MICROSEC

e-Szignó Hitelesítés Szolgáltató

eIDAS Rendelet szerinti minősített weboldal-hitelesítő tanúsítvány szolgáltatási kivonat

ver. 2.11

Hatálybalépés: 2019-09-25

Azonosító	1.3.6.1.4.1.21528.2.1.1.200.2.11
Verzió	2.11
Első verzió hatálybalépése	2018-09-15
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2019-09-23
Hatálybalépés dátuma	2019-09-25

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság

1033 Budapest, Ángel Sanz Briz út 13. C. épület

Verzió	A változás leírása	Hatálybalépés	Készítette
2.7	Új szabályzat az eIDAS követelmények szerint.	2018-09-15	Szabóné Endrődi Csilla, Dr. Szőke Sándor,
2.8	Változások az auditor javaslatai alapján.	2018-12-14	Dr. Szőke Sándor
2.9	Domén validálási követelmények változása. Government Entity típusú ügyfelek bevezetése. Kisebb módosítások. Változások a CABF BR követelményekben.	2019-04-24	Dr. Szőke Sándor
2.10	Kisebb módosítások. Változások a CABF EVG követelményekben.	2019-06-25	Dr. Szőke Sándor
2.11	Éves felülvizsgálat.	2019-09-25	Dr. Szőke Sándor

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság (továbbiakban: Microsec vagy *Hitelesítés-szolgáltató*) által üzemeltetett e-Szignó Hitelesítés Szolgáltató által meghatározott minősített weboldal-hitelesítő tanúsítvány kibocsátása szolgáltatásra vonatkozó *Szolgáltatási kivonat*ot tartalmazza.

A *Szolgáltatási kivonat* a fogyasztók számára összefoglaló tájékoztatást tartalmaz a szolgáltatás igénybevételének feltételeiről a *Szolgáltatási szabályzat* rendelkezéseivel összhangban, a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI. 30.) BM rendelet rendelkezései szerint.

A *Szolgáltatási kivonat* megfelel az eIDAS Rendelet [1] által támasztott követelményeknek, az ezen szabályoknak megfelelően nyújtott szolgáltatás a rendelet szerinti bizalmi szolgáltatás.

1.1. Dokumentum neve és azonosítója

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	eIDAS Rendelet szerinti minősített weboldal-hitelesítő tanúsítvány szolgáltatási kivonat
Dokumentum verziószáma	2.11
Hatálybalépés ideje	2019-09-25

A jelen *Szolgáltatási kivonat* szerint használható *Hitelesítési rend*ek felsorolását és azonosító adatait az 1.1.1 fejezet tartalmazza.

1.1.1. Hitelesítési rendek

A *Hitelesítés-szolgáltató* által kibocsátott valamennyi *Tanúsítvány* hivatkozik arra a *Hitelesítési rend*re, amely alapján a kibocsátás történt.

A jelen *Szolgáltatási kivonat* szerint a *Hitelesítés-szolgáltató* a következő *Hitelesítési rend*ek alapján bocsát ki *Tanúsítvány*okat:

OID	MEGNEVEZÉS	RÖVID NÉV
1.3.6.1.4.1.21528.2.1.1.170.2.11	Minősített, weboldal-hitelesítő tanúsítványokhoz használt, álnevet kizáró hitelesítési rend.	MWJSN

A *Hitelesítési rend*ek rövid nevének képzésének illetve értelmezésének szabályai a függelékben találhatóak.

A felsorolt *Hitelesítési rend*(ek) részletes követelményeit az " e-Szignó Hitelesítés Szolgáltató – eIDAS Rendelet szerinti minősített weboldal-hitelesítő tanúsítvány hitelesítési rend ver.2.11." [15] dokumentum tartalmazza.

Jelen *Hitelesítési rend*ek közül:

- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-2 [9] szabványban definiált [QCP-w] *Hitelesítési rend*nek;
- a PSD2 célra kibocsátott *Tanúsítvány*ok mindegyike megfelel az ETSI TS 119 495 [10] műszaki specifikációban definiált [QCP-w-psd2] *Hitelesítési rend*nek;

Megfelelés az ETSI hitelesítési rendeknek

Amennyiben egy ETSI Hitelesítési Rend egy másik ETSI Hitelesítési Rendre épül, vagyis automatikusan tartalmazza annak valamennyi követelményét, a kibocsátott *Tanúsítvány*okban csak a magasabb szintű Hitelesítési Rend azonosítója kerül feltüntetésre.

	[NCP]	[OVCP]	[EVCP]	[QCP-w]	[QCP-w-psd2]
MWJSN (nem PSD2)	(x)	(x)	(x)	X	
MWJSN (PSD2)	(x)	(x)	(x)	(x)	X

1.2. Területi hatály

A jelen *Szolgáltatási kivonat* a magyar jog alapján Magyarországon, elsősorban magyar *Ügyfel*ek részére, magyar nyelven nyújtott szolgáltatásokra vonatkozó konkrét követelményeket tartalmaz. A *Hitelesítés-szolgáltató* kiterjesztheti a szolgáltatás területi hatályát, ez esetben a magyar viszonyokra alkalmazható előírásoknak megfelelő, azoknál nem enyhébb követelményeket alkalmaz.

1.3. A bizalmi szolgáltató

1.3.1. A Szolgáltató adatai

Név: Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság
Cégjegyzékszám: 01-10-047218 Fővárosi Törvényszék Cégbírósága
Székhely: 1033 Budapest, Ángel Sanz Briz út 13. C épület
Telefonszám: (+36-1) 505-4444
Telefax szám: (+36-1) 505-4445
Internet cím: `https://www.microsec.hu`, `https://www.e-szigno.hu`

A *Hitelesítési rend*, a *Szolgáltatási szabályzat* és az Adatvédelmi szabályzat elérhetősége:

- `https://e-szigno.hu/letoltesek/dokumentumok-es-szabalyzatok/`

Az árlista elérhetősége:

- `https://e-szigno.hu/hitelesites-szolgaltatas/arlista/`

Díjvisszatérítés:
A Szolgáltatási szerződés megszűnése alapesetben az *Előfizető* által megfizetett díjakat nem érinti.

A már kifizetett díjakból a *Hitelesítés-szolgáltató* nem nyújt visszatérítést, kivéve, ha a Szolgáltatási szerződés a *Hitelesítés-szolgáltató* hibájából szűnik meg, vagy ha a *Hitelesítés-szolgáltató* ezt – például egyes csomagok esetében – kifejezetten lehetővé teszi.

A megfelelőségértékelési vizsgálatok tanúsítványai megtekinthetők a TÜViT publikus weboldalán az alábbi linken:

`https://www.tuvit.de/en/services/certification/eidas-conformity-assessment-for-trust-service-provider/`

illetve a *Hitelesítés-szolgáltató* saját weboldalán az alábbi linken:

`https://e-szigno.hu/eidas/eidas.html`

A tanúsítvány azonosítója:

A magyar nemzeti bizalmi lista elérhetősége:

- humán olvasható PDF formátumban: `http://www.nmhh.hu/tl/pub/HU_TL.pdf`
- géppel feldolgozható XML formátumban: `http://www.nmhh.hu/tl/pub/HU_TL.xml`

A Nemzeti Média- és Hírközlési Hatóság bizalmi szolgáltatásokkal kapcsolatos nyilvántartása az alábbi elérhetőségen található:

http://webpub-ext.nmhh.hu/esign2016/

Szolgáltatási szerződés elérhetősége:

A *Hitelesítés-szolgáltató* az *Ügyfel*ekkel kötendő Szolgáltatási szerződést az *Igénylő* kezdeti regisztráció alkalmával megadott értesítési e-mail címére továbbítja.

1.3.2. Az ügyfélszolgálati iroda elérhetősége

A szolgáltató egység neve:	e-Szignó Hitelesítés Szolgáltató
Ügyfélszolgálati iroda:	1033 Budapest, Ángel Sanz Briz út 13., Graphisoft Park South Area, C épület
Ügyfélszolgálati iroda nyitvatartási ideje:	munkanapokon 8:30-16:30 között előzetes időpont egyeztetés alapján
Ügyfélszolgálati iroda telefonszáma:	(+36-1) 505-4444
Ügyfélszolgálati iroda email címe:	`info@e-szigno.hu`
Visszavonási kérelmek fogadása:	`visszavonas@e-szigno.hu`
A szolgáltatással kapcsolatos információk elérése:	`https://www.e-szigno.hu`
Panaszok bejelentésének helye:	Microsec zrt. 1033 Budapest, Ángel Sanz Briz út 13., Graphisoft Park South Area, C épület

Illetékes fogyasztóvédelmi felügyelőség:	Budapest Főváros Kormányhivatal Fogyasztóvédelmi Felügyelőség 1052 Budapest, Városház u. 7. 1364 Budapest, Pf. 144.
Illetékes békéltető testület elérhetősége:	Budapesti Békéltető Testület 1016 Budapest, Krisztina krt. 99. III. em. 310. Levelezési cím: 1253 Budapest, Pf.: 10.

1.4. Tanúsítványfajták

A minősített weboldal-hitelesítő tanúsítvány kibocsátása szolgálatáshoz tartozó *Szolgáltatási szabályzat* által támogatott *Hitelesítési rend*eket a *Szolgáltatási szabályzat* 1.2.1 fejezete mutatja be. Az alkalmazott *Hitelesítési rend* azonosítója minden esetben feltüntetésre kerül a *Tanúsítvány* "Certificate Policies" mezejében.

Az e-Szignó Hitelesítés Szolgáltató több különböző tanúsítványfajtát kínál *Ügyfel*ei részére, amelyek főképp az általuk hitelesen az *Alany*hoz kötött adatok és tulajdonságok körében térnek el:

- *Szervezeti tanúsítvány*ról beszélünk, ha a *Tanúsítvány* alanya *Szervezet*, a *Szervezet* irányítása alatt álló eszköz, vagy ha a *Tanúsítvány* egy természetes személy *Alany* valamely *Szervezet*hez való tartozását mutatja. Ilyen esetben a *Tanúsítvány* "O" mezejében a *Szervezet* neve feltüntetésre kerül. Az ilyen *Tanúsítvány* kizárólag az adott *Szervezet* által meghatározott módon használható.

- *Automata tanúsítvány*ról beszélünk, ha a *Tanúsítvány*ban az *Alany* adatai között feltüntetésre kerül az informatikai eszköz (alkalmazás, rendszer) elnevezése is, amely segítségével az *Alany* a *Tanúsítvány*t használja. *Weboldal-hitelesítő tanúsítvány* esetében az *Alany* nevénél mindig a webszerver domain neve vagy IP címe szerepel, tehát minden *Weboldal-hitelesítő tanúsítvány Automata tanúsítvány*.

- Álneves *Tanúsítvány*ról beszélünk, ha a *Tanúsítvány*ban nem az *Alany* közhiteles nyilvántartásban szereplő hivatalos elnevezése szerepel. Az álneves *Tanúsítvány*okban a kért elnevezés a "Pseudonym" mezőben kerül feltüntetésre, és a "CN" mezőben feltüntetésre kerül, hogy a *Tanúsítvány* álnevet tartalmaz. *Weboldal-hitelesítő tanúsítvány* soha nem lehet álneves.

- Személyes *Tanúsítvány*ról akkor beszélhetünk, ha a *Tanúsítvány* sem "O", sem "Title" mezőt nem tartalmaz. Ilyen csak természetes személyek számára kerül kibocsátásra.

Az e-Szignó Hitelesítés Szolgáltató mind természetes személyek, mind jogi személyek számára bocsát ki *Tanúsítvány*okat. Jogi személyek számára igényelt *Tanúsítvány*ok esetében a képviseletre jogosult természetes személynek vagy az általa meghatalmazott személynek kell eljárnia a *Tanúsítvány* ügyében.

1.5. A tanúsítvány felhasználhatósága

1.5.1. Megfelelő tanúsítvány használat

A *Hitelesítés-szolgáltató* által jelen szolgáltatás keretében kibocsátott végfelhasználói *Tanúsítvány*okhoz tartozó magánkulcsok kizárólag webszerverek azonosítására használhatók fel.

1.5.2. Tiltott tanúsítvány használat

A jelen *Szolgáltatási kivonat* alapján kibocsátott *Tanúsítvány*okat, illetve a hozzájuk tartozó magánkulcsokat weboldalak azonosításától eltérő célra felhasználni tilos.

1.6. Felügyeleti szerv

A *Szolgáltatási szabályzat*ok és a szolgáltatások nyújtása feletti felügyeletet a Nemzeti Média- és Hírközlési Hatóság látja el. A Nemzeti Média- és Hírközlési Hatóság nyilvántartást vezet a követelményeknek megfelelő *Hitelesítési rend*ekről valamint az ezeket alkalmazó *Hitelesítés-szolgáltató*król.

A Nemzeti Média- és Hírközlési Hatóság bizalmi szolgáltatásokkal kapcsolatos nyilvántartása az alábbi elérhetőségen található:

`http://webpub-ext.nmhh.hu/esign2016/`

2. Azonosítás és hitelesítés

2.1. Kezdeti regisztráció, azonosság hitelesítése

A *Hitelesítés-szolgáltató* a törvény által biztosított keretek között tetszőleges kommunikációs csatornát felhasználhat a *Tanúsítvány*t kérelmező személy vagy szervezet azonosságának igazolására, a megadott adatok valódiságának ellenőrzésére.

A *Hitelesítés-szolgáltató* saját hatáskörében, külön indoklás nélkül dönt az igényelt *Tanúsítvány* kiadásának megtagadásáról.

2.1.1. A magánkulcs birtoklásának igazolása

A *Tanúsítvány* kiállítása előtt a *Hitelesítés-szolgáltató* biztosítja illetve meggyőződik arról, hogy a *Tanúsítvány*t kérelmező valóban birtokolja illetve ellenőrzése alatt tartja a *Tanúsítvány*ba kerülő nyilvános kulcshoz tartozó magánkulcsot.

Amennyiben az *Alany* általa biztosított kulcshoz kéri a *Tanúsítvány* kibocsátását – jellemzően szoftveres tanúsítványok esetében –, akkor a *Hitelesítés-szolgáltató* PKCS#10 formátumban fogadja a *Tanúsítványkérelmet*, amely egyúttal igazolja, hogy valóban a magánkulcs birtokosa kért *Tanúsítvány*t az adott megnevezéshez.

2.1.2. Szervezet és domén azonosságának hitelesítése

3.2.2.1 Szervezet azonosságának hitelesítése

A *Szervezet* azonossága ellenőrzésre kerül a következő esetekben:

- amennyiben a kibocsátandó *Tanúsítvány* alanya a *Szervezet*;
- amennyiben a kibocsátandó *Tanúsítvány* alanya a *Szervezet* által üzemeltetett eszköz vagy rendszer (ide értve a *Szervezet* által igényelt *Weboldal-hitelesítő tanúsítvány*okat);

*Szervezeti tanúsítvány*ok kibocsátása előtt a *Hitelesítés-szolgáltató* egy közhiteles nyilvántartás (QGIS) alapján meggyőződik a *Tanúsítvány*ba kerülő szervezeti adatok valódiságáról.

Magán szervezetek ellenőrzése során a *Hitelesítés-szolgáltató* megbizonyosodik róla, hogy a *Szervezet*

- jogilag létezik, hivatalos cégnyilvántartásban szerepel és aktív állapottal rendelkezik,
- fizikailag létezik, a nyilvántartott üzleti címe egy valós cím,
- aktív cég, tényleges üzleti tevékenységet folytat.

Közszféra és szervezetei ellenőrzése során a *Hitelesítés-szolgáltató* megbizonyosodik róla, hogy a *Szervezet*

- a megfelelő kormányzati struktúrában szabályosan bejegyzett kormányzati egység,
- aktív állapottal rendelkezik,
- a *Tanúsítványkérelem*ben megadott név pontosan egyezik a *Szervezet* hivatalosan bejegyzett nevével,
- amennyiben létezik ilyen meghatározza a *Szervezet* alapításának pontos dátumát vagy a létrehozó jogi aktus azonosítóját.

Közszféra és szervezetei ellenőrzése során a *Hitelesítés-szolgáltató* az információt az alábbi forrásokból szerzi be közvetlenül:

- megbízható kormányzati információ forrás az *Igénylő* kormányzati egységével azonos szervezetből
- megbízható kormányzati információ forrás az *Igénylő* felettes kormányzati szervétől
- egy olyan bírótól, amely az állami igazságszolgáltatás aktív tagja az említett politikai alkörzetben

Ezekben az esetekben ellenőrzésre kerül továbbá, hogy:

- a *Szervezet* nevében eljáró természetes személy jogosult-e a *Szervezet* nevében eljárni;
- a *Szervezet* hozzájárult-e a *Tanúsítvány* kibocsátásához.

Az ellenőrzés elvégzéséhez az *Ügyfél*nek a következő adatokat kell megadnia:

- a *Szervezet* hivatalos elnevezése, székhelye és jogállása;
- a *Szervezet* hivatalos nyilvántartási száma (pl. cégjegyzékszám, adószám), ha van ilyen;

- a *Szervezet*en belüli szervezeti egység neve, ha kérik ennek feltüntetését a *Tanúsítvány*ban;

- Amennyiben az *Ügyfél* kéri az *Alany* módosított pénzforgalmi irányelv (PSD2) [2] szerinti adatainak feltüntetését a *Tanúsítvány*ban, akkor az *Ügyfél*nek meg kell adnia az *Alany* pénzforgalmi szolgáltatásait felügyelő hatóság által kiosztott engedélyszámát vagy annak hiányában a hatóság által elismert egyéb azonosítóját, a pénzforgalmi szolgáltatásainak típusát, valamint az említett hatóság nevét.

A *Tanúsítványkérelem*hez csatolni kell a következő igazolásokat illetve bizonyítékokat:

- a kérelem benyújtója által aláírt nyilatkozatot arról, hogy a *Szervezet* azonosítására megadott adatok helyesek és megfelelnek a valóságnak;

- a kérelem benyújtója által aláírt nyilatkozatot arról, hogy a *Szervezet Tanúsítvány*ban feltüntetendő adatai között nem szerepel védjegy, vagy amennyiben szerepel, igazolást arról, hogy a védjegy használatára a *Szervezet* jogosult;

- igazolást arra vonatkozóan, hogy a *Szervezet* nevében *Tanúsítványkérelmet* benyújtó természetes személy jogosult a kérelmet benyújtani [1];

- a *Szervezet* képviseletére jogosult személy aláírási címpéldányát vagy más, az aláírási címpéldánnyal egyenértékű hivatalos dokumentumot, mely a *Szervezet* képviseletére jogosult személyek nevét és aláírását tartalmazza [2];

- a *Szervezet* létezését, elnevezését és jogállását hitelesítő dokumentumot [3].

A *Hitelesítés-szolgáltató* a bemutatott iratok és okmányok érvényességét és hitelességét ellenőrzi.

Külföldön bejegyzett Szervezetek azonosságának ellenőrzése

A *Hitelesítés-szolgáltató* külföldön bejegyzett *Szervezet*ek azonosítását sem zárja ki, amennyiben megvalósítható az adott ország megfelelő nyilvántartásaival való adategyeztetés vagy megbízható harmadik fél által kiadott igazolás beszerzése.

Az adategyeztetés tekintetében a *Hitelesítés-szolgáltató* elfogadja:

- a külföldi ország magyarországi nagykövetsége vagy konzulátusa által kibocsátott igazolást, miszerint az adott szervezet létezik és a megadott adatai helyesek;

- a külföldi országban lévő magyar nagykövetség vagy konzulátus által kibocsátott igazolást, miszerint az adott szervezet létezik és a megadott adatai helyesek.

A *Hitelesítés-szolgáltató* egyéb okmányokat és bizonyítékokat is elfogadhat, amennyiben meggyőződik róla, hogy az a fentiekkel megegyező szintű biztonságot jelentenek. Ezen bizonyítékok beszerzése és a *Hitelesítés-szolgáltató*hoz történő eljuttatása az *Ügyfél* feladata.

A *Hitelesítés-szolgáltató* kizárólag érvényes okmányokat, illetve 3 hónapnál nem régebbi bizonyítékokat fogad el.

[1] A felhatalmazások, jogosultságok ellenőrzésével kapcsolatos részleteket a 2.1.5. fejezet tartalmazza.
[2] Cégbíróságon bejegyzett cégek esetében a fenti iratokat a *Hitelesítés-szolgáltató* is beszerezheti.
[3] Cégbíróságon bejegyzett cégek esetében a fenti iratokat a *Hitelesítés-szolgáltató* is beszerezheti.

A *Hitelesítés-szolgáltató* nem állítja ki a *Tanúsítvány*t, amennyiben belső szabályzatai alapján úgy ítéli meg, hogy nem képes a külföldön kiállított igazolást, okmányt vagy a külföldi szervezet adatait megfelelő biztonsággal ellenőrizni.

A *Hitelesítés-szolgáltató* a bizalmi szerepkörök megfelelő elosztásával és belső adminisztratív folyamatainak segítségével biztosítja, hogy a szervezeti adatok rögzítése és az adatok hitelességének ellenőrzése során legalább két - bizalmi szerepkört ellátó - alkalmazott részvételére van szükség.

3.2.2.2 Domén birtoklásának és kontrolljának hitelesítése

A *Weboldal-hitelesítő tanúsítvány*okban szerepelnie kell legalább egy doménnévnek.

*Weboldal-hitelesítő tanúsítvány*ok kibocsátása előtt a *Hitelesítés-szolgáltató* meggyőződik a *Tanúsítvány*ba kerülő doménnév valódiságáról, valamint az *Igénylő*nek a gyakorlatban bizonyítania kell, hogy rendelkezik az adott doménnév feletti irányítással.

Amennyiben a *Tanúsítvány*ban egynél több doménnév kerül feltüntetésre, a fenti ellenőrzéseket mindegyik esetében el kell végezni.

A *Hitelesítés-szolgáltató* kizárólag az interneten használható nyilvános doménnevekre bocsát ki *Tanúsítvány*t, belső használatú nevekre nem.

A *Hitelesítés-szolgáltató* kizárólag azokra a felső szintű doménekre (TLD) bocsát ki *Tanúsítvány*t, amelyek megtalálhatók az IANA aktuális TLD nyilvántartásában.

A *Hitelesítés-szolgáltató* támogatja a Nemzetközi tartománynevek használatát az IDNA2003 [11] követelményeknek megfelelően.

A *Hitelesítés-szolgáltató*nak a *Tanúsítvány* kibocsátása előtt meg kell győződnie arról, hogy a *Tanúsítvány*ban felsorolt összes teljes doménnév megerősítésre került az alábbi azonosítási eljárások közül legalább egy eljárás felhasználásával a CA/Browser Forum Baseline Requirements aktuális verziójában foglaltak szerint.

3.2.2.2.1 Az Igénylő azonosítása a domén kapcsolattartójaként (BR 3.2.2.4.1)

Ez a validálási módszer nem használatos.

3.2.2.2.2 Email küldése a domén kapcsolattartónak (BR 3.2.2.4.2)

Az *Igénylő* domén feletti kontrolljának ellenőrzése véletlenszám küldéssel email útján és a küldött véletlenszámot tartalmazó megerősítő válasz fogadása által.

A *Hitelesítés-szolgáltató* a véletlenszámot a domén kapcsolattartó regisztrált email címére küldi.

Minden email felhasználható több doménnév azonosítására is.

A *Hitelesítés-szolgáltató* az e fejezetben meghatározott email üzenetet több címzettnek is elküldheti, amennyiben valamennyi címzett a domén nyilvántartás szerinti kapcsolattartó az üzenetben foglalt valamennyi doménnév vonatkozásában.

Minden email egyedi véletlenszámot tartalmaz.

A *Hitelesítés-szolgáltató* változatlan formában és teljes terjedelmében újraküldheti az email üzenetet a véletlenszámmal együtt, amennyiben az üzenet tartalma és a címzettek köre változatlan marad.

A véletlenszám a létrehozásától számított 30 napig érvényes.

3.2.2.2.3 A domén kapcsolattartó felhívása telefonon (BR 3.2.2.4.3)

Ez a validálási módszer nem használatos.

3.2.2.2.4 A domén kapcsolattartónak küldött szerkesztett email (BR 3.2.2.4.4)

Az *Igénylő* domén feletti kontrolljának ellenőrzése egy szerkesztett email címre küldött üzenettel

- email küldése az alábbiak szerint létrehozott legalább egy email címre:
  - "admin",
  - "administrator",
  - "webmaster",
  - "hostmaster" vagy
  - "postmaster"

  helyi cím, amit a kukac ("@") karakter után egy ellenőrzendő doménnév követ,
- amely email tartalmaz egy egyedi véletlenszámot, és
- a küldött véletlenszámot tartalmazó megerősítő válasz fogadása.

Minden email felhasználható több doménnév ellenőrzésére is, amennyiben az emailben használt azonosító doménnév érvényes az emailben megerősítendő valamennyi doménnévre.

A véletlenszám minden emailben egyedi.

Az email teljes egészében újraküldhető beleértve a véletlenszám ismételt használatát, amennyiben az email teljes tartalma és a címzettek köre változatlan marad.

A véletlenszám a létrehozásától számított 30 napig érvényes.

3.2.2.2.5 Domén felhatalmazó dokumentum (BR 3.2.2.4.5)

Ez a validálási módszer nem használatos.

3.2.2.2.6 A weboldal egyeztetett megváltoztatása (BR 3.2.2.4.6)

Az *Igénylő* domén feletti kontrolljának ellenőrzése egy véletlenszámot is tartalmazó egyedi ellenőrző adat *Igénylő* általi elhelyezésével az azonosítandó doménnév alatti

"/.well-known/pki-validation"

speciális könyvtárban lévő fájlban, amely HTTP/HTTPS protokoll felhasználásával egy engedélyezett porton keresztül elérhető:

- a *Hitelesítés-szolgáltató* ellenőrzi a megkívánt weboldal tartalom meglétét az adott fájlban. Az elvárt tartalom nem jelenik meg az információ elérésére használt kérésben.

A *Hitelesítés-szolgáltató* minden *Tanúsítványkérelem* esetében egyedi ellenőrző adatot használ ami 30 napig érvényes.

3.2.2.2.7 DNS megváltoztatása (BR 3.2.2.4.7)

Az *Igénylő* domén feletti kontrolljának ellenőrzése egy ellenőrző adat (véletlenszámot is tartalmazó token) meglétének ellenőrzésével a DNS TXT rekordon az azonosítandó doménnéven.

A *Hitelesítés-szolgáltató* minden *Tanúsítványkérelem* esetében egyedi azonosító adatot használ.

Az azonosító adat 30 napig érvényes.

Az FQDN sikeres validálása után a *Hitelesítés-szolgáltató* kibocsáthat további *Tanúsítvány*okat olyan FQDN-ek számára, amelyek a validált teljes FQDN -re végződnek.

3.2.2.2.8 IP cím (BR 3.2.2.4.8)

Ez a validálási módszer nem használatos.

3.2.2.2.9 Teszt tanúsítvány (BR 3.2.2.4.9)

Ez a validálási módszer nem használatos.

3.2.2.2.10 TLS véletlenszán felhasználásával (BR 3.2.2.4.10)

Ez a validálási módszer nem használatos.

3.2.2.2.11 Egyéb módszerek (BR 3.2.2.4.11)

Ez a validálási módszer nem használatos.

3.2.2.2.12 Az igénylő azonosítása domén kapcsolattartóként (BR 3.2.2.4.12)

Ez a validálási módszer nem használatos.

3.2.2.2.13 Szerkesztett email küldése a DNS CAA kapcsolattartónak (BR 3.2.2.4.13)

Az *Igénylő* domén feletti kontrolljának ellenőrzése egy véletlenszámot tartalmazó email elküldésével majd a véletlenszámot tartalmazó megerősítő email fogadásával.

A *Hitelesítés-szolgáltató* a véletlenszámot a DNS CAA rekord email kontakt címére küldi. A megfelelő CAA forrás adatot az IETF RFC 6844 [14] szabvány Errata 5065 (Appendix A) által módosított 4 fejezete által meghatározott kereső algoritmus szerint találja meg.

A CAA Email kontakt címet a CAA contactemail tulajdonság kell tartalmazza paraméterként. Az email címet az RFC 6532 [13] 3.2 fejezete szerint kell megadni további kiegészítés vagy formázás nélkül.

Példa:

$ORIGIN example.com

CAA 0 contactemail "domainowner@example.com"

Minden email felhasználható több doménnév ellenőrzésére is, amennyiben valamennyi email cím az összes validálandó doménnévhez tartozó DNS CAA email kapcsolati cím. Ugyanaz az email

elküldhető több címzettnek is, amennyiben valamennyi címzett összes validálandó doménnévhez tartozó DNS CAA kapcsolattartó. Az email teljes egészében újraküldhető beleértve a véletlenszám ismételt használatát, amennyiben az email teljes tartalma és a címzettek köre változatlan marad.

A véletlenszám minden emailben egyedi. A véletlenszám a létrehozásától számított 30 napig érvényes.

Az FQDN sikeres validálása után a *Hitelesítés-szolgáltató* kibocsáthat további *Tanúsítvány*okat olyan FQDN-ek számára, amelyek a validált teljes FQDN -re végződnek.

3.2.2.2.14 Szerkesztett email küldése a DNS TXT kapcsolattartónak (BR 3.2.2.4.14)

Az *Igénylő* domén feletti kontrolljának ellenőrzése egy véletlenszámot tartalmazó email elküldésével majd a véletlenszámot tartalmazó megerősítő email fogadásával.

A *Hitelesítés-szolgáltató* a véletlenszámot a validálandó doménnévhez tartozó DNS TXT rekord kapcsolattartói email címére küldi.

A DNS TXT rekordnak a validálandó domén "_validation-contactemail" aldoménjében kell lennie. Ezen TXT rekord teljes RDATA értékének az érvényes email címet kell tartalmaznia az RFC 6532 [13] 3.2 fejezete szerinti formátumban további kiegészítés vagy formázás nélkül, ellenkező esetben az email cím nem használható.

Minden email felhasználható több doménnév ellenőrzésére is, amennyiben valamennyi email cím az összes validálandó doménnévhez tartozó DNS TXT rekord kapcsolattartói email cím. Ugyanaz az email elküldhető több címzettnek is, amennyiben valamennyi címzett az összes validálandó doménnévhez tartozó DNS TXT rekord kapcsolattartó. Az email teljes egészében újraküldhető beleértve a véletlenszám ismételt használatát, amennyiben az email teljes tartalma és a címzettek köre változatlan marad.

A véletlenszám minden emailben egyedi. A véletlenszám a létrehozásától számított 30 napig érvényes.

Az FQDN sikeres validálása után a *Hitelesítés-szolgáltató* kibocsáthat további *Tanúsítvány*okat olyan FQDN-ek számára, amelyek a validált teljes FQDN -re végződnek.

3.2.2.2.15 A domén kapcsolattartó felhívása telefonon (BR 3.2.2.4.15)

Az *Igénylő* domén feletti kontrolljának ellenőrzése a domén kapcsolattartói telefonszám felhívásával és egy megerősítő válasz kapásával.

Minden telefonhívás felhasználható több doménnév ellenőrzésére is, amennyiben a domén kapcsolattartói telefonszám meg van adva az összes validálandó doménhez és a kapcsolattartó megerősíti az összes doménre vonatkozó igénylést. Amennyiben a hívást nem a domén kapcsolattartó veszi fel, a *Hitelesítés-szolgáltató* kérheti a hívás továbbkapcsolását a domén kapcsolattartónak.

Amennyiben a hívást hangposta fogadja, a *Hitelesítés-szolgáltató* meghagyhatja a validálandó domén neveket és egy véletlenszámot. A véletlenszámot a domének validálása céljából vissza kell küldeni a *Hitelesítés-szolgáltató* részére. A véletlenszám a létrehozásától számított 30 napig érvényes.

Az FQDN sikeres validálása után a *Hitelesítés-szolgáltató* kibocsáthat további *Tanúsítvány*okat olyan FQDN-ek számára, amelyek a validált teljes FQDN -re végződnek.

3.2.2.2.16 A DNS TXT Record kapcsolattartó felhívása telefonon (BR 3.2.2.4.16)

Az *Igénylő* domén feletti kontrolljának ellenőrzése a DNS TXT rekord kapcsolattartói telefonszám felhívásával és egy megerősítő válasz kapásával. A DNS TXT rekordnak a validálandó domén "_validation-contactphone" aldoménjében kell lennie. Ezen TXT rekord teljes RDATA értékének az érvényes globális telefonszámot tartalmaznia az RFC 3966 [12] 5.1.4 fejezete szerinti formátumban, ellenkező esetben a telefonszám nem használható.

Minden telefonhívás felhasználható több doménnév ellenőrzésére is, amennyiben a DNS TXT rekord kapcsolattartói telefonszám meg van adva az összes validálandó domén DNS TXT rekordjában és a kapcsolattartó megerősíti az összes doménre vonatkozó igénylést. A hívás nem irányítható át és a *Hitelesítés-szolgáltató* sem kérheti az átirányítását mivel ezt a telefonszámot kifejezetten a domén validálás céljából adták meg.

Amennyiben a hívást hangposta fogadja, a *Hitelesítés-szolgáltató* meghagyhatja a validálandó domén neveket és egy véletlenszámot. A véletlenszámot a domének validálása céljából vissza kell küldeni a *Hitelesítés-szolgáltató* részére. A véletlenszám a létrehozásától számított 30 napig érvényes.

Az FQDN sikeres validálása után a *Hitelesítés-szolgáltató* kibocsáthat további *Tanúsítvány*okat olyan FQDN-ek számára, amelyek a validált teljes FQDN -re végződnek.

3.2.2.2.17 A DNS CAA kapcsolattartó felhívása telefonon (BR 3.2.2.4.17)

Az *Igénylő* domén feletti kontrolljának ellenőrzése a DNS CAA kapcsolattartói telefonszám felhívásával és egy megerősítő válasz kapásával.

Minden telefonhívás felhasználható több doménnév ellenőrzésére is, amennyiben a DNS CAA kapcsolattartói telefonszám meg van adva az összes validálandó domén DNS CAA rekordjában és a kapcsolattartó megerősíti az összes doménre vonatkozó igénylést.

A megfelelő CAA forrás adatot az IETF RFC 6844 [14] szabvány Errata 5065 (Appendix A) által módosított 4. fejezete által meghatározott kereső algoritmus szerint kell megtalálni.

A CAA kapcsolattartói telefonszámot a CAA contactphone tulajdonság kell tartalmazza paraméterként. A teljes paraméter értéknek az érvényes globális telefonszámot kell tartalmaznia az RFC 3966 [12] 5.1.4 fejezete szerinti formátumban, egyéb esetben nem használható. A Globális telefonszám "+" karakterrel és az országkóddal kezdődik és tartalmazhat vizuális tagoló karaktereket.

Példa:

$ORIGIN example.com

CAA 0 contactphone "+36 (1) 123-4567"

A hívás nem irányítható át és a *Hitelesítés-szolgáltató* sem kérheti az átirányítását mivel ezt a telefonszámot kifejezetten a domén validálás céljából adták meg.

Amennyiben a hívást hangposta fogadja, a *Hitelesítés-szolgáltató* meghagyhatja a validálandó domén neveket és egy véletlenszámot. A véletlenszámot a domének validálása céljából vissza kell küldeni a *Hitelesítés-szolgáltató* részére. A véletlenszám a létrehozásától számított 30 napig érvényes.

Az FQDN sikeres validálása után a *Hitelesítés-szolgáltató* kibocsáthat további *Tanúsítvány*okat olyan FQDN-ek számára, amelyek a validált teljes FQDN -re végződnek.

2.1.3. Természetes személy azonosságának hitelesítése

A *Weboldal-hitelesítő tanúsítvány*t igénylő természetes személy azonosságát igazolni kell.

Minősített *Tanúsítvány* kibocsátásakor a természetes személy azonosságát az eIDAS Rendelet [1] 24. cikk (1) bekezdése értelmében személyes jelenlét útján vagy azzal egyenértékű biztosítékot nyújtó módszerrel kell ellenőrizni. A *Hitelesítés-szolgáltató* a 24. cikk (1) bekezdésben leírt azonosítási módokat alkalmazza az alábbiak szerint.

A *Hitelesítés-szolgáltató* a természetes személy azonosságát az alábbi lehetőségek valamelyikének alkalmazásával ellenőrzi.

1. Személyesen történő azonosítás során.

   - A természetes személynek a személyes azonosítás elvégzéséhez személyesen meg kell jelennie a *Regisztráló szervezet* tisztviselője vagy egy közjegyző előtt.
   - A személyes azonosítás során a természetes személy azonossága ellenőrzésre kerül a személyazonosság igazolására alkalmas hatósági igazolványa alapján.

     Az azonosítás az alábbi hatósági igazolványok alapján történik:

     – a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény (a továbbiakban: Nytv. [3]) hatálya alá tartozó természetes személyek esetében a Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolvány az Eüt. 82.§ (3) [5] szerint;
     – a Nytv. [3] hatálya alá nem tartozó természetes személy esetén a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról, illetve a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló törvény [4] szerinti úti okmány alapján az Eüt. 82.§ (4) [5] szerint;
     – a fenti okmányok egyikével sem rendelkező természetes személyek külföldön történő azonosítása során a *Hitelesítés-szolgáltató* csak európai állampolgárok azonosságának ellenőrzése esetében alkalmazza az Eüt. 82.§ (5) [5] bekezdése szerinti személyazonosság ellenőrzést. Ebben az esetben a természetes személy állampolgársága szerinti európai ország által kibocsátott fényképes személyi igazolványt fogadja el, mint személyazonosság igazolására szolgáló megbízható okmányt.

   - A személyazonosság ellenőrzésére szolgáló adatok helyességét a természetes személynek papír alapú írásos nyilatkozatban, saját kezű - az azonosítást végző személy jelenlétében létrehozott - aláírásával igazolnia kell.
   - A természetes személy lakcímét ellenőrizni kell egy lakcím azonosítására alkalmas igazolvány alapján.
   - A *Hitelesítés-szolgáltató* ellenőrzi, hogy a bemutatott igazolványokon történt-e módosítás vagy hamisítás.

Külföldi állampolgárok személyazonosság ellenőrzésének további szabályai

A *Hitelesítés-szolgáltató* olyan külföldi ország közjegyzője által végzett azonosítást ismer el a saját *Regisztráló szervezet*e által végzett azonosítással egyenértékűnek,

- amely külföldi országgal Magyarország a közokiratok kölcsönös elismeréséről szóló kétoldalú nemzetközi egyezményt kötött, vagy
- amely külföldi ország aláírta a külföldön felhasználásra kerülő közokiratok diplomáciai vagy konzuli hitelesítésének (felülhitelesítésének) mellőzéséről Hágában, 1961. október 5. napján kelt egyezményt (Apostille)

A közjegyző által kiállított dokumentumokat az adott egyezmény által megkövetelt formátumban és tartalommal kell benyújtani.

A *Hitelesítés-szolgáltató* akkor fogadja el a külföldi ország közjegyzője előtt aláírt *Tanúsítványkérelmet*, ha a közjegyzői záradékból kitűnik, hogy

- a közjegyző egy hivatalos személyazonosító okmány (személyi igazolvány, útlevél stb.) alapján azonosított az *Igénylő* természetes személyt;
- az *Igénylő* a közjegyző jelenlétében írta alá a *Tanúsítványkérelmet*.

A *Hitelesítés-szolgáltató* minden esetben elfogadja a magyar vagy angol nyelven kiállított eredeti dokumentumokat. Egyéb nyelven kiállított dokumentumok esetében a *Hitelesítés-szolgáltató* kérheti a dokumentumok hiteles - az Országos Fordító és Fordításhitelesítő Iroda (OFFI) által készített - magyar nyelvű fordítását.

A *Hitelesítés-szolgáltató* egyéb okmányokat és bizonyítékokat is elfogadhat, amennyiben meggyőződik róla, hogy az a fentiekkel megegyező szintű biztonságot jelentenek. Ezen bizonyítékok beszerzése és a *Hitelesítés-szolgáltató*hoz történő eljuttatása az *Ügyfél* feladata.

A *Hitelesítés-szolgáltató* kizárólag érvényes okmányokat, illetve 3 hónapnál nem régebbi bizonyítékokat fogad el.

A *Hitelesítés-szolgáltató* nem állítja ki a *Tanúsítvány*t, amennyiben belső szabályzatai alapján úgy ítéli meg, hogy nem képes valamely bemutatott okmányt vagy a személy adatait megfelelő biztonsággal ellenőrizni.

2. Elektronikus aláírás tanúsítványára visszavezetett azonosítással. Ebben az esetben:

   - Az *Igénylő* a *Tanúsítványkérelmet* elektronikus formában nyújtja be egy nem álneves, az igényelt *Tanúsítvány*énál nem alacsonyabb biztonsági besorolású *Tanúsítvány*án alapuló elektronikus aláírással ellátva.
   - Az elektronikus aláírással ellátott *Tanúsítványkérelem*nek tartalmaznia kell a természetes személy lakcímét és az egyértelmű azonosításához szükséges azonosító adatokat.
   - A *Tanúsítványkérelem* hitelességét és sértetlenségét ellenőrizni kell a teljes tanúsítási lánc vizsgálatával.
   - A *Hitelesítés-szolgáltató* csak olyan *Tanúsítvány*on alapuló elektronikus aláírást fogad be, amelyet egy Európai Uniós tagállam bizalmi listájában szereplő bizalmi szolgáltatás keretében bocsátottak ki, és az aláírás létrehozás időpontjában érvényes volt.
   - A *Hitelesítés-szolgáltató* csak olyan *Tanúsítvány*on alapuló elektronikus aláírást fogad be, amelyet az eIDAS Rendelet [1] 24. cikk (1) bekezdése (a) vagy (b) pontja szerinti személy azonosítás alapján bocsátottak ki.

A Szolgáltatási szerződés érvényességének időtartama alatt, amennyiben az *Igénylő* a lejárt vagy visszavont *Tanúsítvány*a helyett újat igényel, vagy a meglevő *Tanúsítvány*a mellé újabb *Tanúsítvány*t igényel ugyanazon Szolgáltatási szerződés keretében, akkor a *Hitelesítés-szolgáltató* felhasználja a korábbi azonosítás során egyeztetett adatokat. A kérelem hitelességét, a *Tanúsítvány*ba kerülő adatok pontosságát és a kérelmet benyújtó személy azonosságát is ellenőrizni kell.

A *Hitelesítés-szolgáltató* a bizalmi szerepkörök megfelelő elosztásával és belső adminisztratív folyamatainak segítségével biztosítja, hogy a személyes adatok rögzítése és az adatok hitelességének ellenőrzése során legalább két - bizalmi szerepkört ellátó - alkalmazott részvételére van szükség.

2.1.4. Nem ellenőrzött alany információk

A *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány*ba csak olyan adatok kerülnek, amelyeket a *Hitelesítés-szolgáltató* ellenőrzött.

2.1.5. Jogok, felhatalmazások ellenőrzése

Szervezeti tanúsítvány kiállítása előtt a *Szervezet* nevében eljáró természetes személy azonosságát igazolni kell a 2.1.3. fejezet előírásai szerint.

Ellenőrizni kell a természetes személy képviseleti jogosultságát.

Egy *Szervezet* nevében eljárhat:

- az adott *Szervezet* képviseletére jogosult természetes személy;
- aki az adott *Szervezet* képviseletére jogosult személytől erre a célra meghatalmazással rendelkezik;
- az adott *Szervezet* képviseletére jogosult személy által kijelölt *Szervezeti ügyintéző*.

A *Szervezeti ügyintéző* kijelölhető a tanúsítvány igénylés során, vagy később is bármikor a megfelelő formanyomtatvány segítségével. Az űrlapon meg kell adni a kijelölt személy(ek) azonosító adatait, amelyek alapján a későbbi eljárás során azonosíthatóak. Az űrlapot a *Szervezet* képviselőjének (saját kezű vagy nem álneves tanúsítványon alapuló minősített elektronikus) aláírással kell ellátnia, amelyet az űrlap befogadásakor a *Hitelesítés-szolgáltató* regisztrációs munkatársai ellenőriznek.

Szervezeti ügyintéző kijelölése nem kötelező, illetve egyidejűleg több *Szervezeti ügyintéző* is kijelölhető. Amennyiben nincs kijelölve *Szervezeti ügyintéző*, akkor az adott szervezet képviseletére jogosult személy láthatja el ezt a feladatot.

A *Hitelesítés-szolgáltató* nyilvántartást vezet a magánszemélyekről, akik a *Szervezet* nevében jogosultak *Tanúsítványkérelem* benyújtására.

A *Szervezet* írásos megkeresésére a kérés validálása után a *Hitelesítés-szolgáltató* átadja a *Szervezet*nek a meghatalmazott *Szervezeti ügyintéző*k aktuális listáját.

2.1.6. Együttműködési képességre vonatkozó követelmények

A *Hitelesítés-szolgáltató* a szolgáltatás nyújtása során nem működik együtt más *Hitelesítés-szolgáltató*kkal.

2.2. Adatkezelési szabályzat

A *Hitelesítés-szolgáltató* az *Ügyfél*ek adatait a jogi előírásoknak megfelelően kezeli. Az Adatkezelési szabályzat elérhető a *Hitelesítés-szolgáltató* honlapján (`https://e-szigno.hu/letoltesek/dokumentumok-es-szabalyzatok/`), további információ a *Szolgáltatási szabályzat* 9.3 pontjában olvasható.

3. A tanúsítványokra vonatkozó követelmények

3.1. A kulcspár és a tanúsítvány használata

3.1.1. A magánkulcs és a tanúsítvány használata

A *Tanúsítvány*hoz tartozó magánkulcs kizárólag webszerverek azonosságának igazolására használható, más felhasználás nem engedélyezett.

Lejárt érvényességű vagy visszavont *Tanúsítvány*hoz tartozó magánkulcs nem használható.

Az *Alany* köteles gondoskodni magánkulcsának és aktivizáló adatának megfelelő védelméről.

A használat során be kell tartani az 1.5. fejezetben leírt korlátozásokat.

3.1.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata

A *Tanúsítvány* felhasználásával végzett webszerver azonosítás során a *Hitelesítés-szolgáltató* által garantált biztonsági szint megtartásához ajánlott, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, különös tekintettel az alábbiakra:

- ellenőrizze a *Tanúsítvány* érvényességét és visszavonási állapotát;
- a *Weboldal-hitelesítő tanúsítvány*okhoz kapcsolódó nyilvános kulcsokat csak webszerver azonosságának igazolására használja;
- a *Tanúsítvány*ra vonatkozó ellenőrzéseket célszerű elvégeznie a teljes tanúsítványláncra vonatkozóan;
- javasolt ellenőrizni, hogy a *Tanúsítvány* a célnak megfelelő *Hitelesítési rend* alapján lett-e kibocsátva;
- vegyen figyelembe minden korlátozást, amely a *Tanúsítvány*ban vagy a *Tanúsítvány*ban meghivatkozott szabályzatokban szerepel.

A *Hitelesítés-szolgáltató* elérhetővé tesz olyan szolgáltatást az *Ügyfel*ei és az *Érintett felek* számára, amely segítségével ellenőrizhetik az általa kibocsátott *Tanúsítvány*okat.

3.2. Tanúsítvány visszavonás és felfüggesztés

A tanúsítvány visszavonás alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* a *Tanúsítvány* érvényességét megszünteti az eredetileg tervezett érvényességi idő lejárta előtt.

A tanúsítvány visszavonás visszafordíthatatlan és végleges állapotváltozást jelent, a visszavont *Tanúsítvány* már soha többé nem lehet újra érvényes.

Weboldal-hitelesítő tanúsítvány nem függeszthető fel.

A visszavont *Tanúsítvány*hoz tartozó magánkulcs használatát azonnal meg kell szüntetni.

A visszavont *Tanúsítvány*hoz tartozó magánkulcsot a visszavonást követően azonnal meg kell semmisíteni, amennyiben ez lehetséges.

Felelősségi szabályok a visszavonással kapcsolatban:

- Amennyiben a *Hitelesítés-szolgáltató* már közzétette a *Tanúsítvány* visszavont állapotát, a *Hitelesítés-szolgáltató* semmilyen felelősséget nem vállal azért, ha az *Érintett fél* a közzétételt követően érvényesnek tekinti a *Tanúsítvány*t.

3.2.1. Ki kérelmezheti a visszavonást

A *Tanúsítvány* visszavonását kezdeményezhetik:

- az *Előfizető*;
- az *Igénylő*
- *Szervezeti tanúsítvány* esetén a *Szervezet* nevében eljárásra jogosult természetes személy;
- az *Előfizető* által bejelentett *Szervezeti ügyintéző*;
- az *Alany* pénzforgalmi szolgáltatási engedélyét kibocsátó hatóság, amennyiben a *Tanúsítvány* az *Alany* módosított pénzforgalmi irányelv (PSD2) [2] szerinti adatait tartalmazza;
- a *Hitelesítés-szolgáltató*.

3.2.2. A visszavonási kérelemre vonatkozó eljárás

A *Hitelesítés-szolgáltató* a tanúsítvány visszavonási kérelem benyújtására legalább az alábbi lehetőségeket biztosítja:

- elektronikus formában, a kérelmező nem álneves, a visszavonni kívánt *Tanúsítvány*nál nem alacsonyabb biztonsági besorolású *Tanúsítvány*án alapuló elektronikus aláírásával ellátva;
- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában ügyfélszolgálati időben, vagy postai úton.
- A *Hitelesítés-szolgáltató* honlapján keresztül a nap 24 órájában.

  A *Hitelesítés-szolgáltató* honlapján benyújtott kérelmeket a *Hitelesítés-szolgáltató* informatikai rendszere azonnal elbírálja, az elbírálás eredményéről az oldalon tájékoztatja a kérelem benyújtóját;

- Rögzített formátumú SMS üzenet küldésével a nap 24 órájában.

  A *Hitelesítés-szolgáltató Ügyfel*ei a visszavonásra szolgáló telefonszámra küldött rövid szöveges üzenetben jelezhetik a *Hitelesítés-szolgáltató*nak, ha magánkulcsuk illetéktelen kezekbe került.

  A szöveges üzenetben érkező kérelmek feldolgozását a *Hitelesítés-szolgáltató* a beérkezést követően haladéktalanul megkezdi. A *Hitelesítés-szolgáltató* rendszere automatikusan generált válaszüzenetet küld a kérelmező telefonszámára a feldolgozás eredményéről és a visszavonás sikerességéről.

  A szöveges üzenetben küldött kérelemben az alábbi adatokat kell megadni egy szóköz karakterrel elválasztva

  – az *Alany* születési dátumát "ÉÉÉÉ-HH-NN" formátumban vagy a *Tanúsítvány*ban szereplő OID-jének utolsó három tagját;
  – a *Tanúsítvány*hoz tartozó felfüggesztési jelszót.

  Példa formailag helyes visszavonási kérelemre:

  – "2.1.134 pacsirta"

  A rejtett telefonszámról küldött SMS alapú visszavonási kérelmeket a *Hitelesítés-szolgáltató* az üzenet tartalmától függetlenül minden esetben elutasítja.

A *Hitelesítés-szolgáltató* a kérelem elbírálása során ellenőrzi a benyújtott kérelem hitelességét és a kérelmet benyújtó jogosultságát.

Érvényes elektronikus aláírással ellátott visszavonási kérelem esetében nincs szükség a kérelmező azonosságának és a kérelem hitelességének további vizsgálatára.

A papíralapon, postai úton történő visszavonási kérelem benyújtása esetében a *Hitelesítés-szolgáltató* ellenőrzi a kérelmen található kézi aláírást.

Visszavonáskor meg kell adni a visszavonás okát. Amennyiben a visszavonást az *Ügyfél* kéri, és a visszavonás okát nem adja meg, a *Hitelesítés-szolgáltató* úgy tekinti, hogy a visszavonás oka az, hogy az *Alany* a tanúsítványt a továbbiakban nem kívánja használni.

Amennyiben a visszavonást az *Ügyfél* kéri kulcskompromittálódás miatt, akkor a *Hitelesítés-szolgáltató* lehetőséget biztosít számára a visszavonási eljárás során, hogy a visszavonandó *Tanúsítvány* helyett kulcscsere keretében új *Tanúsítvány*t igényeljen.

Az írásos formában benyújtott visszavonási kérelmek esetében a *Hitelesítés-szolgáltató* lehetővé teszi, hogy a visszavonást időzítve kérjék egy egy későbbi dátumra.

A visszavonási kérelemnek tartalmaznia kell a *Tanúsítvány* beazonosításához szükséges adatokat.

A kérelmezőnek különösen a következő adatokat kell megadnia:

- az *Alany* pontos megnevezése;
- a *Tanúsítvány* egyedi azonosítója;
- A visszavonás kért dátuma, amennyiben nem azonnali visszavonást kér;
- az *Ügyfél* azonosító adatai.

Amennyiben a benyújtott kérelem hiányos vagy érvénytelen, a *Hitelesítés-szolgáltató* elutasítja a kérelmet. Az elutasítás tényéről és okáról emailben tájékoztatja az *Alany*t és az *Előfizető*t.

Érvényes, hiánytalan kérelem esetén a *Hitelesítés-szolgáltató* dönt a kérelem elfogadásáról és a kért visszavonási időpont függvényében azonnal visszavonja a *Tanúsítvány*t, vagy beállítja a kérelemben megadott napot az időzített visszavonás időpontjaként.

Sikeres visszavonás esetén a *Hitelesítés-szolgáltató* emailben értesíti az *Alany*t és az *Előfizető*t a visszavonás tényéről.

A visszavonásról és a felfüggesztésről további információ található a a *Hitelesítés-szolgáltató* alábbi web oldalán:

`https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/tanusitvany-felfuggesztese-es-visszavonasa.html`

Tanúsítvánnyal kapcsolatos problémák sürgősségi bejelentése

A *Hitelesítés-szolgáltató* egy folyamatosan elérhető 24/7 belső ügyeletet tart fenn a tanúsítvánnyal kapcsolatos problémák sürgősségi bejelentésére. Szükség esetén a bejelentett problémáról értesíti a felügyelő hatóságot, és/vagy visszavonja az érintett *Tanúsítvány*t.

Tanúsítvánnyal kapcsolatos problémák sürgősségi bejelentése az alábbi email címen lehetséges:

`HighPriorityCertificateProblemReport@e-szigno.hu`

További információ és a web alapú bejelentő lap az alábbi címen érhető el:

`https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/tanusitvanyokkal-kapcsolatos-biztonsagi-esemenyek-bejelentese.html`

3.2.3. A végfelhasználói tanúsítványok

A *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*ok érvényességi ideje:

- legfeljebb a kibocsátástól számított 3 év;
- nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozata szerint biztonságosan felhasználhatók;
- nem haladhatja meg a *Tanúsítvány*t kibocsátó szolgáltatói *Tanúsítvány* érvényességi idejét.

A tanúsítvány megújítás keretében a végfelhasználói kulcshoz kibocsátható új *Tanúsítvány*.

A *Tanúsítvány*ok és a magánkulcsok érvényességi idejét befolyásolhatja, ha a Nemzeti Média- és Hírközlési Hatóság új algoritmusokkal kapcsolatos határozatot ad ki, amely szerint a felhasznált kriptográfiai algoritmus vagy kulcsparaméter már nem biztonságos a kibocsátáskor tervezett felhasználási idő végéig.

Amennyiben ez bekövetkezik, a *Hitelesítés-szolgáltató* visszavonja az érintett *Tanúsítvány*okat.

4. A megfelelőség vizsgálata

A *Hitelesítés-szolgáltató* tevékenységét az Európai Uniós szabályozással összhangban a Nemzeti Média- és Hírközlési Hatóság felügyeli. A Nemzeti Média- és Hírközlési Hatóság évente legalább egyszer átfogó helyszíni ellenőrzést tart a *Hitelesítés-szolgáltató* telephelyén. A helyszíni ellenőrzés előtt a *Hitelesítés-szolgáltató* külső auditor igénybevételével átvilágíttatja üzemeltetését és az átvilágításról készült részletes megfelelőségértékelési jelentést annak kézhezvételétől számított három munkanapon belül a Nemzeti Média- és Hírközlési Hatóságnak benyújtja. Az átvizsgálás során azt kell megállapítani, hogy a *Hitelesítés-szolgáltató* működése megfelel-e az eIDAS Rendeletben [1] és a vonatkozó magyar jogszabályokban megállapított követelményeknek, valamint az alkalmazott *Hitelesítési rend*(ek)ben és az ennek megfelelő *Szolgáltatási szabályzat*(ok)ban támasztott követelményeknek.

Az átvilágítás tematikája és módszertana megfelel az alábbi normatív dokumentumoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [7]
- ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [6]
- ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [8]
- ETSI EN 319 411-2 v2.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; [9]

A megfelelőségértékelési vizsgálat eredménye bizalmas dokumentum, csak az arra jogosultak számára hozzáférhető.

A megfelelőségértékelési jelentés alapján kiállított megfelelőségi tanúsítványt a *Hitelesítés-szolgáltató* honlapján közzéteszi.

A *Hitelesítés-szolgáltató* vizsgált és tanúsított elemeket (elektronikus aláírási termékeket, informatikai rendszerelemeket stb.) alkalmaz a szolgáltatásaihoz kapcsolódóan.

A *Hitelesítés-szolgáltató* a szolgáltatások nyújtásához használt valamennyi rendszerelemet biztonsági osztályokba sorolta kockázatmenedzsment rendszere alapján. Ezen rendszerelemekről és a hozzájuk tartozó biztonsági besorolásról a *Hitelesítés-szolgáltató* a kockázatmenedzsment rendszere keretében nyilvántartást vezet.

A *Hitelesítés-szolgáltató* a külső auditon túl saját belső ellenőrzési rendszerrel is rendelkezik, amely segítségével rendszeresen vizsgálja a korábbi auditoknak való megfelelőséget és eltérés esetén megteszi a szükséges lépéseket.

A *Hitelesítés-szolgáltató* 2002 óta rendelkezik az ISO 9001 szabványnak megfelelő minőségirányítási, valamint 2003 óta a ISO/IEC 27001-nek (korábban BS 7799-nek) megfelelő

információbiztonság-irányítási rendszerrel, amelyeket külső auditáló szervezet (Lloyd's Register Quality Assurance) auditál és vizsgál felül folyamatosan (lásd: 1.3. fejezet).

A vonatkozó jogszabályokról és megfelelőségi auditokról további információ található a jelen dokumentum 5.4 fejezetében és a *Szolgáltatási szabályzat* 8. és 9.15 fejezeteiben.

5. Egyéb üzleti és jogi kérdések

5.1. Tevékenységért viselt felelősség és helytállás

5.1.1. Az Ügyfél felelőssége és helytállása

Az *Előfizető* felelőssége

Az *Előfizető* felelősségét a Szolgáltatási szerződés és annak mellékletei (köztük az Általános szerződési feltételek) határozzák meg.

Az *Előfizető* kötelezettségei

Az *Előfizető* köteles a *Hitelesítés-szolgáltató* szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatás igénybevétele során, beleértve a *Tanúsítvány*ok és magánkulcsok igénylését és alkalmazását.

Az *Előfizető* kötelezettségeit a jelen *Szolgáltatási szabályzat*, a Szolgáltatási szerződés és annak elválaszthatatlan részét képező Általános szerződési feltételek és egyéb dokumentumok, valamint a vonatkozó *Hitelesítési rend* tartalmazzák.

Amennyiben az *Előfizető* tudomására jut, hogy az *Előfizető*höz tartozó valamely *Tanúsítvány* nyilvános kulcsához tartozó magánkulcs kompromittálódott vagy a kompromittálódás gyanúja felmerült, az *Előfizető* köteles

- e tényt haladéktalanul jelezni a *Hitelesítés-szolgáltató*nak,
- kezdeményezni a *Tanúsítvány* visszavonását,
- megszüntetni a *Tanúsítvány*hoz tartozó magánkulcsok használatát.

Az *Előfizető* csak olyan szervereken telepítheti a *Tanúsítvány*t és a hozzá tartozó magánkulcsot, amelyek elérhetőek a *Tanúsítvány* "subjectAltName" mezejében felsorolt domének valamelyikén. A használat során be kell tartani a vonatkozó jogi szabályozásból, a Szolgáltatási szerződésből és az Általános szerződési feltételekből származó követelményeket.

Az *Előfizető* jogai

Az *Előfizető* jogosult:

- a szolgáltatások igénybevételére a jelen *Szolgáltatási szabályzat*ban leírtak szerint;
- írásban meghatározni, hogy mely *Alany* kaphasson tanúsítványt;

- a *Tanúsítvány*ok visszavonását kérni;
- *Szervezeti ügyintéző*ket kijelölni.

Az *Igénylő* felelőssége

Az *Igénylő* felelős:

- a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért;
- az általa igényelt *Tanúsítvány*ban szereplő adatok ellenőrzéséért,
- az adataiban illetve a *Tanúsítvány*ban szereplő adatokban bekövetkezett változások haladéktalan bejelentéséért;
- magánkulcsának és *Tanúsítvány*ának a szabályzatoknak megfelelő felhasználásáért;
- magánkulcsának és aktivizáló kódjának biztonságos kezeléséért;
- a *Hitelesítés-szolgáltató* haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyekben;
- általában a kötelezettségei betartásáért.

Az *Igénylő* kötelezettségei

Az *Igénylő* köteles:

- a szolgáltatás igénybevétele előtt megismerni a jelen *Szolgáltatási szabályzat*ot;
- a *Hitelesítés-szolgáltató* által kért, a szolgáltatás igénybevételéhez szükséges adatokat hiánytalanul megadni, a valóságnak megfelelő adatokat szolgáltatni;
- amennyiben az *Igénylő* tudomására jut, hogy az általa megadott, a szolgáltatás igénybevételéhez szükséges adat – különösen valamely *Tanúsítvány*ban is szereplő adat – megváltozott, haladéktalanul köteles:
  - erről írásban értesíteni a *Hitelesítés-szolgáltató*t,
  - kérni a *Tanúsítvány* visszavonását és
  - megszüntetni a *Tanúsítvány* használatát;
- amennyiben az *Igénylő* tudomására jut, hogy az általa igényelt *Tanúsítvány*t visszavonták, vagy a kibocsátó CA magánkulcsa kompromittálódott, haladéktalanul köteles megszüntetni a *Tanúsítvány* használatát;
- a szolgáltatást kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a hivatkozott szabályzatokban és dokumentumokban foglaltaknak megfelelően használni;
- a *Weboldal-hitelesítő tanúsítvány*t kizárólag olyan szerverre telepíteni, amely a *Tanúsítvány*ban szereplő doménnéven elérhető;

- biztosítani, hogy a szolgáltatás igénybevételéhez szükséges adatokhoz és eszközökhöz (jelszavakhoz, titkos kódokhoz, aláírás-létrehozó eszközökhöz) illetéktelen személyek ne férhessenek hozzá;
- a *Hitelesítés-szolgáltató*t haladéktalanul írásban értesíteni, amennyiben valamely Tanúsítvánnyal kapcsolatban jogvita indul;
- a *Tanúsítvány* kiadásához szükséges adatok ellenőrzése érdekében a *Hitelesítés-szolgáltató*val együttműködni és mindent megtenni azért, hogy az ellenőrzés a lehető leghamarabb befejeződhessen;
- kulcs kompromittálódás vagy nem jogszerű használat gyanújának felmerülése esetében a *Hitelesítés-szolgáltató* megkereséseire az *Igénylő* köteles a *Hitelesítés-szolgáltató* által megadott időn belül reagálni;
- tudomásul venni, hogy az *Előfizető* jogosult a *Tanúsítvány* visszavonását kérni;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a *Tanúsítvány*t a *Szolgáltatási szabályzat*ban leírt meghatározott módon, az ott leírt ellenőrzési lépések elvégezése után bocsátja ki;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*okban kizárólag a valóságnak megfelelő adatokat szerepeltet. Ennek megfelelően a *Hitelesítés-szolgáltató* a *Tanúsítvány*ba kerülő adatokat a *Szolgáltatási szabályzat* szerint ellenőrzi;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*t visszavonja, amennyiben tudomására jut, hogy a *Tanúsítvány*ban foglalt adatok nem felelnek meg a valóságnak, vagy a magánkulcs nem az *Igénylő* kizárólagos birtokában vagy használatában van, és ebben az esetben az *Igénylő* köteles a *Tanúsítvány* használatát beszüntetni;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* jogosult a *Tanúsítvány*t visszavonni, amennyiben az *Előfizető* nem fizeti meg határidőre a szolgáltatások díját;
- *Szervezeti tanúsítvány* igénylése esetén köteles tudomásul venni, hogy a *Hitelesítés-szolgáltató* a *Tanúsítvány*t kizárólag a *Képviselt szervezet* hozzájárulása esetén bocsátja ki;
- *Szervezeti tanúsítvány* igénylése esetén köteles tudomásul venni, hogy a *Képviselt szervezet* jogosult a *Tanúsítvány* visszavonását kérni
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* jogosult a *Tanúsítvány*t visszavonni, amennyiben az *Előfizető* megszegi a Szolgáltatási szerződést vagy a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t illegális tevékenységhez használták.

Az *Igénylő* jogai

Az *Igénylő* jogosult:

- *Tanúsítvány*t igényelni a jelen *Szolgáltatási szabályzat*ban leírtak szerint;
- *Tanúsítvány*ának visszavonását kérni jelen *Szolgáltatási szabályzat* szerint, amennyiben ezt a vonatkozó *Hitelesítési rend* lehetővé teszi.

5.1.2. Az Érintett fél felelőssége

Az *Érintett felek* saját belátásuk és/vagy szabályzataik alapján dönthetnek az egyes *Tanúsítvány*ok elfogadásáról és a felhasználás módjáról. Az érvényesség vizsgálata során a *Hitelesítés-szolgáltató* által garantált biztonsági szint megtartásához szükséges, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, ezért különös tekintettel javasolt:

- a *Hitelesítési rend*ben és a *Szolgáltatási szabályzat*ban megfogalmazott követelmények, előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- a *Tanúsítvány* visszavonási állapotának ellenőrzése az aktuális CRL vagy OCSP válasz alapján;
- a *Tanúsítvány* felhasználására vonatkozó valamennyi korlátozás figyelembevétele, amely a *Tanúsítvány*ban, a jelen *Hitelesítési rend*ben és a *Szolgáltatási szabályzat*ban szerepel.

5.2. A felelősség korlátozása

A *Hitelesítés-szolgáltató* kártérítési felelősségének szabályai:

- A *Hitelesítés-szolgáltató* nem felelős az olyan károkért, amelyek abból adódnak, hogy az *Érintett fél* a *Tanúsítvány*ok ellenőrzése és felhasználása során nem a hatályos jogszabályok és a *Hitelesítés-szolgáltató* szabályzatai szerint ajánlottan járt el, illetve nem úgy járt el, ahogyan az az adott helyzetben elvárható.
- A *Hitelesítés-szolgáltató* a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag kötelezettségei felróható megszegéséből bekövetkező, bizonyítható károkért tartozik helytállni.
- A *Hitelesítés-szolgáltató* nem felelős az abból adódó károkért, amikor valamely külső, elháríthatatlan esemény miatt az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni.
- Amennyiben a *Hitelesítés-szolgáltató* a *Tanúsítvány* kibocsátása előtt adategyeztetést végez egy közhiteles adatbázissal, az onnan kapott adatokat hitelesnek fogadja el.

  A *Hitelesítés-szolgáltató* nem vállal felelősséget ezen közhiteles adatbázis által szolgáltatott információk pontatlanságából eredő károkért.
- A *Hitelesítés-szolgáltató* kizárólag azért vállal felelősséget, hogy a szolgáltatásokat a jelen *Szolgáltatási szabályzat*ban, illetve az abban meghivatkozott dokumentumokban (*Hitelesítési rend*ek, szabványok, ajánlások) leírtaknak, valamint saját belső szabályzatainak megfelelően nyújtja.

Adminisztratív folyamatok

A *Hitelesítés-szolgáltató* a vagyoni felelősségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelősség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megőrzi (archiválja) a naplóadatokat.

A *Hitelesítés-szolgáltató* az archivált adatokat az alábbi időtartamokig őrzi meg:

- a *Szolgáltatási szabályzat*ot a hatályon kívül helyezéstől számított 10 évig;
- a *Tanúsítvány*okkal kapcsolatos valamennyi elektronikus és/vagy papír alapú információt legalább
  - a *Tanúsítvány* érvényességének lejáratától számított 10 évig;

Pénzügyi felelősség

A *Hitelesítés-szolgáltató* pénzügyi felelőssége, valamint a megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében a jogszabályi előírásoknak megfelelő óvadékkal rendelkezik.

A *Hitelesítés-szolgáltató* a megbízhatóság biztosítása érdekében a jogszabályi előírásoknak megfelelő felelősségbiztosítással rendelkezik.

Pénzügyi felelősség korlátozása

A *Hitelesítés-szolgáltató* korlátozza a szolgáltatásokkal kapcsolatos kártérítési kötelezettségét, ezen korlátozás mértéke 6.000.000,-HUF *Előfizető*nként vagy *Érintett fél* per *Tanúsítvány*onként.

5.3. Vitás kérdések rendezése

A *Hitelesítés-szolgáltató* törekszik a működése során felmerülő vitás kérdések békés, tárgyalásos rendezésére. A rendezés során a fokozatosság elvét követi.

A *Hitelesítés-szolgáltató* és az *Ügyfél* kölcsönösen megállapodnak abban, hogy bármilyen vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra való terelése előtt megkísérlik a békés úton, tárgyalással történő egyeztetést. A kezdeményező fél kötelessége, hogy minden érintett többi felet haladéktalanul értesítsen és teljes körűen tájékoztasson az ügy minden vonatkozását illetően.

Az *Ügyfél* vitás kérdés felmerülése esetén jogosult az esetleges bírósági eljárást megelőzően a Budapesti Békéltető Testülethez fordulni.

A *Hitelesítés-szolgáltató* tevékenységével vagy a kiadott *Tanúsítvány*ok felhasználásával kapcsolatos kérdéseket, kifogásokat és panaszokat az ügyfélszolgálati iroda címére kell eljuttatni írásos formában. A bejelentés kézhezvételétől számított 3 munkanapon belül a *Hitelesítés-szolgáltató* értesíti a bejelentő felet az általa megadott címen a bejelentés fogadásáról és a kivizsgáláshoz szükséges időről. A megjelölt határidőig a *Hitelesítés-szolgáltató* köteles írásban válaszolni a bejelentőnek. A *Hitelesítés-szolgáltató* a válaszadáshoz szükséges információk megadását kérheti a bejelentőtől. A *Hitelesítés-szolgáltató* a panaszt 30 napon belül kivizsgálja, és az eredményekről értesíti a bejelentőt.

Amennyiben a választ a bejelentő nem tartja kielégítőnek, vagy az alapján nem sikerül a *Hitelesítés-szolgáltató* bevonása nélkül rendezni a felmerült vitát, akkor a bejelentő egyeztetést kezdeményezhet a *Hitelesítés-szolgáltató*val és az *Érintett felek*kel. Az egyeztetés minden résztvevőjét írásban értesíteni kell az egyeztetés időpontjáról azt megelőzően 10 munkanappal, és írásban meg kell számukra küldeni a bejelentést, a *Hitelesítés-szolgáltató* válaszát és egyéb szükséges információkat tartalmazó dokumentumokat.

Amennyiben az egyeztetés a panasz benyújtásától számított 30 napon belül nem vezet eredményre, akkor a bejelentő peres útra terelheti az ügyet. Az *Érintett felek* kölcsönösen alávetik magukat a Budapesti II. és III. Kerületi Bíróság, illetve a Fővárosi Törvényszék kizárólagos illetékességének.

5.4. Irányadó jog

A *Hitelesítés-szolgáltató* tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. A *Hitelesítés-szolgáltató* szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

A. Hivatkozások

[1] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről .

[2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2015/2366 IRÁNYELVE (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről .

[3] 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról .

[4] 2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról .

[5] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól .

[6] ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[7] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;.

[8] ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[9] ETSI EN 319 411-2 v2.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;.

[10] ETSI TS 119 495 V1.3.2 (2019-06); Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.

[11] IETF RFC 3490: Internationalizing Domain Names in Applications (IDNA), March 2003.

[12] IETF RFC 3966: The tel URI for Telephone Numbers, December 2004.

[13] IETF RFC 6532: Internationalized Email Headers, February 2012.

[14] IETF RFC 6844: DNS Certification Authority Authorization (CAA) Resource Record, January 2013.

[15] e-Szignó Hitelesítés Szolgáltató - eIDAS rendelet szerinti minősített weboldal-hitelesítő tanúsítvány hitelesítési rendek.