T X.520	Information technology - Open Systems Interconnection - The Directory: Selected attribute types
{Sz10}	RFC 4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz11}	ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework
{Sz12}	RFC 6960	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP
{Sz13}	MSZ/ISO/IEC 15408	ISO/IEC 15408 (parts 1 to 3): Information technology – Security techniques – Evaluation criteria for IT security
{Sz14}	ISO/IEC 19790	ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz15}	FIPS 140-2	FIPS PUB 140-2 (2001): Security Requirements for Cryptographic Modules

1.6.3.3 *Hivatkozott dokumentumok*

{D1}	ÁSZF-GOVCA	Általános Szerződési Feltételek a NISZ Zrt. kormányzati hitelesítés szolgáltatásaihoz
{D2}		Szolgáltatási Szerződés
{D3}		NISZ Zrt. Szervezeti és Működési Szabályzata
{D4}		NISZ Zrt. Adatvédelmi és adatbiztonsági előírásai
{D5}		NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}		NISZ Zrt. PKI szolgáltatások biztonsági szabályzata
{D7}		NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}		Tanúsítvány profilok a NISZ eIDAS Rendelet szerinti bizalmi szolgáltatásaihoz

2 KÖZZÉTÉTEL ÉS ADATTÁRAK

2.1 *Tanúsítványtár*

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

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

2.2 *Szolgáltatói információ közzététele*

A Szolgáltató a szolgáltatói tanúsítványokat, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokat internetes honlapján (https://hiteles.gov.hu) teszi közzé.

A Szolgáltató a végfelhasználói tanúsítványokat belső tanúsítványtárában tárolja, a kiadott tanúsítványt az Aláíró számára rendelkezésre bocsátja. A szolgáltató a végfelhasználói tanúsítványt internetes honlapján nyilvánosan elérhető, kereshető tanúsítványtárában csak akkor teszi közzé, ha Aláíró a tanúsítvány közzétételéhez hozzájárult.

A Szolgáltató a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos visszavonási állapot információkat CRL és OCSP formájában is biztosítja. A visszavonási állapot információk közzétételével kapcsolatos információkat a 4.10 fejezet tartalmazza.

2.3 *A közzététel gyakorisága*

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

Szolgáltató a végfelhasználói tanúsítványokat a nyilvánosan kereshető tanúsítványtárban Aláíró hozzájárulása esetén a kibocsátást követő 24 órán belül teszi közzé.

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

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

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

2.4 *Hozzáférés-ellenőrzések*

Szolgáltató olvasás céljára korlátozás nélküli hozzáférést biztosít a szolgáltatói tanúsítványokhoz, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokhoz, a tanúsítványokkal kapcsolatos visszavonási információkhoz.

A végfelhasználói tanúsítványokkal kapcsolatban biztosítja a nyilvános tanúsítványtár kereshetőségét a tanúsítványban tárolt adatok alapján.

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

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

3 AZONOSÍTÁS ÉS HITELESÍTÉS

3.1 *Elnevezések*

3.1.1 Nevek típusa

A tanúsítványban szereplő nevek megadása megfelel az {Sz9} ITU-T X.520 ajánlásnak.
A tanúsítvány `Issuer` mezőjében szereplő név az alábbi {Sz9} ITU-T X.520 szerinti attribútumokat tartalmazza:

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

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

A tanúsítvány `Subject` mezőjében szereplő név az alábbi {Sz9} ITU-T X.520 szerinti attribútumokat tartalmazza:

- `countryName`;
- `givenName` és `surname`;
- `serialNumber`; és
- `commonName`.

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

3.1.2 Nevek jelentése

A tanúsítvány `Issuer` mezőjében szereplő attribútumok jelentése megegyezik az {Sz9} 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 {Sz9} ITU-T X.520 szerintivel. Ezen túl, az alábbi szabályok érvényesek:

- `countryName`: "HU"
- `surname`: betű szerint azonosan megegyezik az eSzemélyi-be foglalt viselt vezetéknévvel, amely egy vagy több családi nevet és "DR." jelzést tartalmazhat, egymástól szóköz karakterrel elválasztva
- `givenName`: betű szerint azonosan megegyezik az eSzemélyi-be foglalt viselt utónévvel, amely egy vagy több keresztnevet és "DR." jelzést tartalmazhat, egymástól szóköz karakterrel elválasztva.
- `serialNumber`: az eSzemélyi okmányszámát tartalmazza, tartalma és jelentése megfelel az {Sz4} EN 319 412-1 5.1.3 fejezetében leírtaknak
- `commonName`: a `surname` és `givenName` egymás után fűzése, egymástól szóköz karakterrel elválasztva

3.1.3 Előfizetők névtelensége és álnév használata

Az Aláírók névtelensége és álnév használata nem megengedett.

3.1.4 Különféle név formák megjelenítési szabályai

A tanúsítványba foglalt megkülönböztető nevek (Distinguished Name) ASN.1 szintaxisa az {Sz8} RFC 5280 szerinti, megjelenítési szabályait az {Sz10} 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 eSzemélyi-jének okmányszámát.

3.1.6 Márkanevek elismerése, hitelesítése és szerepe

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

3.2 Kezdeti azonosítás

Az Aláíró személyazonosságának igazolását, a tanúsítványhoz való jogosultságának elbírálását, valamint a tanúsítványba foglalandó adatainak ellenőrzését a Regisztrációs Szervezet végzi el, a természetes személy személyes jelenléte útján az okmányigénylési eljárásrendnek megfelelően.

3.2.1 A magánkulcs birtoklása

Aláíró magánkulcsának (kulcspárjának) generálása minden esetben magán az eSzemélyi tároló elemén, az erre szolgáló biztonsági funkciójának használatával történik. Az eSzemélyi tároló elemének elektronikus aláírással kapcsolatos funkcióját ellátó részének műszaki-technikai kialakítása biztosítja, hogy a magánkulcs a kártyát soha, semmilyen körülmények között nem hagyja el. Az eSzemélyi tároló elemének elektronikus aláírással kapcsolatos funkcióját ellátó része QSCD tanúsítással rendelkezik. Az eSzemélyi-t Aláíró kizárólagosan birtokolja.

3.2.2 A szervezeti azonosság hitelesítése

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

3.2.3 A személyazonosság hitelesítése

A személyazonosság ellenőrzését és hitelesítését a Regisztrációs Szervezet a 3.2 fejezet elején leírt eljárással végzi el.

3.2.4 Előfizető nem ellenőrzött adatai

Szolgáltató a Regisztrációs Szervezet útján ellenőrzi Aláírónak minden, a tanúsítvány alanyának megkülönböztető nevébe (`Subject`) kerülő adatát.

Szolgáltató Aláíró tanúsítványba foglalt adatai közül nem ellenőrzi az email címet, mely az állampolgár nyilatkozata alapján a tanúsítvány tulajdonos alternatív nevei (`Subject Alternative Name`) kiterjesztésében feltüntetésére kerülhet. Az email cím valódiságáról Aláíró írásban nyilatkozott a Szolgáltatási Szerződés megkötésekor.

3.2.5 Jogosultság ellenőrzése

A Regisztrációs Szervezet {J5} Nytv. szabályai szerint ellenőrzi és elbírálja Aláírónak a tanúsítványhoz való jogosultságát.

3.2.6 Együttműködési kritériumok

Szolgáltató a Szolgáltatások nyújtása során nem működik együtt más hitelesítés-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

A tanúsítvány visszavonási kérelmet fogadó fél a kérelmező azonosítását és hitelesítését az alábbiak szerint végzi:

a) Aláíró kérelmező esetében: a Regisztrációs Szervezet a 3.2 fejezetben leírt eljárással vagy a Kormányzati Ügyfélvonal (1818) a visszavonási jelszónak a telefon nyomógombjaival történő megadásával azonosítja és hitelesíti Aláírót;

a) okmányérvénytelenítést, illetve át nem vett okmányt jelző hatóság esetében: a Szolgáltató PKI, tanúsítvány alapú X.509 azonosítással, valamint a visszavonási kérelmen elhelyezett elektronikus bélyegző ellenőrzésével hitelesíti a kezdeményezőt.

4 A TANÚSÍTVÁNYOK ÉLETCIKLUSA

A tanúsítványok életciklusának folyamataiban Szolgáltatón kívül a Regisztrációs Szervezet és a Kártyakibocsátó Szervezet működik közre. Szolgáltató teljes körűen felelős a közreműködők tevékenységért, valamint azért, hogy jelen szabályzatban leírt követelmények teljesülnek.

A Szolgáltató felelős minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okozott, azon kötelezettségei megszegéséből eredően, mely kötelezettségek az esemény időpontjában hatályos, vonatkozó jogszabályban meghatározottak.

A Szolgáltató nem felelős olyan kárért, melyre bizonyítja, hogy az szándékos vagy gondatlan közrehatása nélkül következett be.

Szolgáltató nem felelős a tanúsítvány felhasználására vonatkozó korlátozások be nem tartásából származó károkért.

4.1 Tanúsítványigénylés

4.1.1 Ki nyújthat be tanúsítványigénylést

Tanúsítványigénylést olyan állampolgár nyújthat be, aki tároló elemmel ellátott állandó személyazonosító igazolvány igénylésére a {J5} Nytv. szerint jogosult, vagy érvényes, tároló elemmel ellátott állandó személyazonosító igazolvánnyal már rendelkezik. Az igénylő tanúsítványra jogosultságának elbírálását a Regisztrációs Szervezet végzi.

4.1.2 Igénylési folyamat és felelősségek

A tanúsítványigénylés folyamata röviden a következő:

- tájékoztatás
- regisztráció
- Szolgáltatási Szerződés megkötése
- tanúsítványkérelem előállítása

A folyamatban közvetlenül a Regisztrációs Szervezet, közvetett módon a Kártyakibocsátó Szervezet vesz részt. A Felek a folyamat során PKI autentikációval és titkosítással védett biztonságos csatornán, elektronikus bélyegzővel hitelesített üzenetek formájában kommunikálnak egymással. A Felek felelősségeit a 9.6 fejezet tartalmazza.

Tájékoztatás

A Szolgáltatási Szerződés megkötése előtt igénylőt a Regisztrációs Szervezet ügyintézője teljes körűen és közérthetően tájékoztatja az alábbiakról:

- az elektronikus aláírás használati lehetőségeiről és jogszabályi feltételeiről;
- az aláírás létrehozásához használt adat (magánkulcs) használatával kapcsolatos intézkedésekről;
- az aláírást létrehozó eszköz használatáról;
- az aláírás létrehozásához használt adat védelméhez szükséges biztonsági intézkedésekről;
- az aláíró és az aláírást ellenőrizni kívánó felek felelősségéről, kötelezettségeiről;
- tanúsítványok visszavonásának lehetőségéről;
- tanúsítványok kibocsátásának körülményeiről;
- a tanúsítvány érvényességéről, érvényességi idejének lejártáról;

- a szolgáltatási szabályzat tartalmáról és elérhetőségéről;
- a tanúsítvánnyal kapcsolatos, a tanúsítványban meghatározott tárgybeli, időbeli, földrajzi vagy egyéb korlátozásokról;
- a szolgáltatói nyilvános kulcsról, valamint annak elérhetőségéről;
- arról, hogy a szolgáltatás igénybe vétele díjmentes;
- arról, hogy a szolgáltatás minősített bizalmi szolgáltatásnak minősül;
- a panaszok benyújtására, a jogviták rendezésére vonatkozó szabályokról;
- arról, hogy lehetősége van hozzájárulni vagy megtiltani tanúsítványának a nyilvános tanúsítványtárban való közzétételéről;
- arról, hogy döntése szerint kérheti vagy megtilthatja az email címének feltüntetését a tanúsítványban.

Regisztráció

Igénylő a {J5} Nytv. és {J6} SzigR. szerinti okmányigénylési eljárásrendnek megfelelően a Regisztrációs Szervezet irodájában személyesen megjelenik új eSzemélyi igénylése céljából, vagy meglevő eSzemélyi-jére aláírói tanúsítvány igénylése céljából és érvényes eSzemélyi-jét bemutatja.

A 3.2 fejezetben leírt azonosítási eljárást követően, az abból származó és közhiteles nyilvántartások alapján ellenőrzött adatokkal a Regisztrációs Szervezet ügyintézője az igénylő tanúsítványba kerülő, valamint a Szolgáltatási Szerződés megkötéséhez szükséges adatait regisztrálja, majd kinyomtatja a Szolgáltatási Szerződést.

Szolgáltatási szerződés megkötése

A Szolgáltatási Szerződés tartalmazza a hatályos jogszabályoknak megfelelő tartalmi elemeket, továbbá az igénylő szükséges nyilatkozatait (például azt, hogy hozzájárul vagy megtiltja tanúsítványának a nyilvános tanúsítványtárban történő közzétételét).

Igénylő ellenőrzi a Szolgáltatási Szerződésben szereplő adatok helyességét és saját kezű aláírásával igazolja az adatok valódiságát.

Az eSzemélyi elektronikus aláírás funkciójához szükséges aktiváló PIN kódot és a tanúsítvány visszavonásához szükséges visszavonási jelszót tartalmazó lezárt borítékot az ügyintéző személyesen adja át, az átvételről szóló elismervényt igénylő aláírja.

Regisztrációs Szervezet intézkedik arról, hogy az aláírt Szolgáltatási Szerződés, valamint az aktiváló PIN kódot és visszavonási jelszót tartalmazó lezárt boríték átvételét igazoló átvételi elismervény Szolgáltatónak megküldésre kerüljön.

Tanúsítványkérelem előállítása

Amennyiben állampolgár a tanúsítványt új eSzemélyi okmánnyal együttesen igényelte, a Regisztrációs Szervezet a Kártyakibocsátó Szervezettel együttműködve gondoskodik arról, hogy az okmány legyártásra és Aláíró adataival megszemélyesítésre kerüljön, az eSzemélyi tároló elemén - az erre a célra szolgáló biztonsági funkciójának felhasználásával – az aláírói kulcspár létrejöjjön, az ahhoz tartozó tanúsítványkérelem összeállításra és Szolgáltatónak megküldésre kerüljön. Az állampolgár nyilatkozik arról, hogy az elkészült eSzemélyi-t személyesen az okmányirodában veszi át, vagy postai úton, saját kezébe történő kézbesítéssel kéri.

Amennyiben az állampolgár a tanúsítványt meglevő, érvényes eSzemélyi-jére utólag igényelte, a Regisztrációs Szervezet a Kártyakibocsátó Szervezettel együttműködve gondoskodik arról, hogy az eSzemélyi tároló elemén - az erre a célra szolgáló biztonsági funkciójának felhasználásával - az aláírói kulcspár létrejöjjön, az ahhoz tartozó tanúsítványkérelem összeállításra és Szolgáltatónak megküldésre kerüljön.

4.2 *Tanúsítványigénylés feldolgozása*

4.2.1 Azonosítási és hitelesítési műveletek

A tanúsítványkérelem igénylőjét (Aláírót) a Regisztrációs Szervezet azonosítja a 3.2 fejezetben leírt eljárással. Regisztrációs Szervezet csak olyan Aláíró számára állít össze tanúsítványkérelmet, akit sikeresen azonosított és aki tanúsítvány igénylésére jogosult.

Szolgáltató csak és kizárólag a Regisztrációs Szervezettől származó, a Kártyakibocsátó Szervezet által létrehozott tanúsítványkérelmet fogad el. Szolgáltató az informatikai rendszert PKI autentikációval azonosítja, a tanúsítványkérelmek hitelességét a kérelmen elhelyezett, aláírás időpontját hitelesítő időbélyeget is tartalmazó, elektronikus bélyegző ellenőrzésével bírálja el.

4.2.2 Tanúsítványigénylés elfogadása vagy visszautasítása

Szolgáltató elfogadja a sikeresen azonosított Regisztrációs Szervezettől származó tanúsítványkérelmet, melynek hitelességét az elektronikus bélyegző érvényesítésével ellenőrizte.

Szolgáltató visszautasítja a tanúsítványkérelmet, ha az nem a Regisztrációs Szervezettől származik, vagy ha az azon elhelyezett elektronikus bélyegző nem érvényes.

4.2.3 Tanúsítványigénylés feldolgozás időtartama

Szolgáltató a tanúsítványkérelmeket a beérkezését követően haladéktalanul feldolgozza.

4.3 *Tanúsítvány kibocsátás*

4.3.1 Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek

Szolgáltató ellenőrzi és hosszú távú érvényesítésre alkalmas formára egészíti ki a tanúsítványkérelmen elhelyezett elektronikus bélyegzőt, majd tárolja azt belső nyilvántartásaiban. Kiállítja a tanúsítványt a kérelemből származó adatokkal, azt tanúsításválaszban adja vissza.

Szolgáltató tanúsításválasza alapján a Kártyakibocsátó Szervezet gondoskodik a kibocsátott tanúsítvány és az ahhoz tartozó szolgáltatói tanúsítványok (tanúsítványlánc) tárolásáról az eSzemélyi tároló elemének elektronikus aláírás funkciót ellátó részén.

4.3.2 Előfizető értesítése a tanúsítvány kibocsátásról

Amennyiben a tanúsítvány kibocsátása új eSzemélyi igénylése kapcsán történt:

- ha az állampolgár az eSzemélyi átvételére az okmányirodai személyes átvételt választotta, akkor a Regisztrációs Szervezet értesíti Előfizetőt az átvétel időpontjáról és helyéről;
- ha az állampolgár az eSzemélyi átvételére a postai utat jelölte meg, akkor a Regisztrációs Szervezet gondoskodik arról, hogy a Postai Szolgáltató az eSzemélyi-t kézbesítse.

Amennyiben a tanúsítvány kibocsátása meglevő eSzemélyi-re utólag történt, Aláíró értesítése nem szükséges, mert az személyes jelenlétében zajlott le.

4.4 Tanúsítvány-elfogadás

4.4.1 Tanúsítvány Előfizető általi elfogadása

Aláíró kötelezettsége, hogy az átvett tanúsítványban feltüntetett adatok helyességét mihamarabb ellenőrizze. Amennyiben bármilyen eltérést talál, haladéktalanul intézkednie kell a tanúsítvány visszavonásáról. Ha a tanúsítvány fenti okból való visszavonása az átvételt követő harminc napon belül nem történik meg, vagy az Aláíró a tanúsítványhoz kapcsolódó magánkulccsal elektronikus aláírást hozott létre, akkor a tanúsítvány Aláíró által elfogadottnak minősül.

Ha Aláíró az új eSzemélyi-re igényelt tanúsítványt, és azt az átvételre való felhívást követően sem vette át, akkor az eSzemélyi kiállításától számított hatvanadik nap elteltével - az eljáró hatóság adatszolgáltatása alapján - Szolgáltató a tanúsítványt visszavonja.

4.4.2 Tanúsítvány közzététele

Amennyiben Aláíró ahhoz írásban hozzájárult, Szolgáltató haladéktalanul közzé teszi a kibocsátott tanúsítványt a nyilvános tanúsítványtárban.

4.4.3 További felek értesítése a tanúsítvány kibocsátásáról

Nincs kikötés.

4.5 A kulcspár és a tanúsítvány használata

4.5.1 Az Előfizető magánkulcs- és tanúsítvány használata

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

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

Aláírónak a magánkulcs- és tanúsítvány használata során be kell tartania a 9.6.3 fejezetben ismertetett kötelezettségeit, különösen gondoskodnia kell az aláírást létrehozó eszköz (eSzemélyi) és az aláírás aktivizáló adat (PIN kód) illetéktelen hozzáférés elleni védelméről.

4.5.2 Az Érintett Felek nyilvános kulcs- és tanúsítvány használata

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

- a tanúsítványok, valamint az elektronikus aláírások ellenőrzését olyan megbízható alkalmazással végezze, amely megfelel a jelen szolgáltatási szabályzat 1.6.3.1 fejezetében felsorolt jogszabályoknak és amely képes az 1.6.3.2 fejezetben megadott műszaki szabványok támogatására és azokat helyesen valósítja meg;
- az előző pontban említett aláírás ellenőrző alkalmazást megbízható, vírusmentes környezetben használja, továbbá az aláírás ellenőrző alkalmazás beállítási lehetőségei helyesen legyenek konfigurálva;
- a tanúsítványokat csak olyan alkalmazásokban fogadja el, melyek összhangban vannak a

a tanúsítvány "kulcshasználat" (`KeyUsage`) és "kiterjesztett kulcshasználat" (`ExtendedKeyUsage`) kiterjesztésének tartalmával;

- végezze el a tanúsítványra az {Sz8} RFC 5280 6. fejezetében leírt tanúsítási útvonal felépítést és érvényesítést, valamint visszavonás ellenőrzést, a tanúsítványt, illetve az ezen alapuló elektronikus aláírást csak ezen ellenőrzések pozitív eredménye esetén fogadja el;
- vegyen figyelembe minden korlátozást, amely a tanúsítványban vagy a tanúsítvány által hivatkozott szabályzatokban szerepel, különös tekintettel a tanúsítvánnyal egy alkalommal vállalható kötelezettségvállalás mértékére (tranzakciós limit, azaz a `QcStatements` kiterjesztésben a `QcLimitValue` mező értéke), mivel az ezen összeghatárt meghaladó ügyletekben létrehozott és aláírt elektronikus dokumentumokból származó követelésekért, illetve az így okozott kárért a Szolgáltató nem felel.

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

4.6 Tanúsítványok megújítása

Az irányadó szabvány ({Sz7} RFC 3647) szerint a tanúsítvány megújítás az a folyamat, amely során Szolgáltató az Aláíró változatlan nyilvános kulcsát és változatlan adatait hitelesíti új érvényességi időtartamra szóló új tanúsítvány kibocsátásával. Ebben az értelemben Szolgáltató nem nyújt tanúsítvány megújítási szolgáltatást, a kulcspárok élettartamára vonatkozó biztonsági megfontolásokból.

A köznapi értelemben vett tanúsítvány megújítást Szolgáltató lehetővé teszi a lejáratot megelőző hatvan napon belül, Aláíró ez irányú kérelmére. Ebben az esetben Aláíró eSzemélyi-jének tároló elemén - a meglevő kulcspár és tanúsítvány törlésével, illetve felülírásával egyidejűleg - új kulcspár kerül előállításra, és új tanúsítvány kerül kiadásra, melynek érvényességi időszaka a kibocsátás időpontjával kezdődik és attól számított két évig[3], vagy ha az eSzemélyi korábban lejár, akkor annak lejáratának időpontjáig tart.

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.

---

[3] Ezen szabály alól kivételt képeznek a 2019. évben kiadott tanúsítványok, melyek érvényessége 1 év.

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 Tanúsítvány-módosítás

A Szolgáltató nem nyújt tanúsítvány módosítás szolgáltatást. Aláíró a meglevő tanúsítványában foglalt adatok módosulása esetén új tanúsítványt kell igényeljen.

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 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

Szolgáltató visszavonja a tanúsítványt, ha:

- Aláíró ezt kéri:
    - nem kívánja a továbbiakban használni az eSzemélyi elektronikus aláírás funkcióját;
    - fennáll az a lehetőség vagy gyanú, hogy az eSzemélyi elektronikus aláírás funkciójával illetéktelen személy visszaél;
    - adatváltozás vagy egyéb ok miatt (például a tanúsítványba foglalt email cím

  megszűnése, megváltozása miatt).
- Szolgáltató az eljáró hatóságtól megkapja az át nem vett okmányokra vonatkozó információt;
- Szolgáltató megkapja az eSzemélyi érvénytelenné válására vonatkozó hatósági adatszolgáltatást, az alábbi esetekben:
    - az eSzemélyi eltulajdonítása, megsemmisülése, megrongálódása, elvesztése bejelentését követően; vagy
    - az eSzemélyi bármilyen más okból kifolyólag letiltásra vagy érvénytelenítésre kerül (pl. Aláíró adatváltozást jelentett be).
- Szolgáltató a Szolgáltatásokkal kapcsolatos rendellenességről szerez tudomást;
- Szolgáltató tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak illetve a bizalmi szolgáltatási rendnek, amely hatálya alatt a tanúsítvány kibocsátásra került, vagy a tanúsítványt jogellenesen használták, vagy az elektronikus aláírás létrehozásához használt adat (magánkulcs) nem Aláíró kizárólagos birtokában van;
- a Felügyeleti Szerv jogerős és végrehajtható határozatában elrendeli a visszavonást;
- a visszavonást jogszabály kötelezővé teszi;
- Szolgáltató a tevékenységét befejezi;
- a tanúsítvány formátuma vagy műszaki tartalma (pl. kriptográfiai algoritmus vagy kulcsméret már nem biztonságos) elfogadhatatlan kockázatot jelent az Érintett Felek részére;
- a tanúsítványban felhasznált kriptográfiai algoritmus, kulcshossz, azok paraméterei már nem biztosítják az Alany és a nyilvános kulcs hiteles összekapcsolását a tanúsítvány érvényességének hátralevő időszakára.

4.9.2 Ki kezdeményezheti a visszavonást

Visszavonást kezdeményezhet, a 4.9.1 fejezetben megjelölt esetekben:

- Aláíró;
- az át nem vett okmányokat jelző eljáró hatóság;
- az eSzemélyi érvénytelenítéséről jogszabály alapján döntő hatóság;
- Szolgáltató (ideértve azt az esetet is, amikor a visszavonás a Felügyeleti Szerv határozata vagy jogszabályi előírás miatt történik).

4.9.3 Visszavonási kérelemre vonatkozó eljárás

Aláíró a tanúsítványának visszavonását a Regisztrációs Szervezet irodáiban személyesen vagy telefonon a Szolgáltató Telefonos Ügyfélszolgálatán (Kormányzati Ügyfélvonal – 1818) kérheti.

Az át nem vett okmányt jelző hatóság, illetve az okmány érvénytelenítéséről jogszabály alapján döntő hatóság adatszolgáltatása alapján a Regisztrációs Szervezet a Szolgáltatónak eljuttatott elektronikus bélyegzővel hitelesített elektronikus üzenetben nyújtja be a visszavonási kérelmet.

Szolgáltató a 3.4 fejezetben leírt módon ellenőrzi a kérelmező azonosságát és a visszavonási kérelem hitelességét. Ha az ellenőrzések sikeresek, Szolgáltató elvégzi a tanúsítvány visszavonását és közzé teszi a megváltozott visszavonási állapot információt, valamint elektronikus levélben értesíti Aláírót a tanúsítvány visszavonásáról. Ha az ellenőrzések valamelyike sikertelen, Szolgáltató a visszavonási kérelmet visszautasítja.

Abban az esetben, ha az Aláíró vagy a Szolgáltató által használt kulcs algoritmusa, paramétere nem megfelelően erős a kulcshoz kapcsolódó tanúsítvány teljes érvényességi időtartamára, Szolgáltató intézkedik az érintett tanúsítványok megfelelő időben történő visszavonásáról, melynek időpontjáról az Aláírókat és az Érintett Feleket előzetesen értesíti.

A Szolgáltató biztosítja, hogy tanúsítvány visszamenőleges visszavonása ne történhessen meg.

Szolgáltató az egyszer már visszavont tanúsítvány érvényességét soha nem állítja vissza érvényesre.

Szolgáltató nem biztosít olyan lehetőséget, hogy a kérelmező egy általa megjelölt jövőbeni időpontra kérje a tanúsítvány visszavonását.

4.9.4 Kivárási idő visszavonási kérelem esetén

Szolgáltató nem alkalmaz kivárási időt a visszavonási kérelmek teljesítése során.

4.9.5 Visszavonási kérelem feldolgozásának időbelisége

Szolgáltató a visszavonási kérelmet sikeres ellenőrzések esetén a benyújtástól számított három óra időtartamon belül feldolgozza.

4.9.6 Visszavonás ellenőrzésének ajánlása az Érintett Felek számára

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

4.9.7 CRL kibocsátási gyakoriság

A végfelhasználói tanúsítványokra vonatkozó CRL kibocsátásának gyakorisága: 24 óránként egy CRL. A kibocsátott CRL érvényessége 24 óra. A CRL tartalmazza a következő kibocsátás időpontját (a `nextUpdate` mezőben). Szolgáltató minden kibocsátáskor törli a CRL-ről azokat a tanúsítványokat, melyek érvényessége a CRL kibocsátásnak időpontjában már lejárt.

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

4.9.8 CRL előállítása és közzététele között leghosszabb idő

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

4.9.9 OCSP szolgáltatás biztosítása

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

4.9.10 OCSP alapú visszavonás ellenőrzés követelményei

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

4.9.11 Visszavonási állapot közlés más formái

Szolgáltató, a honlapján elérhető nyilvános tanúsítványtárban is közzé teszi a visszavonási állapot információt, tájékoztatási jelleggel. Ez az információ elektronikus aláírás ellenőrzéséhez nem használható fel. Ez a figyelmeztetés a nyilvános tanúsítványtárban is feltüntetésre kerül.

4.9.12 Különleges követelmények a kulcs kompromittálódása esetére

Szolgáltató a szolgáltatói magánkulcsának kompromittálódása esetén az eseményről honlapján tájékoztatást tesz közzé, Aláírókat email-ben értesíti.

A produktív hitelesítő központ magánkulcsának kompromittálódása esetén Szolgáltató képes az összes érintett végfelhasználói tanúsítvány visszavonására és az érintett CRL-nek a 24 órán belüli kibocsátására és közzétételére, majd ezt követően, az adott szolgáltatói tanúsítvány visszavonására és az érintett CRL-nek a 12 órán belüli kibocsátására és közzétételére.

4.9.13 Felfüggesztés körülményei

Mivel Aláíró a tanúsítvány felfüggesztését a {J6} SzigR. rendelkezései értelmében nem kezdeményezheti, Szolgáltató nem nyújt felfüggesztési szolgáltatást.

4.9.14 Ki kérelmezhet felfüggesztést

Nincs kikötés.

4.9.15 Felfüggesztésre vonatkozó eljárás

Nincs kikötés.

4.9.16 A felfüggesztés megengedett időtartama

Nincs kikötés.

4.10 Visszavonási állapot szolgáltatások

4.10.1 Működési jellemzők

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

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

CRL

A Szolgáltató által kibocsátott CRL megfelel a {Sz8} RFC 5280 szabványnak.

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

A CRL minden esetben tartalmazza a következő kibocsátás időpontját (`nextUpdate`). A záró CRL (az adott hitelesítő központ által kiadott utolsó CRL) esetén a `nextUpdate` mező tartalma a „99991231235959Z” RFC 5280 {Sz9} szerinti speciális időpont. Szolgáltató biztosítja, hogy az új CRL kibocsátása a `nextUpdate` mezőben jelzett időpont előtt minden esetben megtörténik

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

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

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

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

Végfelhasználói tanúsítványokra vonatkozó CRL elérhetősége	http://cca.hiteles.gov.hu/crl/GOVCA-CCA.crl
Szolgáltatói tanúsítványokra vonatkozó CRL elérhetősége	http://qca.hiteles.gov.hu/crl/GOVCA-ROOT.crl

OCSP

A Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz12} RFC 6960 szabványnak.

Az OCSP szolgáltatást Szolgáltató az {Sz12} RFC 6960 2.2 fejezetében meghatározott "Authorized Responder" elvnek megfelelően működteti.

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

Az OCSP válaszadó számára minimum 4 és maximum 21 óránként új, 24 órás érvényességű tanúsítvány kerül kiadásra, annak érdekében, hogy az OCSP választ aláíró tanúsítvány visszavonási állapotát ne kelljen ellenőrizni, ennek jelzésére az OCSP válaszadó tanúsítványában szerepel az `id-pkix-ocsp-nocheck` kiterjesztés.

Az OCSP szolgáltatás keretében a Szolgáltató biztosítja a visszavonási információt a tanúsítvány lejáratát követően is, 10 évig, illetve az érintett hitelesítő központ működtetési időtartamában. Egy adott hitelesítő központ működtetésének megszüntetésekor záró CRL kerül kiadásra, és ezzel egyidejűleg Szolgáltató az OCSP válaszadó működését átkonfigurálja olyan módon, hogy minden OCSP kérés visszautasításra kerüljön („unathorized” hibajelzéssel.

Végfelhasználói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége	http://cca.ocsp.hiteles.gov.hu/ocsp-cca
Szolgáltatói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége	http://qocsp.hiteles.gov.hu/ocsp-root

4.10.2 Szolgáltatás rendelkezésre állása

A CRL, illetve az OCSP szolgáltatás az év minden napján, napi 24 órában elérhető, 99,9%-os rendelkezésre állással, úgy hogy a kiesés nem lépheti túl esetenként a 3 órás időtartamot.

4.10.3 Opcionális lehetőségek

Nincs kikötés.

4.11 Az előfizetés vége

Aláíró szerződéses viszonya megszűnik a tanúsítvány lejáratával vagy ha a tanúsítvány érvényességének lejárata előtt Aláíró kérésére vagy bármely más okból kifolyólag a tanúsítvány visszavonásra kerül.

4.12 Kulcsletét és visszaállítás

Szolgáltató nem nyújt kulcsletét és visszaállítás szolgáltatást.

4.12.1 Kulcsletét és visszaállítás szabályai

Nincs kikötés.

4.12.2 Rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Nincs kikötés.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

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

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

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

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

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

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

Szolgáltató a tanúsítványok előállításában, a visszavonási információk menedzsmentjében közreműködő informatikai rendszereit, berendezéseit és eszközeit a legmagasabb védelmi szintet képező központi géptermében helyezi el.

5.1 *Fizikai óvintézkedések*

5.1.1 Telephely elhelyezése és szerkezeti felépítése

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

5.1.2 Fizikai hozzáférés

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

Ehhez biztosítja az alábbiakat:

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

5.1.3 Áramellátás és légkondicionálás

A Szolgáltató a gépteremben olyan szünetmentes áramellátó rendszert alkalmaz, amely:

- megfelelő teljesítménnyel rendelkezik a gépterem informatikai és kisegítő létesítményi berendezései áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózat feszültség ingadozásai, feszültség kimaradásai és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramellátó berendezés biztosítja - üzemanyag utántöltéssel - tetszőlegesen hosszú időtartamig az áramellátást.

Szolgáltató a gépteremben olyan légkondicionáló berendezést alkalmaz, mely biztosítja az alábbiakat:

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

5.1.4 Beázás és elárasztás veszélyeztetettség

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

5.1.5 Tűzmegelőzés és tűzvédelem

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

5.1.6 Adathordozók tárolása

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

5.1.7 Selejt kezelése és megsemmisítése

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

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

Szolgáltató azt az adatmentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható, olyan külső helyszínen tárolja, mely megfelelő fizikai és működési védelemmel rendelkezik. Biztosítja helyszínek között a mentett adatok biztonságos továbbítását.

Az adatmentést, vagy abból a helyreállítást rendszerüzemeltető bizalmi munkakört betöltő személy végzi el.

5.2 *Eljárásbeli előírások*

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

Az eljárásbeli szabályokat a következő szabályzatok tartalmazzák:

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

5.2.1 Bizalmi munkakörök

Szolgáltató az alábbi bizalmi munkaköröket azonosította, melyektől a szolgáltatások biztonsága függ:

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

f) regisztrációs felelős: a végtanúsítványok előállításának, kibocsátásának jóváhagyásáért, az életciklus menedzsment tevékenységek és adminisztráció szabályszerű végzéséért felelős személy;

g) visszavonás felelős: a végtanúsítványok visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.*

* A vonatkozó jogszabály ({J12} 84/2012. (IV. 21.) Korm. rendelet) a visszavonás felelős feladatkörét a regisztrációs felelős tevékenységi körébe tartozóan rögzíti.

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

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

A bizalmi munkakörökön kívül Szolgáltató bizalmi szerepköröket is alkalmaz. A bizalmi szerepkört betöltő személy munkaviszonyban áll a Szolgáltatóval vagy a Regisztrációs és Kártyakibocsátó Szervezettel. Szolgáltató az alábbi bizalmi szerepköröket azonosítja:

Az eSzemélyi elektronikus aláírás funkciójához tartozó tanúsítványok kapcsán fontos szerepkör a külső ügyfélkapcsolati munkatárs (jellemzően okmányirodai ügyintéző), aki többek között:

- tájékoztatja Aláírót az eSzemélyi okmányhoz igényelhető tanúsítvánnyal kapcsolatos információkról;
- az okmányigénylési eljárásrend szerint személyesen azonosítja az Aláírót;
- felveszi és rögzíti a tanúsítványigényléshez és a Szolgáltatási Szerződés megkötéséhez szükséges adatokat, azokat ellenőrzi közhiteles nyilvántartásokkal és Aláíróval is ellenőrizteti;
- közreműködik a Szolgáltatási Szerződés megkötésében;
- átadja Aláírónak a PIN borítékokat.

A külső ügyfélkapcsolati munkatársak tevékenységét a regisztrációs felelős ellenőrzi.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

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

- szolgáltatói kulcspár létrehozása;
- szolgáltatói magánkulcs mentése és visszaállítása;
- szolgáltató magánkulcs aktiválása;
- szolgáltatói magánkulcs megsemmisítése.

5.2.3 Bizalmi munkakörökben elvárt azonosítás és hitelesítés

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

5.2.4 Egymást kizáró munkakörök

Szolgáltató biztosítja, hogy a bizalmi munkakörök vonatkozásában:

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

5.3 Személyzetre vonatkozó előírások

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

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

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

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

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

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

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

A regisztrációs felelős esetén középfokú szakirányú végzettség és legalább egy év informatikai biztonsággal összefüggésben szerzett szakmai gyakorlat szükséges.

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

Az egyes bizalmi munkakörök betöltéséhez elvárt szakirányú végzettségek meghatározását a Szolgáltató belső, nem nyilvános szabályzata tartalmazza.

5.3.2 Biztonsági háttér ellenőrzés eljárásai

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

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, ami a büntetlenséget befolyásolhatja (a büntetlen előéletet három hónapnál nem régebbi erkölcsi

bizonyítvánnyal kell igazolni);
- nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkoztatástól eltiltás hatálya alatt.

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

Az 5.2.1 fejezetben meghatározott bizalmi munkakör betöltését a legmagasabb szintű biztonsági ellenőrzés (a nemzetbiztonsági szolgálatokról szóló 1885. évi CXXV. törvényben meghatározott nemzetbiztonsági ellenőrzés) előzi meg. A többi, a Szolgáltatások nyújtásával kapcsolatos munkakörben, a munkakör betöltését fokozott szintű, a Szolgáltató által végzett biztonsági ellenőrzés előzi meg. Mind a legmagasabb, mind a fokozott biztonsági ellenőrzés lefolytatásához szükséges az érintett személy hozzájárulása. Nem tölthet be bizalmi munkakört az a személy, akinél a biztonsági ellenőrzés kockázatot tár fel.

A bizalmi munkakörhöz történő hozzárendeléskor az érintett személy:
- pontos és írásos munkakör leírást vesz át a fölérendelt vezetőtől vagy a Szolgáltató humán szervezetétől;
- titoktartási nyilatkozatot kell aláírnia, melyben három év titoktartási kötelezettség szerepel a kilépés időpontjától számítva;
- szükséges mértékű oktatásban részesül, annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és gyakorolni tudja.

Kilépéskor:

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

5.3.3 Képzési követelmények

A bizalmi munkakörökben Szolgáltató olyan személyeket foglalkoztat, akik az adott munkakör vagy szerepkör ellátásához szükséges mértékben elsajátították:
- a PKI elméletet;
- 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 éles informatikai rendszereihez csak a képzést sikeresen záró alkalmazottak kaphatnak hozzáférési jogosultságot.

5.3.4 Továbbképzési gyakoriságok és követelmények

Szolgáltató gondoskodik arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést tart.

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

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

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

Szolgáltató legalább évente egyszer továbbképzést biztosít az újonnan ismertté vált sebezhetőségekről, az IT biztonság aktuális gyakorlatáról, a munkatársak saját szakterületét érintően.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Nincs kikötés.

5.3.6 Felhatalmazás nélküli tevékenységek büntető következményei

Szolgáltató a dolgozóval kötött munkaszerződésben szabályozza a dolgozó felelősségre vonásának lehetőségét a dolgozó által elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

5.3.7 Szerződéses munkavállalókra vonatkozó követelmények

Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztat.

Az egyéb feladatok ellátására, vállalkozási vagy megbízásos szerződés keretében a beszállítóval Szolgáltató írásos megállapodást köt. A szerződő fél titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a szerződés teljesítésében közreműködő személyek a munkavégzés során birtokukba kerülő üzleti titkokat és bizalmas információkat illetéktelen személynek fel nem fedik, más módon sem hasznosítják, és amely tartalmazza a megszegése esetén alkalmazott szankciókat.

5.3.8 A személyzet számára biztosított dokumentációk

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

Minden bizalmi munkakört betöltő munkatárs megkapja írásban:

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

5.4 A biztonsági naplózás folyamatai

5.4.1 Naplózott esemény típusok

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

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

A Szolgáltatások nyújtásával kapcsolatos események különösen az alábbiak:

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

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

5.4.2 Naplóállomány feldolgozásának gyakorisága

Szolgáltató biztosítja a naplóállományok rendszeres ellenőrzését és kiértékelését.

A Szolgáltatások nyújtásával kapcsolatos események naplóállományait naponta feldolgozzák a rendszervizsgálók.
Az informatikai rendszer eseményeinek naplóállományait a rendszervizsgálók rendszeres időközönként, a biztonsági szabályzatban meghatározott sűrűséggel végzik el.

5.4.3 Naplóállomány megőrzési időtartama

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

5.4.4 Naplóállomány védelme

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

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

5.4.5 Naplóállomány mentési folyamatai

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

5.4.6 Naplózás gyűjtési rendszere

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

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

5.4.7 Rendellenes naplóeseményeket kiváltó alanyok értesítése

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

5.4.8 Sebezhetőség értékelések

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

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

A kiértékelést követően Szolgáltató megteszi a megfelelő intézkedéseket annak érdekében, hogy a feltárt sebezhetőség kihasználhatósága ne következzen be.

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

5.5 Adatok archiválása

5.5.1 A tárolt adatok típusai

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

Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:

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

5.5.2 Archívum megőrzési időtartama

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

5.5.3 Archívum védelme

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

5.5.4 Archívum mentési eljárásai

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

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

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

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

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

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

5.5.6 Archívum gyűjtési rendszere

A naplóállományok és az egyéb elektronikusan keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül gyűjti. A védett informatikai rendszerből történő kimozgatás során az adatok minősített időbélyeget tartalmazó elektronikus aláírással vagy bélyegzővel kerülnek hitelesítésre.

A Regisztrációs Irodákban keletkezett papíralapú iratokat kísérőjegyzékkel ellátva a Belföldi Állami Futárszolgálat szállítja a Kártyakibocsátó Szervezet központi telephelyére, ahol azokat Szolgáltató átveszi, majd elhelyezi a saját dokumentumtárában tárolás és megőrzés céljából.

5.5.7 Archívum hozzáférés és ellenőrzés eljárásai

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

Szolgáltató a Regisztrációs Szervezet közreműködésével biztosítja Aláíró számára a róla tárolt személyes adatokra vonatkozó tájékoztatást.

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

5.6 Kulcs átállás

Szolgáltató biztosítja, hogy a hitelesítő központok folyamatosan rendelkezzenek a működésükhöz szükséges érvényes kulccsal és tanúsítvánnyal.

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

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

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

Szolgáltató a tervezett kulcs átállást megelőzően legalább 30 nappal értesíti a felügyeleti szervet és vele egyeztet a szükséges feladatokról.

5.7 Helyreállítás rendkívüli üzemi helyzetek esetén

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

A visszavonási nyilvántartások, a kibocsátott tanúsítványokat tartalmazó nyilvántartás és a visszavonás kezelési szolgáltatás 3 órát meghaladó kiesése esetén Szolgáltató haladéktalanul értesíti a Felügyelet Szervet.

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

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

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

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

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

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

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

Szolgáltató kialakította és fenntartja azt a tartalék CA rendszert, mely a rendkívüli üzemeltetési helyzetben képes a tanúsítványtár és a nyilvános szabályzatok elérhetőségét, a visszavonás kezelési szolgáltatások teljes értékű működését, a CRL-ek közzétételét biztosítani.

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

A rendkívüli üzemeltetési helyzetben Szolgáltató a lehető legrövidebb időn belül tájékoztatást tesz közzé internetes honlapján, valamint, lehetőség szerint, elektronikus levélben értesíti azokat a személyeket, akiket az esemény érint.

A biztonságot érintő vagy a sértetlenség megszűnését eredményező incidens esetén – amennyiben annak hátrányos kihatása van a Szolgáltatást igénybe vevő Előfizetőkre – Szolgáltató indokolatlan késedelem nélkül értesíti az érintett Előfizetőket.

5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

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

5.7.3 Szolgáltató magánkulcsának kompromittálódása esetén követendő eljárás

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

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

5.7.4 Üzletmenet folytonosság helyreállás katasztrófát követően

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

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

5.8 A szolgáltatási tevékenység megszüntetése

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

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

- A tervezett megszűnés előtt kellő időben tárgyalásokat kezdeményez más minősített bizalmi szolgáltatókkal a Szolgáltatásokkal járó kötelezettségek - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig - átadás-átvételéről.
- Szolgáltató gondoskodik a Szolgáltatások megszüntetéséből fakadó, a felhasználói közösséget érintő zavarok minimalizálásáról. Különösképpen gondoskodik a tanúsítvány visszavonási kezelés és közzététel szolgáltatások folyamatos fenntartásáról.
- A megszüntetés előtt legalább 60 nappal korábban:
    - értesíti a Felügyeleti Szervet, és internetes honlapján tájékoztatja az felhasználói közösség tagjait;
    - megszünteti a nevében eljáró Közreműködő Felek felhatalmazásait, felbontja a velük kötött szerződéseket, és jogosultságaikat megvonja (így a regisztráció, a tanúsítvány kérelmek fogadása megszűnik);
    - beszünteti a tanúsítványok előállítását és kibocsátását;
    - egy másik minősített bizalmi szolgáltatóval megállapodást köt a Szolgáltatásokkal járó kötelezettségek átadás-átvételéről, és ennek másolatát megküldi a Bizalmi Felügyeletnek;
- A megszüntetés előtt legalább 20 nappal korábban:
    - visszavonja az összes végfelhasználói tanúsítványt és kibocsájtja a záró CRL-t;
    - leállítja a visszavonás kezelés szolgáltatást;
    - visszavonja az érintett szolgáltató tanúsítványokat és kibocsájtja a záró CRL-t;
    - a szolgáltatói magánkulcsokat és azok mentéseit olyan módon semmisíti meg, hogy azok használata a továbbiakban már nem lehetséges;
    - beszünteti a tanúsítványok és visszavonási állapot információk közzétételét (mind a CRL publikációt, mind az OCSP szolgáltatást) és gondoskodik arról, hogy ezzel egyidejűleg a visszavonási információk az átvevő szolgáltatónál elérhetővé váljanak;
- A megszüntetés napjával:
    - Szolgáltató az informatikai rendszerében foglalt adatokról teljes körű, időbélyegzővel és elektronikus aláírással vagy bélyegzővel ellátott mentést készít. Szolgáltató a mentett adatállományokat védi a jogosulatlan módosítástól, és biztosítja, hogy az adatállomány tartalmához jogosulatlan személy nem férhet hozzá. Szolgáltató a megkötött szerződés révén biztosítja, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek.

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

Szolgáltató a tanúsítványok és visszavonási listák aláírására használt kulcspárokat fizikailag védett környezetben, az erre szolgáló HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, más személy jelenlétének kizárásával generálja. Szolgáltató a tanúsítványok hitelesítésére használt kulcspárok előállítását dokumentált „kulcs-ceremónia” eljárás szerint végzi, melyről a vonatkozó szabványi követelményeinek megfelelő jegyzőkönyv készül. A kriptográfiai modul megfelel a 6.2.1 fejezet szerinti követelményeknek, a magánkulcsok teljes életciklusuk alatt a kriptográfiai modulban maradnak.

Aláíró kulcspárját Szolgáltató megbízásából a Kártyakibocsátó Szervezet fizikailag védett és biztonságos környezetben, magán az eSzemélyi-n, annak QSCD tanúsítással rendelkező tároló elemén generálja.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

Amennyiben a tanúsítvány kiadása az új eSzemélyi okmány igénylésével egyidejűleg történt, a magánkulcs eljuttatása az Aláíróhoz a {J6} SzigR. szerinti eljárásnak megfelelően, a Regisztrációs Szervezetnél, az eSzemélyi Aláírónak való személyes átadásával történik meg vagy Aláíró választása szerint az eSzemélyi-t a Postai Szolgáltató kézbesíti személyesen Aláíró vagy meghatalmazottja részére. A postai úton továbbított, át nem vett eSzemélyi-t Aláíró vagy meghatalmazottja veheti át a kézbesítésre megjelölt cím szerint illetékes járási hivatalban. Ha az eSzemélyi a kiállításától számított hatvan napon belül nem kerül átvételre, a rajta levő tanúsítványt Szolgáltató az erre vonatkozó hatósági adatszolgáltatás alapján visszavonja.

Amennyiben a tanúsítvány kiadása meglévő (nem újként igényelt) eSzemélyi-re történt, a magánkulcs eljuttatása Aláíró számára nem szükséges, mivel a kulcspár előállítása Aláíró jelenlétében a már birtokában levő eSzemélyi tároló elemén, az erre szolgáló biztonsági funkciójának használatával történik, a Kártyakibocsátó Szervezet informatikai rendszere által, a Regisztrációs Szervezet helyszínén.

6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A hitelesítő központ a tanúsítványba foglalandó nyilvános kulcsot a Kártyakibocsátó Szervezettől fogadja el, mely során:

- azonosítja Kártyakibocsátó Szervezetet PKI tanúsítvány-alapú (X.509) azonosítással és a kommunikáció során titkosítási protokollt alkalmaz (SSL/TLS);
- ellenőrzi az elektronikus üzenet hitelességét az elektronikus bélyegző ellenőrzésével, melynek során, ha szükséges, aláírás időpontját hitelesítő időbélyegzőt helyez el;
- ellenőrzi, hogy az elektronikus bélyegző a Kártyakibocsátó Szervezet számára az erre a célra meghatározott tanúsítvánnyal került létrehozásra.

A hitelesítő központ Aláírótól tanúsítványba foglalandó nyilvános kulcsot nem fogad közvetlenül, csak a Kártyakibocsátó Szervezet közreműködésével.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

Szolgáltató a nyilvános kulcsait a szolgáltatói tanúsítványban teszi közzé a 2.2 fejezetben leírtak szerint. A szolgáltatói tanúsítvány elérhetősége minden esetben szerepel a kérdéses tanúsítvány `AuthorityInformationAccess` kiterjesztésében.

Aláírók számára Szolgáltató a nyilvános kulcsait az aláírói tanúsítványhoz kapcsolódó tanúsítványlánc formájában - mely az eSzemélyi-n, mint aláírást létrehozó eszközön tárolásra kerül - teszi közzé.

Érintett Feleknek a szolgáltatói tanúsítványokra az {Sz8} RFC 5280 6. fejezetében leírt tanúsítási útvonal felépítést és érvényesítést javasolt elvégezniük az érintett nyilvános kulcs használata előtt.

6.1.5 Kulcs méretek

Szolgáltató a Szolgáltatások nyújtása során - mind a szolgáltatói, mind a végfelhasználói kulcsok tekintetében - a Felügyeleti Szerv vonatkozó határozatának megfelelő szabványos algoritmusokat, paramétereket és kulcshosszakat használ.

A Szolgáltató biztosítja, hogy a közreműködő felek a jelen szolgáltatási szabályzatban meghatározott, megfelelő, szabványos algoritmusokat, paramétereket és kulcshosszakat használják.

Szolgáltató a Felügyeleti Szerv 2013. novemberi határozatának megfelelően az alábbi algoritmus készleteket és kulcshosszakat használja:

"Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató"	SHA256withRSA	4096 bit
"Minősített Állampolgári Tanúsítványkiadó"	SHA256withRSA	4096 bit
OCSP válaszadó	SHA256withRSA	2048 bit

Az Aláírók kulcspárjainak algoritmusa és mérete: ECC (Elliptic Curve Cryptography) P-256.

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

Amennyiben az Előfizetők vagy a Szolgáltató által használt kulcspárok algoritmusa vagy valamely paramétere nem kellően erős a kapcsolódó tanúsítvány teljes érvényességi időtartamára vonatkozóan, Szolgáltató értesíti Előfizetőket és az érintett feleket, valamint előjegyzi az érintett tanúsítványok visszavonását.

6.1.6 A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

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

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

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

A szolgáltatói magánkulcsok használati célja kizárólag tanúsítványok és visszavonási listák aláírása. Az OCSP válaszadó magánkulcsának használati célja kizárólag OCSP válaszok aláírása.

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

Szolgáltató a tanúsítványokban a `KeyUsage` és `ExtendedKeyUsage` kiterjesztésekben az {Sz11} ITU-T X.509 v3 szabványnak megfelelően jelzi a kulcs használat célját.

	kiterjesztés		**kiterjesztés**	
	kritikus?	**KeyUsage**	**kritikus?**	**ExtendedKeyUsage**
CA tanúsítványa	igen	`KeyCertSign` `CRLSign`	-	-
OCSP válaszadó tanúsítványa	igen	`ContentCommitment`[4]	nem	`OCSPSigning`
Aláíró tanúsítványa	igen	`ContentCommitment`	-	-

6.2 Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1 Kriptográfiai modul szabványok és szabályozások

Szolgáltató a szolgáltatói magánkulcsok előállítására, tárolására és használatára olyan kriptográfiai modult alkalmaz, amely:

- olyan megbízható rendszer, amelynek értékelése az MSZ/ISO/IEC 15408 {Sz13} szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten történt meg; vagy
- megfelel az ISO/IEC 19790 {Sz14} követelményeinek; vagy
- megfelel a FIPS 140-2 {Sz15} 3-as, illetve annál magasabb szintű követelményeknek.

Szolgáltató megbízásából, illetve Aláíró kezdeményezésére a Kártyakibocsátó Szervezet az aláírói magánkulcsokat (kulcspárokat) magán az eSzemélyin állítja elő, amely tároló elemének elektronikus aláírással kapcsolatos funkcióját ellátó része rendelkezik a minősített elektronikus aláírást és minősített elektronikus bélyegzőt létrehozó eszközök megfelelőségét tanúsító szervezetekről és a kijelölésükre vonatkozó szabályokról szóló 41/2016. (X.13.) BM rendelet szerinti - Belügyminisztérium által 2018. augusztus 30-i kijelölési engedélyben megnevezett - tanúsító szervezet (MATRIX Kft.) által kiadott tanúsítvánnyal[5].

A tanúsítvány száma: E-IDS18T_TAN-QSCD, érvényesség kezdete: 2019.04.11, érvényesség vége: 2020.04.26. A QSCD termékmegnevezése: ID&Trust Kft. által fejlesztett IDentity Applet Suite Version 3.2 azonosítójú alkalmazásból és NXP J2E120_M65 / J3E120_M65 / J2E082_M65 / J3E082_M65 v2.4.2 R3 Secure Smart Card Controllerekből álló intelligens kártya.

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

---

[4] X.509 előző verzióiban és RFC 5280-ben: nonRepudation

[5] A tanúsítvány, valamint a kapcsolódó tanúsítási jelentés elérhető a tanúsító szervezet http://matrix-tanusito.hu honlapján

Amennyiben a QSCD tanúsítása megszűnik (lejár), Szolgáltató visszavonja az összes olyan tanúsítványt, 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

Szolgáltató a hitelesítő központokban alkalmazza a több szereplős "n-ből m" ellenőrzést a gyökér hitelesítő központ kulcsgondozási funkcióinak aktivizálásánál.

6.2.3 Magánkulcs letét

Szolgáltató a hitelesítő központok magánkulcsait nem teszi letétbe semmilyen célból.

Szolgáltató nem nyújt az Aláírók számára magánkulcs letét szolgáltatást.

6.2.4 Magánkulcs visszaállítása

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

A Szolgáltató megbízásából eljáró Regisztrációs Szervezet és Kártyakibocsátó Szervezet az Aláíró magánkulcsát semmilyen formában nem menti, nem tárolja.

6.2.5 Magánkulcs mentése

A hitelesítő központok szolgáltatói magánkulcsai biztonsági okokból mentésre kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik, megfelelő biztonsági óvintézkedések és eljárási szabályok betartásával, melyek garantálják a magánkulcs sértetlenségét és bizalmasságát. A mentett példányok titkosított formában, fizikailag biztonságos környezetben kerülnek megőrzésre.

Szolgáltató, a Regisztrációs Szervezet és Kártyakibocsátó Szervezet az Aláíró magánkulcsát semmilyen formában nem menti, nem tárolja.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

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

Aláíró kulcspárja Szolgáltató megbízásából a Kártyakibocsátó Szervezet által, biztonságos módon, magán az eSzemélyi elektronikus tároló elemén kerül előállításra, így annak bejuttatása a kriptográfiai modulba nem szükséges.

6.2.7 Magánkulcs kriptográfiai modulban történő tárolásának módja

A hitelesítő központok magánkulcsai teljes életciklusuk alatt a 6.2.1 fejezetben leírt HSM modulban kerülnek tárolásra. A kulcsok tárolása során Szolgáltató betartja a HSM modul tanúsítási jelentésében foglalt előírásokat.

Az Aláírók magánkulcsai teljes életciklusuk alatt a 6.2.1 fejezetben leírt eSzemélyi tároló elemén kerülnek tárolásra.

6.2.8 Magánkulcs aktiválásának módja

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

Aláíró a magánkulcs aktiválását a számára átadott, PUK és PIN kódokat tartalmazó borítékban levő tájékoztatóban előírtaknak megfelelően kell végezze.

6.2.9 Magánkulcs aktív állapotának megszüntetési módja

Szolgáltató biztosítja, hogy az aktivált HSM modul jogosulatlan hozzáférés ellen védett legyen. A HSM modul működése során csak az azonosított és feljogosított Kártyakibocsátó Szervezettől érkezett hiteles tanúsítványkérelmekre kiadott tanúsítványok, visszavonási listák és opcionálisan OCSP válaszok aláírására használható. A magánkulcs eltávolításra kerül a HSM modulból, amikor a hitelesítő központ működése megszűnik.

6.2.10 Magánkulcs megsemmisítésének módja

Szolgáltató a hitelesítő központok magánkulcsát visszaállíthatatlan módon megsemmisíti, amikor használatuk már nem szükséges vagy a kapcsolódó tanúsítvány lejárt vagy visszavonásra került. A magánkulcs és az aktiválásához szükséges minden adat megsemmisítését olyan módon végzi, hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkezhető vagy levezethető.

Új tanúsítvány igénylése esetén Aláíró magánkulcsa az eSzemélyi tároló elemén törlésre, illetve felülírásra kerül.

6.2.11 Kriptográfiai modul értékelése

Lásd a 6.2.1 fejezetben.

6.3 Kulcspár gondozás egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

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

6.3.2 Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

A kulcspár felhasználás időtartama azonos a nyilvános kulcs hitelességét igazoló tanúsítvány érvényességi idejével.

"Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató"	20 év
"Minősített Állampolgári Tanúsítványkiadó"	legfeljebb15 év
OCSP válaszadó	legfeljebb 30 nap
Aláírói tanúsítvány	legfeljebb 2 év *

*: Az Aláíró tanúsítványának érvényességi ideje két év, ha a kibocsátás időpontjában az eSzemélyi érvényességéből több mint két év van hátra; ellenkező esetben a tanúsítvány érvényességének vége megegyezik az eSzemélyi lejárati dátumával. Kivételt képeznek a 2019. évben kiadott tanúsítványok, melyek érvényessége 1 év.

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

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

Az eSzemélyi tároló eleméhez rendelt PUK kódot és Aláíró elektronikus aláírás létrehozásához használt adatának (magánkulcsának) használatát engedélyező PIN kódot Szolgáltató nevében és megbízásából a Kártyakibocsátó Szervezet védett környezetben és biztonságos módon állítja elő.

6.4.2 Aktivizáló adatok védelme

Az eSzemélyi tároló eleméhez rendelt PUK és PIN kódot tartalmazó borítékokat a Kártyakibocsátó Szervezet fizikailag védett környezetben, az eSzemélyi-től elkülönítve tárolja. Kártyakibocsátó Szervezet a kódokat csak abból a célból rögzíti, hogy azok a Regisztrációs Szervezet által az Aláíró számára átadásra kerüljenek.

A kódokat tartalmazó borítékokat a Regisztrációs Szervezet Aláírónak az eSzemélyi igénylésekor, illetve a Szolgáltatási Szerződés megkötésekor személyesen adja át.

Az átvételt követően Aláírónak saját felelősségi körében kell biztosítania a kódok kizárólagos birtoklását és védelmét.

6.4.3 Aktivizáló adatok egyéb szempontjai

Az Aláíró által személyesen átvett PUK és PIN kódokat tartalmazó borítékban levő PIN kód úgynevezett "aktiváló" PIN kód, ami azt jelenti, hogy az elektronikus aláírás létrehozásához használt adat (magánkulcs) első használata előtt, az aktiváló PIN kód megadása után kell létrehoznia az aláírói hozzáférés jogosultságot biztosító PIN kódot, amellyel a továbbiakban használhatja a magánkulcsot (az eSzemélyi-t) elektronikus aláírás létrehozására.

A PIN kód sikertelen megadása esetén a PUK kódot kell megadnia a PIN kód cseréjéhez.

A PUK kód hiányában vagy sikertelen megadása esetén a PIN kód cseréjét Aláíró a Regisztrációs Szervezetnél, személyazonosságának igazolásával, személyesen kérheti.

6.5 *Informatikai biztonsági óvintézkedések*

6.5.1 Informatikai biztonsági műszaki követelmények meghatározása

Az informatikai biztonság műszaki követelményeit Szolgáltató az {Sz1} EN 319 401, {Sz2} EN 319 411-1 és {Sz3} EN 319 411-2 szabványoknak a minősített szolgáltatások nyújtására vonatkozó, informatikai biztonsági műszaki követelményeiben határozza meg, melyek különösen az alábbiak:

#	hivatkozás	leírás
1.	EN 319 401 REQ-7.4-01 REQ-7.4-02 REQ-7.4-03	A Szolgáltató rendszerei csak feljogosított személyek számára férhetők hozzá. A szolgáltató belső hálózatát tűzfalakkal kell megvédeni a jogosulatlan hozzáférés ellen, beleértve az előfizetők és harmadik felek hozzáférését is. A tűzfalakon le kell tiltani minden protokollt és hozzáférést, amely nem szükséges a működtetéséhez.
2.	EN 319 401 REQ-7.4-10	Az érzékeny adatokat meg kell védeni az ellen, hogy újrafelhasznált tároló objektumokon (pl. törölt fájlok) át jogosulatlan személyek számára hozzáférhető váljanak.
3.	EN 319 411-1 GEN-6.5.5-02 GEN-6.5.5-03	Tanúsítvány előállítása során a lokális hálózati komponenseket (pl. router) fizikailag és logikailag biztonságos környezetben kell fenntartani, és ezek konfigurációját a követelményeknek való megfelelés vonatkozásában rendszeres időközönként ellenőrizni kell.
4.	EN 319 411-1 GEN-6.5.5-04	Multi-faktoros azonosítást kell alkalmazni minden olyan személy és folyamat azonosítására, mely tanúsítvány előállítását közvetlenül kiválthatja.
5.	EN 319 411-1 GEN-6.5.5-05	A tanúsítványtárakat kezelő alkalmazásoknak hozzáférés ellenőrzést kell végrehajtaniuk minden esetben, amely tanúsítvány hozzáadását, törlését vagy a kapcsolódó információk megváltoztatását eredményezheti.
6.	EN 319 411-1 GEN-6.5.5-06	A visszavonási státuszt kezelő alkalmazásnak hozzáférés ellenőrzést kell végrehajtaniuk minden esetben, amely a visszavonási státusz információ megváltozását eredményezheti.
7.	EN 319 411-1 GEN-6.5.5-07	A Szolgáltató erőforrásainak folyamatos monitorozását és riasztást kell megvalósítani arra, hogy Szolgáltató képes legyen észlelni a jogosulatlan és/vagy a normálistól eltérő hozzáférési kísérleteket és az ellenintézkedéseket kellő időn belül megtegye.

6.5.2 Informatikai biztonsági értékelés

Szolgáltató az informatikai rendszerek biztonsági értékelését az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezései szerint végzi.

6.6 *Életciklusra vonatkozó műszaki óvintézkedések*

6.6.1 Rendszerfejlesztési óvintézkedések

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

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató belső információbiztonsági szabályzata tartalmazza, amely pontosan meghatározza a tervezés és előkészítés, a projekt és kivitelezés, a működtetés és a menedzselés, valamint a visszacsatolás, illetve visszavonás/rekonstrukció ciklus időszakok feladatait és az alkalmazott módszertanokat. A belső információbiztonsági szabályzat figyelembe veszi az {Sz3} EN 319 411-2 szabvány 6.5.6 fejezetében előírt követelményeket.

6.6.2 Biztonságkezelési óvintézkedések

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

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

6.6.3 Életciklus biztonsági óvintézkedések

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

biztonsági ellenőrzés típusa		végzi	rendszeresség
operatív	IT infrastruktúra	rendszerüzemeltető operátorok	naponta
	szolgáltatás nyújtásához használt alkalmazások és naplóik	rendszervizsgálók	naponta
belső ellenőrzés	IT infrastruktúra	biztonsági tisztviselő	évente egyszer
	szolgáltatás nyújtásához használt alkalmazások és naplóik	biztonsági tisztviselő	évente egyszer
külső ellenőrzés	IT infrastruktúra	külső auditor	évente egyszer
	szolgáltatás nyújtásához használt alkalmazások	külső auditor	évente egyszer

6.7 Hálózatbiztonsági óvintézkedések

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

6.8 Időforrások

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

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

7 TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

7.1 *Tanúsítvány profil*

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

7.1.1 Verziószám

A tanúsítványok verziószáma: V3.

7.1.2 Tanúsítvány kiterjesztések

A tanúsítványokban alkalmazott kiterjesztések mindenben követik az {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.

7.1.3 Algoritmus azonosítók

A tanúsítványok aláírásához alkalmazott algoritmus azonosítók az alábbiak:
`SHA256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}`

7.1.4 Név formák

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

7.1.5 Név megszorítások

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

7.1.6 Hitelesítési rend objektumazonosító

Szolgáltató a tanúsítványokban feltünteti a hitelesítési rend objektumazonosítóját.

7.1.7 Szabályzati megszorítások kiterjesztés használata

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

7.1.8 Szabályzat minősítők szintaktikája és szemantikája

A tanúsítványban feltüntetett szabályzat minősítők (`PolicyQualifiers`) és megfelelő szöveg (`UserNotice`) jelzi a tanúsítvány alkalmazhatóságát.

7.1.9 A kritikus hitelesítési rendek (Certificate Policies) kiterjesztés feldolgozása

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

7.2 *CRL profil*

Szolgáltató által kiadott visszavonási listák megfelelnek az {Sz8} RFC 5280 műszaki szabványnak.

7.2.1 Verziószám

A visszavonási listák verziószáma: V2.

7.2.2 CRL és CRL bejegyzés kiterjesztések

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

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

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

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

7.3 *OCSP profil*

Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz12} RFC 6960 műszaki szabványnak.

7.3.1 Verziószám

Az OCSP válaszok verziószáma: V1.

7.3.2 OCSP kiterjesztések

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

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

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

8 MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

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

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

8.1 Vizsgálatok gyakorisága és körülményei

Szolgáltató a vonatkozó jogszabályok alapján bejelentette az elektronikus aláírással kapcsolatos szolgáltatások nyújtására vonatkozó szándékát a Nemzeti Média- és Hírközlési Hatóság (NMHH) számára és kérte a nyilvántartásba vételét a minősített hitelesítés-szolgáltatók nyilvántartásába 2013. szeptember 2-án. Szolgáltató nyilvántartásba vételére az NMHH erről szóló, 2013. november 4-i keltezésű határozata szerint, a jogerőre emelkedés napjával, 2013. november 23-án került sor.

A 2016. június 30. napjáig terjedő időszakban Szolgáltató elvégeztetett egy külső elektronikus aláírási szakértői vizsgálatot, az ezen időszakban hatályos jogszabályok ({J4} Eat., valamint a {J9} 3/2005 IHM rendelet) előírásai szerint.

2016. július 1. napjával kezdődően, Szolgáltató legalább 24 havonta egyszer megfelelőségértékelést és 12 havonta egyszer felülvizsgálatot végeztet a {J1} eIDAS szerint, a 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott megfelelőségértékelő szervezettel a {J1} eIDAS, illetve a {J3} E-ügyintézési tv. követelményeinek való megfelelés tárgykörben, mely szervezetet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére. Az elkészült megfelelőség értékelési jelentést annak kézhezvételétől számított három munkanapon belül benyújtja a Felügyeleti Szervnek.

Az e pont szerint készített első megfelelőségértékelési jelentést Szolgáltató legkésőbb 2017. július 1. napjáig benyújtja a Felügyeleti Szervnek.

Szolgáltató belső és külső vizsgálatokat végez, illetve végeztet annak érdekében, hogy a Szolgáltatásokkal kapcsolatos folyamatai, eszközei, személyzete megfeleljenek a hatályos jogszabályi, szabványi és szakmai követelményeknek.

Szabályzatainak megfelelőségét Szolgáltató saját szervezete részéről a Hitelesítési Rend és Szabályozási Csoport vizsgálja meg. A Szolgáltatások megfelelőségének vizsgálatára Szolgáltató saját belső ellenőrzéséket hajt végre.

A Szolgáltató nyilvános szabályzatait a Felügyeleti Szerv is megvizsgálja a Szolgáltató nyilvántartásba vételi eljárása során, valamint a szabályzatok módosításakor, és megfelelőség esetén közzé teszi a kötelezően benyújtandó szabályzatokat. A Felügyeleti Szerv rendszeres időközönként átfogó helyszíni ellenőrzés keretében ellenőrzi Szolgáltató tevékenységét.

Szolgáltató rendelkezik minőségbiztosítási rendszerrel és információbiztonsági irányítási rendszerrel, melyek megfelelő működését független rendszervizsgáló ellenőrzési tevékenysége biztosítja.

Szolgáltató a külső, illetve a saját ellenőrző szervezet által végzett belső vizsgálatokat a {D6} PKI szolgáltatások biztonsági szabályzatában megjelölt rendszerességgel - évente legalább egyszer biztosítja.

8.2 Auditor azonosítása és képesítése

A megfelelőségértékelés előkészítésére, illetve az információbiztonsági rendszer ellenőrzésére Szolgáltató külső rendszervizsgálót alkalmaz.

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

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

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

8.3 Auditor függetlensége

A megfelelőségértékelő szervezet, annak munkatársai, valamint a külső rendszervizsgáló teljes mértékben függetlenek Szolgáltatótól.

8.4 Audit során vizsgált területek

Az audit 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.

Az audit során megvizsgálásra kerül, hogy Szolgáltató és az általa nyújtott Szolgáltatások megfelelnek-e:

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

8.5 Hiányosságok esetén végrehajtandó tevékenységek

Az üzemszerű ellenőrzések, belső és külső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére Szolgáltató intézkedési tervet készít. A hiányosságokat késlekedés nélkül orvosolja, az intézkedéseket dokumentálja és ellenőrzi.

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

8.6 Eredmény kommunikációja

A belső és külső auditot, szakértői elemzést végző személyek csak a megbízójuknak adhatnak információt a Szolgáltató tevékenységével kapcsolatban. 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. Szolgáltató nem köteles a konkrét hiányosságot nyilvánosságra hozni.

9 EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1 Díjak

9.1.1 Tanúsítvány kibocsátás díja

Szolgáltató a tanúsítvány kibocsátásáért díjat nem számít fel.

Az 1990. évi XCIII. törvényben meghatározott esetekben az állampolgárt (Aláíró) terheli a személyazonosító igazolvány kiadására irányuló eljárás illetéke.

9.1.2 Tanúsítványhozzáférés díja

Szolgáltató a közzétett tanúsítványok elérésért nem számít fel díjat.

9.1.3 Visszavonási és állapot információ hozzáférés díja

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

9.1.4 Egyéb szolgáltatások díja

Nincs kikötés.

9.1.5 Visszatérítési szabályzat

Visszatérítéssel kapcsolatos rendelkezéseket Szolgáltató nem állapít meg.

9.2 Anyagi felelősség

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

9.2.1 Biztosítási fedezet

A Szolgáltató rendelkezik olyan felelősségbiztosítással, mely egyaránt kiterjed az elektronikus aláírással, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, és amely fedezetet biztosít az összes károsultnak okozott kárra, a tanúsítványban jelzett tranzakciós limit értékének legalább ötszöröséig. A tranzakciós limit összegét a Szolgáltatási Szerződés rögzíti, valamint a tanúsítvány minősített tanúsítvány nyilatkozatok (`QCStatements`) kiterjesztése tartalmazza (a `QcLimitValue` mezőben). A biztosítási szerződésben szereplő felelősségvállalási érték 3.000.000 Ft, vagy ennél esetenként magasabb összeg.

A felelősségbiztosítás a fentieken túl kiterjed az alábbiakra is:

- a {J3} E-ügyintézési tv. 88. §-ban foglalt kötelezettsége nem teljesítése miatt a Bizalmi Felügyeletnél felmerült, az E-ügyintézési tv. 89. §-a szerinti költségekre;

- a {J1} eIDAS 17. cikk (4) bekezdés e) pontja alapján a Bizalmi Felügyelet által felkért megfelelőségértékelő szervezet eljárásainak költségeire, ha ezt a Bizalmi Felügyelet eljárási költségként érvényesíti.

9.2.2 További követelmények

Szolgáltató rendelkezik a {J12} 24/2016 rendelet 20. §-a szerinti, huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával.

9.2.3 Felelősségbiztosítás vagy garancia végfelhasználók számára

Nincs kikötés.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

Szolgáltató minden olyan adatot és információt bizalmasnak tekint, melyek nem kerültek tételes felsorolásra a 9.3.2 fejezetben.

9.3.2 Bizalmasnak nem tekintett információk köre

Nem bizalmasnak tekintetett információk az alábbiak:

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

9.3.3 Bizalmas információk védelmének felelőssége

Szolgáltató a bizalmas információkhoz való hozzáférést csak az arra feljogosított személyek és szervezetek számára teszi lehetővé. A bizalmas információk védelmét a személyzet megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel juttatja érvényre.

9.4 Személyes adatok védelme

9.4.1 Adatvédelmi terv

Szolgáltató rendelkezik mind társasági szintű adatvédelmi tervvel ({D4}), mind pedig a Szolgáltatásokra vonatkozó adatvédelmi tájékoztatóval, melyek nyilvános dokumentumok, és elérhetők Szolgáltató internetes honlapján. Ezen dokumentumok összhangban vannak a nemzetközi és hazai vonatkozó jogszabályokkal.

9.4.2 Bizalmasként kezelendő személyes adatok

Szolgáltató csak Aláírótól közvetlenül, annak kifejezett hozzájárulásával gyűjt személyes adatot és csak olyan mértékben, ami a tanúsítvány kiállításához, valamint Aláíró tájékoztatásához, személyazonosságának megállapításához szükséges.

Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

- Aláíró minden adatát, ha Aláíró nem járult hozzá tanúsítványának közzétételéhez;
- Aláírónak azon adatait, melyek a tanúsítványba nem kerülnek befoglalásra, ha Aláíró írásban hozzájárult tanúsítványának közzétételéhez.

9.4.3 Bizalmasként nem kezelendő személyes adatok

Szolgáltató nem bizalmasként kezelendő személyes adatnak tekinti Aláírónak a tanúsítványba foglalt adatai, amennyiben Aláíró tanúsítványa közzétételéhez írásban hozzájárult.

Továbbá, nem bizalmas adat a tanúsítványhoz kapcsolódó státusz információ, minden tanúsítvány vonatkozásában. A státusz információba beleértendő a tanúsítvány - esetleges - visszavonásának oka és időpontja.

9.4.4 Személyes adatok védelmének felelőssége

Szolgáltató gondoskodik a személyes adatok védelméről, működése és szabályzatai megfelelnek a {J13} GDPR rendelkezéseinek.

9.4.5 Hozzájárulás a személyes adatok felhasználásához

Aláírónak a Szolgáltatási Szerződés aláírásával hozzá kell járulnia a tanúsítvány kiállításához és a szerződés megkötéséhez szükséges adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához.

Aláíró választása szerint hozzájárulhat vagy megtilthatja tanúsítványának nyilvános közzétételét.

9.4.6 Felfedés hatósági vagy polgári peres eljárás keretében

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

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

9.4.7 Egyéb, felfedést eredményező körülmények

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

9.5 Szellemi tulajdonjogok

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

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

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

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 Szolgáltató felelőssége és helytállása

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

Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a {J11} Polgári Törvénykönyv 6:519. §-a szerint, a vele szerződéses jogviszonyban álló Aláíróval szemben a szerződésszegésért való felelősség ({J11} Polgári Törvénykönyv 6:142. §) szabályai szerint felelős az elektronikus aláírással hitelesített elektronikus dokumentummal okozott kárért, ha megszegte a bizalmi szolgáltatási rendben és a jelen szolgáltatási szabályzatban, valamint az Aláíróval megkötött Szolgáltatási Szerződésben előírtakat, vagy az esemény időpontjában hatályos jogszabály - {J4} Eat. vagy {J1} eIDAS - szerinti, rá vonatkozó kötelezettségeket. E kötelezettségek megtartását kétség esetén Szolgáltatónak kell bizonyítania. Szolgáltató sajátjaként felel a Közreműködő Felek vagy egyéb alvállalkozók által a Szolgáltatások nyújtása során okozott kárért.

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

Szolgáltató nem felel:

- Aláírónak a magánkulccsal, illetve az eSzemélyi tároló elemén levő aláírást létrehozó eszközzel kapcsolatos tevékenységért;
- az Érintett Felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért;
- az Érintett Felek vagy mások által kibocsátott szabályzatokért.

Szolgáltató kötelezettsége

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

9.6.2 A regisztrációs szervezet felelőssége

9.6.2.1 Regisztrációs Szervezet felelőssége

Szolgáltató a Regisztrációs Szervezettel megkötött együttműködési megállapodásban megköveteli a bizalmi szolgáltatási rend és a vonatkozó szolgáltatás szabályzat előírásainak maradéktalan betartását.

Regisztrációs Szervezet felelőssége a tanúsítvány kiadásával kapcsolatban:

- A tanúsítvány kibocsátását kérő személy teljes körű és közérthető tájékoztatása a 4.1.2 fejezetben meghatározottakról;
- az igénylő azonosítása a 3.2 fejezetben leírt eljárással;
- az igénylő aláírói tanúsítványra jogosultságának elbírálása;
- a tanúsítványba foglalandó adatok egyeztetése és ellenőrzése közhiteles nyilvántartások alapján;
- a regisztrációhoz és a Szolgáltatási Szerződés megkötéséhez szükséges, egyeztetett és ellenőrzött adatok rögzítése az erre szolgáló informatikai rendszerben;
- közreműködés a Szolgáltatási Szerződés megkötésében;
- PUK és PIN kódokat, továbbá a visszavonási jelszót tartalmazó borítékok átadása személyesen Aláírónak, arról az átvételi elismervény felvétele;
- kezdeményezni azt, hogy a Kártyakibocsátó Szervezet az eSzemélyi tároló elemét Aláíró részére megszemélyesítse;
- közreműködni abban, hogy Szolgáltató által Aláíró számára kibocsátott tanúsítvány az eSzemélyi-re felírásra kerüljön;
- annak biztosítása, hogy az eSzemélyi Aláíró számára személyes átadásra vagy kézbesítésre kerüljön, valamint hogy Aláíró a megfelelő eSzemélyi-t (a sajátját) kapja kézhez.

Regisztrációs Szervezet felelőssége a tanúsítványok visszavonásával kapcsolatban:

- intézkedni arról, hogy Aláíró kérésére a visszavonási igény rögzítésre kerüljön és a visszavonást kezdeményezze a Szolgáltató felé;
- intézkedni arról, hogy a bármilyen okból (eltulajdonítás, megsemmisülés, elvesztés, adatváltozás, elhalálozás miatt) érvénytelenített eSzemélyi-hez tartozó tanúsítvány visszavonását kezdeményezze a Szolgáltató felé.

9.6.2.2 Kártyakibocsátó Szervezet felelőssége

Szolgáltató a Kártyakibocsátó Szervezettel megkötött együttműködési megállapodásban megköveteli a bizalmi szolgáltatási rend és a vonatkozó szolgáltatás szabályzat előírásainak maradéktalan betartását.

Kártyakibocsátó Szervezet felelőssége:

- az eSzemélyi tároló elemén, mint elektronikus aláírást létrehozó eszközön a Felügyeleti Szerv vonatkozó határozatának megfelelő algoritmusú és paraméterű kulcspárok generálása szigorúan védett és biztonságos környezetben és módon, a QSCD tanúsítási jelentésében meghatározott előírások betartásával;
- aktivizáló adatok és visszavonási jelszavak előállítása és tárolása biztonságos módon, a kártyáktól elkülönítve;
- az eSzemélyi-nek, mint elektronikus aláírást létrehozó eszköznek a megszemélyesítése, úgy, hogy az Aláíró adataival megfelelően kitöltött és Aláíró eSzemélyi-jének tároló elemén előállított magánkulcshoz tartozó nyilvános kulcsot tartalmazó tanúsítványkérelem kerüljön összeállításra;
- a tanúsítványkérelmek hitelesítése elektronikus bélyegzővel és a kérelmek eljuttatása Szolgáltató részére;

- Szolgáltató által kibocsátott tanúsítvány felírása az eSzemélyi tároló elemére;
- az eSzemélyi biztonságos tárolása annak kézbesítéséig;
- annak biztosítása, hogy az eSzemélyi - a Regisztrációs Szervezet, illetve a Postai Szolgáltató által – Aláíró számára átadásra kerüljön és Aláíró a megfelelő eSzemélyi-t kapja kézhez;
- annak biztosítása - a Regisztrációs Szervezettel együttműködve -, hogy az eSzemélyi aktiválását csak Aláíró legyen képes elvégezni;
- a tanúsítvány visszavonási kérelmek hitelesítése elektronikus bélyegzővel és a kérelmek eljuttatása Szolgáltató részére.

9.6.3 Aláíró felelőssége és helytállása

Aláíró jogai

- Aláíró jogosult a Szolgáltatások igénybe vételére jelen szolgáltatási szabályzatban, a Szolgáltatási Szerződésben és az Általános Szerződési Feltételekben leírtak szerint.
- Aláíró akkor jogosult tanúsítvány igényelni, ha a {J5} Nytv. és {J6} SzigR.-ben a tároló elemmel ellátott, állandó személyazonosító igazolvány igénylésére meghatározott feltételek fennállnak.
- Aláíró jogosult meghatározni, hogy a számára kiadott tanúsítvány a Szolgáltató internetes honlapján közzétett nyilvános tanúsítványtárban megjelenjen-e.
- Aláíró jogosult meghatározni a szolgáltatási szerződés megkötésekor, hogy az általa ekkor megadott email cím a tanúsítványba befoglalásra kerüljön-e.
- Aláíró jogosult meghatározni az eSzemélyi tároló elemén levő aláírás létrehozó eszköz átvételének módját.
- Aláíró jogosult a számára kiadott tanúsítvány visszavonását kérni.
- Aláíró jogosult az értesítési email címének változása esetén annak bejelentésére, az erre a célra rendszeresített - a Szolgáltató honlapjáról letölthető – űrlap kitöltésével, elektronikus aláírásával és az ekozig@1818.hu címre történő beküldésével, mely esetben a változást Szolgáltató átvezeti a saját nyilvántartásában. Szolgáltató ilyen esetben nem vonja vissza Aláíró jelenlegi tanúsítványát és nem ad ki új tanúsítványt, tekintettel Aláírónak az értesítési email címváltozás bejelentő lapon tett nyilatkozatára, miszerint a tanúsítványba foglalt email címe változatlanul létezik és azt használja.

Aláíró felelőssége

- Aláíró felelős a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért.
- Aláíró felelős a tanúsítványban szereplő adatok ellenőrzéséért.
- Aláíró felelős azért, hogy a tanúsítványt érintő összes adatának megváltozását haladéktalanul bejelentse, beleértve mindazon adataiban bekövetkezett változásokat is, melyeket a regisztrációs eljárás és a Szolgáltatási Szerződés megkötése során megadott.
- Aláíró felelős az eSzemélyi-nek mint minősített elektronikus aláírást létrehozó eszköznek, valamint a kapcsolódó magánkulcsnak a rendeltetésszerű felhasználásáért, a szabályzatoknak és a QSCD tanúsítási jelentésében előírtaknak megfelelően.
- Aláíró felelős a magánkulcsnak, az aktivizáló kódjainak és a visszavonási jelszónak a biztonságos kezeléséért.
- Aláíró felelős azért, hogy a magánkulcsot és a kapcsolódó tanúsítványt csak a tanúsítvány érvényességi időtartamán belül használja, a tanúsítvány visszavonása esetén azok használatát haladéktalanul és végérvényesen beszüntesse.
- Aláíró felelős azért, hogy a magánkulcs és a kapcsolódó tanúsítvány használatát haladéktalanul és végérvényesen beszüntesse, amennyiben tudomására jut, hogy a Szolgáltató valamely, a tanúsítvány kibocsátásában érintett hitelesítő központja

kompromittálódott.

- Aláíró felelős Szolgáltatót haladéktalanul értesíteni és teljes körűen tájékoztatni vitás ügyekben.
- Aláíró felelős a Szolgáltatási Szerződésben és a {D1} Általános Szerződési Feltételekben meghatározott kötelezettségei betartásáért.

Aláíró kötelezettsége

- Aláíró köteles a Szolgáltatások igénybe vétele előtt jelen szolgáltatási szabályzatot megismerni.
- Aláíró köteles tudomásul venni, hogy Szolgáltató a tanúsítványt a jelen szabályzatban leírt módon és eljárásokkal bocsátja ki.
- Aláíró köteles a Szolgáltatások igénybe vételéhez szükséges adatokat hiánytalanul és a valóságnak megfelelően szolgáltatni.
- Aláíró köteles tudomásul venni, hogy a számára kibocsátott tanúsítványban a jogszabályokban előírt adatok – valamint, rendelkezésétől függően az email címe - befoglalásra kerülnek.
- Aláíró köteles a tanúsítványba foglalt bármely adata (beleértve a tanúsítványba foglalt email címet is) megváltozása esetén haladéktalanul kérni a tanúsítvány visszavonását.
- Aláíró köteles az értesítési email címének változását 8 napon belül bejelenteni.
- Aláíró kötelezettsége, hogy a tanúsítványt és a kapcsolódó magánkulcsot, csak jogszabályokban megengedett és nem tiltott célra, valamint a szabályzatokban és hivatkozott dokumentumokban foglaltaknak megfelelően használja.
- Aláíró köteles az eSzemélyi-t, mint elektronikus aláírást létrehozó eszközt megbízható informatikai környezetben és alkalmazásokkal használni.
- Aláíró köteles biztosítani, hogy a Szolgáltatások igénybe vételéhez szükséges - saját hatáskörébe tartozó - adatokhoz és eszközökhöz illetéktelen személyek ne férhessenek hozzá.
- Aláíró köteles Szolgáltatót haladéktalanul írásban értesíteni, amennyiben valamely a Szolgáltatásokban kiadott tanúsítvánnyal vagy azon alapuló elektronikus aláírással kapcsolatban jogvita indul.
- Aláíró köteles az eSzemélyi eltulajdonítását, megsemmisülését, megrongálódását vagy elvesztését a Regisztrációs Szervezetnél haladéktalanul bejelenteni.
- Aláíró haladéktalanul köteles a magánkulcs nem jogszerű használatának vagy kompromittálódásának gyanúja esetén a tanúsítvány visszavonását kérni.
- Aláíró köteles tudomásul venni, hogy Szolgáltató a tanúsítványt a Regisztrációs Szervezet értesítése alapján haladéktalanul visszavonja, amennyiben az eSzemélyi bármilyen okból kifolyólag letiltásra vagy érvénytelenítésre került.
- Aláíró köteles tudomásul venni, hogy Szolgáltató jogosult a tanúsítványt visszavonni, amennyiben Aláíró a Szolgáltatási Szerződést megszegi vagy Szolgáltató tudomására jut, hogy a tanúsítványt illegális tevékenységhez használták.
- Aláíró köteles tudomásul venni, hogy Szolgáltató a tanúsítványt a Felügyeleti Szerv erre vonatkozó határozata esetén visszavonja.

9.6.4 Érintett Felek felelőssége és helytállása

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

- a szolgáltatási szabályzatban foglalt követelmények és előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;

- a tanúsítvány felhasználására vonatkozó valamennyi korlátozás figyelembe vétele, amely a tanúsítványban vagy a szolgáltatási szabályzatban szerepel
- a tőle elvárható magatartás tanúsítása a tanúsítvány ellenőrzésekor.

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

9.6.5 Egyéb felek felelőssége és helytállása

Nincs kikötés.

9.7 Helytállás érvénytelenségi köre

Szolgáltató kizárja felelősségét, amennyiben:

- az Érintett Fél nem körültekintően jár el a tanúsítványok ellenőrzése és felhasználásra során, azaz nem jelen szolgáltatási szabályzatnak vagy a hatályos jogszabályoknak megfelelően jár el;
- Aláíró nem tartja be az eSzemélyi, továbbá annak tároló elemén levő aláírást létrehozó eszköz, illetve a magánkulcs kezelésével kapcsolatos előírásokat;
- az Érintett Felek vagy mások által kibocsátott szabályzatok nem felelnek meg jelen bizalmi szolgáltatási rendnek;
- az Internet, vagy annak egy részének működőséi hibájából fakadóan tájékoztatási vagy egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- Aláíró által megadott értesítési email cím - melynek valódiságáról Aláíró írásban nyilatkozott - időközben megváltozott vagy megszűnt és ebből fakadóan Szolgáltató Aláírót nem tudja értesíteni;
- a károkozás a Felügyeleti Szerv Szolgáltatónak kiadott, hatályos határozatában közölt kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8 Felelősség korlátozása

Szolgáltató korlátozza a kártérítési felelősségét:

- a tanúsítvánnyal egy alkalommal vállalható kötelezettség mértékében (tranzakciós limit), mely a Szolgáltatási Szerződésben és a tanúsítványban feltüntetésre kerül;
- összességében az összes tanúsítvánnyal és káreseménnyel kapcsolatban fizetendő kártérítési összeg tekintetében.

Szolgáltató nem felelős az olyan károkért, melyek a tanúsítványban feltüntetett, egy alkalommal vállalható kötelezettségvállalás összeghatárát (tranzakciós limit) meghaladó ügyletekben aláírt elektronikus dokumentumokból származnak.

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

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

9.9 Kártérítések

A kártérítésekről a jelen szabályzat 9.8 fejezetében leírtakon túl a {D2} Szolgáltatási Szerződés és a {D1} Általános Szerződési Feltételek rendelkeznek.

9.10 Hatályosság és megszűnés

9.10.1 Hatályosság

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

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

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

9.10.2 Megszűnés

A szolgáltatási szabályzat a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

9.10.3 Megszűnés után is hatályban maradó rendelkezések

A megszűnés után is hatályban maradó rendelkezéseket – amennyiben ilyenek vannak - a {D1} Általános Szerződési Feltételek és a {D2} Szolgáltatási Szerződés tartalmazza.

9.11 Egyéni hirdetmények és kommunikáció a részvevőkkel

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

9.12 Módosítások

9.12.1 Módosítás eljárása

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

9.12.2 Értesítés módszere és időtartama

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

9.12.3 OID megváltozását előidéző körülmények

A szolgáltatási szabályzat új verziójával az OID verziószámot jelentő része megfelelően változik.

9.13 Vitás kérdések rendezése

Bármely vitás kérdés felmerülése esetén Aláírónak kötelessége a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása a kérdés minden vonatkozását illetően, a vita jogi útra terelése előtt.

Panaszt a Telefonos Ügyfélszolgálat postacímére (NISZ Zrt. Kormányzati Ügyfélvonal, 1389 Budapest, Pf. 133) írásban, a 1818 hívószámán telefonon, vagy e-mailben az ekozig@1818.hu címre küldve lehet előterjeszteni Szolgáltató részére. Szolgáltató visszaigazolást küld a panasz kézhezvételéről. A panaszt a Szolgáltató az előterjesztéstől számított 30 napon belül kivizsgálja és ennek eredményéről a panaszost elektronikus aláírással ellátott válasz üzenetben tájékoztatja.

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

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

9.14 Irányadó jog

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

9.15 Hatályos jognak megfelelés

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

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Nincs kikötés.

9.16.2 Átruházás

A Szolgáltatások nyújtásában érintett Közreműködő Felek vagy alvállalkozók csak a Szolgáltató előzetes írásbeli felhatalmazásával vagy jogszabályi felhatalmazás alapján adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3 Részleges érvénytelenség

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

9.16.4 Igényérvényesítés

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

9.16.5 Force Majeure (Vis maior)

Vis maior: Az olyan – a Szolgáltató és a Közreműködő Felek akaratától, cselekedeteitől és személyétől függetlenül bekövetkező és érdekkörén kívül eső elháríthatatlan – esemény (pl. sztrájk, háború, polgári felkelés, természeti katasztrófa, a Felek bármelyikének partnerénél felmerülő elháríthatatlan fizikai vagy jogi akadály vagy más elháríthatatlan szükséghelyzet) minősül vis maiornak, amely megakadályozza vagy lehetetlenné teszi a jelen szolgáltatási szabályzatban foglalt követelmény teljesítését, feltéve, hogy ezen körülmények a jelen szolgáltatási szabályzat hatálybalépését követően keletkeznek, illetőleg azt megelőzően következtek be, ám a jelen szolgáltatási szabályzat teljesítésére kiható következményeik az említett időpontban még nem voltak előre láthatóak.

Szolgáltató nem felelős a vis maior esetekből fakadó károkért.

9.17 Egyéb rendelkezések

9.17.1 Hozzáférhetőség a fogyatékossággal élő személyek számára

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