e-Szignó Hitelesítés Szolgáltató

eIDAS Rendelet szerinti weboldal-hitelesítő tanúsítvány szolgáltatási szabályzat

ver. 2.12

Hatálybalépés: 2019-12-12

Azonosító	1.3.6.1.4.1.21528.2.1.1.167.2.12
Verzió	2.12
Első verzió hatálybalépése	2016-07-01
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2019-12-10
Hatálybalépés dátuma	2019-12-12

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság

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

Verzió	A változás leírása	Hatálybalépés	Készítette
2.0	Új szabályzat az RFC 3647 és az eIDAS követelmények szerint.	2016-07-01	Szabóné Endrődi Csilla, Dr. Szőke Sándor, Réti Kornél
2.1	Módosítások az NMHH észrevételei alapján.	2016-09-05	Szomolya Melinda, Dr. Szőke Sándor
2.2	Módosítások a tanúsító észrevételei alapján.	2016-10-30	Dr. Szőke Sándor
2.3	Módosítások az NMHH észrevételei alapján.	2017-04-30	Dr. Szőke Sándor
2.4	Éves felülvizsgálat.	2017-09-30	Dr. Szőke Sándor
2.6	Teljes felülvizsgálat. Domén validálási módszerek változása. Közjegyzői személy azonosítás bevezetése. Kisebb módosítások.	2018-03-24	Dr. Szőke Sándor
2.7	Éves felülvizsgálat.	2018-09-15	Dr. Szőke Sándor
2.8	Változások az auditor javaslatai alapján.	2018-12-14	Dr. Szőke Sándor
2.9	Domén validálási követelmények változása. Kisebb módosítások. Változások a CABF BR követelményekben.	2019-04-24	Dr. Szőke Sándor
2.10	Kisebb módosítások.	2019-06-25	Dr. Szőke Sándor
2.11	Éves felülvizsgálat.	2019-09-25	Dr. Szőke Sándor
2.12	Változások az auditor javaslatai alapján.	2019-12-12	Dr. Szőke Sándor

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zrt. (továbbiakban: Microsec vagy *Hitelesítés-szolgáltató*) által üzemeltetett e-Szignó Hitelesítés Szolgáltató weboldal-hitelesítő tanúsítványok kibocsátása szolgáltatásra vonatkozó *Szolgáltatási szabályzat*a.

A *Hitelesítés-szolgáltató* szolgáltatásait a vele szerződéses viszonyban álló *Ügyfel*ek részére biztosítja.

Jelen *Szolgáltatási szabályzat* a fenti szolgáltatások nyújtásának kereteit, a részletes eljárási és egyéb működési szabályokat tartalmazza. Ajánlásokat fogalmaz meg a szolgáltatások segítségével létrehozott *Tanúsítvány*ok ellenőrzésében az *Érintett felek* számára.

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

A *Hitelesítés-szolgáltató* a bizalmi szolgáltatás nyújtását 2016. július 1-jén jelentette be a Nemzeti Média- és Hírközlési Hatóságnak.

1.1. Áttekintés

Jelen *Szolgáltatási szabályzat* célja, hogy összefoglalja mindazokat az információkat, amelyeket a *Hitelesítés-szolgáltató*val kapcsolatba kerülő *Ügyfel*eknek tudniuk érdemes. Ezzel elő kívánja segíteni, hogy *Ügyfel*ei és leendő *Ügyfel*ei:

- minél könnyebben megismerhessék a *Hitelesítés-szolgáltató* által kínált szolgáltatások részleteit, feltételeit és a szolgáltatás nyújtásának gyakorlati hátterét;
- átláthassák a *Hitelesítés-szolgáltató* működését, és ennek révén minél könnyebben eldönthessék, hogy a szolgáltatások megfelelnek-e, illetve az egyes szolgáltatások melyik típusa felel meg igényeiknek, elvárásaiknak.

Jelen dokumentum feladata továbbá, hogy segítségével a *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány*ok, *Tanúsítvány visszavonási list*ák, online 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 dokumentum tartalmilag és formailag megfelel az IETF RFC 3647 [23] keretrendszer követelményeinek. Kilenc fejezetből áll, amelyek tartalmazzák a *Hitelesítés-szolgáltató* által megfogalmazott biztonsági követelményeket, folyamatokat és a szolgáltatás nyújtása során követendő gyakorlatot. Az IETF RFC 3647 által meghatározott felépítés szigorú megtartása érdekében azok a fejezetek is szerepelnek a dokumentumban, amelyeknél a *Hitelesítés-szolgáltató* nem ír elő követelményt, ilyen esetben a fejezetben a "Nincs megkötés" szöveg szerepel.

A végfelhasználóknak az igénybe vett szolgáltatással kapcsolatos tevékenységére vonatkozó előírásokat jelen *Szolgáltatási szabályzat*on kívül az Általános szerződési feltételek, a szolgáltatóval kötött Szolgáltatási szerződés, a *Hitelesítés-szolgáltató* által alkalmazott *Hitelesítési rend*ek (lásd: 1.2.1. fejezet) illetve egyéb, a *Hitelesítés-szolgáltató*tól független szabályzat illetve dokumentum is tartalmazhat.

1.2. Dokumentum neve és azonosítója

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	eIDAS Rendelet szerinti weboldal-hitelesítő tanúsítvány szolgáltatási szabályzat
Dokumentum verziószáma	2.12
Hatálybalépés ideje	2019-12-12

A jelen *Szolgáltatási szabályzat* szerint használható *Hitelesítési rend*ek felsorolását és azonosító adatait az 1.2.1 fejezet tartalmazza.

1.2.1. Hitelesítési rendek

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

A *Hitelesítési rend*eket azonosító OID első hét száma a Microsec egyedi azonosítója az alábbiak szerint:

(1)	International Organization for Standardization (ISO)	Nemzetközi Szabványügyi Szervezet (ISO)
(3)	Organization identification schemes registered according to ISO/IEC 6523-2	Az ISO/IEC 6523-2 szerint regisztrált szervezeti azonosító rendszer
(6)	United States Department of Defense (DoD)	Amerikai Védelmi Minisztérium (DoD)
(1)	Internet	Internet
(4)	Private projects	Magán projektek
(1)	Private enterprises	Magán vállalatok
(21528)	MICROSEC Ltd.	Microsec zrt.

A további számok rendszerét a Microsec saját hatáskörben osztotta ki, értelmezésük az alábbiak szerinti:

(1.3.6.1.4.1.21528)	MICROSEC Ltd.
(2)	e-Szignó Hitelesítés Szolgáltató
(1)	dokumentumok
(1)	nyilvános dokumentumok
(x)	dokumentum egyedi azonosító sorszáma
(y)	dokumentum verziója
(z)	dokumentum alverziója

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

OID	MEGNEVEZÉS	RÖVID NÉV
1.3.6.1.4.1.21528.2.1.1.159.2.12	III. hitelesítési osztályba tartozó, weboldal-hitelesítő tanúsítványokhoz használt, álnevet kizáró hitelesítési rend.	HWJSN
1.3.6.1.4.1.21528.2.1.1.161.2.12	II. hitelesítési osztályba tartozó, weboldal-hitelesítő tanúsítványokhoz használt, álnevet kizáró hitelesítési rend.	KWJSN, KWTSN
1.3.6.1.4.1.21528.2.1.1.162.2.12	Automatikus kibocsátás során kibocsátott, weboldal-hitelesítő tanúsítványok kibocsátását szabályozó, álnevet kizáró hitelesítési rend.	AWxSN

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 weboldal-hitelesítő tanúsítvány hitelesítési rendek ver.2.12." [39] dokumentum tartalmazza.

A III. hitelesítési osztályba tartozó *Tanúsítvány*ok kibocsátása a *Hitelesítés-szolgáltató* által előzetesen elvégzett személyes regisztrációhoz kötött, a II. hitelesítési osztályba tartozó *Tanúsítvány*ok kibocsátása távoli regisztráció alapján is megengedett.

A *Weboldal-hitelesítő tanúsítvány*ok esetében az *Alany* nevénél a doménnév vagy IP cím szerepel.

A *Weboldal-hitelesítő tanúsítvány* nem lehet álneves.

A *Hitelesítés-szolgáltató* működése megfelel a CA/Browser Forum által kibocsátott "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" [34] követelményrendszer aktuális verziójának, amely a

`https://cabforum.org/baseline-requirements-documents/`

címen érhető el. A jelen *Szolgáltatási szabályzat* és a Baseline Requirements ellentmondása esetén a Baseline Requirements követelményei az irányadók.

Jelen *Hitelesítési rend*ek közül:

- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [13] szabványban definiált [LCP] *Hitelesítési rend*nek.
- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [13] szabványban definiált [DVCP] *Hitelesítési rend*nek.
- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [13] szabványban definiált [OVCP] *Hitelesítési rend*nek, amennyiben a *Tanúsítvány*ban feltüntetésre kerül a szervezet neve.
- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [13] szabványban definiált [IVCP] *Hitelesítési rend*nek, amennyiben a *Tanúsítvány*ban feltüntetésre kerül a természetes személy neve.

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.

	[LCP]	[DVCP]	[OVCP]	[IVCP]
HWJSN	(x)		X	
KWJSN	(x)		X	
KWTSN	(x)			X
AWxSN	(x)	X		

1.2.2. Hatály

Tárgyi hatály

A *Szolgáltatási szabályzat* az 1.3.1. fejezetben ismertetett szolgáltatások nyújtására és igénybevételére vonatkozik.

Időbeli hatály

A *Szolgáltatási szabályzat* jelen verziója 2019-12-12

-i hatálybalépési dátumtól visszavonásig hatályos. A hatályosság automatikusan megszűnik a szolgáltatások beszüntetésekor vagy a *Szolgáltatási szabályzat* újabb verziójának hatályba lépésekor.

Személyi hatály

A *Szolgáltatási szabályzat* személyi hatálya kiterjed az 1.3. alfejezetben azonosított közösség minden tagjára.

Területi hatály

A jelen *Szolgáltatási szabályzat* a magyar jog alapján Magyarországon nyújtott szolgáltatásokra vonatkozó konkrét követelményeket tartalmaz.

A *Hitelesítés-szolgáltató* kiterjesztheti a szolgáltatás területi hatályát, ez esetben a *Szolgáltatási szabályzat* előírásainak megfelelő, azoknál nem enyhébb követelményeket alkalmaz. A külföldi *Ügyfel*ek számára nyújtott szolgáltatások *Szolgáltatási szabályzat*tól eltérő részletes feltételeit egyedi Szolgáltatási szerződésben szabályozhatja.

1.2.3. Biztonsági szintek

A *Hitelesítés-szolgáltató* a vonatkozó követelmények figyelembevételével biztonsági szinteket határozott meg az alábbiak szerint.

A *Tanúsítvány Alany* autentikáció erőssége alapján csökkenő sorrendben:

- minősített *Tanúsítvány*ok [M****];
- nem minősített, e-Szignó Hitelesítés Szolgáltató által kiadott III. hitelesítési osztályba tartozó *Tanúsítvány*ok [H****];
- nem minősített, e-Szignó Hitelesítés Szolgáltató által kiadott II. hitelesítési osztályba tartozó *Tanúsítvány*ok [K****];
- nem minősített, nem e-Szignó Hitelesítés Szolgáltató által kiadott *Tanúsítvány*ok.

A használt hordozó alapján a biztonság szerint csökkenő sorrendben:

- *Minősített elektronikus aláírást létrehozó eszköz*ön kibocsátott *Tanúsítvány*ok [***B*];
- *Hardver kriptográfiai eszköz*ön kibocsátott *Tanúsítvány*ok [***H*];
- egyéb módon, pl. szoftveresen kibocsátott *Tanúsítvány*ok [***S*].

A két szempont figyelembevételével a *Hitelesítés-szolgáltató* az alábbi összesített sorrendet állapította meg a biztonság szerint csökkenő sorrendben:

- minősített, *Minősített elektronikus aláírást létrehozó eszköz*ön kibocsátott *Tanúsítvány*ok [M**B*];
- minősített, *Hardver kriptográfiai eszköz*ön kibocsátott *Tanúsítvány*ok [M**H*];
- minősített, egyéb módon, pl. szoftveresen kibocsátott *Tanúsítvány*ok [M**S*];
- nem minősített, e-Szignó Hitelesítés Szolgáltató által kiadott III. hitelesítési osztályba tartozó *Tanúsítvány*ok [H**S*];
- nem minősített, e-Szignó Hitelesítés Szolgáltató által kiadott II. hitelesítési osztályba tartozó *Tanúsítvány*ok [K**S*];
- nem minősített, nem e-Szignó Hitelesítés Szolgáltató által kiadott *Tanúsítvány*ok.

A *Hitelesítés-szolgáltató* az *Ügyfel*ekkel való kommunikáció során támogatja az elektronikus csatornák használatát és a lehető legtöbb ügy intézése során lehetővé teszi az elektronikus aláírás használatát.

Általános szabály, hogy a *Tanúsítvány*okkal kapcsolatos ügyek intézése során az *Ügyfél* saját aláíró *Tanúsítvány*át is használhatja az elektronikus dokumentumok hitelesítésére, amennyiben annak fenti lista szerinti biztonsági besorolása nem alacsonyabb az ügyintézés alá eső *Tanúsítvány*énál.

A *Hitelesítés-szolgáltató* egyedi elbírálás alapján speciális esetekben, egyes részfeladatok tekintetében eltérhet a fenti lista szigorú alkalmazásától (pl. a III. hitelesítési osztályba tartozó *Tanúsítvány*okhoz tartozó kezdeti személyes azonosítást új minősített *Tanúsítvány* igénylése vagy a meglévő módosítása esetén az azonos azonosítási eljárási szabályok következtében elfogadja a minősített *Tanúsítvány*nál megkövetelt azonosításnak is).

1.3. PKI szereplők

A jelen *Szolgáltatási szabályzat* keretei között nyújtott szolgáltatásokat alkalmazó közösség az alábbiakból áll:

- a Microsec e-Szignó Hitelesítés Szolgáltató,
- a Microsec e-Szignó Hitelesítés Szolgáltató *Ügyfel*ei (*Előfizető*k és *Alany*ok),
- *Érintett felek*,
- egyéb szereplők.

1.3.1. Hitelesítés-szolgáltató

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`

Az ügyfélszolgálati iroda elérhetősége:

A szolgáltató egység neve:	e-Szignó Hitelesítés Szolgáltató
Ügyfélszolgálati iroda:	
	1033 Budapest, Ángel Sanz Briz út 13., Graphisoft Park Déli Terüet, 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 Déli Terület, 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.

A Szolgáltató bemutatása

A Microsec zrt. a 910/2014/EU rendelet [1] (továbbiakban: eIDAS) szerinti EU minősített bizalmi szolgáltató.

A Microsec zrt. (illetve jogelődje, a Microsec Kft.) az elektronikus aláírással kapcsolatos szolgáltatásainak nyújtását a 2001. évi XXXV. törvény [4] (továbbiakban: Eat.) hatálya alatt indította el:

- 2002. május 30-tól kezdve nyújt az Eat. szerinti nem minősített elektronikus aláírás hitelesítés-szolgáltatást, időbélyegzés szolgáltatást és aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatást (regisztrációs szám: MH 6834 1/2002);
- 2005. május 15-től kezdve nyújt az Eat. szerinti minősített hitelesítés-szolgáltatást, időbélyegzés szolgáltatást és aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatást;
- 2007. február 1-től kezdve nyújt az Eat. szerinti minősített elektronikus archiválás szolgáltatást (a nyilvántartásba vételről szóló határozat ügyiratszáma: HL-3549- 2/2007).

2016. július 1-én az eIDAS és az azt kiegészítő 2015. évi CCXXII törvény [8] hatálybalépésével európai szinten egységesen megváltozott az elektronikus aláírással kapcsolatos szolgáltatások teljes rendszere.

A Microsec 2016. július 1-jétől nyújtja eIDAS Rendelet szerinti nem minősített bizalmi szolgáltatásait, valamint elindította természetes személyek számára az eIDAS Rendelet szerinti minősített aláíró tanúsítványok kibocsátását.

Microsec 2016. december 20-ától nyújtja az alábbi eIDAS Rendelet szerinti minősített bizalmi szolgáltatásait:

- minősített elektronikus bélyegző tanúsítványok kibocsátása
- minősített elektronikus időbélyegzés
- minősített elektronikus archiválás.

Microsec 2019. január 2-ától nyújtja az alábbi eIDAS Rendelet szerinti minősített bizalmi szolgáltatást:

- minősített weboldal hitelesítő tanúsítvány kibocsátás.

Minőség és információbiztonság

A Microsec kiemelten fontosnak tartja *Ügyfel*ei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a *Hitelesítés-szolgáltató* ISO 9001 szabványnak megfelelő minőségirányítási rendszert üzemeltet 2002. január 23. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A Microsec nagy figyelmet fordít az általa üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a ISO/IEC 27001-nek megfelelő információbiztonság-irányítási rendszert (korábban BS 7799) üzemeltet 2003. május 19. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A minőségirányítási rendszer és az információbiztonság-irányítási rendszer hatóköre kiterjed a Microsec által nyújtott bizalmi szolgáltatásokra is.

A Microsec kétszintű kockázatelemzése az információ technológiai kockázatokon túlmenően kiterjed a teljes szervezetre és az üzleti kockázatokra is. A kockázatelemzés legalább évente felülvizsgálatra kerül. A kockázatelemzés eredménye alapján a *Hitelesítés-szolgáltató*

- intézkedéseket hoz a feltárt sérülékenységek megszüntetésére, és/vagy
- elfogadja az azonosított maradvány kockázatokat a döntés indokainak rögzítésével.

A *Hitelesítés-szolgáltató* honlapján minden érintett fél számára elérhetővé teszi Információbiztonsági Politikáját az alábbi linken:

`https://www.microsec.hu/hu/biztonsagi-garanciak`

Az Információbiztonsági politika minden változása ily módon kerül publikálásra a web oldalon keresztül.

A *Hitelesítés-szolgáltató* azok bizalmas jellege miat nem hozza nyilvánosságra belső Biztonsági szabályzatait. Alvállalkozót, szerződéses partnereit és az egyéb érintett feleket a szerződés megkötésekor a szükséges mértékben tájékoztatja a rájuk vonatkozó biztonsági szabályokról.

Hitelesítés-szolgáltatást nyújtó üzletág

A Microsec szervezetén belül önálló üzleti egységként működő e-Szignó Hitelesítés Szolgáltató látja el a *Tanúsítvány*ok előállítását és menedzsmentjét, a tanúsítványtár és tanúsítvány-visszavonási állapot információk közzétételét, az *Elektronikus aláírást létrehozó eszköz*ök menedzselését és rendelkezésre bocsátását, valamint az online tanúsítvány-állapot szolgáltatást. A szabályzatok menedzselésével kapcsolatos feladatokat is ez a szervezeti egység látja el. Az e-Szignó Hitelesítés Szolgáltató rendelkezik saját *Regisztráló szervezet*tel.

Szolgáltatások

A *Hitelesítés-szolgáltató* az eIDAS Rendelet [1] által meghatározott alábbi bizalmi szolgáltatásokat nyújthatja az *Előfizető* számára jelen *Szolgáltatási szabályzat* keretében:

- weboldal hitelesítésére szolgáló tanúsítványok kibocsátása

A(z) weboldal hitelesítésére szolgáló tanúsítványok kibocsátása szolgáltatás

A *Hitelesítés-szolgáltató* weboldal hitelesítésére szolgáló tanúsítványok kibocsátása szolgáltatás nyújtása érdekében az *Előfizető*vel Szolgáltatási szerződést köt, amelynek keretében az *Előfizető* által meghatározott *Alany*ok számára *Tanúsítvány*(oka)t bocsát ki. A *Tanúsítvány* hitelesen összekapcsolja az azonosított *Alany* adatait és az általa birtokolt magánkulcshoz tartozó nyilvános kulcsot. Egy Szolgáltatási szerződés keretében több *Alany*nak és több *Tanúsítvány* is kibocsátható.

Weboldal-hitelesítő tanúsítvány esetében az *Alany* a webszerver, amit a *Tanúsítvány*ban feltüntetett doménnév vagy IP cím azonosít. Az *Igénylő* az a természetes személy, aki az adott *Tanúsítvány* igénylése során eljár.

Az érvényes előfizetéssel rendelkező *Igénylő* a következő műveleteket kezdeményezheti:

- az *Igénylő Tanúsítvány*t igényelhet a *Hitelesítés-szolgáltató*tól, a *Tanúsítvány* kibocsátása valamely *Hitelesítési rend* vagy rendek szerint történik;
- az *Igénylő* kérheti a *Tanúsítvány*a visszavonását;

Az *Előfizető* is kérheti a hozzá tartozó *Alany Tanúsítvány*ának visszavonását. Ezen műveleteket az *Előfizető* által erre feljogosított és a *Hitelesítés-szolgáltató*nál bejelentett ún. *Szervezeti ügyintéző* is kérheti.

A *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*ok visszavonási állapotát tartalmazó *Tanúsítvány visszavonási list*ákat nyilvánosan elérhetővé teszi. A *Hitelesítés-szolgáltató* magát a *Tanúsítvány*t is nyilvánosságra hozza, amennyiben az *Igénylő* ehhez hozzájárul. A visszavont és a lejárt *Tanúsítvány* érvénytelen.

A *Hitelesítés-szolgáltató* a rendszerének tesztelése céljából teszt tanúsítványokat is kibocsát. A teszt tanúsítványokhoz nem fűződik semmilyen joghatás.

A *Hitelesítés-szolgáltató* külön kérésre egyedi elbírálás alapján az éles rendszerében is kibocsáthat ingyenes *Tanúsítvány*okat tesztelési célból. Az ily módon kibocsátott *Tanúsítvány*ok használata során különös gondossággal kell eljárni, mert azokhoz az éles *Tanúsítvány*okkal megegyező joghatás társul.

Tanúsítványfajták

A jelen *Szolgáltatási szabályzat*ban támogatott *Hitelesítési rend*eket az 1.2.1. fejezet 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* a benne szereplő doménnév vagy IP cím valamely *Szervezet*hez való tartozását mutatja. Ilyen esetben a *Tanúsítvány* "O" mezejében a *Szervezet* neve feltüntetésre kerül. *Weboldal-hitelesítő tanúsítvány*ban kizárólag olyan *Szervezet* neve tüntethető fel, amely a domén vagy IP cím jogos használója, tulajdonosa, vagy az előbbiek által erre feljogosított szervezet.

- *Weboldal-hitelesítő tanúsítvány* soha nem lehet álneves.

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.

Teszt tanúsítványok

A *Hitelesítés-szolgáltató* – egyrészt saját rendszerének tesztelése céljából, másrészt azért, hogy harmadik felek tesztelhessék a szolgáltatásokat – teszt tanúsítványokat is kibocsát. A

teszt tanúsítványokhoz semmilyen joghatás nem tartozik, és a *Hitelesítés-szolgáltató* sem kibocsátásukért, sem felhasználásukért, sem a hozzájuk kapcsolódó szolgáltatások rendelkezésre állásáért nem vállal felelősséget.

A *Hitelesítés-szolgáltató* az éles szolgáltatást nyújtó legfelső szintű (gyökér) *Hitelesítő egység* alatt nem bocsát ki teszt tanúsítványt.

A teszt tanúsítványok kibocsátása a külön erre a célra létrehozott és üzemeltetett "Microsec e-Szigno Test Root CA 2008" gyökér alatt történik.

A *Hitelesítés-szolgáltató* a teszt tanúsítványokat a "Certificate Policies" mezőben is jelzi az alábbiak szerint (lásd 7.1.2):

- az 1.3.6.1.4.1.21528.2.1.1.9 OID-t tünteti fel a *Tanúsítvány*ban *Hitelesítési rend*ként, vagy
- az 1.3.6.1.4.1.21528.2.1.1.100 OID-t tünteti fel a *Tanúsítvány*ban *Hitelesítési rend*ként, vagy
- semmilyen *Hitelesítési rend*et nem tüntet fel a *Tanúsítvány*ban.

Hitelesítő egységek

Az alábbiakban az e-Szignó Hitelesítés Szolgáltató rendszerében megjelenő, jelen *Szolgáltatási szabályzat* hatálya alá tartozó *Hitelesítő egység*eit mutatjuk be. A *Hitelesítés-szolgáltató* tanúsítvány-hierarchiájáról a

`https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/szolgaltatoi-tanusitvanyok.html`

weboldalon található további információ.

Aktív, SHA-256 alapú RSA hierarchia

- "Microsec e-Szigno Root CA 2009" – Gyökér hitelesítő egység

  SHA-256 alapú *Tanúsítvány*okat bocsát ki a *Hitelesítés-szolgáltató Hitelesítő egység*ei részére. E *Hitelesítő egység* önhitelesített tanúsítvánnyal (SHA-256 alapú) rendelkezik.

- "Online e-Szigno SSL CA 2016"

  Ezen egység kizárólag automatikusan bocsát ki nem minősített *Weboldal-hitelesítő tanúsítvány*okat. A "Microsec e-Szigno Root CA 2009" hitelesíti felül. Ezen egység nem bocsát ki álneves *Tanúsítvány*t.

- "e-Szigno SSL CA 2014"

  Ezen egység kizárólag a III. hitelesítési osztály szerinti *Weboldal-hitelesítő tanúsítvány*okat és hálózati azonosításra használt *Tanúsítvány*okat bocsát ki. A "Microsec e-Szigno Root CA 2009" hitelesíti felül. Ezen egység nem bocsát ki álneves *Tanúsítvány*t.

- "Class2 e-Szigno SSL CA 2016"

  Ezen egység kizárólag a II. hitelesítési osztály szerinti *Weboldal-hitelesítő tanúsítvány*okat és hálózati azonosításra használt *Tanúsítvány*okat bocsát ki. A "Microsec e-Szigno Root CA 2009" hitelesíti felül. Ezen egység nem bocsát ki álneves *Tanúsítvány*t.

- OCSP válaszadók

  Minden SHA-256 alapú tanúsítvánnyal rendelkező *Hitelesítő egység* külön, dedikált OCSP válaszadó egységet hitelesít felül, amely az adott *Hitelesítő egység* által kibocsátott *Tanúsítvány*ok visszavonási állapotára vonatkozóan ad választ. Az OCSP válaszadó egységek neve az adott *Hitelesítő egység* neve mögött az "OCSP Responder" szöveget tartalmazza. Az OCSP válaszadók *Tanúsítvány*ában "OCSPSigning" kiterjesztett kulcshasználat szerepel.

A fenti egységek SHA-256 alapú tanúsítvánnyal rendelkeznek, és SHA-256 alapú *Tanúsítvány*okat, illetve OCSP válaszokat bocsátanak ki. A fenti hierarchiában minden szolgáltatói és végfelhasználói RSA kulcs legalább 2048 bites.

Legújabb, ECC alapú hierarchia

- "e-Szigno Root CA 2017" – Gyökér hitelesítő egység

  ECC alapú *Tanúsítvány*okat bocsát ki a *Hitelesítés-szolgáltató Hitelesítő egység*ei részére. E *Hitelesítő egység* önhitelesített tanúsítvánnyal (ECC alapú) rendelkezik.

- "e-Szigno Online SSL CA 2017"

  Ezen egység kizárólag automatikusan bocsát ki nem minősített *Weboldal-hitelesítő tanúsítvány*okat. Az "e-Szigno Root CA 2017" hitelesíti felül. Ezen egység nem bocsát ki álneves *Tanúsítvány*t.

- "e-Szigno Class3 SSL CA 2017"

  Ezen egység kizárólag a III. hitelesítési osztály szerinti *Weboldal-hitelesítő tanúsítvány*okat és hálózati azonosításra használt *Tanúsítvány*okat bocsát ki. Az "e-Szigno Root CA 2017" hitelesíti felül. Ezen egység nem bocsát ki álneves *Tanúsítvány*t.

- "e-Szigno Class2 SSL CA 2017"

  Ezen egység kizárólag a II. hitelesítési osztály szerinti *Weboldal-hitelesítő tanúsítvány*okat és hálózati azonosításra használt *Tanúsítvány*okat bocsát ki. Az "e-Szigno Root CA 2017" hitelesíti felül. Ezen egység nem bocsát ki álneves *Tanúsítvány*t.

- OCSP válaszadók

  Minden ECC alapú tanúsítvánnyal rendelkező *Hitelesítő egység* külön, dedikált OCSP válaszadó egységet hitelesít felül, amely az adott *Hitelesítő egység* által kibocsátott *Tanúsítvány*ok visszavonási állapotára vonatkozóan ad választ. Az OCSP válaszadó egységek neve az adott *Hitelesítő egység* neve mögött az "OCSP Responder" szöveget tartalmazza. Az OCSP válaszadók *Tanúsítvány*ában "OCSPSigning" kiterjesztett kulcshasználat szerepel.

A fenti egységek mindegyike ECC alapú tanúsítvánnyal rendelkezik.

A fenti hierarchiában minden végfelhasználói RSA kulcs legalább 2048 bites.

Szolgáltatói *Gyökér tanúsítvány*ok közzététele

A *Hitelesítés-szolgáltató* a "Microsec e-Szigno Root CA 2009" gyökér *Tanúsítvány*ának lenyomatát az Expressz 2010. június 17-ei számában tette közzé. Valamennyi *Gyökér tanúsítvány* elérhető az e-Szignó Hitelesítés Szolgáltató honlapján keresztül.

- A "Microsec e-Szigno Root CA 2009" *Gyökér tanúsítvány*ának SHA-1 lenyomata[1]:
  `89 df 74 fe 5c f4 0f 4a 80 f9 e3 37 7d 54 da 91 e1 01 31 8e`,
  ugyanezen tanúsítvány SHA-256 lenyomata:
  `3c 5f 81 fe a5 fa b8 2c 64 bf a2 ea ec af cd e8 e0 77 fc 86 20 a7 ca e5 37 16 3d f3 6e db f3 78`
- Az "e-Szigno Root CA 2017" *Gyökér tanúsítvány*ának SHA-1 lenyomata:
  `89 d4 83 03 4f 9e 9a 48 80 5f 72 37 d4 a9 a6 ef cb 7c 1f d1`,
  ugyanezen tanúsítvány SHA-256 lenyomata:
  `be b0 0b 30 83 9b 9b c3 2c 32 e4 44 79 05 95 06 41 f2 64 21 b1 5e d0 89 19 8b 51 8a e2 ea 1b 99`

A "Microsec e-Szigno Root CA 2009" *Gyökér tanúsítvány*át tartalmazzák illetve terjesztik az alábbi megbízhatótanúsítvány-tárak:

- Microsoft Windows tanúsítványtár,
- Network Security Services (NSS) tanúsítványtár,
- Google Android v2.3 (Gingerbread) változatától,
- Apple iOS 7.1.2 változatától.
- Apple Mac OS X 10.9.4 változatától.

Az "e-Szigno Root CA 2017" *Gyökér tanúsítvány* bejelentése és elfogadtatása a megbízhatótanúsítvány-tárakba folyamatban van.

További információ a

`https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/bongeszo-tamogatas.html`

oldalon található arról, hogy mely más böngészőprogramokban és tanúsítványtárakban szerepelnek alapértelmezetten a *Hitelesítés-szolgáltató Gyökér tanúsítvány*ai.

A *Hitelesítés-szolgáltató* többi saját *Tanúsítvány*a az önhitelesített *Gyökér tanúsítvány*ok alapján ellenőrizhető, ezért ezen *Tanúsítvány*okat a *Hitelesítés-szolgáltató* csak a honlapján teszi közzé. Amennyiben – jogszabály, vagy hitelesítés-szolgáltatók közötti szerződés vagy kölcsönös megegyezés keretében – a *Hitelesítés-szolgáltató* egyes *Hitelesítő egység*ei számára más hitelesítés-szolgáltató is bocsát ki *Tanúsítvány*t, a *Hitelesítés-szolgáltató* ezen *Tanúsítvány*okat is közzéteheti honlapján. A *Hitelesítés-szolgáltató* számára ilyen módon kibocsátott *Tanúsítvány*ok esetén a

[1] Ugyanezen gyökér (trust anchor) korábban másik tanúsítvánnyal működött. A korábbi *Gyökér tanúsítvány* SHA-1 lenyomata: `a6 5c b4 73 3d 94 a5 c8 65 a8 64 64 7c 2c 01 27 2c 89 b1 43`, és az SHA-256 lenyomata: `8e 8c 6e bf 77 dc 73 db 3e 38 e9 3f 48 03 e6 2b 6b 59 33 be b5 1e e4 15 2f 68 d7 aa 14 42 6b 31`. E lenyomatokat a *Hitelesítés-szolgáltató* a Magyar Hírlap 2009. június 22-ei számában tette közzé. A gyökér korábbi *Gyökér tanúsítvány*a szerint ellenőrzött *Tanúsítvány*ok és aláírások szintén érvényesnek tekinthetőek.

Hitelesítés-szolgáltató vállalja, hogy a *Hitelesítés-szolgáltató*t felül- vagy kereszthitelesítő másik szolgáltató hitelesítési rendjét betartja, és az ezen tanúsítvánnyal kapcsolatban benne foglaltakat magára nézve kötelezőnek ismeri el.

A szolgáltatói *Tanúsítvány*ok lejárta előtt a *Hitelesítés-szolgáltató* új szolgáltatói kulcsokat generál, illetve új *Hitelesítő egység*eket indít, és megteszi a szükséges lépéseket, hogy a szolgáltatói *Tanúsítvány*ok változása ne veszélyeztesse a szolgáltatások folytonosságát.

Láncolt hitelesítés-szolgáltatás

A *Hitelesítés-szolgáltató* jogosult láncolt hitelesítés-szolgáltatást nyújtani, amelynek keretében a *Hitelesítés-szolgáltató* valamely *Hitelesítő egység*e *Tanúsítvány*t bocsát ki egy másik hitelesítés-szolgáltató (továbbiakban: felülhitelesített hitelesítés-szolgáltató) irányítása alatt álló *Hitelesítő egység* számára.

Ezen felülhitelesítés a következő feltételekkel történik:

- A felülhitelesített hitelesítés-szolgáltatóval a *Hitelesítés-szolgáltató* szerződést köt, a felülhitelesítés pontos feltételeit e szerződés szabályozza. A felülhitelesített hitelesítés-szolgáltató maga köt szerződést a hozzá tartozó *Ügyfel*ekkel, e szerződésben a felülhitelesített hitelesítés-szolgáltató jelenik meg hitelesítés-szolgáltatóként.
- A *Hitelesítés-szolgáltató* teljes felelősséget vállal a láncolt hitelesítés-szolgáltató tevékenységéért.
- A felülhitelesített hitelesítés-szolgáltató kizárólag valamely jól definiált kör részére bocsáthat ki *Tanúsítvány*t.
- A felülhitelesített hitelesítés-szolgáltatónak nyilvánosságra kell hoznia a hitelesítési rendjét, és e hitelesítési rend szerint kell működnie.
- A *Hitelesítés-szolgáltató* jogosult rendszeresen ellenőrizni a felülhitelesített szolgáltató működését.
- A *Hitelesítés-szolgáltató* visszavonja a felülhitelesítés során kibocsátott *Tanúsítvány*t, amennyiben a felülhitelesített hitelesítés-szolgáltató nem felel meg saját hitelesítési rendjének, vagy amennyiben a felülhitelesített hitelesítés-szolgáltató jelzi, hogy a felülhitelesített szolgáltatói kulcsa kompromittálódott.
- Amennyiben a *Hitelesítés-szolgáltató* más hitelesítés szolgáltató számára bocsát ki szolgáltatói *Tanúsítvány*t, ezt bejelenti a Nemzeti Média- és Hírközlési Hatóságnak. Amennyiben a felülhitelesített szolgáltató belföldi és nyilvános körben használható *Tanúsítvány*okat bocsát ki, a felülhitelesített szolgáltató köteles a felülhitelesítést bejelenteni a Nemzeti Média- és Hírközlési Hatóságnak, és köteles kérni a nyilvántartásba vételét (amennyiben még nem szerepel a Nemzeti Média- és Hírközlési Hatóság nyilvántartásában). Más, alárendelt szolgáltatásként nyújtott elektronikus aláírással kapcsolatos szolgáltatásokra (pl. időbélyegzés) is ennek megfelelő szabályok vonatkoznak.

1.3.2. Regisztráló szervezetek

A *Hitelesítés-szolgáltató* a regisztrációt, a *Tanúsítvány*ok kibocsátásával kapcsolatos egyéb feladatokat, valamint a további tanúsítvány menedzsment feladatokat központilag, a saját szervezetén belül működő ügyfélszolgálati iroda keretében valósítja meg.
Az iroda feladatai:

- a végfelhasználói *Tanúsítvány*okban feltüntetett *Alany* regisztrációja,
- a *Tanúsítvány*ok kibocsátásához kapcsolódó adminisztrációs és regisztrációs tevékenység,
- az *Ügyfel*ekkel való kapcsolattartás (kérdések, bejelentések, kérelmek és panaszok fogadása, valamint feldolgozásának kezdeményezése),
- tanúsítvány műveletek (visszavonás, tanúsítvány megújítás, tanúsítvány módosítás és kulcscsere) elvégzése.

A *Hitelesítés-szolgáltató* által üzemeltetett ügyfélszolgálati iroda fogadja a különböző tanúsítvány műveletekre vonatkozó kérelmeket és kezdeményezi azok feldolgozását.
A *Regisztráló szervezet* a következő helyeken végezhet regisztrációs tevékenységet:

- a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában;
- a *Regisztráló szervezet* munkatársai kiszállhatnak az *Ügyfel*ekhez, és a helyszínen mobil regisztrációs tevékenységet végezhetnek a *Hitelesítés-szolgáltató* belső szabályzatai szerint.

1.3.3. Ügyfelek

A *Hitelesítés-szolgáltató* által nyújtott szolgáltatások *Ügyfel*ei:

- *Előfizető*
  - Szolgáltatási szerződést köt a *Hitelesítés-szolgáltató*val
  - elfogadja az Általános szerződési feltételeket
    ,
  - meghatározza az *Igénylő*k körét,
  - kijelölhet *Szervezeti ügyintéző*ket,
  - felelős a szolgáltatás igénybevételével kapcsolatos díjak megfizetéséért.
- *Igénylő*
  - az adott *Weboldal-hitelesítő tanúsítvány* igénylése során eljár

1.3.4. Érintett felek

Az *Érintett fél* nem feltétlenül áll szerződéses viszonyban a *Hitelesítés-szolgáltató*val. A tevékenységére vonatkozó ajánlásokat a *Szolgáltatási szabályzat* 4.5.2, 4.9.6, 9.6.4 és 9.9.3 fejezetei és az abban megnevezett egyéb szabályzatok tartalmazzák.
A *Hitelesítés-szolgáltató* az *Érintett fél*lel elsősorban az internetes honlapon keresztül tart kapcsolatot.

1.3.5. Egyéb szereplők

Amennyiben a *Tanúsítvány* egy *Szervezet* tevékenységének érdekében történő felhasználás céljából kerül kibocsátásra az *Igénylő* részére, akkor a *Képviselt szervezet* a szóban forgó *Szervezet*, amely szintén megjelölésre kerül a *Tanúsítvány*ban.

1.4. A tanúsítvány felhasználhatósága

1.4.1. Megfelelő tanúsítvány használat

A *Hitelesítés-szolgáltató* által jelen *Szolgáltatási szabályzat* alapján kibocsátott végfelhasználói *Tanúsítvány*okhoz tartozó magánkulcsok kizárólag webszerverek azonosítására használhatók fel.

1.4.2. Tiltott tanúsítvány használat

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

1.5. A dokumentum adminisztrálása

1.5.1. A dokumentum adminisztrációs szervezete

Jelen *Szolgáltatási szabályzat* adminisztrációját ellátó szervezet adatai az alábbi táblázatban találhatók:

Szervezet neve	Microsec e-Szignó Hitelesítés Szolgáltató
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13. C épület
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
Email cím	info@e-szigno.hu

1.5.2. Kapcsolattartó személy

Jelen *Szolgáltatási szabályzat*tal kapcsolatos kérdésekben közvetlenül az alábbi személyhez lehet fordulni:

Kapcsolattartó	Folyamatszervezés részleg vezetője
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13. C épület
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
Email cím	info@e-szigno.hu

1.5.3. A Szolgáltatási szabályzat *Hitelesítési rend*nek való megfelelőségéért felelős személy/szervezet

Egy *Szolgáltatási szabályzat*nak a benne meghivatkozott *Hitelesítési rend*nek való megfelelőségéért és az abban foglaltak szerinti szolgáltatás nyújtásáért az adott *Szolgáltatási szabályzat*ot kibocsátó szolgáltató a felelős.

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/`

1.5.4. A Szolgáltatási szabályzat elfogadási eljárása

A *Szolgáltatási szabályzat* új verziójának illetve tetszőleges módosításának megírása, elfogadása és kibocsátása egységes folyamatok szerint – a 9.12.1 fejezetben részletezett módon – történik.

1.6. Fogalmak és rövidítések

1.6.1. Fogalmak

II. hitelesítési osztály	Olyan nem minősített *Hitelesítési rend*ek csoportja, amelyek az *Igénylő* távoli regisztrációja alapján is lehetővé teszik a *Tanúsítvány* kibocsátását.
III. hitelesítési osztály	Olyan nem minősített *Hitelesítési rend*ek csoportja, amelyek a *Tanúsítvány* kibocsátását az *Igénylő* személyes regisztrációjához kötik.
Adatközpont	Számítógépes rendszerek és a hozzájuk kapcsolódó komponensek elhelyezésére és üzemeltetésére kialakított létesítmény. Ezek a komponensek rendszerint magukba foglalják a távközlési rendszereket és kommunikációs kapcsolatokat, redundáns áramforrást, adattárolókat, légkondicionáló, tűzvédelmi és biztonsági rendszereket.
Alany (Subject)	*Weboldal-hitelesítő tanúsítvány* esetében az *Alany* a webszerver, amelyet a doménnév vagy IP cím azonosít.
Alany szolgáltatói egyedi azonosítója	A *Hitelesítés-szolgáltató* által az *Alany* számára adott egyedi azonosító. Az azonosító a *Tanúsítvány* "Subject DN Serial Number" mezőjében szerepel, a 3.1.1. fejezetben meghatározott követelmények szerint.

Bizalmi felügyelet	"A *Bizalmi szolgáltatás*ok felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [8] 91.§ 1. bekezdés)
Bizalmi szolgáltatás (Trust Service)	"Rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások: • elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy • *Weboldal-hitelesítő tanúsítvány*ok létrehozása, ellenőrzése és érvényesítése; vagy • elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése; " (eIDAS [1] 3. cikk 16. pont)
Bizalmi szolgáltatási rend (Trust Service Policy)	"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. " (2015. évi CCXXII. törvény [8] 1. § 8. pont)
Bizalmi szolgáltató (Trust Service Provider)	"Egy vagy több *Bizalmi szolgáltatás*t nyújtó természetes vagy jogi személy; a *Bizalmi szolgáltató* lehet minősített vagy nem minősített *Bizalmi szolgáltató*." (eIDAS [1] 3. cikk 19. pont)
Certificate Transparency (CT) naplószolgáltató	A Certificate Transparency [32] által definiált naplószolgáltató, amely a kibocsátott *Tanúsítvány*okat vagy az ahhoz tartozó *Előtanúsítvány*okat tárolja.
Elektronikus dokumentum	"Elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom." (eIDAS [1] 3. cikk 35. pont)
Elektronikus időbélyegző (Electronic Time Stamp)	"Olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban. " (eIDAS [1] 3. cikk 33. pont)

Előfizető (Subscriber)	A Szolgáltatóval valamely szolgáltatás igénybevétele érdekében Szolgáltatási szerződést kötő személy vagy szervezet.
Előtanúsítvány	A Certificate Transparency [32] által definiált aláírt adatstruktúra (PreCert), amely a kibocsátandó *Tanúsítvány*ban megjelenítendő, *Alany*ra vonatkozó adatokat tartalmazza.
Érintett fél (Relying Party)	Az a kommunikáló fél, aki egy weboldal elérésekor azonosítja a webszervert a *Weboldal-hitelesítő tanúsítvány*a alapján, továbbá azok a szoftvergyártók, akik olyan internet böngészőket vagy alkalmazásokat készítenek, amelyek működésük során *Weboldal-hitelesítő tanúsítvány*okat használnak.
Felfüggesztés	A *Tanúsítvány* érvényességének ideiglenes megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* felfüggesztése nem végleges, a felfüggesztett *Tanúsítvány* érvényessége visszaállítható.
Gyökér tanúsítvány (Root Certificate)	Más néven legfelső szintű tanúsítvány. Önhitelesített *Tanúsítvány*, amelyet adott *Hitelesítő egység* saját maga számára bocsátott ki, azaz saját magánkulcsával van aláírva, így a saját – a tanúsítványban szereplő – nyilvános kulcsával ellenőrizhető.
Hardver kriptográfiai eszköz (HSM: Hardware Security Module)	Egy olyan hardver alapú biztonságos eszköz, mely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására.
Hitelesítés-szolgáltató	Olyan *Bizalmi szolgáltató*, aki/amely a hitelesítés-szolgáltatás keretében azonosítja az igénylő személyét, *Tanúsítvány*t bocsát ki, nyilvántartásokat vezet, fogadja a *Tanúsítvány*okkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a *Tanúsítvány*hoz tartozó szabályzatokat, és a *Tanúsítvány* aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.
Hitelesítő egység	A *Hitelesítés-szolgáltató* rendszerének egy egysége, amely *Tanúsítvány*ok digitális aláírását végzi. Egy *Hitelesítő egység*hez mindig egy elektronikus aláírás vagy bélyegző létrehozásához használt adat (magánkulcs) tartozik. Előfordulhat, hogy egy *Hitelesítés-szolgáltató* egyszerre több *Hitelesítő egység*et is működtet.

Hitelesítési rend (Certificate Policy)	"Olyan *Bizalmi szolgáltatási rend*, amely *Bizalmi szolgáltatás* keretében kibocsátott *Tanúsítvány*ra vonatkozik." (2015. évi CCXXII. törvény [8] 1. § 24. pont)
Igénylő	Az a természetes személy, aki az adott *Tanúsítvány* igénylése során eljár.
Képviselt szervezet	Az a *Szervezet*, amelynek a nevében a *Szervezeti ügyintéző* eljár a *Szervezet*hez tartozó *Tanúsítvány*okkal kapcsolatos ügyekben.
Kompromittálódás	Egy kriptográfiai kulcs abban az esetben tekintendő kompromittálódottnak, ha vélelmezhető, hogy illetéktelen személynek is hozzáférése van hozzá.
Köztes hitelesítő egység	Olyan *Hitelesítő egység* amelynek *Tanúsítvány*át egy másik *Hitelesítő egység* bocsátotta ki.
Kriptográfiai kulcs (Cryptographic Key)	Olyan – kriptográfiai transzformációt vezérlő – egyedi digitális jelsorozat, amelynek ismerete szükséges titkosításhoz és dekódoláshoz, illetve digitális aláírás előállításához és ellenőrzéséhez.
Kulcsgondozás (Key Management)	A kriptográfiai kulcsok előállítása, a felhasználókhoz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, amely szoros kapcsolatban áll az alkalmazott biztonsági eljárásmóddal.
Magánkulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az *Igénylő*nek szigorúan titokban kell tartania. Webszerver azonosságának igazolása esetében a webszervernek a magánkulcsát kell használnia az azonosságát ellenőrző eljárás során. A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok kibocsátása során a *Hitelesítő egység* magánkulcsát használja arra, hogy a *Tanúsítvány*t védő elektronikus aláírást vagy bélyegzőt elhelyezze rajta.
Nemzetközi tartománynév (Internationalized Domain Name)	Olyan internetes tartománynév, aminek legalább egy címkéjét (a pontokkal elválasztott részek) az alkalmazások ASCII kódtáblán kívül eső karakterekkel mutatják – pl. "ékezet.example.com". Ezeket a tartományneveket az internetes névfeloldást végző DNS-ben a Punycode átírás segítségével ASCII karakterláncokként tárolják.

Nyilvános kulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. A nyilvánosságra hozatal jellemzően egy *Tanúsítvány* formájában történik, amely összekapcsolja a szereplő nevét az ő nyilvános kulcsával. Webszerver azonosságának igazolása esetében a webszervernek a nyilvános kulcsa szükséges ahhoz, hogy az azonosságát ellenőrizni lehessen. A *Tanúsítvány*ok hitelességét az őket kibocsátó *Hitelesítő egység* nyilvános kulcsa segítségével lehet ellenőrizni.
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	Aszimmetrikus kulcsú kriptográfiára épülő infrastruktúra, beleértve a kriptográfiai algoritmusokat, kulcsokat, tanúsítványokat, a rájuk vonatkozó szabványokat és jogszabályokat, a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.
Regisztrációs igény	A *Tanúsítványkérelem* és a szolgáltatói szerződés előkészítése céljából az *Ügyfél* által a Szolgáltatónak előzetesen megadott adatok és nyilatkozatok, amelyben többek között felhatalmazza a Szolgáltatót az adatok kezelésére.
Regisztráló szervezet (Registration Authority)	Szervezet, amely ellenőrzi a *Tanúsítvány*ba kerülő adatok valódiságát, az *Igénylő* személy azonosságát, ellenőrzi, hogy a *Tanúsítványkérelem* hiteles-e, és azt egy arra jogosult személy nyújtotta-e be.
Rendkívüli üzemeltetési helyzet	Olyan, a *Hitelesítés-szolgáltató* üzemmenetében zavart okozó rendkívüli helyzet, amikor a *Hitelesítés-szolgáltató* rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
SCT - Signed Certificate Timestamp	A CT naplószolgáltató által az *Előtanúsítvány* illetve a *Tanúsítvány* nyilvánosságra hozatalakor küldött aláírt válasz (az aláírt *Tanúsítvány* időbélyegzője), mely az *Előtanúsítvány* illetve a *Tanúsítvány* adott naplóba történő felvételét igazolja.
Szerver autentikációs tanúsítvány	Olyan *Tanúsítvány* amely egy adott szerver, vagy annak egy szolgáltatásának azonosítására szolgál. Az ilyen *Tanúsítvány*okban a CN mezőben egy adott doménnév vagy IP cím szerepel. Ilyenek például a CISCO VPN szerver, domén kontroller, SCEP szerver, VPN szerver számára kiadott *Tanúsítvány*ok.
Szervezet	Jogi személy.

Szervezeti tanúsítvány	Olyan *Tanúsítvány*, amelyben szerepel a *Szervezet* megnevezése. Ilyen esetben a *Tanúsítvány* "O" mezejében a *Szervezet* neve feltüntetésre kerül.
Szervezeti ügyintéző	Az *Előfizető* képviseletében eljáró természetes személy, aki jogosult az *Előfizető* nevében a *Tanúsítványkérelem* benyújtására, a *Tanúsítvány* kibocsátás jóváhagyására, az *Előfizető*höz kapcsolódó *Tanúsítvány*ok igénylése, cseréje és visszavonása során eljárni.
Szolgáltatási szabályzat (Trust Service Practice Statement)	"A *Bizalmi szolgáltató* nyilatkozata az egyes *Bizalmi szolgáltatás*ok nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről. " (2015. évi CCXXII. törvény [8] 1. § 41. pont)
Szolgáltatási szerződés	"A *Bizalmi szolgáltató* és a *Bizalmi szolgáltatás*i ügyfél között létrejött szerződés, amely a *Bizalmi szolgáltatás* nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza. " (2015. évi CCXXII. törvény [8] 1. § 42. pont)
Tanúsítvány (Certificate)	"Az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a *Weboldal-hitelesítő tanúsítvány*, valamint mindazon, a *Bizalmi szolgáltatás* keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a tanúsítványra vonatkozó érvényesítési adatot és a tanúsítvány használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen. " (2015. évi CCXXII. törvény [8] 1. § 44.)
Tanúsítványkérelem	Az *Igénylő* által, a Szolgáltató számára a *Tanúsítvány* kibocsátás érdekében benyújtott adatok és nyilatkozatok, amelyekben többek között az *Igénylő* megerősíti a *Tanúsítvány*ba kerülő adatok valódiságát.
Tanúsítványtár	Különböző *Tanúsítvány*okat tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott *Tanúsítvány*okat publikálja, de Tanúsítványtárnak nevezzük az *Érintett fél* számítógépén a használt alkalmazás számára elérhető *Tanúsítvány*okat tartalmazó rendszert is.
Ügyfél	Az *Előfizető* és a hozzá tartozó összes *Igénylő* együttes elnevezése.

Visszavonás	A *Tanúsítvány* érvényességének megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* visszavonása végleges, visszavont *Tanúsítvány* többet nem tehető érvényessé.
Visszavonási állapot nyilvántartás	A *Hitelesítés-szolgáltató* által vezetett belső nyilvántartás a felfüggesztett, illetőleg a visszavont *Tanúsítvány*okról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját másodperc pontossággal.
Weboldal hitelesítő tanúsítvány (Certificate for Website Authentication)	"Olyan igazolás, amely lehetővé teszi a weboldal hitelesítését és a weboldalt ahhoz a természetes vagy jogi személyhez kapcsolja, akinek vagy amelynek részére a tanúsítványt kiállították. " (eIDAS [1] 3. cikk 38. pont) Egy *Weboldal-hitelesítő tanúsítvány*ban a név mezőben a webszerver doménneve vagy IP címe szerepel.
Wildcard doménnév	Olyan doménnév, amely egy csillag karakterből ("*"), az azt követő pont karakterből ("."), majd az azt követő teljes doménnévből (FQDN) áll.
Wildcard tanúsítvány	Olyan *Weboldal-hitelesítő tanúsítvány*, amely *Weboldal-hitelesítő tanúsítvány*ban feltüntetett bármely doménnév legelső pozícióján egy csillag ("*") karaktert tartalmaz.

1.6.2. Rövidítések

CA	Certification Authority	Hitelesítés-szolgáltató
CAA	Certification Authority Authorization	Hitelesítés-szolgáltató felhatalmazás
CP	Certificate Policy	Hitelesítési rend
CPS	Certification Practice Statement	Hitelesítés-szolgáltatási szabályzat
CRL	Certificate Revocation List	Tanúsítvány visszavonási lista
DVC	Domain Validation Certificate	Domén hitelesített tanúsítvány
DVCP	Domain Validation Certificate Policy	Domén hitelesített tanúsítási rend
eIDAS	electronic Identification, Authentication and Signature	A 910/2014/EU rendelet általánosan használt hivatkozása
FQDN	Fully Qualified Domain Name	teljesen minősített tartománynév vagy abszolút/teljes doménnév
IDN	Internationalized Domain Name	Nemzetközi tartománynév
IVC	Individual Validation Certificate	Személy hitelesített tanúsítvány
IVCP	Individual Validation Certificate Policy	Személy hitelesített tanúsítási rend
LDAP	Lightweight Directory Access Protocol	Protokoll címtár szolgáltatás eléréséhez
NMHH		Nemzeti Média- és Hírközlési Hatóság
OCSP	Online Certificate Status Protocol	Online tanúsítvány-állapot protokoll
OID	Object Identifier	Objektum azonosító
OVC	Organizational Validation Certificate	Szervezet hitelesített tanúsítvány
OVCP	Organizational Validation Certificate Policy	Szervezet hitelesített tanúsítási rend

PKI	Public Key Infrastructure	Nyilvános kulcsú infrastruktúra
QCP	Qualified Certificate Policy	Minősített hitelesítési rend
RA	Registration Authority	Regisztráló szervezet
TSP	Trust Service Provider	Bizalmi szolgáltató

2. Közzététel és tanúsítványtár

2.1. Adatbázisok - tanúsítványtárak

A *Hitelesítés-szolgáltató* a honlapján (https://www.e-szigno.hu) és LDAP protokollon (ldap://ldap.e-szigno.hu) keresztül is közzéteszi szolgáltatói *Tanúsítvány*ait, valamint az általa kibocsátott azon végfelhasználói *Tanúsítvány*okat, amelyek közzétételéhez az *Igénylő* hozzájárult.

A *Hitelesítés-szolgáltató* publikálja a működése alapjául szolgáló *Hitelesítési rend*et, *Szolgáltatási szabályzat*ot valamint a szerződési feltételeket tartalmazó egyéb dokumentumokat.

A *Hitelesítés-szolgáltató* biztosítja, hogy szolgáltatói *Tanúsítvány*ait, a *Tanúsítványtár*at és a visszavonási információkat közzétevő rendszer rendelkezésre állása éves szinten legalább 99%-os legyen és egy kiesés hossza legfeljebb 24 óra legyen.

A *Hitelesítés-szolgáltató* a weboldalán megadott Certificate Transparency naplószolgáltatókon keresztül közzéteszi azon *Előtanúsítvány*ait, amelyek közzétételéhez az *Igénylő* hozzájárult.

A *Hitelesítés-szolgáltató* a kiadott *Előtanúsítvány*okat nem tárolja a saját *Tanúsítványtár*ában és saját szolgáltatásai keretében nem publikálja azokat.

2.2. A tanúsítványokra vonatkozó információk közzététele

A *Hitelesítés-szolgáltató* közzéteszi a honlapján a

- szolgáltatói *Tanúsítvány*ait;
- a végfelhasználói *Tanúsítvány*okat, amennyiben a *Tanúsítvány*hoz tartozó *Igénylő* ehhez hozzájárul;

Szolgáltatói tanúsítványok

A *Hitelesítés-szolgáltató* az alábbi módszerekkel teszi közzé az általa működtetett hitelesítő egységek, valamint az online tanúsítvány-állapot szolgáltatásban részt vevő egységek *Tanúsítvány*ával kapcsolatos állapot információkat:

- A gyökér hitelesítő egységek megnevezését, illetve *Gyökér tanúsítvány*aik lenyomatát a *Szolgáltatási szabályzat*ban (lásd: 1.3.1. fejezet). Az állapotváltozásukkal kapcsolatos információk elérhetőek a *Hitelesítés-szolgáltató* honlapján.
- A köztes (nem gyökér) hitelesítő egységek *Tanúsítvány*ainak állapotváltozását nyilvánosságra hozza a *Tanúsítvány visszavonási list*ákon, saját honlapján, valamint az online tanúsítvány-állapot válasz szolgáltatás keretében.

- Az online tanúsítvány-állapot válaszokat aláíró válaszadók számára a *Hitelesítés-szolgáltató* – a legjobb nemzetközi gyakorlatnak megfelelően – rendkívül rövid érvényességi idejű (24 óraig érvényes) *Tanúsítvány*t bocsát ki, ezzel kiküszöbölve azt, hogy a *Tanúsítvány* visszavonási állapotát ellenőrizni kelljen.

  Minden OCSP válaszadói *Tanúsítvány* tartalmaz egy jelzést, miszerint a visszavonási állapotát nem kell ellenőrizni.

  Kulcs kompromittálódás vagy bármilyen egyéb probléma esetén az OCSP válaszokat aláíró régi magánkulcshoz nem kerül kibocsátásra újabb *Tanúsítvány*. A *Hitelesítés-szolgáltató* az OCSP válaszadói *Tanúsítvány*okat ezt követően új, biztonságos magánkulcshoz bocsátja ki. Az OCSP válaszok ellenőrzését bővebben az 4.5.2. fejezet tartalmazza.

Végfelhasználói tanúsítványok

A *Hitelesítés-szolgáltató* az általa kibocsátott végfelhasználói *Tanúsítvány*okkal kapcsolatos állapot információkat a következő módszerekkel teszi közzé:

- a *Tanúsítvány visszavonási list*ákon,
- az online tanúsítvány-állapot válasz szolgáltatás keretében.

A végfelhasználói *Tanúsítvány* visszavonási állapotát a *Hitelesítés-szolgáltató* nyilvánosságra hozza, ehhez nem szükséges az *Igénylő* hozzájárulása. Az állapot információk közlésének módszereit illetően lásd még a 4.10. fejezetet.

2.2.1. Szolgáltatói információ közzététele

A *Hitelesítés-szolgáltató* nyilvánosságra hozza szerződéses feltételeit és szabályzatait a honlapján elektronikus formában az alábbi linken:

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

A honlapon a hatálybalépés előtt publikálásra kerülnek a bevezetésre váró új dokumentumok.

A honlapon az érvényben levő dokumentumokon kívül elérhető valamennyi dokumentum összes korábbi verziója is.

A szabályzatok és szerződési feltételek aktuális verziója nyomtatott formában olvasható a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában.

A *Hitelesítés-szolgáltató* a szerződéskötést követően tartós adathordozón bocsátja az *Ügyfél* rendelkezésére a *Hitelesítési rend*et, a *Szolgáltatási szabályzat*ot és a Szolgáltatási szerződést.

A *Hitelesítés-szolgáltató* értesíti *Ügyfel*eit az Általános szerződési feltételek változásáról.

2.3. A közzététel időpontja vagy gyakorisága

2.3.1. Kikötések és feltételek közzétételi gyakorisága

A *Szolgáltatási szabályzat*tal kapcsolatos új verziók közzététele a 9.12. fejezetben ismertetett eljárásoknak megfelelően történik.

A *Hitelesítés-szolgáltató* szükség szerint hozza nyilvánosságra egyéb szabályzatait, szerződéses feltételeit, illetve azok újabb változatait.

A *Hitelesítés-szolgáltató* a rendkívüli információkat a jogszabályi előírásoknak megfelelően, – annak hiányában pedig szükség szerint – késedelem nélkül közzé teszi.

2.3.2. Tanúsítványok nyilvánosságra hozatalának gyakorisága

A *Hitelesítés-szolgáltató* az egyes *Tanúsítvány*ok nyilvánosságra hozatala kapcsán a következő gyakorlatot követi:

- az általa működtetett gyökér hitelesítő egységek *Tanúsítvány*ait a szolgáltatás megkezdését megelőzően teszi közzé;
- az általa működtetett köztes hitelesítő egységek *Tanúsítvány*ait a kibocsátást követően 5 munkanapon belül hozza nyilvánosságra;
- a *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítvány*ra vonatkozó *Előtanúsítvány*t a *Tanúsítvány* kibocsátását megelőzően hozza nyilvánosságra a Certificate Transparency naplószolgáltatókon keresztül;
- a *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítvány*okat a kibocsátást követően haladéktalanul megjeleníti a *Tanúsítványtár*ban az *Igénylő* hozzájárulása esetén.

2.3.3. A megváltozott visszavonási állapot közzétételének gyakorisága

A *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*okkal, valamint a szolgáltatói *Tanúsítvány*okkal kapcsolatos állapot információk az online tanúsítvány-állapot szolgáltatás keretén belül az állapotváltozást követően azonnal elérhetőek.

A *Tanúsítvány*ok állapotára vonatkozó információk a *Tanúsítványtár*ban és a *Tanúsítvány visszavonási list*ákon is megjelennek. A *Tanúsítvány visszavonási list*ák kibocsátási gyakoriságával kapcsolatos gyakorlatot a 4.10. fejezet tárgyalja.

2.4. A tanúsítványtár elérésének szabályai

A *Hitelesítés-szolgáltató* által közzétett *Tanúsítvány*ok és állapot információk nyilvánosak, bárki számára biztosított a hozzáférési lehetőség a közzététel sajátosságainak megfelelően.

A *Hitelesítés-szolgáltató* által közölt információkat kizárólag a *Hitelesítés-szolgáltató* egészítheti ki, törölheti vagy módosíthatja. A *Hitelesítés-szolgáltató* különböző védelmi mechanizmusokkal akadályozza meg az információk jogosulatlan módosítását.

3. Azonosítás és hitelesítés

3.1. Elnevezések

A fejezet az alkalmazott *Hitelesítési rend*eknek megfelelően kibocsátott *Tanúsítvány*okba kerülő adatokkal kapcsolatban tartalmaz követelményeket.

A *Tanúsítvány* alapmezői között található Kibocsátó azonosító (Issuer), illetve *Alany* azonosító (Subject) mezők megfelelnek az IETF RFC 5280 [27] illetve IETF RFC 6818 [29] ajánlások szerinti egyedi név formátum előírásainak, ezen kívül a *Hitelesítés-szolgáltató* támogatja a kiterjesztések között található Alternatív név mezők (Subject Alternative Names), (Issuer Alternative Names) kitöltését is.

A *Hitelesítés-szolgáltató* a *Tanúsítvány* mezők tartalmát a névformátumokra vonatkozó követelmények keretei között lerövidítheti, vagy egy adott névtípust többször is feltüntethet egy *Tanúsítvány*ban.

3.1.1. Név típusok

Az *Alany* megnevezése

A *Tanúsítvány* alanyának megnevezése (a "Subject" mező tartalma) a következő módon épül fel:

- commonName (CN) – OID: 2.5.4.3 – Az *Alany* neve

  A mezőben egy teljes doménnév vagy IP cím szerepel, amely megegyezik a "Subject Alternative Names" mezőben feltüntetett értékek valamelyikével.

  Mindig kitöltésre kerül.

  Csak létező és az *Igénylő* által jogosan használt doménnév vagy IP cím kerül feltüntetésre.

  Weboldal-hitelesítő tanúsítvány nem lehet álneves.

- Surname – OID: 2.5.4.4 – Természetes személy vezetékneve

  IVCP típusú *Weboldal-hitelesítő tanúsítvány* esetében a *Tanúsítvány*ban feltüntetett természetes személy vezetékneve kerül ebbe a mezőbe.

  DVCP és OVCP *Tanúsítvány* esetében nem kerül kitöltésre.

  *Weboldal-hitelesítő tanúsítvány*ban kizárólag a domén vagy IP cím mögött álló személy, vagy az előbbiek által erre feljogosított személy neve tüntethető fel, és csak akkor, ha az *Igénylő* ezt kéri. A jelen mezőben szereplő vezetéknevet a természetes személy teljes, a *Hitelesítés-szolgáltató* által a 3.2.3 fejezetben leírtak szerint ellenőrzött nevéből kell képezni.

- Given Name – OID: 2.5.4.42 – Természetes személy keresztneve

  IVCP típusú *Weboldal-hitelesítő tanúsítvány* esetében a *Tanúsítvány*ban feltüntetett természetes személy keresztneve kerül ebbe a mezőbe.

  DVCP és OVCP *Tanúsítvány* esetében nem kerül kitöltésre.

  *Weboldal-hitelesítő tanúsítvány*ban kizárólag a domén vagy IP cím mögött álló személy, vagy az előbbiek által erre feljogosított személy neve tüntethető fel, és csak akkor, ha az Igénylő ezt kéri. A jelen mezőben szereplő keresztnevet a természetes személy teljes, a *Hitelesítés-szolgáltató* által a 3.2.3 fejezetben leírtak szerint ellenőrzött nevéből kell képezni.

- Pseudonym (PSEUDO) – OID: 2.5.4.65 – Alany álneve

  Nem kerül kitöltésre.

- Serial Number – OID: 2.5.4.5 – Az *Alany* egyedi azonosítója

  A *Tanúsítvány*ban legalább egy kitöltött "Serial Number" mező szerepel, amely teljesíti az alábbi követelményeket, és ezáltal alkalmas arra, hogy az IETF RFC 4043 [25] ajánlás szerinti "Permanent Identifier" kiterjesztés használata esetén az *Alany* állandó azonosítójának részét képezze:

– az azonosító értéke a *Tanúsítvány*ban megnevezett, a *Hitelesítés-szolgáltató* által azonosított *Alany*hoz tartozik, és a *Hitelesítés-szolgáltató* rendszerén belül egyedi;
– a *Hitelesítés-szolgáltató* garantálja, hogy két általa kibocsátott *Tanúsítvány*ban kizárólag akkor szerepel megegyező azonosító érték, ha a két *Tanúsítvány* ugyanahhoz az *Alany*hoz tartozik.

E mező az *Alany* megnevezésének része, és nem azonos a *Tanúsítvány* IETF RFC 5280 által definiált sorozatszámával.

.

– A *Hitelesítés-szolgáltató* által az *Alany* számára adott egyedi azonosító OID formátumú: "1.3.6.1.4.1.21528.2.x.y.z"
  * Ebben az első számjegyek rögzítettek (1.3.6.1.4.1.21528.2: ez a *Hitelesítés-szolgáltató* saját globálisan egyedi azonosítója),
  * "x" a *Hitelesítés-szolgáltató* által kiosztott belső azonosító,
  * "y" a *Hitelesítés-szolgáltató* által kiosztott belső azonosító,
  * "z" egy automatikusan kiosztott, az adott "x.y" értékpáron belül egyedi sorszám.

  Így az "x.y.z" értékhármas a *Hitelesítés-szolgáltató* rendszerén belül az *Alany*t egyértelműen azonosítja.

  Mivel az azonosító első része a *Hitelesítés-szolgáltató*t globálisan egyedi módon, az azonosító fennmaradó része pedig az *Alany*t a *Hitelesítés-szolgáltató* rendszerén belül meghatározza, ezért a teljes azonosító az *Alany*t önmagában is globálisan egyedi módon azonosítja.

  Egy *Alany*hoz tartozhat több különböző OID, de egy OID csak egyetlen *Alany*hoz tartozhat. Az *Alany* minden esetben jogosult friss (még ki nem osztott) OID-t kérni.

  A *Hitelesítés-szolgáltató* kizárólag akkor ad két *Tanúsítvány*nak azonos OID-t, ha meggyőződött arról, hogy a két *Tanúsítvány*hoz tartozó *Alany* azonos.

  Weboldal-hitelesítő tanúsítvány esetén ez az OID a "Subject DN" mezőben megadott tulajdonost és a "Subject Alternative Names" mezőben megadott doménnév halmazt együttesen azonosítja egyedi módon.

– A *Tanúsítvány* tartalmazhat további "Serial Number" mezőket is. Az azonosító szerepelhet
  * az ETSI EN 319 412-1 5.1.3 fejezete szerinti formátumban (például: "TINHU-8123456790"),
  * (Név:Érték) formátumban (például: "Szig.szam:AAAAAA"), vagy
  * más, az *Ügyfel*ek által kért formátumban.

A "Serial Number" mezőben a *Hitelesítés-szolgáltató* – a szabványoknak megfelelően – nem használ ékezetes karaktereket.

- Organization (O) – OID: 2.5.4.10 – A *Szervezet* megnevezése

  OVCP *Tanúsítvány* esetében az "O" mezőben szerepel a *Szervezet* teljes vagy rövid neve, amelyet a *Hitelesítés-szolgáltató* a 3.2.2 fejezetben leírtak szerint ellenőrzött.

  DVCP és IVCP *Tanúsítvány* esetében nem kerül kitöltésre.

A mező csak abban az esetben kerül kitöltésre, ha az *Igénylő* ezt kéri (ekkor *Szervezeti tanúsítvány*ról beszélünk). Ebben a mezőben kizárólag olyan szervezet tüntethető fel, amely a domén használója, tulajdonosa, vagy az előbbiek által erre feljogosított szervezet.

Az *Igénylő* kérésére ebben a mezőben feltüntethető az *Igénylő* által jogosan használt védjegy, márkanév vagy DBA (Doing Business As) is.

Bizalmi szolgáltató számára kibocsátott szolgáltatói *Tanúsítvány* esetében az "O" mező a szolgáltatást nyújtó szervezet valódi nevét tartalmazza.

- Organization Identifier (OrgId) – OID: 2.5.4.97 – Szervezet azonosítója

  OVCP *Tanúsítvány* esetében az "O" mezőben feltüntetett *Szervezet* azonosítója kerül ebbe a mezőbe.

  Csak olyan adat kerül bele, amelyet a *Hitelesítés-szolgáltató* ellenőrzött.

  OVCP *Tanúsítvány* esetében a mező kitöltése opcionális.

  DVCP és IVCP *Tanúsítvány* esetében a mező nem tölthető ki.

- Organizational Unit (OU) – OID: 2.5.4.11 – Szervezeti egység elnevezése

  OVCP *Tanúsítvány* esetében az "O" mezőben feltüntetett szervezethez kapcsolódó szervezeti egység elnevezése, vagy védjegy vagy egyéb információ kerülhet ebbe a mezőbe.

  Csak olyan adat kerülhet bele, amelyet a *Hitelesítés-szolgáltató* ellenőrzött, és amire az adott *Szervezet*nek használati joga van.

  Az "OU" mező csak akkor kerülhet kitöltésre, ha az "O", "L" és "C" mezők is ki vannak töltve.

  Kitöltése opcionális.

  DVCP és IVCP *Tanúsítvány* – esetében nem kerül kitöltésre.

- CountryName (C) – OID: 2.5.4.6 – Ország azonosítója

  DVCP *Tanúsítvány* esetében a doménhez vagy IP címhez kapcsolódó ország, vagy ha ez nem egyértelműen eldönthető, akkor az *Igénylő* országának ISO 3166-1 [19] szerinti kétbetűs kódja.

  OVCP *Tanúsítvány* esetében az "O" mezőben szereplő *Szervezet* székhelye szerinti ország ISO 3166-1 [19] szerinti kétbetűs kódja.

  IVCP *Tanúsítvány* esetében az "SN" és "GN" mezőkben megnevezett természetes személy lakcíme szerinti ország ISO 3166-1 [19] szerinti kétbetűs kódja.

  Mindig kitöltésre kerül.

  Magyarország esetében a "C" mező értéke: "HU".

- Street Address (SA) – OID: 2.5.4.9 – Cím adatok

  Nem kerül kitöltésre.

- Locality Name (L) – OID: 2.5.4.7 – Településnév

  DVCP *Tanúsítvány* esetében nem kerül kitöltésre.

  OVCP *Tanúsítvány* esetében az "O" mezőben szereplő *Szervezet* székhelye szerinti település megnevezése.

IVCP *Tanúsítvány* esetében az "SN" és "GN" mezőkben megnevezett természetes személy lakcíme szerinti település megnevezése.

- State or Province Name – OID: 2.5.4.8 – Tagállam, tartomány elnevezése

  DVCP *Tanúsítvány* esetében nem kerül kitöltésre.

  OVCP *Tanúsítvány* esetében az "O" mezőben szereplő *Szervezet* székhelye szerinti tagállam vagy tartomány neve, vagy a "C" mezőben megadott ország teljes neve.

  IVCP *Tanúsítvány* esetében az "SN" és "GN" mezőkben megnevezett természetes személy lakcíme szerinti tagállam vagy tartomány neve, vagy a "C" mezőben megadott ország teljes neve.

  Kitöltése opcionális.

- Postal Code – OID: 2.5.4.17 – Irányítószám

  DVCP *Tanúsítvány* esetében nem kerül kitöltésre.

  OVCP *Tanúsítvány* esetében az "O" mezőben szereplő *Szervezet* székhelyének postai irányítószáma.

  IVCP *Tanúsítvány* esetében az "SN" és "GN" mezőkben megnevezett természetes személy lakcímének postai irányítószáma.

  Kitöltése opcionális.

- Title (T) – OID: 2.5.4.12 – Alany titulusa

  Nem kerül kitöltésre.

- Email address (EMAIL) – OID: 1.2.840.113549.1.9.1 – Az *Alany* email címe

  Nem kerül kitöltésre.

A jelen *Szolgáltatási szabályzat* szerint kibocsátott *Tanúsítvány*ok tartalmazhatnak a fentieken túl további – a hivatkozott *Hitelesítési rend*eknek megfelelő – "Subject DN" mezőket is. Ezekben csak ellenőrzött, szöveges értékek szerepelhetnek (nem szerepelhet adat hiányát jelző érték, pl. ".", "-" vagy " ").

Kiterjesztések

- Az Alany alternatív nevei - "Subject Alternative Names"

  A "Subject Alternative Names" mező nem kritikus kiterjesztésként szerepel a *Tanúsítvány*ban. Tartalma az alábbiak szerint kerül kitöltésre.

  A "Subject Alternative Names" mezőben mindig szerepel legalább egy bejegyzés.

  Minden bejegyzés vagy egy "dNSName", ami egy teljesen minősített doménnevet (FQDN) tartalmaz, vagy egy "iPAddress", ami egy szerver IP címét tartalmazza.

  A *Hitelesítés-szolgáltató* a *Tanúsítvány* kibocsátása előtt megbizonyosodik róla, hogy az *Igénylő* kontrollal rendelkezik az adott doménnév vagy IP cím felett, vagy a domén regisztráló illetve az IP cím kiadója felhatalmazta annak használatára.

  A "Subject Alternative Names" mező nem tartalmazhat lefoglalt IP címet vagy belső nevet.

A "dNSName" bejegyzésben nem szerepelhet aláhúzás (underscore "_") karaktert tartalmazó doménnév.

Wildcard doménnév használata engedélyezett.

A tanúsítványt kibocsátó hitelesítő egység megnevezése

A *Tanúsítvány*ok kibocsátójának azonosítója ("Issuer" mező) a következő módon épül fel:

- commonName (CN) – OID: 2.5.4.3
  A *Tanúsítvány*t kibocsátó hitelesítő egység angol nyelvű megnevezése (lásd: 1.3.1. fejezet).
- Organization (O) – OID: 2.5.4.10
  "Microsec Ltd."
  A *Hitelesítés-szolgáltató* neve angolul, ékezet nélkül.
- Organization Identifier (OrgId) – OID: 2.5.4.97
  Kitöltése opcionális.
- Organizational Unit (OU) – OID: 2.5.4.11
  Nem kerül kitöltésre.
- Locality (L) – OID: 2.5.4.7
  "Budapest"
  A *Hitelesítés-szolgáltató* székhelye szerinti város neve ékezet nélkül.
- CountryName (C) – OID: 2.5.4.6
  "HU"
  A *Hitelesítés-szolgáltató* székhelye szerinti ország kétbetűs kódja.
- Email address (EMAIL) – OID: 1.2.840.113549.1.9.1
  "info@e-szigno.hu"
  Kitöltése opcionális.

A *Tanúsítvány* kibocsátójának szolgáltatói *Tanúsítvány*ában, az alany azonosító mezőben ugyanezen adatok szerepelnek.

A tanúsítványt kibocsátó hitelesítő egység alternatív nevei

A végfelhasználói *Tanúsítvány*okban a kibocsátó alternatív nevei ("Issuer Alternative Names") mező nem kerül kitöltésre.

A végfelhasználói *Tanúsítvány* kibocsátójának szolgáltatói *Tanúsítvány*ában szereplő elnevezések:

- Az SHA-256 alapú szolgáltatói *Tanúsítvány*ok esetén az alternatív név mezőben legfeljebb csak az email cím ("rfc822Name") kerülhet kitöltésre.

3.1.2. A nevek értelmezhetősége

A "SubjectDN" mezőre a következő szabályok érvényesek:

- az azonosítónak értelmezhetőnek kell lennie;
- a *Tanúsítvány*ban szereplő személynevet a *Hitelesítés-szolgáltató* által a 3.2.3 fejezetben leírtak szerint ellenőrzött formában kell feltüntetni;
- a *Tanúsítvány*ban szereplő *Szervezet* nevét a *Hitelesítés-szolgáltató* által a 3.2.2 fejezetben leírtak szerint ellenőrzött formában kell feltüntetni.

3.1.3. Álnevek használata

Weboldal-hitelesítő tanúsítvány nem lehet álneves.

3.1.4. A különböző elnevezési formák értelmezési szabályai

Az azonosítók értelmezése érdekében az *Érintett felek*nek a jelen dokumentumban leírtak alapján ajánlott eljárniuk. Amennyiben az azonosító, illetve a *Tanúsítvány*ban foglalt bármely más adat értelmezésével kapcsolatban az *Érintett fél*nek segítségre lenne szüksége, akkor a *Hitelesítés-szolgáltató*val közvetlenül is felveheti a kapcsolatot. A *Hitelesítés-szolgáltató* ilyen esetben az *Ügyfél* egyéb adatairól többlet tájékoztatást – feltéve, ha jogszabály ezt nem írja elő – nem ad, csak a *Tanúsítvány*ban feltüntetett adatok értelmezését segítő információt szolgáltatja.

3.1.5. A nevek egyedisége

Az *Alany* a *Hitelesítés-szolgáltató Tanúsítványtár*ában egyedi névvel rendelkezik. Az egyediség biztosítása érdekében a *Hitelesítés-szolgáltató* minden *Alany*nak ad egy – a *Hitelesítés-szolgáltató* nyilvántartásában egyedi – azonosítót, amelyet szerepeltet az *Alany* egyedi azonosítója "Subject DN Serial Number" mezőben.

Az *Alany*ok szolgáltatói egyedi azonosítóinak (OID) kiosztása a beérkezett tanúsítványkérelmek elbírálásának sorrendje szerint történik, ezzel garantálva a *Tanúsítvány*ban szereplő "Subject" mező egyediségét.

Eljárások a nevekre vonatkozó vitás kérdések megoldására

A *Hitelesítés-szolgáltató* meggyőződik az *Ügyfél* jogosultságáról a feltüntetett nevek használatára vonatkozóan. Jogszerűtlen név- vagy adathasználat miatt a *Hitelesítés-szolgáltató*nak jogában áll visszavonni a kérdéses *Tanúsítvány*t.

3.1.6. Márkanevek elismerése, azonosítása, szerepük

Az *Igénylő* által igényelt végfelhasználói *Tanúsítvány* mezőiben előfordulhatnak védjegyek, ezek jogos használatáról a *Hitelesítés-szolgáltató* meggyőződik, illetve reklamáció esetén jogosult a *Tanúsítvány* visszavonására.

Amennyiben az *Ügyfél* olyan *Tanúsítvány*t igényel, amelyben egy márkanév vagy védjegy feltüntetését kéri, akkor a használat jogszerűségéről az *Ügyfél*nek kell bizonyítékot szolgáltatnia, amelyet a *Hitelesítés-szolgáltató* a *Tanúsítvány* kibocsátása előtt ellenőriz az European Union Intellectual Property Office által üzemeltetett oldal segítségével:

`https://www.tmdn.org/tmview/welcome`

A kért védjegy vagy márkanév csak akkor tüntethető fel a *Tanúsítvány*ban, ha:

- a védjegy vagy márkanév az *Igénylő* szervezete által került bejegyzésre;
- az *Igénylő* rendelkezik a védjegyet vagy márkanevet bejegyző által kiállított védjegyhasználati hozzájárulással.

A védjegy vagy márkanév az alábbi módokon tüntethető fel a *Tanúsítvány*ban:

- az "O" mezőben, ez esetben a védjegyet zárójelben követi a szervezet hivatalos - szükség szerint rövidített - elnevezése. Ebben az esetben az *Igénylő* kérésére feltüntethető a *Tanúsítvány*ban a védjegy vagy márkanév mellett a megfelelő (C), (R) vagy (TM) jelzés is.
- az "OU" mezőben, ebben az esetben a védjegyet vagy márkanevet minden esetben követi a megfelelő (C), (R) vagy (TM) jelzés.

A (C), (R) vagy (TM) jelzések bármelyike csak jogos védjegyhasználat esetében kerül feltüntetésre a *Tanúsítvány*ban a védjegyet követően.

A *Hitelesítés-szolgáltató* a szolgáltatása során az "e-Szignó" védjegyet alkalmazza. A védjegy az E-Szignó Bt. tulajdona, a védjegy használatához a tulajdonos hozzájárulását adta.

3.2. 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.

3.2.1. A magánkulcs birtoklásának igazolása

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

Amennyiben az *Igénylő* 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.

3.2.2. 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 alapján meggyőződik a *Tanúsítvány*ba kerülő szervezeti adatok valódiságáról.
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;

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 [2];
- 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 [3];
- a *Szervezet* létezését, elnevezését és jogállását hitelesítő dokumentumot [4].

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

[2] A felhatalmazások, jogosultságok ellenőrzésével kapcsolatos részleteket a 3.2.5. fejezet tartalmazza.
[3] Cégbíróságon bejegyzett cégek esetében a fenti iratokat a *Hitelesítés-szolgáltató* is beszerezheti.
[4] Cégbíróságon bejegyzett cégek esetében a fenti iratokat a *Hitelesítés-szolgáltató* is beszerezheti.

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.

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 IP címnek vagy doménnévnek.

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

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

Amennyiben a *Tanúsítvány*ban "*" dzsóker karaktert tartalmazó doménnév kerül feltüntetésre (wildcard tanúsítvány), a *Hitelesítés-szolgáltató* meggyőződik róla, hogy az *Igénylő* a wildcard doménnév által lefedett teljes doménnévtér jogosult használója. A *Hitelesítés-szolgáltató* nem bocsát ki olyan *Tanúsítvány*t, amelyben a "*" dzsóker karakter a legmagasabb szintű regisztrálható doménnév helyén, azaz közvetlenül egy nyilvános domén végződés bal oldalán található (pl. "*.com", "*.co.uk").

A *Hitelesítés-szolgáltató* kizárólag az interneten használható nyilvános doménnevekre és IP címekre bocsát ki *Tanúsítvány*t, belső használatú nevekre és lefoglalt IP címekre 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 [22] 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.

A módszer Wildcard doménnevek validálására is használható.

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 [30] 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 [28] 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.

A módszer Wildcard doménnevek validálására is használható.

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

[28] 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.

A módszer Wildcard doménnevek validálására is használható.

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.

A módszer Wildcard doménnevek validálására is használható.

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 [24] 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.

A módszer Wildcard doménnevek validálására is használható.

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 [30] 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 [24] 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.

A módszer Wildcard doménnevek validálására is használható.

3.2.2.3 IP cím azonosítása

A fejezetben kerülnek felsorolásra azok az eljárások és folyamatok amelyekkel igazolható az *Igénylő* jogosultsága vagy kontrollja a *Tanúsítvány*ba kerülő IP címek felett.

A *Hitelesítés-szolgáltató* igazolja, hogy a *Tanúsítvány* kibocsátása előtt minden, a *Tanúsítvány*ban feltüntetésre kerülő IP címet ellenőriz legalább egy, a fejezetben felsorolt módszer felhasználásával.

Az *Igénylő* jogosultságát igazoló vizsgálati eredmények több *Tanúsítvány* kibocsátása során is felhasználhatók, amennyiben a vizsgálat megkezdésének időpontja a *Tanúsítvány* kibocsátását megelőzően a 4.2.1. fejezetben meghatározott időtartamnál nem korábban volt.

A *Hitelesítés-szolgáltató* nyilvántartást vezet a kibocsátott *Tanúsítvány*okban foglalt IP címek ellenőrzéséről, amelyből megállapítható hogy mely IP cím mely BR követelmény alapján lett ellenőrizve.

3.2.2.3.1 Weboldal egyeztetett módosítása (BR 3.2.2.5.1)

Az *Igénylő* által kért IP cím feletti kontroll megerősítése a *Hitelesítés-szolgáltató* által előállított véletlenszám közlésével a "/.well-known/pki-validation" könyvtárban elhelyezett fájlban, amit a *Hitelesítés-szolgáltató* a kért IP címen ér el HTTP/HTTPS protokoll felhasználásával egy engedélyezett porton keresztül.

A véletlenszám nem szerepelhet a kiolvasásra szolgáló kérésben.

A *Hitelesítés-szolgáltató*nak minden *Tanúsítványkérelem* ellenőrzéséhez egyedi véletlenszámot kell használnia, amelynek érvényessége nem haladhatja meg a 30 napot.

3.2.2.3.2 Email, fax, SMS vagy postai levél küldése az IP cím kapcsolattartójának (BR 3.2.2.5.2)

Az *Igénylő* által kért IP cím feletti kontroll megerősítése a *Hitelesítés-szolgáltató* által előállított véletlenszám küldésével majd a válaszban kapott véletlenszám ellenőrzésével email, fax, SMS vagy postai levél felhasználásával. A véletlenszámot az IP cím kapcsolattartójának email címére, SMS számára, fax számára vagy postai levelezési címére kell küldeni.

A küldött email, SMS, fax vagy postai levél egyszerre több IP cím feletti kontrol ellenőrzésére is felhasználható.

A *Hitelesítés-szolgáltató* az email, SMS, fax vagy postai levél üzenetet egyszerre több címzettnek is elküldheti, amennyiben azok mindegyike az IP cím regisztáló szervezet által nyilvántartott IP cím kapcsolattartó valamennyi kért IP cím esetében.

Minden email, SMS, fax vagy postai levél egyedi véletlenszámot kell tartalmazzon.

A *Hitelesítés-szolgáltató* újraküldheti az emailt, SMS-t, faxot vagy postai levelet változatlan tartalommal az összes címzettnek beleértve a változatlan véletlenszámot is, amennyiben az üzenet tartalma és a címzettek köre változatlan.

A megerősítő válaszba foglalandó véletlenszám érvényességi ideje nem haladhatja meg a 30 napot.

3.2.2.3.3 Reverz IP cím keresés alapján (BR 3.2.2.5.3)

Az *Igénylő* által kért IP cím feletti kontroll megerősítése az IP címhez tartozó doménnév megkeresésével reverz IP cím kereséssel és a talált doménnév feletti jogosultság vagy kontroll ellenőrzésével a 3.2.2.2. fejezet szerinti módszerek felhasználásával.

3.2.2.3.4 Egyéb módszer (BR 3.2.2.5.4)

Ez a validálási módszer nem használatos.

3.2.2.3.5 Az IP cím kapcsolattartó felhívása telefonon (BR 3.2.2.5.5)

Az *Igénylő* által kért IP cím feletti kontroll megerősítése az IP cím kapcsolattartó telefonszámának felhívásával és az *Igénylő* által az IP címre beadott *Tanúsítványkérelem* szóbeli megerősítésével. A *Hitelesítés-szolgáltató*nak az IP címet regisztráló szervezet által nyilvántartott IP cím kapcsolattartói telefonszámot kell felhívnia. Minden hívásnak ugyanarra a számra kell irányulnia.

Amennyiben a hívást nem az IP cím kapcsolattartója fogadja, a *Hitelesítés-szolgáltató* kérheti a hívás átirányítását az IP cím kapcsolattartónak.

Amennyiben a hívás hangpostára érkezik, a *Hitelesítés-szolgáltató* meghagyhatja a véletlenszámot és az ellenőrzendő IP címe(ke)t hangüzenetben. A véletlenszámot az igény jóváhagyásához vissza kell juttatni a *Hitelesítés-szolgáltató*hoz.

A megerősítő válaszba foglalandó véletlenszám érvényességi ideje nem haladhatja meg a 30 napot.

3.2.2.3.6 ACME “http-01” eljárás IP címekhez (BR 3.2.2.5.6)

Ez a validálási módszer nem használatos.

3.2.2.3.7 ACME “tls-alpn-01” eljárás IP címekhez (BR 3.2.2.5.7)

Ez a validálási módszer nem használatos.

3.2.3. Természetes személy azonosságának hitelesítése

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

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

1. Személyesen történő azonosítás során.

   A III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetében:

   - 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) [8] 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 [5] szerinti úti okmány alapján az Eüt. 82.§ (4) [8] 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) [8] 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.

A II. hitelesítési osztályba tartozó *Tanúsítvány*ok esetében:

- a természetes személy azonosításához személyes találkozásra nincs szükség, ilyen esetben a *Hitelesítés-szolgáltató* távolról is azonosíthatja az *Igénylő*t;
- az *Igénylő* eljuttatja a *Hitelesítés-szolgáltató*nak valamely személyazonosság igazolására alkalmas hatósági igazolványának másolatát.
- az *Igénylő* eljuttatja a *Hitelesítés-szolgáltató*nak a lakcímének igazolására alkalmas hatósági igazolványának másolatát.
- A személyazonosság ellenőrzésére szolgáló adatok helyességét a természetes személynek nyilatkozatban, saját kezű aláírással ellátva igazolnia kell.
- A *Hitelesítés-szolgáltató* a II. hitelesítési osztályba tartozó tanúsítványok esetén is végez adategyeztetést megbízható harmadik féllel vagy közhiteles nyilvántartásokkal.
- A természetes személy lakcímét ellenőrizni kell egy lakcím azonosítására alkalmas igazolvány alapján.
- A bemutatott igazolványok hitelességét a *Hitelesítés-szolgáltató* ebben az esetben is ellenőrzi. Továbbá a *Hitelesítés-szolgáltató* megbízható kommunikációs csatornán keresztül ellenőrzi, hogy a *Tanúsítványkérelmet* valóban az azonosított *Igénylő* küldte. Ekkor a *Hitelesítés-szolgáltató* megerősítést kér az *Igénylő* részéről egy olyan elérhetőségén keresztül, amelyet nem az igénylési eljárás során adott meg, hanem más forrásból származik. Megfelelő elektronikus azonosító eszközzel történt azonosítás vagy megfelelő elektronikus aláírással benyújtott *Tanúsítványkérelem* esetén nincs szükség további megbízható kommunikációs csatornán keresztüli megerősítésre.
- Az *Igénylő* választása szerint a III. hitelesítési osztály szerint is igazolhatja személyazonosságát.

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 (lásd 1.2.3. fejezet) – *Tanúsítvány*án alapuló elektronikus aláírással ellátva.
   - Az elektronikus aláírással ellátott *Tanúsítványkérelem*nek tartalmaznia kell a természetes személy 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 az Európai Uniós fő bizalmi listán publikált nemzeti bizalmi listán szereplő bizalmi szolgáltatás keretében bocsátottak ki, és az aláírás létrehozás időpontjában érvényes volt.

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 *Tanúsítványkérelem* hitelességét, a *Tanúsítvány*ba kerülő adatok érvényességét és az *Igénylő* személyazonosságát a *Hitelesítés-szolgáltató* ilyen esetben is ellenőrzi.

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.

3.2.4. Nem ellenőrzött alany információk

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

3.2.5. Jogok, felhatalmazások ellenőrzése

Szervezeti tanúsítvány kiállítása előtt a *Szervezet* nevében eljáró természetes személy azonosságát igazolni kell a 3.2.3. 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.

3.2.6. Együttműködési képességre vonatkozó követelmények

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

3.2.7. Email cím megerősítése

A *Hitelesítés-szolgáltató* weboldalán benyújtott kérelmek esetében a *Tanúsítványkérelem* űrlap kitöltése előtt a *Hitelesítés-szolgáltató* validálja az *Igénylő* email címét az email cím feletti kontroll ellenőrzésével. A weboldal az űrlap kitöltése előtt kéri az *Igénylő* email címének megadását és

nem enged más adatot kitölteni. A *Hitelesítés-szolgáltató* a megadott email címre kiküld egy véletlenszámot is tartalmazó, korlátozott érvényességi idejű, igénylésenként egyedi URL-t. Az *Igénylő* csak a kapott egyedi linkre kattintva tudja folytatni az űrlap kitöltését. A beérkező *Tanúsítványkérelem*hez így minden esetben tartozik egy - a működés során ellenőrzött - email cím.

Egyéb módon benyújtott *Tanúsítványkérelem* esetében a *Hitelesítés-szolgáltató* egy véletlenszámot is tartalmazó email-t küld az ellenőrzendő email címre. Az *Igénylő*-nek egy válasz email küldésével kell megerősítenie az igénylést. A válasz emailnek tartalmaznia kell a *Hitelesítés-szolgáltató* által küldött véletlenszámot és a *Tanúsítványkérelem* beadása során az *Igénylő* által megadott jelszót. A véletlenszám érvényességi ideje 30 nap.

3.3. Azonosítás és hitelesítés kulcscsere kérelem esetén

A kulcscsere alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* egy adott *Alany* részére úgy bocsát ki új *Tanúsítvány*t, hogy a nyilvános kulcs lecserélésre kerül. Kulcscsere csak a Szolgáltatási szerződés időtartama alatt kérhető.

Kulcscsere kérelem esetén a *Hitelesítés-szolgáltató* ellenőrzi az érintett *Tanúsítvány* létezését és megvizsgálja annak érvényességét.

Kulcscsere kérelmeket a *Hitelesítés-szolgáltató* érvényes és nem érvényes (visszavont vagy lejárt) *Tanúsítvány*okhoz is elfogad.

A kulcscserével kapcsolatos eljárás részletei a 4.7. fejezetben olvashatóak.

A II. hitelesítési osztályba tartozó tanúsítványok esetében a *Hitelesítés-szolgáltató* nem végez kulcscserét. Új kulcsot tartalmazó *Tanúsítvány* kibocsátása kizárólag az új *Tanúsítvány* igénylésének folyamata keretében történik.

3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

Az *Igénylő* azonosítása a 3.2.3. fejezetben leírtak szerint történik.

Amennyiben az új *Tanúsítvány* a lecserélendő *Tanúsítvány*énál nem későbbi érvényességgel kerül kiadásra, a *Hitelesítés-szolgáltató* az ellenőrzés során felhasználja az eredeti *Tanúsítvány* kibocsátásakor elvégzett vizsgálatok eredményeit.

3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Kulcscsere kérelmeket – kizárólag a Szolgáltatási szerződés érvényessége alatt – visszavont vagy lejárt *Tanúsítvány*okhoz is elfogad a *Hitelesítés-szolgáltató*.

Az *Igénylő* azonosítása a 3.2.3. fejezetben leírtak szerint történik.

3.4. Azonosítás és hitelesítés tanúsítvány megújítás esetén

Tanúsítvány megújítás alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* egy adott *Alany* részére változatlan *Alany* azonosító adatokkal, változatlan nyilvános kulccsal, de új érvényességi időszakra bocsát ki új *Tanúsítvány*t. *Tanúsítvány* megújítás csak a Szolgáltatási szerződés érvényessége alatt, és csak még érvényes *Tanúsítvány*okhoz kérhető.

3.4.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

Az *Igénylő* azonosítása a 3.2.3. fejezetben leírtak szerint történik.

3.4.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen *Tanúsítvány* nem újítható meg.

3.5. Azonosítás és hitelesítés tanúsítvány módosítás esetén

Tanúsítvány módosítás alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* egy adott *Alany* részére új *Tanúsítvány*t bocsát ki változatlan nyilvános kulccsal, de megváltozott *Alany* azonosító adatokkal.

3.5.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

Az *Igénylő* azonosítása a 3.2.3. fejezetben leírtak szerint történik.

3.5.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen *Tanúsítvány* nem módosítható.

3.6. Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási kérelem esetén

A *Hitelesítés-szolgáltató* fogadja és feldolgozza a *Tanúsítvány*ok visszavonására vonatkozó kérelmeket, valamint a *Tanúsítvány*ok visszavonását érintő (pl. a magánkulcs kompromittálódásával vagy a *Tanúsítvány* nem megfelelő használatával kapcsolatos) bejelentéseket.

A *Hitelesítés-szolgáltató* a kérelmek gyors teljesítése mellett biztosítja, hogy a kérelmeket csak az arra jogosult felektől fogadja el. A kérelmeket benyújtó személyek azonossága, a kérelmek hitelessége ellenőrzésre kerül.

Az erre vonatkozó kérelmek azonosítási és hitelesítési vonatkozásait a 4.9. fejezet tárgyalja.

*Weboldal-hitelesítő tanúsítvány*ok esetében felfüggesztésre nincs lehetőség.

3.7. Ellenőrzött kommunikációs csatorna

Az *Igénylő*vel létesítendő kapcsolat és a *Tanúsítvány* kibocsátás engedélyezése céljából a *Hitelesítés-szolgáltató* hitelesít egy telefonszámot, fax számot, email címet vagy postai címet az *Igénylő*vel létesítendő Ellenőrzött kommunikációs csatornaként.

Az *Igénylő*vel létesítendő Ellenőrzött kommunikációs csatorna hitelesítése során a *Hitelesítés-szolgáltató*

- igazolja, hogy az Ellenőrzött kommunikációs csatorna az *Igénylő*höz tartozik az alábbi információkon alapulva:

  - a megfelelő telefon szolgáltató által biztosított adatok alapján;
  - Minősített kormányzati információs forrás igénybe vételével;
  - közjegyző által kiállított hiteles igazolás alapján;
  - az *Igénylő* személyes jelenlétére alapozva.

- megerősíti az Ellenőrzött kommunikációs csatornát. A *Hitelesítés-szolgáltató* regisztrációs tisztviselője kapcsolatba lép az *Igénylő*vel az Ellenőrzött kommunikációs csatorna használatával. Az Ellenőrzött kommunikációs csatorna megbízhatóságát az *Igénylő* személyes jelenlétével vagy a Kommunikációs csatorna ellenőrzési jelszó használatával igazolja.

4. A tanúsítványok életciklusára vonatkozó követelmények

Új *Alany* számára új *Tanúsítvány* kibocsátását meg kell, hogy előzze a Regisztrációs igény *Hitelesítés-szolgáltató*hoz történő eljuttatása, az *Előfizető* részéről a Szolgáltatási szerződés aláírása, valamint az *Igénylő* részéről a *Tanúsítványkérelem* aláírása.

Tanúsítványcserének nevezzük azt a folyamatot, amikor egy korábban már regisztrált (és ennek során azonosított) *Alany* egy meglévő (érvényes Szolgáltatási szerződés alapján kibocsátott) *Tanúsítvány*a helyett új *Tanúsítvány*t igényel.

Tanúsítványcserére az alábbi okokból kerülhet sor:

- Tanúsítvány *megújítás* esetén az *Ügyfél* olyan *Tanúsítvány*t igényel, amelybe az *Alany* korábbi *Tanúsítvány*ában lévőkkel megegyező adatok kerülnek, és a két *Tanúsítvány* ugyanazon nyilvános kulcshoz kerül kibocsátásra. A Tanúsítvány *megújítás* részleteit a 4.6. fejezet tartalmazza.

- Tanúsítvány *módosítás* esetén az *Alany Tanúsítvány*ban szereplő adatainak változására tekintettel kéri a *Tanúsítvány* megváltoztatását. *Tanúsítvány* módosítási kérelmet a *Tanúsítvány* érvényességi ideje alatt lehet a *Hitelesítés-szolgáltató*hoz benyújtani. A *Tanúsítvány* módosítás során az új *Tanúsítvány* azonos nyilvános kulcshoz kerül kibocsátásra. A *Tanúsítvány* módosítás részleteit a 4.8. fejezet tartalmazza.

- *Kulcscsere* esetén a *Hitelesítés-szolgáltató* az új *Tanúsítvány*t új nyilvános kulcshoz bocsátja ki a *Tanúsítvány* érvényességi ideje alatt vagy a lejáratot követően. A *kulcscsere* részleteit a 4.7. fejezet tartalmazza.

Amennyiben egy – érvényes Szolgáltatási szerződéssel rendelkező – *Ügyfél* új *Tanúsítvány*t igényel, a Szolgáltatási szerződés módosítása szükséges.

Egy kibocsátott *Tanúsítvány* állapota lehet érvényes, visszavont vagy lejárt. Az állapotváltozásokkal kapcsolatos szabályokat a 4.9. fejezet tartalmazza, illetve a *Tanúsítvány*ok állapotának lekérdezhetőségéről szól a 4.10. fejezet.

Egy *Tanúsítvány* fenntartását az arra vonatkozó Szolgáltatási szerződés hatálya alatt végzi a *Hitelesítés-szolgáltató*. A Szolgáltatási szerződés lezárásával kapcsolatos előírást a 4.11. fejezet tartalmazza.

4.1. Tanúsítványkérelem

Új *Tanúsítvány* kiadásához *Tanúsítványkérelem* benyújtására van szükség.
Az első *Tanúsítványkérelem* benyújtását megelőzően az *Igénylő Regisztrációs igény*t kell, hogy benyújtson a *Hitelesítés-szolgáltató*nak, ez történhet a *Hitelesítés-szolgáltató* honlapján keresztül is. A *Regisztrációs igény*ben az *Igénylő* megadja a *Tanúsítvány*ba kerülő adatokat, meg kell jelölnie, hogy pontosan milyen *Tanúsítvány*t igényel, és felhatalmazást kell adnia a *Hitelesítés-szolgáltató* számára a személyes adatainak kezelésére.

A *Hitelesítés-szolgáltató* mindaddig nem tekinti a *Regisztrációs igény*ben szereplő adatokat hitelesnek, amíg az *Igénylő* a *Tanúsítványkérelem*ben meg nem erősíti azokat. Amennyiben új Szolgáltatási szerződés megkötésére van szükség, a *Hitelesítés-szolgáltató* a *Regisztrációs igény*ben megadott adatok alapján előkészíti az *Előfizető*vel kötendő Szolgáltatási szerződést. A Szolgáltatási szerződésnek tartalmaznia kell, hogy annak keretében mely *Alany*ok milyen szolgáltatás keretében, milyen típusú *Tanúsítvány*t jogosultak igényelni.

Új *Tanúsítvány* igényelhető egy már korábban megkötött Szolgáltatási szerződés keretében is. Ha az abban megjelölt valamely *Tanúsítvány* helyett kerül kibocsátásra az új *Tanúsítvány* (Tanúsítványcsere), a Szolgáltatási szerződés módosítása nem szükséges. Ha a meglevő(kö)n kívül új *Tanúsítvány* kibocsátását kéri az *Ügyfél*, akkor a Szolgáltatási szerződést is módosítani kell.

A *Hitelesítés-szolgáltató* a szerződés megkötését megelőzően tájékoztatja az *Előfizető*t a *Tanúsítvány* használatával kapcsolatos kikötésekről és feltételekről.

Amennyiben az *Igénylő* nem azonos az *Előfizető*vel, akkor az *Igénylő* számára is megadja a fenti tájékoztatást.

A *Hitelesítés-szolgáltató* a tájékoztatást tartalmazó dokumentumokat közérthető módon megfogalmazva, elektronikusan letölthető formában hozza nyilvánosságra, valamint kérelemre az ügyfélszolgálati irodáján nyomtatott formában is elérhetővé teszi. Az Ügyfélszolgálati irodában az Ügyfélnek lehetősége van a tájékoztató áttanulmányozására és a konzultációra.

A *Tanúsítványkérelem*ben az *Igénylő*nek a következő adatokat kell megadnia:

- a *Tanúsítvány*ba kerülő adatok (pl. doménnév, IP cím, *Szervezet* neve, város, ország);
- az *Igénylő* személyazonosító adatai (teljes név, személyazonosító okmány száma, anyja neve, születés helye, ideje);
- az *Igénylő* elérhetőségei (telefonszám, email cím);
- *Szervezeti tanúsítvány* igénylése esetében a *Szervezet* adatai (hivatalos elnevezése, székhelye, azonosító adatai);
- az *Előfizető* adatai (számlázási adatok).

A *Tanúsítványkérelem*mel együtt a *Hitelesítés-szolgáltató* bekéri a következő okmányokat, igazolásokat, meghatalmazásokat illetve nyilatkozatokat (távoli azonosítás esetén ezek másolatát):

- az *Igénylő* azonosításához szükséges okmányokat a 3.2.3 fejezetnek megfelelően;
- *Szervezeti tanúsítvány* igénylése esetén a *Szervezet* azonosításához szükséges okmányokat a 3.2.2 fejezetnek megfelelően;

- *Szervezeti tanúsítvány* igénylése esetén a *Szervezet* által kiadott igazolást vagy meghatalmazást arról, hogy az igénylő személy jogosult a *Szervezet* képviseletére a 3.2.5. fejezetnek megfelelően;
- amennyiben a kért *Tanúsítvány*ban szerepel márkanév vagy védjegy, akkor annak igazolását, hogy az *Igénylő* jogosult annak használatára a 3.1.6. fejezetnek megfelelően.

4.1.1. Ki nyújthat be tanúsítványkérelmet

Tanúsítványkérelmet természetes személyek nyújthatnak be saját maguk vagy az általuk képviselt szervezet számára történő *Tanúsítvány* kibocsátása céljából. *Szervezeti tanúsítvány* esetében a képviseletre a 3.2.5 fejezet szerinti személyek jogosultak, más személyektől érkező *Tanúsítványkérelem* automatikusan elutasításra kerül.

A *Tanúsítvány* kibocsátás előfeltétele az adott *Tanúsítvány* kibocsátására és fenntartására vonatkozó érvényes (az *Előfizető* és a *Hitelesítés-szolgáltató* által aláírt) Szolgáltatási szerződés megléte.

A *Tanúsítványkérelmet* az *Igénylő* a következő módokon nyújthatja be:

- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában vagy a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál, előzetesen egyeztetett időpontban (ekkor a III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a személyes azonosítás megtörténik a találkozás során);
- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájába eljuttatva (ekkor a III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a személyes azonosításra más időpontban kerül sor);
- elektronikus formában, egy nem álneves, az igényelt *Tanúsítvány*énál nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) *Tanúsítvány*ának felhasználásával elektronikusan aláírva vagy elektronikus bélyegzővel ellátva, a *Hitelesítés-szolgáltató* email címére megküldve.

Az *Előfizető*nek és az *Igénylő*nek a *Tanúsítvány* igénylése során meg kell adniuk elérhetőségi adataikat.

4.1.2. A bejegyzés folyamata és a résztvevők felelőssége

A kérelem feldolgozása során a *Hitelesítés-szolgáltató* regisztrációs munkatársa meggyőződik a *Tanúsítványkérelmet* benyújtó személyazonosságáról (lásd: 3.2.3 fejezet).

Egy másik — megbízható -– kommunikációs csatornán a *Hitelesítés-szolgáltató* regisztrációs munkatársa ellenőrzi, hogy a *Tanúsítványkérelem* valóban attól a személytől származik, akinek az adatai (igazolványai) a *Tanúsítványkérelem*ben szerepelnek.

Szervezeti tanúsítvány igénylése esetén a *Hitelesítés-szolgáltató* azonosítja a *Szervezet*et (lásd: 3.2.2. fejezet) illetve meggyőződik arról, hogy az igénylő személy jogosult a *Szervezet* képviseletére (lásd: 3.2.5. fejezet) illetve a *Szervezet*hez kapcsolódó *Tanúsítvány* igénylésére (lásd: 3.2.2. fejezet).

Az *Igénylő* meg kell adjon minden szükséges információt az azonosítási eljárások lefolytatásához.

A *Hitelesítés-szolgáltató* szükség szerint adategyeztetést végez közhiteles (kormányzati) adatbázisokkal (például a személy és lakcímnyilvántartással vagy a cégnyilvántartással). Amely adatbázisok esetén ez megoldható, ott a *Hitelesítés-szolgáltató* az adategyeztetést elektronikusan végzi.

A folyamat során a *Hitelesítés-szolgáltató* meghatározza az *Alany* egyedi nevét, ennek keretében globálisan egyedi azonosítót (OID) rendel az *Alany*hoz. Ez a 3.1. fejezetben tárgyaltaknak megfelelően történik.

A *Hitelesítés-szolgáltató* nyilvántartásba veszi az *Igénylő*, illetve a *Szervezet* azonosságára vonatkozó, a szolgáltatás nyújtásához és a kapcsolattartáshoz szükséges minden információt.

A *Hitelesítés-szolgáltató* nyilvántartásba veszi az *Előfizető*vel előzetesen aláírt Szolgáltatási szerződést, amelynek tartalmaznia kell az *Előfizető* nyilatkozatát arra vonatkozóan, hogy kötelezettségeit megismerte és azok betartását vállalja.

A *Hitelesítés-szolgáltató* nyilvántartásba veszi az *Igénylő* által aláírt *Tanúsítványkérelmet*, amelynek tartalmaznia kell a következőket:

- annak megerősítését, hogy a *Tanúsítványkérelem*ben megadott adatok pontosak;
- azt, hogy hozzájárul ahhoz, hogy a *Hitelesítés-szolgáltató* a kérelemben megadott adatait nyilvántartsa és kezelje;
- azt, hogy hozzájárul-e a *Tanúsítvány* és az *Előtanúsítvány* közzétételéhez;
- nyilatkozatot arról, hogy az igényelt *Tanúsítvány*ban nem szerepel márkanév vagy védjegy, vagy hogy szerepel és annak jogos felhasználója.

A *Hitelesítés-szolgáltató* a fenti nyilvántartásokat megőrzi legalább a hatályos jogszabályokban előírt időtartamig.

A *Hitelesítés-szolgáltató* archiválja a szerződéseket, a tanúsítványkérelem űrlapot és valamennyi igazolást, amelyet a *Képviselt szervezet*, az *Igénylő* vagy az *Előfizető* benyújtottak.

Amennyiben az *Igénylő* személyazonossága, vagy *Szervezeti tanúsítvány* esetében a *Szervezet* azonossága nem állapítható meg minden kétséget kizáróan, vagy valamely, a tanúsítványkérelem űrlapon feltüntetett adat nem helyes, akkor a *Hitelesítés-szolgáltató* belső szabályzatainak megfelelően lehetőséget adhat az *Ügyfél*nek a hiányos vagy hibás adatok korrigálására, illetve a hiányzó igazolások átadására a *Tanúsítványkérelem* benyújtásától számított 3 hónapon belül.

4.2. A tanúsítványkérelem feldolgozása

4.2.1. Az igénylő azonosítása és hitelesítése

A *Hitelesítés-szolgáltató* az igénylőt a 3.2 fejezetnek megfelelően azonosítja illetve ellenőrzi a kérelem hitelességét.

Szervezeti tanúsítvány igénylése esetén a *Szervezet*et is azonosítja, valamint a jogosultságok ellenőrzése is megtörténik a 3.2. fejezetnek megfelelően. A *Hitelesítés-szolgáltató* nyilvántartásba vesz minden, az *Alany*, valamint *Szervezeti tanúsítvány* esetében a *Szervezet* azonosságának igazolására használt információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és az annak érvényességével kapcsolatos esetleges korlátozásokat is.

A *Hitelesítés-szolgáltató* legfeljebb 825 napig felhasználhatja vagy újra használhatja a *Tanúsítvány*ba kerülő információ validálása érdekében a 3.2 fejezetnek megfelelően beszerzett dokumentumokat illetve saját maga által elvégzett vizsgálatok eredményeit.

A *Hitelesítés-szolgáltató* nyilvántartást vezet a magas kockázatú *Tanúsítványkérelmek*ről, amely tartalmazza az összes elutasított *Tanúsítványkérelmet* és az összes, biztonsági ok miatt visszavont *Tanúsítvány*t.

A *Tanúsítvány* kibocsátás engedélyezése előtt a *Hitelesítés-szolgáltató* ellenőrzi a nyilvántartást. Amennyiben a nyilvántartásban megtalálható az igényelt domain, az *Előfizető* vagy az *Igénylő* bármelyike, a *Hitelesítés-szolgáltató* kiemelten kezeli a *Tanúsítványkérelem* elbírálását a helyes feldolgozás biztosítása érdekében.

4.2.2. A tanúsítványkérelem elfogadása vagy visszautasítása

A *Hitelesítés-szolgáltató* az összeférhetetlenség elkerülése érdekében biztosítja személyi és szervezeti függetlenségét az *Előfizető*kkel szemben. Nem minősül az összeférhetetlenség megsértésének, amikor a *Hitelesítés-szolgáltató* munkatársai számára bocsát ki *Tanúsítvány*t.

A *Hitelesítés-szolgáltató* a *Tanúsítvány* kibocsátása előtt ellenőrzi a *Tanúsítványkérelem*ben megadott, a *Tanúsítvány*ba kerülő valamennyi információ hitelességét.

Az elbírálási folyamat részeként a *Hitelesítés-szolgáltató* ellenőrzi a kibocsátandó *Tanúsítvány* subjectAltName kiterjesztésében szereplő valamennyi dNSName CAA rekordját az IETF RFC 6844 [30] specifikációban meghatározott folyamat szerint, minden mező esetében követve az IETF RFC 6844 specifikációban leírt végrehajtási utasításokat.

A *Hitelesítés-szolgáltató* csak abban az esetben bocsátja ki a kért *Tanúsítvány*t, ha valamennyi dNSName CAA "issue" és "issuewild" mezeje üres, vagy azok valamelyikében az alábbi érték szerepel:

- e-szigno.hu

Közvetlenül a *Tanúsítvány* kibocsátása előtt a *Hitelesítés-szolgáltató* automatikusan ismét ellenőrzi a CAA rekord tartalmát.

A *Hitelesítés-szolgáltató* a *Tanúsítványkérelem* feldolgozása után elfogadja, vagy visszautasítja a *Tanúsítványkérelem* teljesítését.

Amennyiben az azonosított természetes személy vagy szervezet azonossága nem állapítható meg minden kétséget kizáróan, vagy valamely, a *Tanúsítványkérelem* űrlapon feltüntetett adat nem helyes, és ezeket az *Ügyfél* a *Hitelesítés-szolgáltató* kérésére sem korrigálta vagy egészítette ki, akkor a *Hitelesítés-szolgáltató* elutasítja a kérelmet.

A *Tanúsítványkérelem* elutasítása esetén az elutasítás tényéről a *Hitelesítés-szolgáltató* tájékoztatja az *Igénylő*t és az *Előfizető*t, de a *Hitelesítés-szolgáltató* nem köteles döntését megindokolni.

4.2.3. A tanúsítványkérelem feldolgozásának időtartama

A *Hitelesítés-szolgáltató* a benyújtott *Tanúsítványkérelem* elbírálását, amennyiben minden szükséges adat és dokumentum a rendelkezésre áll, 5 munkanapon belül elvégzi.

4.3. A tanúsítvány kibocsátása

A III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a *Hitelesítés-szolgáltató* csak a *Tanúsítványkérelem* elfogadása esetén állítja ki a *Tanúsítvány*t az *Alany* részére. A kiállított *Tanúsítvány* csak az *Alany Tanúsítványkérelem*ben megadott és az elbírálás során a *Hitelesítés-szolgáltató* által ellenőrzött adatait tartalmazza.

A II. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a *Hitelesítés-szolgáltató* csak a *Regisztrációs igény*ben megadott adatok ellenőrzése valamint az aláírt *Tanúsítványkérelem* és Szolgáltatási szerződés kézhezvétele után állítja ki a *Tanúsítvány*t az *Alany* részére. A kiállított *Tanúsítvány* csak az *Alany Regisztrációs igény*ben megadott és az elbírálás során a *Hitelesítés-szolgáltató* által ellenőrzött adatait tartalmazza.

4.3.1. A Hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során

A *Tanúsítvány*ok kibocsátása szigorúan szabályozott és ellenőrzött folyamatok szerint történik, amelyek részleteit a *Hitelesítés-szolgáltató* belső szabályzatai és előírásai rögzítik.

A *Hitelesítés-szolgáltató* a bizalmi szerepkörök megfelelő elosztásával és belső adminisztratív folyamatainak segítségével biztosítja, hogy a *Tanúsítvány* kibocsátás során legalább két - bizalmi szerepkört ellátó - alkalmazott részvételére van szükség.

Amennyiben az *Igénylő* ehhez hozzájárult, a *Tanúsítvány*hoz tartozó *Előtanúsítvány*t *Hitelesítés-szolgáltató* az ismert Certificate Transparency naplószolgáltatókon keresztül közzéteszi, és a naplószolgáltatók által küldött aláírt SCT-ket elhelyezi a kibocsátandó *Tanúsítvány*ban.

4.3.2. Az Ügyfél értesítése a tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* a *Tanúsítvány* kibocsátásáról értesíti az *Igénylő*t és az *Előfizető*t, valamint lehetővé teszi az *Igénylő* számára a *Tanúsítvány* átvételét.

4.4. A tanúsítvány elfogadása

4.4.1. A tanúsítvány elfogadás módja

A III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén az *Igénylő*nek a *Tanúsítvány* átvétele során ellenőriznie kell a *Tanúsítvány*ban szereplő adatok helyességét és erről írásbeli nyilatkozatot kell tennie. A nyilatkozat aláírásával az *Igénylő* igazolja a *Tanúsítvány* átvételét.

A II. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén az *Igénylő* (vagy képviselője) ellenőrzi a *Tanúsítvány*ban szereplő adatok helyességét és erről írásbeli nyilatkozatot tesz. Az *Igénylő* (vagy képviselője) nem tesz külön nyilatkozatot a kiállított *Tanúsítvány* átvételéről. A Szolgáltatási szerződés aláírásával az *Előfizető* egyúttal igazolja a *Hitelesítési rend* a *Szolgáltatási szabályzat* és a szerződési feltételeket tartalmazó egyéb dokumentumok elfogadását is.

4.4.2. A tanúsítvány közzététele

A *Tanúsítvány* átvételéről szóló nyilatkozat kézhezvételét követően – amennyiben az *Igénylő* ehhez hozzájárult – a *Hitelesítés-szolgáltató* haladéktalanul közzéteszi a *Tanúsítvány*t a nyilvános *Tanúsítványtár*ában.

4.4.3. További szereplők értesítése a tanúsítvány kibocsátásról

Szervezeti tanúsítvány esetén a *Tanúsítvány* kibocsátásáról a *Hitelesítés-szolgáltató* haladéktalanul értesíti a *Képviselt szervezet Szervezeti ügyintézőjét* is.

4.5. A kulcspár és a tanúsítvány használata

4.5.1. 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 1.4. fejezetben leírt korlátozásokat.

4.5.2. 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.

4.6. Tanúsítvány megújítás

A tanúsítvány megújítás alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* ugyanarra a nyilvános kulcsra változatlan *Alany* azonosító adatokkal egy új *Tanúsítvány*t állít ki új érvényességi időszakra.

Ha az *Alany* a *Tanúsítvány*t a lejáratot követően is használni szeretné, akkor kezdeményeznie kell a *Tanúsítvány* megújítását. *Tanúsítvány* megújítási kérelem a *Tanúsítvány* érvényességi ideje alatt nyújtható be a *Hitelesítés-szolgáltató*hoz. A *Tanúsítvány* megújítás műszakilag új *Tanúsítvány* kibocsátását jelenti, amelybe az előzőben szereplővel megegyező *Alany*t azonosító adatok, azonban új érvényességi időtartam kerül. A *Tanúsítvány*ban esetleg változhatnak további adatok is, mint például a CRL és OCSP hivatkozások vagy a *Tanúsítvány* aláírására használt szolgáltatói kulcs.

4.6.1. A tanúsítvány megújítás körülményei

A tanúsítvány megújítás csak az alábbi feltételek egyidejű teljesülése esetén engedélyezett:

- a *Tanúsítvány* megújítási kérelem a *Tanúsítvány* érvényességi ideje alatt benyújtásra kerül;
- a megújítandó *Tanúsítvány* nincs visszavonva;
- a *Tanúsítvány*hoz tartozó magánkulcs nem kompromittálódott;
- a *Tanúsítvány*ban szereplő *Alany* azonosító adatok érvényben vannak.

Tanúsítvány megújítási kérelmet a *Hitelesítés-szolgáltató* csak a Szolgáltatási szerződés hatálya alatt fogad el.

Ha az *Alany* korábbi *Tanúsítvány*a visszavonásra került vagy lejárt, akkor új *Tanúsítvány*t csak kulcscsere (lásd: 4.7. fejezet) vagy új *Tanúsítvány* igénylése (lásd: 4.6. fejezet) keretében igényelhet.

Amennyiben az *Alany* valamely, a *Tanúsítvány*ban is szereplő adata megváltozik, akkor az új *Tanúsítvány*t Tanúsítvány módosítás (lásd: 4.8. fejezet) keretében kell igényelnie.

A *Tanúsítvány* megújítása során a *Hitelesítés-szolgáltató* tájékoztatja az *Igénylő*t arról, ha a korábbi *Tanúsítvány* kibocsátása óta változtak a *Tanúsítvány* használatával kapcsolatos kikötések illetve feltételek. Amennyiben az *Igénylő* nem azonos az *Előfizető*vel, akkor az *Előfizető* számára is megadja a fenti tájékoztatást.

A Tanúsítvány megújítás az érvényben levő Szolgáltatási szerződés keretében történik, és nincs szükség annak módosítására.

4.6.2. Ki kérelmezheti a tanúsítvány megújítást

A tanúsítvány megújítást olyan személy kezdeményezheti, aki a kérelem benyújtás időpontjában jogosult lenne ugyanilyen típusú új *Tanúsítványkérelem* benyújtására is.

A tanúsítvány megújítási kérelemben a kérelmezőnek nyilatkoznia kell, hogy a *Tanúsítvány*ban szereplő *Alany* azonosító adatok érvényben vannak.

A *Hitelesítés-szolgáltató* jogosult a *Tanúsítvány* megújítását kezdeményezni, ha a *Tanúsítvány* kibocsátásához használt szolgáltatói aláíró kulcsát soron kívül le kell cserélnie.

A *Tanúsítvány* megújítási kérelmek benyújtására a következő lehetőségeket biztosítja a *Hitelesítés-szolgáltató*:

- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában vagy a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál, előzetesen egyeztetett időpontban (ekkor a III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a személyes azonosítás megtörténik a találkozás során);
- elektronikus formában, a kérelmező nem álneves, a módosítani kívánt *Tanúsítvány*nál nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) *Tanúsítvány*ának felhasználásával elektronikusan aláírva vagy elektronikus bélyegzővel ellátva;
- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájába eljuttatva (ekkor a III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a személyes azonosításra más időpontban kerül sor);

4.6.3. A tanúsítvány megújítási kérelmek feldolgozása

A tanúsítvány megújítási kérelem elbírálása során a *Hitelesítés-szolgáltató* ellenőrzi, hogy:

- a benyújtott tanúsítvány megújítási kérelem hiteles;
- a tanúsítvány megújítási kérelem benyújtója rendelkezik a szükséges jogosultságokkal, felhatalmazásokkal;
- a tanúsítvány megújítási kérelem benyújtója nyilatkozott a *Tanúsítvány*ba kerülő *Alany* adatok változatlanságáról és érvényességéről;
- a *Tanúsítvány* megújítási kérelem a *Tanúsítvány* érvényességi ideje alatt került benyújtásra;
- a megújítandó *Tanúsítvány* nincs visszavonva;
- az aktuálisan elérhető információk alapján a kiadandó *Tanúsítvány* tervezett érvényessége alatt a felhasznált kriptográfiai algoritmusok még használhatók lesznek.

A tanúsítvány megújítás során alkalmazott azonosítás és hitelesítés módját a 3.4. fejezet írja le.

4.6.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* értesíti az *Igénylő*t és az *Előfizető*t az új *Tanúsítvány* kibocsátásáról.

4.6.5. A megújított tanúsítvány elfogadása

A megújított *Tanúsítvány* személyes találkozás nélkül is átvehető (letölthető).

Az *Alany* a *Tanúsítvány* használatba vételével fogadja el a *Tanúsítvány*t, nincs szükség külön nyilatkozat tételére.

4.6.6. A megújított tanúsítvány közzététele

A *Hitelesítés-szolgáltató* az eredeti *Tanúsítvány* kibocsátásával megegyező módon publikálja a megújított *Tanúsítvány*t és a hozzá tartozó *Előtanúsítvány*t.

4.6.7. További szereplők értesítése a tanúsítvány kibocsátásáról

Szervezeti tanúsítvány esetén a *Tanúsítvány* kibocsátásáról a *Hitelesítés-szolgáltató* haladéktalanul értesíti a *Képviselt szervezet Szervezeti ügyintéző*jét is.

4.7. Kulcscsere

A kulcscsere alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* egy adott *Alany* részére úgy bocsát ki új *Tanúsítvány*t, hogy a nyilvános kulcs lecserélésre kerül.

A kulcscsere során kiállított új *Tanúsítvány*ban opcionálisan változhatnak további adatok is, mint például az érvényességi idő, a CRL és OCSP hivatkozások vagy a *Tanúsítvány* aláírására használt szolgáltatói kulcs.

A II. hitelesítési osztályba tartozó tanúsítványok esetében a *Hitelesítés-szolgáltató* nem végez kulcscserét. Új kulcsot tartalmazó *Tanúsítvány* kibocsátása kizárólag az új *Tanúsítvány* igénylésének folyamata keretében történik.

4.7.1. A kulcscsere körülményei

A kulcscsere végrehajtásának nem feltétele, hogy a korábbi *Tanúsítvány* érvényes legyen, de kulcscsere kérelmet a *Hitelesítés-szolgáltató* csak a Szolgáltatási szerződés hatálya alatt fogad el.

A kulcscsere során a *Hitelesítés-szolgáltató* tájékoztatja az *Igénylő*t arról, ha a korábbi *Tanúsítvány* kibocsátása óta változtak a *Tanúsítvány* használatával kapcsolatos kikötések illetve feltételek. Amennyiben az *Igénylő* nem azonos az *Előfizető*vel, akkor az *Előfizető* számára is megadja a fenti tájékoztatást.

A kulcscsere az érvényben levő Szolgáltatási szerződés keretében történik, és nincs szükség annak módosítására.

4.7.2. Ki kérelmezheti a kulcscserét

A kulcscserét olyan személy kezdeményezheti, aki a kérelem benyújtásának időpontjában jogosult lenne új *Tanúsítványkérelem* benyújtására is.

A kulcscsere kérelemben a kérelmezőnek nyilatkoznia kell, hogy a *Tanúsítvány*ban szereplő *Alany* azonosító adatok érvényben vannak, vagy meg kell adnia az új adatokat és nyilatkoznia kell azok helyességéről.

Kulcscsere kérelmek benyújtására a következő lehetőségeket biztosítja a *Hitelesítés-szolgáltató*:

- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában vagy a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál, előzetesen egyeztetett időpontban (ekkor a III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a személyes azonosítás megtörténik a találkozás során);
- elektronikus formában, egy nem álneves, az igényelt *Tanúsítvány*énál nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) *Tanúsítvány*ának felhasználásával elektronikusan aláírva vagy elektronikus bélyegzővel ellátva, a *Hitelesítés-szolgáltató* email címére megküldve.
- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájába eljuttatva (ekkor a III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a személyes azonosításra más időpontban kerül sor).

4.7.3. A kulcscsere kérelmek feldolgozása

A benyújtott kulcscsere kérelem elbírálása során a *Hitelesítés-szolgáltató* ellenőrzi, hogy:

- a benyújtott kérelem hiteles;
- a kérelem benyújtója rendelkezik a szükséges jogosultságokkal, felhatalmazásokkal;
- a kérelemben megadott adatok érvényesek;

- az aktuálisan elérhető információk alapján a kiadandó *Tanúsítvány* tervezett érvényessége alatt a felhasznált kriptográfiai algoritmusok még használhatók lesznek.

Kulcscsere kérelem teljesítését megelőzően a kérelmezőt azonosítani kell a 3.3. fejezetben megadottak szerint.

4.7.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* értesíti az *Igénylő*t és az *Előfizető*t az új *Tanúsítvány* kibocsátásáról.

4.7.5. A kulcscserével megújított tanúsítvány elfogadása

A *Hitelesítés-szolgáltató* az *Igénylő* azonosítását követően adja át az új nyilvános kulcshoz kibocsátott *Tanúsítvány*t.

4.7.6. A kulcscserével megújított tanúsítvány közzététele

A *Hitelesítés-szolgáltató* az eredeti *Tanúsítvány* kibocsátásával megegyező módon publikálja a megújított *Tanúsítvány*t és a hozzá tartozó *Előtanúsítvány*t.

4.7.7. További szereplők értesítése a tanúsítvány kibocsátásáról

Szervezeti tanúsítvány esetén a *Tanúsítvány* kibocsátásáról a *Hitelesítés-szolgáltató* haladéktalanul értesíti a *Képviselt szervezet Szervezeti ügyintéző*jét is.

4.8. Tanúsítvány módosítás

A tanúsítvány módosítás alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* egy adott *Alany* részére bocsát ki új *Tanúsítvány*t változatlan nyilvános kulccsal, de megváltozott *Alany* azonosító adatokkal.

A *Tanúsítvány* módosítása műszakilag új *Tanúsítvány* kibocsátását jelenti. A korábbi, már nem érvényes adatokat tartalmazó *Tanúsítvány*t a *Hitelesítés-szolgáltató* köteles visszavonni (lásd: 4.9. fejezet).

A tanúsítvány módosítás során kiállított új *Tanúsítvány*ban változhatnak további adatok is, mint például az érvényességi idő, a CRL és OCSP hivatkozások vagy a *Tanúsítvány* aláírására használt szolgáltatói kulcs.

4.8.1. A tanúsítvány módosítás körülményei

A tanúsítvány módosítás szükségessé válik az alábbi esetekben:

- az *Alany Tanúsítvány*ban szereplő adatai megváltoznak;
- a *Hitelesítés-szolgáltató Tanúsítvány* kibocsátó rendszerében megváltozik az adott *Tanúsítvány*t kibocsátó CA valamely a "Subject DN"-ben szereplő azonosító adata vagy a nyilvános kulcsa és így szolgáltatói *Tanúsítvány*a;

- a *Tanúsítvány*ban a *Hitelesítés-szolgáltató* által megadott, a szolgáltatásra jellemző adatok (tanúsítvány profil) megváltoznak.

A tanúsítvány módosítás feltételei:

- *Tanúsítvány* módosítási kérelem a *Tanúsítvány* érvényességi ideje alatt benyújtásra kerül;
- a megújítandó *Tanúsítvány* nincs visszavonva;
- a *Tanúsítvány*hoz tartozó magánkulcs nem kompromittálódott.

Tanúsítvány módosítási kérelmet a *Hitelesítés-szolgáltató* csak a Szolgáltatási szerződés hatálya alatt fogad el.

Ha az *Alany* korábbi *Tanúsítvány*a visszavonásra került vagy lejárt, akkor új *Tanúsítvány*t csak kulcscsere (lásd: 4.7. fejezet) vagy új *Tanúsítvány* igénylése (lásd: 4.6. fejezet) keretében igényelhet.

Az új *Tanúsítvány* kibocsátása során a *Hitelesítés-szolgáltató* tájékoztatja az *Igénylő*t arról, ha a korábbi *Tanúsítvány* kibocsátása óta változtak a *Tanúsítvány* használatával kapcsolatos kikötések illetve feltételek.

Amennyiben az *Igénylő* nem azonos az *Előfizető*vel, akkor az *Előfizető* számára is megadja a fenti tájékoztatást.

A tanúsítvány módosítás az érvényben levő Szolgáltatási szerződés keretében történik, és nincs szükség annak módosítására.

4.8.2. Ki kérelmezheti a tanúsítvány módosítást

A tanúsítvány módosítást olyan személy kezdeményezheti, aki a kérelem benyújtásának időpontjában jogosult lenne új *Tanúsítványkérelem* benyújtására is.

A tanúsítvány módosítási kérelemben a kérelmezőnek meg kell adnia az új adatokat és nyilatkoznia kell azok helyességéről.

A *Hitelesítés-szolgáltató* kezdeményezi a *Tanúsítvány* módosítását, amennyiben bármilyen forrásból tudomására jut az *Alany Tanúsítvány*ban szereplő adataiban bekövetkezett változás.

Tanúsítvány módosítási kérelmek benyújtására a következő lehetőségeket biztosítja a *Hitelesítés-szolgáltató*:

- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában vagy a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál, előzetesen egyeztetett időpontban (ekkor a III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a személyes azonosítás megtörténik a találkozás során);
- elektronikus formában, egy nem álneves, az igényelt *Tanúsítvány*énál nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) *Tanúsítvány*ának felhasználásával elektronikusan aláírva vagy elektronikus bélyegzővel ellátva, a *Hitelesítés-szolgáltató* email címére megküldve.
- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájába eljuttatva (ekkor a III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a személyes azonosításra más időpontban kerül sor);

4.8.3. A tanúsítvány módosítási kérelmek feldolgozása

A benyújtott *Tanúsítvány* módosítási kérelem elbírálása során a *Hitelesítés-szolgáltató* ellenőrzi, hogy:

- a benyújtott kérelem hiteles;
- a kérelem benyújtója rendelkezik a szükséges jogosultságokkal, felhatalmazásokkal;
- a kérelemben megadott új adatok érvényesek;
- a kérelem a *Tanúsítvány* érvényességi ideje alatt került benyújtásra;
- az aktuálisan elérhető információk alapján a kiadandó *Tanúsítvány* tervezett érvényessége alatt a felhasznált kriptográfiai algoritmusok még használhatók lesznek.

A *Hitelesítés-szolgáltató* az új *Alany* azonosító adatok valódiságának ellenőrzése során ugyanúgy jár el, mint az új *Tanúsítvány* kibocsátása előtti kezdeti ellenőrzésnél.

Tanúsítvány módosítása kérelem teljesítését megelőzően a kérelmezőt azonosítani kell a 3.5. fejezetben megadottak szerint.

4.8.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* értesíti az *Igénylő*t és az *Előfizető*t az új *Tanúsítvány* kibocsátásáról.

4.8.5. A módosított tanúsítvány elfogadása

Mivel a Tanúsítvány módosítás során nem történik új kulcs generálása, így nem kell kulcsot átadni az *Alany* részére. A módosított *Tanúsítvány* személyes találkozás nélkül is átvehető (letölthető). Az *Alany* a *Tanúsítvány* használatba vételével fogadja el a *Tanúsítvány*t, nincs szükség külön nyilatkozat tételére.

4.8.6. A módosított tanúsítvány közzététele

A *Hitelesítés-szolgáltató* az eredeti *Tanúsítvány* kibocsátásával megegyező módon publikálja a megújított *Tanúsítvány*t és a hozzá tartozó *Előtanúsítvány*t.

4.8.7. További szereplők értesítése a tanúsítvány kibocsátásáról

Szervezeti tanúsítvány esetén a *Tanúsítvány* kibocsátásáról a *Hitelesítés-szolgáltató* haladéktalanul értesíti a *Képviselt szervezet Szervezeti ügyintéző*jét is.

4.9. 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.

4.9.1. A tanúsítvány visszavonás körülményei

Végfelhasználói tanúsítvány visszavonásának okai

A *Hitelesítés-szolgáltató* intézkedik a végfelhasználói *Tanúsítvány* visszavonásáról az alábbi esetekben:

- az *Igénylő* vagy az *Előfizető* írásban kéri a *Tanúsítvány* visszavonását;
- az *Igénylő* vagy az *Előfizető* értesíti a *Hitelesítés-szolgáltató*t arról, hogy az eredeti *Tanúsítványkérelmet* nem hagyta jóvá, és utólag sem ad erre jóváhagyást;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódott;
- a *Hitelesítés-szolgáltató* bizonyítékot szerez arról, hogy a *Tanúsítvány*ban szereplő valamely teljes minősítésű domain név vagy IP cím feletti kontrol vagy engedély ellenőrzésére nem támaszkodhat;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő nyilvános kulcs már nem felel meg a 6.1.5. és 6.1.6. fejezetekben meghatározott követelményeknek;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t jogellenesen használták;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy az *Előfizető* megszegte a Szolgáltatási szerződés vagy az Általános szerződési feltételek szerinti egy vagy több kötelezettségét;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő doménnév (FQDN) vagy IP cím használati jogosultsága megszűnt (pl.: a bíróság megtiltotta a domén használatát vagy a tulajdonos nem hosszabbította meg a domén regisztrációját);
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a wildcard tanúsítványt megtévesztő doménnév hitelesítésére használták;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő adatokban lényeges változás történt;
- a *Tanúsítvány* módosítása az *Alany*ra vonatkozó adatok változása miatt;

- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t nem a CABF Baseline Requirements, a vonatkozó *Hitelesítési rend* illetve *Szolgáltatási szabályzat* szerint bocsátották ki;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban foglalt bármely adat pontatlan;
- a *Hitelesítés-szolgáltató* már nem jogosult *Tanúsítvány*okat kibocsátani és a meglévő *Tanúsítvány*okra vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodik;
- a visszavonást előírja a *Hitelesítés-szolgáltató Hitelesítési rend*je vagy *Szolgáltatási szabályzat*a;
- a *Hitelesítés-szolgáltató* értesül egy bemutatott vagy bizonyított eljárásról, amellyel az *Előfizető* magánkulcsa meghatározható, olyan módszereket fejlesztettek ki, amelyekkel az könnyen kiszámítható a nyilvános kulcs alapján (pl. a Debian gyenge kulcsok, lásd `http://wiki.debian.org/SSLkeys`), vagy ha egyértelmű bizonyíték van arra, hogy a magánkulcs létrehozásához használt eljárás hibás volt.
- ha a *Tanúsítvány*t a *Hitelesítés-szolgáltató* harmadik féltől származó dokumentum alapján állította ki, és e harmadik fél ezen igazolást írásban visszavonja;
- a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t kibocsátó hitelesítő egység magánkulcsa kompromittálódhatott;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy az *Előfizető* nem teljesítette valamely anyagi kötelezettségét a vonatkozó Szolgáltatási szerződésnek megfelelően;
- a Szolgáltatási szerződés megszűnik;
- a *Hitelesítés-szolgáltató* tevékenységét befejezte;
- a bizalmi felügyelet ezt jogerős és végrehajtható határozatában elrendeli;
- a visszavonást jogszabály kötelezővé teszi.

Szolgáltatói Tanúsítvány visszavonásának okai

A *Hitelesítés-szolgáltató* köteles intézkedni az általa üzemeltetett köztes hitelesítő egység *Tanúsítvány*ának visszavonásáról az alábbi esetekben:

- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató írásban kéri a *Tanúsítvány* visszavonását;
- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató értesíti a kibocsátó *Hitelesítés-szolgáltató*t arról, hogy az eredeti *Tanúsítvány* kérelmet nem hagyta jóvá, és utólag sem ad erre jóváhagyást;

- a *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem a kizárólagos birtokában van;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő nyilvános kulcs már nem felel meg a 6.1.5 és 6.1.6 fejezetekben meghatározott követelményeknek;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t jogellenesen használták;
- amennyiben a *Tanúsítvány*t nem a vonatkozó *Hitelesítési rend* illetve *Szolgáltatási szabályzat* szerint bocsátották ki vagy a köztes hitelesítő egység működése nem felel meg a rá vonatkozó *Hitelesítési rend*nek vagy *Szolgáltatási szabályzat*nak;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő valamely információ téves vagy félrevezető;
- a kibocsátó CA vagy a köztes CA bármilyen okból megszünteti a tevékenységét, és nem állapodott meg más *Hitelesítés-szolgáltató*-val a *Tanúsítvány* visszavonási szolgáltatás nyújtásáról ;
- amennyiben a *Hitelesítés-szolgáltató* már nem lenne jogosult *Tanúsítvány*okat kibocsátani és a meglevő *Tanúsítvány*okra vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;
- a visszavonást előírja a kibocsátó CA *Hitelesítési rend*je vagy *Szolgáltatási szabályzat*a;
- a *Tanúsítvány* módosítása a hitelesítési egységre, vagy a *Hitelesítés-szolgáltató*ra vonatkozó adatok változása miatt;
- amennyiben a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);
- a *Hitelesítés-szolgáltató* a tevékenységét befejezte;
- a visszavonást jogszabály kötelezővé teszi.

Más Szolgáltató által üzemeltetett köztes CA Tanúsítvány visszavonásának okai

A *Hitelesítés-szolgáltató* köteles intézkedni a más hitelesítés-szolgáltató által üzemeltetett köztes hitelesítő egység *Tanúsítvány*ának visszavonásáról az alábbi esetekben:

- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató írásban kéri a *Tanúsítvány* visszavonását;
- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató értesíti a kibocsátó *Hitelesítés-szolgáltató*t arról, hogy az eredeti *Tanúsítvány* kérelmet nem hagyta jóvá, és utólag sem ad erre jóváhagyást;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató kizárólagos birtokában van;

- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő nyilvános kulcs már nem felel meg a 6.1.5 és 6.1.6 fejezetekben meghatározott követelményeknek;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t jogellenesen használták;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t nem a vonatkozó *Hitelesítési rend* illetve *Szolgáltatási szabályzat* szerint bocsátották ki vagy a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató működése nem felel meg a rá vonatkozó *Hitelesítési rend*nek vagy *Szolgáltatási szabályzat*nak;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő valamely adat téves vagy félrevezető;
- a kibocsátó CA vagy a köztes CA bármilyen okból megszünteti a tevékenységét, és nem állapodott meg más *Hitelesítés-szolgáltató*-val a *Tanúsítvány* visszavonási szolgáltatás nyújtásáról ;
- amennyiben a *Hitelesítés-szolgáltató* már nem lenne jogosult *Tanúsítvány*okat kibocsátani és a meglevő *Tanúsítvány*okra vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;
- a visszavonást előírja a kibocsátó CA *Hitelesítési rend*je vagy *Szolgáltatási szabályzat*a;
- a *Tanúsítvány* módosítása a hitelesítési egységre, vagy az azt üzemeltető hitelesítés-szolgáltatóra vonatkozó adatok változása miatt;
- ha a *Tanúsítvány*t *Hitelesítés-szolgáltató* harmadik féltől származó dokumentum alapján állította ki, és e harmadik fél ezen igazolást írásban visszavonja;
- amennyiben a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);
- a hitelesítési egységet működtető hitelesítés-szolgáltató, vagy a *Tanúsítvány*át kibocsátó *Hitelesítés-szolgáltató* a tevékenységét befejezte;
- a visszavonást jogszabály kötelezővé teszi.

4.9.2. 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*;
- a *Hitelesítés-szolgáltató*.

4.9.3. 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 (lásd 1.2.3. fejezet) *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. A kulcscsere szabályait a 4.7. fejezet tartalmazza.

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`

4.9.4. A visszavonási kérelemre vonatkozó kivárási idő

A *Hitelesítés-szolgáltató* nem alkalmaz kivárási időt a visszavonási kérelmek teljesítése során.

4.9.5. A visszavonási eljárás maximális hossza

A visszavonási kérelmeket a *Hitelesítés-szolgáltató* legkésőbb a kérelem beérkezését követő 24 órán belül feldolgozza.

A személyesen benyújtott kérelmek esetén a megérkezés időpontja az, amikor a *Hitelesítés-szolgáltató* ügyfélszolgálati munkatársa átveszi a kérelmet.

A postán küldött kérelmek esetén a megérkezés időpontja az, amikor a kérelem nyitvatartási időben a *Hitelesítés-szolgáltató*hoz megérkezik.

Az elektronikus levélben (email) küldött kérelmek esetén a megérkezés időpontja az, amikor a levél nyitvatartási időben a *Hitelesítés-szolgáltató* szerverén lévő, erre a célra elkülönített `visszavonas@e-szigno.hu` postafiókba ér. A nyitvatartási időn kívül érkező elektronikus levelek a legközelebbi nyitvatartási idő kezdetén tekinthetőek megérkezettnek.

A *Hitelesítés-szolgáltató* kizárólag az 1.2. fejezetben megjelölt címekre küldött kérelmekre vállalja e követelmények teljesítését, más csatornákon vagy címekre – különösen a *Hitelesítés-szolgáltató* egyes munkatársainak közvetlenül – küldött kérelmek feldolgozásával kapcsolatban semmilyen rendelkezésre állást nem vállal.

A *Hitelesítés-szolgáltató* a honlapján keresztül benyújtott visszavonási kérelmeket a nap 24 órájában késedelem nélkül feldolgozza.

A *Hitelesítés-szolgáltató* a rögzített formátumú SMS üzenet küldéséve benyújtott visszavonási kérelmeket az üzenet beérkezését követően a nap 24 órájában késedelem nélkül feldolgozza.

A *Hitelesítés-szolgáltató* a *Weboldal-hitelesítő tanúsítvány*okkal kapcsolatos problémabejelentéseket 24 órán belül kivizsgálja, és dönt a további szükséges lépésekről.

A *Hitelesítés-szolgáltató* a vizsgálat során az alábbi körülményeket veszi alapul a döntés meghozatalához:

- a bejelentett probléma jellege;
- a visszavonás következményei;
- az adott Tanúsítvánnyal vagy *Előfizető*vel kapcsolatban kapott bejelentések száma;
- a bejelentést tevő személy vagy szervezet;
- vonatkozó jogi szabályozás.

A *Hitelesítés-szolgáltató* a *Weboldal-hitelesítő tanúsítvány*okat a 4.9.1-ben meghatározott feltételek bekövetkezését követően legkésőbb 24 órán belül visszavonja.

A *Hitelesítés-szolgáltató* a *Weboldal-hitelesítő tanúsítvány*okat kibocsátó köztes hitelesítési egységek *Tanúsítvány*ait a 4.9.1-ben meghatározott feltételek bekövetkezését követően legkésőbb 7 napon belül visszavonja.

4.9.6. Az Érintett felek számára javasolt eljárás a visszavonási információ ellenőrzésére

A *Tanúsítvány*ban foglalt információ elfogadását és felhasználását megelőzően a *Hitelesítés-szolgáltató* által garantált biztonsági szint megtartásához szükséges, hogy az *Érintett felek* megfelelően gondosan járjanak el, így különösen javasolt ellenőrizniük a tanúsítási láncban található

valamennyi *Tanúsítvány* érvényességét a vonatkozó műszaki szabványoknak megfelelően. Az ellenőrzésnek ki kell terjednie a *Tanúsítvány*ok érvényességének ellenőrzésére, a szabályzatok és a kulcshasználat megkötéseire, az egyes *Tanúsítvány*okban meghivatkozott CRL vagy OCSP alapú visszavonási státusz információk ellenőrzésére.

4.9.7. A visszavonási lista kibocsátás gyakorisága

A *Hitelesítés-szolgáltató* naponta legalább egyszer kibocsát új *Tanúsítvány visszavonási list*át a végfelhasználói *Tanúsítvány*okat kibocsátó hitelesítési egységeire.

A *Tanúsítvány visszavonási list*ák érvényességi ideje 25 óra.

A *Hitelesítés-szolgáltató* naponta bocsát ki ugyanabban az időpontban új *Tanúsítvány visszavonási list*át a köztes hitelesítési egységeire. A *Tanúsítvány visszavonási list*ák érvényességi ideje 25 óra.

4.9.8. A visszavonási lista előállítása és közzététele közötti idő maximális hossza

A *Tanúsítvány visszavonási lista* (CRL) előállítása és közzététele között legfeljebb 5 perc telik el.

4.9.9. Valós idejű tanúsítvány állapot ellenőrzés lehetősége

A *Hitelesítés-szolgáltató* valós idejű tanúsítvány-állapot (OCSP) szolgáltatást nyújt.

4.9.10. A valós idejű tanúsítvány állapot ellenőrzésre vonatkozó követelmények

A valós idejű tanúsítvány-állapot szolgáltatás megfelel a 4.10 fejezet követelményeinek.

A *Hitelesítés-szolgáltató* GET metódussal is nyújt OCSP szolgáltatást.

4.9.11. A visszavonási hirdetmények egyéb elérhető formái

A *Hitelesítés-szolgáltató* a publikus tanúsítványtárában elérhetővé teszi – az állapotuk megjelölésével – a visszavont *Tanúsítvány*okat is, így a tanúsítványtárban keresve az *Ügyfel*ek és *Érintett felek* személyesen (alkalmazás segítsége nélkül) is ellenőrizhetik egy *Tanúsítvány* visszavonási állapotát.

4.9.12. A kulcs kompromittálódásra vonatkozó speciális követelmények

A *Hitelesítés-szolgáltató* valamely hitelesítési egysége magánkulcsának kompromittálódása esetén megtesz minden ésszerű erőfeszítést annak érdekében, hogy az eseményről értesítse az *Érintett felek*et. A szolgáltatói *Tanúsítvány*ok állapotváltozását nyilvánosságra hozza a honlapján.

A *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány*okhoz tartozó magánkulcs kompromittálódása esetén a *Hitelesítés-szolgáltató* képes a kompromittálódott magánkulcshoz tartozó végfelhasználói *Tanúsítvány* visszavonására. A visszavonási ok információt (reasonCode) ilyen esetben a "keyCompromise (1)" (kulcs kompromittálódás) értékre állítja.

4.9.13. A felfüggesztés körülményei

A *Weboldal-hitelesítő tanúsítvány*ok érvényességét nem lehet felfüggeszteni.

4.9.14. Ki kérelmezheti a felfüggesztést

Nem értelmezhető.

4.9.15. A felfüggesztési kérelemre vonatkozó eljárás

Nem értelmezhető.

4.9.16. A felfüggesztés maximális hossza

Nem értelmezhető.

4.10. Tanúsítvány állapot szolgáltatások

A *Tanúsítvány*ok visszavonási állapotának lekérdezésére a *Hitelesítés-szolgáltató* a következő lehetőségeket biztosítja:

- OCSP – online tanúsítvány állapot lekérdezési szolgáltatás;
- CRL – *Tanúsítvány visszavonási lista*.

A *Hitelesítés-szolgáltató* egy belső *Visszavonási állapot nyilvántartás*t üzemeltet, amely tartalmazza valamennyi - a *Hitelesítés-szolgáltató* által kiadott - *Tanúsítvány* aktuális visszavonási állapotát, beleértve az érvényes, a visszavont és a felfüggesztett állapotokat.

Visszavonás esetén a folyamat sikeres lezárását követően a *Tanúsítvány* új állapota azonnal – lásd: 4.9. fejezet – megjelenik a *Hitelesítés-szolgáltató Visszavonási állapot nyilvántartás*sában.

A *Visszavonási állapot nyilvántartás* a lejárt érvényességű *Tanúsítvány*ok visszavonási állapotát is tartalmazza, azok a kibocsátó CA érvényességi idejének végéig elérhetők maradnak.

A *Hitelesítés-szolgáltató* a *Tanúsítvány visszavonási list*ákat a belső *Visszavonási állapot nyilvántartás* alapján állítja elő, így a visszavonási állapot változások megjelennek a változás után kibocsátott első *Tanúsítvány visszavonási list*ában.

Az OCSP szolgáltatás válaszadó egységei által kibocsátott OCS válaszok minden esetben a *Visszavonási állapot nyilvántartás*ból származó az OCSP válaszban jelzett időpontnak megfelelő információn alapulnak.

A *Hitelesítés-szolgáltató* által kibocsátott OCSP válasz csak az adott hitelesítő egység által aláírt, a *Hitelesítés-szolgáltató Tanúsítványtár*ában szereplő *Tanúsítvány*okra vonatkozóan tartalmazhat "good" állapot információt.

4.10.1. Működési jellemzők

A *Hitelesítés-szolgáltató* egyes hitelesítő egységei az alábbi gyakorisággal bocsátanak ki *Tanúsítvány visszavonási list*át:

- A *Hitelesítés-szolgáltató* SHA-256 alapú rendszerében működtetett produktív (nem gyökér) hitelesítő egységek az adott hitelesítő egység által kiadott bármely *Tanúsítvány* visszavonási állapotának változása esetén a változástól számított 60 percen belül, de legfeljebb 24 óránként bocsátanak ki CRL-t.
- A "Microsec e-Szigno Root CA 2009" gyökér hitelesítő egység legfeljebb 24 óránként bocsát ki CRL-t.
- Az "e-Szigno Root CA 2017" gyökér hitelesítő egység legfeljebb 24 óránként bocsát ki CRL-t.
- A *Hitelesítés-szolgáltató* ECC alapú rendszerében működtetett produktív (nem gyökér) hitelesítő egységek az adott hitelesítő egység által kiadott bármely *Tanúsítvány* visszavonási állapotának változása esetén a változástól számított 60 percen belül, de legfeljebb 24 óránként bocsátanak ki CRL-t.

Valamennyi *Tanúsítvány visszavonási lista* érvényességi ideje 25 óra.

Az egyes *Tanúsítvány*okra vonatkozó mindenkori aktuális *Tanúsítvány visszavonási list*ák az alábbi oldalon érhetők el:

`https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/szolgaltatoi-tanusitvanyok.html`

A *Tanúsítvány visszavonási list*ák hatálybalépésének időpontja ("thisUpdate") egyúttal azt az időpontot is jelöli, amikor a hitelesítő egység a *Tanúsítvány visszavonási list*át összeállította és aláírását megkezdte. Ezt követően a *Tanúsítvány visszavonási lista* publikálásáig hosszú *Tanúsítvány visszavonási list*ák esetén egy vagy két perc is eltelhet. A következő *Tanúsítvány visszavonási lista* megjelenése (következő frissítés, "nextUpdate") azt a legkésőbbi időpontot jelzi, amikortól kezdve a következő lista a nyilvánosság számára elérhető. Ennek megfelelően a *Tanúsítvány visszavonási lista* hatálybalépési időpontja és a következő *Tanúsítvány visszavonási lista* megjelenési időpontja között a fenti időintervallumoknál hosszabb időintervallumok is megjelenhetnek, ez nem befolyásolja azt, hogy a *Tanúsítvány visszavonási list*ák megjelenése között legfeljebb 24 óra telik el.

Tekintettel arra, hogy a felkínált szolgáltatások közül OCSP segítségével állapítható meg egy *Tanúsítvány* érvényessége a leggyorsabban és legegyszerűbben, a *Hitelesítés-szolgáltató* az OCSP használatát javasolja *Ügyfel*ei számára.

Online tanúsítvány-állapot szolgáltatás (OCSP)

A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok visszavonási állapotát OCSP szolgáltatás segítségével is közzéteszi.

Az SHA-256 alapú tanúsítványok tekintetében a *Hitelesítés-szolgáltató* az IETF RFC 6960 szerinti "authorized responder" elv szerint nyújtja az OCSP szolgáltatást, így minden egyes hitelesítő egysége külön OCSP válaszadót hitelesít felül, amely az adott hitelesítő egység által kibocsátott tanúsítványok állapotára vonatkozóan nyújt információt (1.3.1. fejezet).

Az OCSP szolgáltatás fő jellemzői:

- Az OCSP szolgáltatás nyilvánosan és ingyenesen érhető el, a *Tanúsítvány visszavonási list*ákhoz hasonlóan bármely *Érintett fél* igénybe veheti. Lekérdezéskor nincsen szükség autentikációra.

- Az OCSP szolgáltatás a tanúsítványokban feltüntetett URL-eken érhető el.
- Az OCSP szolgáltatás megfelel az IETF RFC 5019 [26] követelményeinek, így támogatja a nagy terhelésű PKI rendszereket is, amelyek egy könnyített megoldást igényelnek a kommunikációs igény és a kliens oldali feldolgozási igény csökkentése érdekében.
- Az IETF RFC 6960 "Response Pre-production" eljárása alapján, a kibocsátott OCSP válasz a lekérdezést megelőzően is létrejöhet, és nem feltétlenül tartalmaz "nonce" elemet. A *Hitelesítés-szolgáltató* egyazon választ több lekérdezésre is visszaadhatja. Az OCSP válaszban szereplő "thisUpdate" és "producedAt" időpontok megegyeznek, de ezek megelőzhetik a lekérdezés időpontját.
- A válaszban szereplő "nextUpdate" időpont mindig ki van töltve, és a válaszadói tanúsítvány lejáratánál nem későbbi időpontot tartalmaz.
- a kibocsátott OCSP válaszban szereplő "thisUpdate" érték nem lehet 24 óránál régebbi, vagyis a *Hitelesítés-szolgáltató* legalább 24 óránként frissíti az OCSP válaszokat.
- Az OCSP válaszban szereplő "nextUpdate" és "thisUpdate" értékek különbsége nem lehet nagyobb, mint 10 nap.
- Az OCSP válaszban szereplő "nextUpdate" érték nem lehet későbbi, mint a "BasicOCSPResponse.certs" mezőben található *Tanúsítvány*ok "notAfter" értékeinek maximuma, vagy a tanúsítvány mező hiányában a "BasicOCSPResponse" mezőben hivatkozott *Tanúsítvány*t kibocsátó *Tanúsítvány* "notAfter" értéke.
- Az OCSP válaszok mindig a *Hitelesítés-szolgáltató Visszavonási állapot nyilvántartás*ában szereplő aktuális információt tartalmazzák, azonban ha az OCSP válasz "thisUpdate" időpontja korábbi, mint az az időpont, amelyre nézve az ellenőrzést végezzük — amely vagy korábbi vagy egybeesik a lekérdezés időpontjával -–, akkor az OCSP válasz nem egyértelmű bizonyíték harmadik fél számára a *Tanúsítvány* visszavonási állapotára vonatkozóan.

4.10.2. A szolgáltatás rendelkezésre állása

A *Hitelesítés-szolgáltató* biztosítja a *Tanúsítványtár*, valamint a *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány*ok használatára vonatkozó kikötések és feltételek folyamatos elérhetőségét éves szinten legalább 99%-os rendelkezésre állás mellett, ahol az eseti szolgáltatáskiesések maximális időtartama legfeljebb 24 óra.

A *Hitelesítés-szolgáltató* biztosítja a *Visszavonási állapot nyilvántartás*ok és a visszavonás kezelési szolgáltatás éves szinten legalább 99%-os rendelkezésre állását, ahol az eseti szolgáltatáskiesések időtartama legfeljebb 24 óra.

A *Visszavonási állapot nyilvántartás*ok válaszideje normál terhelés esetén 10 másodpercnél kevesebb.

4.10.3. Opcionális lehetőségek

A *Hitelesítés-szolgáltató* a jelen fejezetben ismertetettek szerint többféle (CRL illetve kétféle OCSP) szolgáltatást is nyújt, amelyek keretében az *Ügyfel*ek és *Érintett felek* ellenőrizhetik a *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány*ok visszavonási állapotát. Mindezeken

kívül a *Hitelesítés-szolgáltató* publikus *Tanúsítványtár*ában is elérhetővé teszi – az állapotuk megjelölésével – a visszavont *Tanúsítvány*okat is, így a *Tanúsítványtár*ban keresve az *Ügyfel*ek és *Érintett felek* személyesen (alkalmazás segítsége nélkül) is ellenőrizhetik egy *Tanúsítvány* visszavonási állapotát.

4.11. Az előfizetés vége

Az *Ügyfél*lel kötött szerződés megszűnése esetén a *Hitelesítés-szolgáltató* visszavonja a szerződés keretében kibocsátott *Tanúsítvány*okat.

4.12. Magánkulcs letétbe helyezése és visszaállítása

A *Hitelesítés-szolgáltató* a *Weboldal-hitelesítő tanúsítvány*hoz tartozó magánkulcshoz nem nyújt kulcsletét szolgáltatást.

4.12.1. Kulcsletét és visszaállítás rendje és szabályai

A *Weboldal-hitelesítő tanúsítvány*hoz tartozó magánkulcs nem helyezhető letétbe.

4.12.2. Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

A *Weboldal-hitelesítő tanúsítvány*hoz tartozó magánkulcs nem helyezhető letétbe, így ezzel kapcsolatban nem kell szimmetrikus rejtjelező kulcsokat kezelni.

5. Elhelyezési, eljárásbeli és üzemeltetési előírások

A *Hitelesítés-szolgáltató* széles körben elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmaz.

A *Hitelesítés-szolgáltató* nyilvántartást vezet a szolgáltatás nyújtásával kapcsolatos rendszerelemekről és erőforrásokról, és ezekkel kapcsolatos kockázatelemzést végez. Az egyes elemekkel kapcsolatban a kockázatokkal arányos védelmi megoldásokat alkalmaz.

A *Hitelesítés-szolgáltató* figyelemmel kíséri a kapacitás igényeket és biztosítja, hogy megfelelő feldolgozási teljesítmény és tárolási kapacitás álljon rendelkezésre a szolgáltatás nyújtásához.

5.1. Fizikai követelmények

A *Hitelesítés-szolgáltató* gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen és a kritikus szolgáltatások eszközeit érintő fizikai kockázatát minimalizálja.

A fizikai óvintézkedések célja a *Hitelesítés-szolgáltató* által birtokolt információra illetve fizikai zónáira irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken valósítják meg a *Hitelesítés-szolgáltató* rendszerében.

A biztosított védelem mértéke megfelel a *Hitelesítés-szolgáltató* által végzett kockázatelemzésben megállapított fenyegetettség mértékének.

A megfelelő védelem biztosítása érdekében:

- A *Hitelesítés-szolgáltató* védett számítógéptermében valósítja meg a szigorúbban védendő szolgáltatásokat. Ez a számítógépterem speciálisan erre a célra lett tervezve és kialakítva, tervezésénél különböző védelmi szempontok [a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés (beléptetés ellenőrzése és felügyelete), áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása stb.] egységes érvényesítésére került sor.
- A *Hitelesítés-szolgáltató* ügyfélszolgálati irodája úgy lett kialakítva, hogy reális költségek mellett képes legyen kielégíteni a regisztrációs szolgáltatásokkal szemben támasztott követelményeket.
- A *Hitelesítés-szolgáltató* úgy alakította ki mobil regisztrációs egységeit, hogy azok megfeleljenek a regisztrációs szolgáltatásokkal szemben támasztott követelményeknek.
- A *Hitelesítés-szolgáltató* valamennyi kritikus szolgáltatását egy külön biztonsági zónában valósítja meg, az ehhez szükséges valamennyi eszközt egy – a biztonsági zóna részét képező – védett számítógépteremben helyezi el.

5.1.1. A telephely elhelyezése és szerkezeti felépítése

A *Hitelesítés-szolgáltató* informatikai rendszereit fizikai és logikai védelemmel ellátott, megfelelően biztonságos *Adatközpont*ban helyezte el és üzemelteti, amely megakadályozza az illetéktelen hozzáférést. Az *Adatközpont* elhelyezése és kialakítása során egymásra épülő és egymást támogató védelmi megoldásokat alkalmaz – őrzés, biztonsági zárak, behatolás érzékelők, videó megfigyelő rendszer, beléptető rendszer stb. – amelyek együttesen egy erős védelmi szintet biztosítanak a szolgáltatásban részt vevő informatikai rendszerek és a szolgáltató által tárolt bizalmas adatok megóvására.

5.1.2. Fizikai hozzáférés

A *Hitelesítés-szolgáltató* védi a szolgáltatás nyújtásában részt vevő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében. A *Hitelesítés-szolgáltató* biztosítja, hogy:

- az *Adatközpont*ba történő minden belépés regisztrálásra kerül;
- az *Adatközpont*ba csak a megfelelő jogosultságokkal rendelkező, bizalmi szerepkört betöltő munkatársak léphetnek be önállóan;
- az önálló jogosultsággal nem rendelkező személyek csak indokolt esetben, a szükséges ideig tartózkodhatnak a gépteremben megfelelő jogosultságú kísérő személyzettel;
- a belépési logokat folyamatosan archiválják és legalább hetente megvizsgálják.

Az eszközök aktivizáló adatai (jelszavak, PIN kódok) a géptermen belül sem tárolhatók nyílt formában.

Jogosulatlan személyek jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják;
- a bejelentkezett terminálokat nem hagyják felügyelet nélkül;
- nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet.

A gépterem elhagyásakor az adminisztrátornak ellenőriznie kell, hogy:

- az *Adatközpont* minden berendezése megfelelően biztonságos üzemállapotban van;
- egyetlen terminálon sem maradt bejelentkezve;
- a fizikai tároló eszközök megfelelően be lettek zárva;
- a fizikai védelmet biztosító rendszerek, berendezések megfelelően működnek;
- a riasztó rendszer aktiválva lett.

A rendszeres fizikai biztonsági vizsgálatokat kijelölt felelősök végzik. A vizsgálatok eredményét megfelelő naplóbejegyzésekben rögzítik.

5.1.3. Áramellátás és légkondicionálás

A *Hitelesítés-szolgáltató Adatközpont*jában olyan szünetmentes áramellátó rendszert alkalmaz, amely:

- megfelelő teljesítménnyel rendelkezik az adatközpont informatikai és a kisegítő létesítményi rendszerei áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózatból érkező feszültség ingadozások, feszültség kimaradások, tüskék és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramtermelő berendezéssel rendelkezik, amely - üzemanyag utántöltést lehetővé téve - tetszőleges időtartamig képes a szükséges energia biztosítására.

Az *Adatközpont*ba nem juthat be közvetlenül a külső környezet levegője. Az *Adatközpont* levegőjének tisztaságát megfelelő szűrőrendszer alkalmazása biztosítja, amely kiszűri a levegőből a különféle szennyeződéseket (por, szennyező anyagok, korrozív anyagok, mérgező vagy gyúlékony anyagok). A szellőző rendszer megfelelő szűrés mellett biztosítja az operátorok biztonságos munkavégzéséhez szükséges mennyiségű friss levegőt.

A levegő nedvességtartalma az informatikai rendszerek által megkívánt szintre van csökkentve.

A *Hitelesítés-szolgáltató* megfelelő teljesítményű hűtőrendszert használ a szükséges üzemi hőmérséklet biztosítása, az informatikai eszközök túlhevülésének megakadályozása érdekében.

5.1.4. Beázás és elárasztódás veszély kezelése

A *Hitelesítés-szolgáltató* biztonsági zónájának kialakítása során fontos szempont volt a beázás és elárasztódás veszélyének minimalizálása. A biztonsági zóna teljes területe mentes a vizesblokkoktól, nincs a közelében sem csatorna sem vízvezeték. A védett számítógépteremben a biztonságot tovább növeli az álpadló alkalmazása.

5.1.5. Tűz megelőzés és tűzvédelem

A *Hitelesítés-szolgáltató Adatközpont*jában az illetékes tűzoltóparancsnokság által jóváhagyott tűzvédelmi rendszer működik.

Minden helyiségben jól látható helyen található a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készülék.

5.1.6. Adathordozók tárolása

A *Hitelesítés-szolgáltató* megvédi valamennyi adathordozóját a jogosulatlan hozzáféréstől és a véletlen rongálódástól. Minden napló és archív adatot legalább két példányban hoz létre. A példányokat egymástól fizikailag elkülönítve tárolja, egymástól biztonságos távolságra lévő helyszíneken. A tárolt adathordozókat védi a káros környezeti behatásoktól, mint pl. alacsony vagy magas hőmérséklet, szennyeződés, nedvesség, napfény, erős mágneses tér, erős sugárzás.

A *Hitelesítés-szolgáltató* az elsődleges adathordozókat kódzáras, tűzálló páncélszekrényekben tárolja a hitelesítő szervezet operátori helyiségében, a másolati példányokat páncélszekrényben az ügyfélszolgálati irodában.

5.1.7. Hulladék megsemmisítése

A *Hitelesítés-szolgáltató* a környezetvédelmi előírások betartásával gondoskodik feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről.

A *Hitelesítés-szolgáltató* a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat még tartalmuk törlése után sem használja fel nem bizalmas minősítésű adatok tárolására, az ilyen eszközök nem vihetők ki a *Hitelesítés-szolgáltató* területéről. A *Hitelesítés-szolgáltató* a meghibásodott vagy bármely más okból használhatatlanná, feleslegessé vált, bizalmas minősítésű adatokat tartalmazó adathordozókat – a selejtezési szabályzatának megfelelően – fizikailag megsemmisíti:

- a papíralapú dokumentumokat iratmegsemmisítő géppel felaprítja;
- a merevlemezeket szétszereli és a kritikus alkatrészeket összetöri;
- az optikai lemezeket erre alkalmas iratmegsemmisítő géppel megsemmisíti.

5.1.8. A mentési példányok fizikai elkülönítése

A *Hitelesítés-szolgáltató* legalább heti rendszerességgel előállít olyan mentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható. A mentéseket - legalább az utolsó teljes mentést is beleértve - egy olyan külső helyszínen tárolja, amelynek a fizikai és működési védelme

azonos az elsődleges helyszínével. Az elsődleges és a tartalék helyszínek között biztosítja az adatok biztonságos továbbítását.

A mentett állományokból legalább évente szúrópróbaszerű kiválasztással jegyzőkönyvezett helyreállítási tesztet végez.

5.2. Eljárásbeli előírások

A *Hitelesítés-szolgáltató* gondoskodik arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltesse.

Az eljárásbeli óvintézkedések célja, hogy a bizalmi szerepkörök kijelölésével és elkülönítésével, az egyes szerepkörök felelősségének dokumentálásával, az egyes feladatokhoz szükséges személyzeti létszámok, a kizáró szerepkörök, valamint az egyes szerepkörökben elvárt azonosítás és hitelesítés meghatározásával kiegészítse, egyúttal fokozza a fizikai környezetre és személyzetre vonatkozó óvintézkedések hatásosságát.

A *Hitelesítés-szolgáltató* belső irányítási rendszere biztosítja a jogszabályoknak és belső szabályzatainak megfelelő működést. Rendszerében minden rendszerelemhez és minden folyamathoz egyértelműen hozzárendelhető az adott rendszerelemért, vagy folyamatért felelős személy. A *Hitelesítés-szolgáltató* rendszerében élesen elkülönülnek egymástól a fejlesztési és üzemeltetési folyamatok. A rendszer megfelelő működését a független rendszervizsgáló és a *Hitelesítés-szolgáltató* belső folyamatainak rendszeres ellenőrzése biztosítja.

5.2.1. Bizalmi szerepkörök

A *Hitelesítés-szolgáltató* feladatai ellátásához 24/2016. BM rendelet [9] előírásainak megfelelő bizalmi szerepköröket (a rendelet szövegezésében bizalmi munkaköröket) hozott létre. A jogosultságok és funkciók oly módon lettek megosztva az egyes bizalmi szerepkörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére.

A *Hitelesítés-szolgáltató* a következő bizalmi szerepköröket határozza meg az alábbi felelősségi körökkel:

A *Hitelesítés-szolgáltató* informatikai rendszeréért általánosan felelős vezető: Az informatikai rendszerért felelős személy.

Biztonsági tisztviselő: Biztonságtechnikai főmunkatárs, a szolgáltatás biztonságáért általánosan felelős személy.

Rendszeradminisztrátor: Infrastruktúra adminisztrátor. Feladata a *Hitelesítés-szolgáltató* rendszereinek telepítése, konfigurálása, karbantartása. Felelős a rábízott rendszerelemek megbízható és folyamatos működéséért, valamint a technológia fejlődésének nyomon követéséért, az egyes rendszerelemekben való biztonsági rések felderítéséért és megoldási javaslatok kidolgozásáért.

Operátor: Rendszerüzemeltető, az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.

Független rendszervizsgáló: A *Hitelesítés-szolgáltató* naplózott, illetve archivált adatállományát vizsgáló, a *Hitelesítés-szolgáltató* által a szabályszerű működés érdekében megvalósított

kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.

Regisztrációs felelős: A végfelhasználói *Tanúsítvány*ok előállításának, kibocsátásának, visszavonásának jóváhagyásáért felelős személy;

Perszonalizáció területén tevékenykedő tisztviselő: Feladata a tanúsítványkérelmek összeállítása;

A bizalmi szerepkörök ellátására a *Hitelesítés-szolgáltató* biztonságért felelős vezetője formálisan kinevezi a *Hitelesítés-szolgáltató* munkatársait.

Bizalmi szerepkört csak a *Hitelesítés-szolgáltató*val munkaviszonyban álló személyek láthatnak el, megbízási szerződés keretében a bizalmi szerepkörök nem láthatók el.

A bizalmi szerepkörökről a *Hitelesítés-szolgáltató* naprakész nyilvántartást vezet, a változásokat haladéktalanul bejelenti a Nemzeti Média- és Hírközlési Hatóságnak.

5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

A *Hitelesítés-szolgáltató* biztonsági és üzemeltetési szabályzata előírja, hogy csak védett környezetben, kettő, bizalmi szerepkört betöltő munkatárs egyidejű fizikai jelenlétében végezhetők el az alábbi műveletek:

- a *Hitelesítés-szolgáltató* saját szolgáltatói kulcspárjának generálása;
- a szolgáltatói magánkulcs mentése;
- a szolgáltatói magánkulcs aktiválása;
- a szolgáltatói magánkulcs megsemmisítése.

A felsorolt műveleteket végrehajtó személyek közül legalább az egyiknek rendszeradminisztrátornak kell lennie és a másik személy nem lehet független rendszervizsgáló.

A felsorolt műveletek végrehajtása során illetéktelen személy nem lehet jelen a helyiségben.

5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés

A *Hitelesítés-szolgáltató* informatikai rendszerét kezelő felhasználók egyedi azonosító adatokkal rendelkeznek, amely lehetővé teszi a felhasználók biztonságos azonosítását és hitelesítését.

A felhasználók a hitelesítés-szolgáltatás szempontjából kritikus informatikai rendszerekhez csak azonosítás és hitelesítés után férhetnek hozzá.

Az azonosító és hitelesítő adatok a felhasználói jogosultságok megszűnésekor haladéktalanul visszavonásra kerülnek.

Az informatikai rendszer minden felhasználója és az adminisztratív folyamatok minden szereplője személy szerint kerül azonosításra. A fizikai hozzáférés ellenőrzéséhez a *Hitelesítés-szolgáltató* RFID kártyára épülő beléptető rendszert használ, a logikai hozzáférés ellenőrzése *Elektronikus aláírást létrehozó eszköz*ön kiadott VPN *Tanúsítvány*ok segítségével történik. Sikeres hitelesítés nélkül egyetlen biztonsági szempontból kritikus feladatot sem lehet végrehajtani. A *Hitelesítés-szolgáltató* minden munkatársa annak megfelelő hozzáférési jogosultsággal rendelkezik, amely a feladatköre ellátásához elengedhetetlenül szükséges.

5.2.4. Egymást kizáró szerepkörök

A *Hitelesítés-szolgáltató* munkatársai egyidejűleg több bizalmi szerepkört is betölthetnek, de a *Hitelesítés-szolgáltató* biztosítja, hogy:

- a biztonsági tisztviselő és a regisztrációs felelős nem töltheti be a független rendszervizsgálói szerepkört;
- a rendszeradminisztrátor nem töltheti be a biztonsági tisztviselő és a független rendszervizsgálói szerepkört;
- az informatikai rendszerért általánosan felelős vezető nem láthatja el a biztonsági tisztviselő és a független rendszervizsgáló feladatkörét.

A fentieken túl a *Hitelesítés-szolgáltató* törekszik a bizalmi szerepkörök teljes szétválasztására.

5.3. Személyzetre vonatkozó előírások

A *Hitelesítés-szolgáltató* gondoskodik arról, hogy személyzeti politikája, illetve a munkatársak alkalmazására vonatkozó gyakorlata fokozza és támogassa a *Hitelesítés-szolgáltató* működésének megbízhatóságát. A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a visszaélések kockázatának csökkentése.

A *Hitelesítés-szolgáltató* már a felvételi szakaszban foglalkozik a személyi biztonsággal, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését. Valamennyi bizalmi szerepkör esetén a szerepkört betöltő személyeknek kinevezésükkor érvényes erkölcsi bizonyítvánnyal kell rendelkezniük. Minden bizalmi szerepkört betöltő alkalmazottnak és külső félnek – aki a *Hitelesítés-szolgáltató* szolgáltatásaival kapcsolatba kerül – titoktartási nyilatkozatot kell aláírnia.

A *Hitelesítés-szolgáltató* egyúttal biztosítja valamennyi munkakör betöltéséhez a szükséges közös, általános, illetve az egyes szerepkörök betöltéséhez szükséges speciális szakmai ismeretek megszerzését, illetve továbbfejlesztését.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

Felvételi követelményként a *Hitelesítés-szolgáltató* minden dolgozója számára legalább középfokú végzettséget ír elő, de a *Hitelesítés-szolgáltató* a továbbiakban is gondot fordít arra, hogy dolgozói megfelelő képzésben részesüljenek. Közvetlenül a felvételt követően a *Hitelesítés-szolgáltató* új dolgozóit képzésben részesíti, melynek keretében el kell sajátítania a munkája elvégzéséhez szükséges ismereteket. Regisztrációs tisztviselő szerepkört csakis olyan munkatárs tölthet be, aki olyan tanfolyamot végzett, amelyen elsajátította a *Hitelesítés-szolgáltató* által elfogadott igazolványok (személyi igazolvány, útlevél és jogosítvány) felismerését. A *Hitelesítés-szolgáltató* általában támogatja a dolgozók szakmai fejlődését, valamint elvárja, hogy a dolgozók saját szakterületükön önállóan fejlesszék tudásukat. A *Hitelesítés-szolgáltató* bizonyos dolgozóinak munkaköri kötelessége a technikai és üzleti újdonságok felderítése és összegyűjtése, rendszerezése, és ezen ismeretek megosztása munkatársaikkal.

A *Hitelesítés-szolgáltató*nál bizalmi szerepkört csak olyan személy tölthet be, akinek a befolyásmentességét és szakértelmét a *Hitelesítés-szolgáltató* igazolni tudja. A bizalmi szerepkört

betöltő személyeknek mentesnek kell lenniük az összeférhetetlenségtől, amely veszélyeztethetné a *Hitelesítés-szolgáltató* tevékenységének pártatlanságát.

Az informatikai rendszerért általánosan felelős vezető csak olyan személy lehet, aki rendelkezik:

- szakirányú felsőfokú végzettséggel (matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség);
- legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal.

5.3.2. Előélet vizsgálatára vonatkozó eljárások

A *Hitelesítés-szolgáltató* vezető munkakörben illetve bizalmi szerepkörben csak olyan alkalmazottakat foglalkoztat, akik:

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, amely a büntetlenséget befolyásolhatja;
- nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkozástól eltiltás hatálya alatt.

Kinevezéskor a *Hitelesítés-szolgáltató* vezető munkakört betöltő alkalmazottjának nyilatkozatával, bizalmi szerepkört betöltő alkalmazottjának 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolnia büntetlen előéletét.

A *Hitelesítés-szolgáltató* a felvételi eljárás során ellenőrzi a jelentkező önéletrajzában megadott releváns információk valódiságát, úgy mint előző munkahely, szakmai referenciák, legfontosabb képzettség.

5.3.3. Képzési követelmények

A *Hitelesítés-szolgáltató* az újonnan felvett alkalmazottakat képzésben részesíti, amely során elsajátítják az adott munkakör ellátásához szükséges mértékben:

- a PKI alapismereteket;
- a *Hitelesítés-szolgáltató* informatikai rendszerének sajátosságait és kezelésének módját;
- a szerepkörük ellátásához szükséges speciális ismereteket;
- a *Hitelesítés-szolgáltató* nyilvános és belső szabályzataiban meghatározott folyamatokat, eljárásokat;
- az egyes tevékenységek jogi következményeit;
- az alkalmazandó informatikai biztonsági szabályokat;
- az adatvédelmi szabályokat.

A *Hitelesítés-szolgáltató* a regisztrációban közreműködő munkatársakat képzésben részesíti a *Tanúsítvány*ba kerülő adatok ellenőrzésével kapcsolatos veszélyekről és kockázatokról.

A regisztrációban közreműködő munkatársaknak kinevezésük előtt sikeres vizsgát kell tenniük a vonatkozó adatellenőrzési követelmények és eljárások ismeretéből, és ennek megtörténtét a *Hitelesítés-szolgáltató* dokumentálja.

A *Hitelesítés-szolgáltató* éles informatikai rendszereihez csak a képzést sikeresen teljesítő alkalmazottak kapnak hozzáférési jogosultságot.

5.3.4. Továbbképzési gyakoriságok és követelmények

A *Hitelesítés-szolgáltató* gondoskodik arról, hogy az alkalmazottak folyamatosan a megfelelő tudással rendelkezzenek, így szükség esetén továbbképzést, vagy ismétlő jellegű képzést kell tartani.

A *Hitelesítés-szolgáltató* továbbképzést tart, ha folyamataiban vagy informatikai rendszerében változás áll be.

A képzési anyag legalább 12 havonta felülvizsgálatra kerül, és tartalmazza az új fenyegetéseket és biztonsági megoldásokat.

A továbbképzés megfelelően dokumentálásra kerül, amelyből egyértelműen megállapítható a továbbképzés tematikája és a résztvevő dolgozók köre.

5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

A *Hitelesítés-szolgáltató* nem alkalmaz kötelező jellegű körforgást az egyes munkabeosztások között.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

A *Hitelesítés-szolgáltató* a dolgozókkal kötendő munkaszerződésben szabályozza a dolgozók felelősségre vonásának lehetőségeit a dolgozó által elkövetett mulasztások, hibák, vétlen vagy szándékos károkozások esetére. Amennyiben egy munkatárs – szándékosan vagy gondatlanul – kötelezettségeit megsérti, vele szemben a *Hitelesítés-szolgáltató* szankciót alkalmazhat, amelyet az elkövetés módjára és következményeire tekintettel állapít meg. Szankcióként alkalmazható a jutalom megvonása, fegyelmi eljárás, elbocsátás, kinevezés visszavonása vagy büntetőjogi felelősségre vonás kezdeményezése.

Valamennyi bizalmi szerepkört betöltő munkatárs a szerepkörbe kinevezéskor a foglalkoztatási dokumentumok részeként:

- írásos tájékoztatást kap jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról;
- munkaköri leírást kap, mely tartalmazza az őt érintő biztonsági feladatokat;
- titoktartási nyilatkozatot ír alá, melyben a biztonsági intézkedések be nem tartásával járó, őt érintő következmények (büntető szankciók) is megtalálhatóak.

A felsorolt dokumentumok tartalmazzák azokat a munkajogi következményeket és egyéb szankciókat, amelyek kötelezettségszegés esetén alkalmazhatóak.

5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

A *Hitelesítés-szolgáltató* bizalmi munkakörben csak vele munkaviszonyban álló személyt alkalmaz.

Az egyéb feladatok ellátására alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket a *Hitelesítés-szolgáltató* lehetőség szerint a korábban már minősített beszállítók listájáról választ. A beszállítókkal a *Hitelesítés-szolgáltató* a munkavégzést megelőzően írásban szerződést köt.

Valamennyi szerződő fél – még a tényleges munkavégzés megkezdése előtt – titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során későbbiekben megismert üzleti/vállalati titkokat illetéktelen személynek nem fedi fel, egyéb módon nem hasznosítja. A titoktartási nyilatkozat tartalmazza a megszegése esetén alkalmazandó szankciókat is. A szerződés alapján foglalkoztatott külső munkavállalókkal szemben elvárás a megfelelő szakismeret megléte, részükre a *Hitelesítés-szolgáltató* nem tart képzéseket.

5.3.8. A személyzet számára biztosított dokumentációk

A *Hitelesítés-szolgáltató* folyamatosan biztosítja a dolgozók részére a szerepkörük ellátásához szükséges aktuális dokumentációk, szabályzatok rendelkezésre állását.

Minden bizalmi munkakört betöltő munkatárs írásban megkapja a következő dokumentumokat:

- a *Hitelesítés-szolgáltató* szervezeti biztonsági szabályzata;
- aláírandó titoktartási nyilatkozat;
- egyéni munkaköri leírás;
- a tervezett és rendkívüli továbbképzések alkalmával az adott oktatási formához tartozó oktatási segédanyagokat.

A szervezeti biztonsági szabályzatban bekövetkező változásokról írásos értesítő formájában minden dolgozó tájékoztatást kap.

5.4. Naplózási eljárások

A *Hitelesítés-szolgáltató* a biztonságos informatikai környezet fenntartása érdekében a teljes informatikai rendszerét átfogó eseménynaplózó és ellenőrző rendszert üzemeltet.

5.4.1. A tárolt események típusai

A *Hitelesítés-szolgáltató* az általánosan elfogadott informatikai biztonsági gyakorlatnak megfelelően naplóz minden olyan biztonsággal kapcsolatos eseményt, amely információt szolgáltathat az informatikai rendszerben vagy annak fizikai környezetében történt eseményekről, változásokról. Minden naplóbejegyzésnél eltárolja:

- az esemény időpontját;
- az esemény típusát;

- a végrehajtás sikerességét illetve sikertelenségét;
- a felhasználó vagy rendszer azonosítóját, aki/amely az eseményt kiváltotta.

Az összes lényeges naplóbejegyzést elérhetővé teszi a független rendszervizsgálók részére, akik a *Hitelesítés-szolgáltató* működésének megfelelőségét vizsgálják.

A *Hitelesítés-szolgáltató* naplózza minimálisan az alábbi eseményeket:

- BELSŐ ÓRA
  - a belső óra szinkronizációja az UTC időhöz, beleértve az üzemszerű újrakalibrálásokat is;
  - a szinkronizáció elvesztése;
- NAPLÓZÁS
  - a naplózó rendszer vagy egyes komponenseinek leállítása, újraindítása;
  - a naplózás bármilyen beállításának módosítása, mint pl. gyakoriság, riasztási küszöb érték, vizsgált esemény;
  - a tárolt naplózási adatok módosítása vagy törlése;
  - a naplózó rendszer hibája miatt végzett tevékenységek;
- RENDSZER BEJELENTKEZÉSEK
  - sikeres bejelentkezések, sikertelen bejelentkezési próbálkozások bizalmi szerepkörökbe;
  - jelszó alapú azonosítás esetén:
    - az engedélyezett sikertelen bejelentkezési próbálkozások számának megváltoztatása;
    - az engedélyezett sikertelen bejelentkezési próbálkozások számának elérése felhasználói bejelentkezéskor;
    - sikertelen bejelentkezések miatt zárolt felhasználó újbóli engedélyezése;
  - az azonosítási technika változtatása (például jelszó alapúról PKI alapúra);
- KULCSKEZELÉS
  - a szolgáltatói kulcsok teljes életciklusára vonatkozó valamennyi esemény (kulcsgenerálás, betöltés, elmentés stb.);
- TANÚSÍTVÁNY KEZELÉS
  - szolgáltatói *Tanúsítvány*ok kibocsátásával, állapotváltozásával kapcsolatos minden esemény;
  - minden kérés, beleértve a *Tanúsítvány* kibocsátást, kulcscserét, megújítást, visszavonást;
  - a kérések feldolgozásával kapcsolatos események;

  - a *Tanúsítvány* kibocsátásával kapcsolatban végrehajtott minden ellenőrzési tevékenység, ide értve az ellenőrzéssel kapcsolatban történt telefonbeszélgetések időpontját, telefonszámot, a hívott személy nevét és a megtudott információkat;
  - tanúsítványkérelmek elutasítása;
  - *Tanúsítvány* kibocsátása, állapotváltozása;
- ADATMOZGÁSOK
  - bármilyen, a biztonság szempontjából kritikus adat manuális bevitele a rendszerbe;
  - a rendszer által fogadott, biztonsági szempontból fontos adatok, üzenetek;
- CA KONFIGURÁCIÓ
  - a CA tetszőleges komponensének átparaméterezése, a beállításon történt bármilyen változtatás;
  - felhasználók felvétele, törlése;
  - felhasználói szerepkörök, jogosultságok megváltoztatása;
  - a tanúsítvány profil megváltoztatása;
  - CRL profil megváltoztatása;
  - új CRL lista előállítása;
  - OCSP válasz generálása;
  - *Időbélyegző* generálása;
  - az előírt időpontossági küszöb túllépése;
- HSM
  - HSM installálása;
  - HSM eltávolítása;
  - HSM selejtezése, megsemmisítése;
  - HSM szállítása;
  - HSM tartalmának törlése (nullázás);
  - HSM feltöltése kulcsokkal, tanúsítványokkal;
- KONFIGURÁCIÓ VÁLTOZÁSA
  - hardver;
  - szoftver;
  - operációs rendszer;
  - javító csomag;
- FIZIKAI HOZZÁFÉRÉS, TELEPHELY BIZTONSÁG
  - személy belépése a CA komponenseket tartalmazó biztonsági területre és onnan kilépése;

  - hozzáférés egy CA rendszer komponenshez;
  - a fizikai biztonság ismert vagy gyanított megsértése;
  - tűzfal és router forgalmak;
- MŰKÖDÉSI RENDELLENESSÉGEK
  - rendszerösszeomlás, hardver hiba;
  - szoftveres hibák;
  - szoftverintegritás ellenőrzési hiba;
  - hibás vagy rossz helyre továbbított üzenetek;
  - hálózatot ért támadások, támadási kísérletek;
  - berendezés hiba;
  - elektromos hálózati üzemzavar;
  - szünetmentes tápegység hiba;
  - lényeges hálózati szolgáltatás hozzáférési hiba;
  - a *Hitelesítési rend* vagy a *Szolgáltatási szabályzat* megsértése;
  - operációs rendszer órájának törlése;
- EGYÉB ESEMÉNYEK
  - személy kinevezése biztonsági szerepkörbe;
  - operációs rendszer telepítése;
  - PKI alkalmazás telepítése;
  - rendszer elindítása;
  - belépési kísérlet a PKI alkalmazásba;
  - jelszó módosítási, beállítási kísérlet;
  - a belső adatbázis elmentése, visszaállítása mentésből;
  - fájl műveletek (pl. létrehozás, átnevezés, áthelyezés);
  - adatbázis hozzáférés.

5.4.2. A naplófájl feldolgozásának gyakorisága

A *Hitelesítés-szolgáltató* független rendszervizsgálói a keletkezett naplóbejegyzéseket minden munkanapon átvizsgálják.

A kiértékelés során meggyőződnek a vizsgált naplóállományok hitelességéről és sértetlenségéről, ellenőrzik a bejegyzésekben talált hibaüzeneteket, szükség esetén dokumentálják az eltérést és intézkedéseket hoznak az eltérés okának megszüntetése érdekében.

Az informatikai rendszerek ellenőrzésére a *Hitelesítés-szolgáltató* automatizált ellenőrző rendszereket is használ, amelyek előre beállított szempontok szerint folyamatosan figyelik a keletkező naplóbejegyzéseket és szükség esetén riasztják az üzemeltetés munkatársait. Az automatizált ellenőrző rendszerekből kapott értesítéseket az IT üzemeltetés munkatársai 24 órán belül feldolgozzák és az eredményeket kiértékelik.

A vizsgálat ténye, a vizsgálat eredményei és az esetleges feltárt hiányosságok elhárítása érdekében meghozott intézkedések megfelelően dokumentálásra kerülnek.

5.4.3. A naplófájl megőrzési időtartama

Az online rendszerből való kitörlés előtt a naplóállományokat a *Hitelesítés-szolgáltató* archiválja és gondoskodik azok biztonságos megőrzéséről az 5.5.2 fejezetben meghatározott ideig.

Ezen időtartamig a *Hitelesítés-szolgáltató* biztosítja az archivált adatok olvashatóságát, megőrzi az ehhez szükséges szoftver és hardver eszközöket.

5.4.4. A naplófájl védelme

A *Hitelesítés-szolgáltató* az előírt megőrzési ideig tárolja és védi a keletkezett naplóállományokat. A megőrzési idő teljes időtartama alatt biztosítja a naplóadatok:

- védelmét az illetéktelen felfedés ellen: a naplóállományokhoz csak az arra jogosultak – elsősorban a független rendszervizsgálók – férhetnek hozzá;
- rendelkezésre állását: a jogosultak számára biztosítja a naplóállományokhoz való hozzáférést;
- integritását: megakadályozza például a naplóállományokban bármilyen adat módosítását, törlését, bejegyzések sorrendjének megváltoztatását.

A *Hitelesítés-szolgáltató* a naplóbejegyzéseket minősített *Időbélyegző*vel látja el, a naplóbejegyzések törlések és beszúrások észrevétlen végrehajtását kizáró módon kerülnek tárolásra.

A naplóállományt a véletlen és szándékos rongálások ellen biztonsági mentések védik. A személyes adatokat tartalmazó naplóbejegyzések esetében a *Hitelesítés-szolgáltató* gondoskodik az adatok bizalmas tárolásáról. A naplóállományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán feltétlenül szükségük van. A *Hitelesítés-szolgáltató* a hozzáféréseket biztonságos módon ellenőrzi. A naplóállományokat a *Hitelesítés-szolgáltató* biztonságos környezetben őrzi. Az állományokról a működés másodlagos helyszínén másolati példányokat is tart.

5.4.5. A naplófájl mentési eljárásai

Az üzemeltetés során az egyes rendszerekben folyamatosan keletkező naplóbejegyzésekből napi naplóállományok generálódnak.

A napi naplóállományokat a *Hitelesítés-szolgáltató* 2 példányban archiválja és a példányokat egymástól fizikailag elkülönülő helyszíneken az előírt ideig megőrzi.

A mentés operatív folyamatait a *Hitelesítés-szolgáltató* mentési szabályzatai írják le részletesen.

5.4.6. A naplózás adatgyűjtési rendszere

A naplóbejegyzéseket az egyes alkalmazások automatikusan gyűjtik és továbbítják a naplózó rendszer felé.

A naplózó funkciók automatikusan indulnak a rendszer indításakor és a rendszer működésének teljes időtartama alatt folyamatosan működnek.

Az automatikus vizsgáló és naplózó rendszerek működési rendellenessége esetén a *Hitelesítés-szolgáltató* felfüggeszti az érintett területek működését az üzemzavar elhárításáig.

5.4.7. Az eseményeket kiváltó alanyok értesítése

A hibaeseményt kiváltó személyeket, szervezeteket és alkalmazásokat a *Hitelesítés-szolgáltató* nem feltétlenül értesíti minden esetben, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az esemény kiváltásában érintett *Ügyfel*eknek ilyen esetben kötelességük a *Hitelesítés-szolgáltató*val való együttműködés a hiba feltárása érdekében.

5.4.8. Sebezhetőség felmérése

A naplóbejegyzések napi rendszerességgel végzett feldolgozásán túl a *Hitelesítés-szolgáltató* szakemberei figyelik a nyilvánosan elérhető információt a lehetséges sérülékenységekről, szoftver javító csomagokról. Elemzik a gyűjtött információt, osztályba sorolják a sérülékenységet és szükség esetén értesítik a vezetőséget az eredményről és intézkedési tervet javasolnak a rendszer biztonságának növelésére.

Minden nagyobb jelentőségű feltárt hiányosság vagy külső fenyegetettség esetén az észlelésétől számított 48 órán belül, de legalább évente egyszer a *Hitelesítés-szolgáltató* szakemberei átfogó sebezhetőség vizsgálatot végeznek, amely segítségével feltérképezik a potenciális belső és külső fenyegetettségeket, amelyek jogosulatlan hozzáféréseket eredményezhetnek, hatással lehetnek a *Tanúsítvány* kiadási folyamatra, vagy lehetővé teszik a *Tanúsítvány*ban tárolt adatok módosítását.

A vizsgálat eredményei alapján a *Hitelesítés-szolgáltató*

- intézkedési tervet hoz létre és hajt végre a sérülékenységek megszüntetése érdekében, vagy
- dokumentálja a döntés alapjául szolgáló tényeket, elfogadja a maradvány kockázatokat és nem hoz intézkedési tervet a sérülékenység megszüntetésére.

Az új program verziókat vagy program javító csomagokat a *Hitelesítés-szolgáltató* először a teszt rendszeren telepíti és csak a sikeres tesztek elvégzése után kerülnek telepítésre a szolgáltatásokat nyújtó éles rendszeren.

Az új szoftver verziók vagy javító csomagok nem kerülnek bevezetésre az éles rendszeren, amennyiben olyan további sérülékenységet vagy instabilitást okoznak a rendszer működésében, ami nagyobb gondot eredményez az alkalmazásukból származó előnynél. Az alkalmazás mellőzésének okát a *Hitelesítés-szolgáltató* dokumentálja.

5.5. Adatok archiválása

5.5.1. Az archivált adatok típusai

A *Hitelesítés-szolgáltató* felkészült elektronikus és papíralapú dokumentumok megfelelően biztonságos, hosszú idejű archiválására.

A *Hitelesítés-szolgáltató* minimálisan az alábbi jellegű információt archiválja:

- a *Hitelesítés-szolgáltató* akkreditációjával kapcsolatos valamennyi irat;
- a *Hitelesítési rend*(ek) és *Szolgáltatási szabályzat*(ok) valamennyi kibocsátott verziója;
- az Általános szerződési feltételek valamennyi kibocsátott verziója;

- a *Hitelesítés-szolgáltató* működésével kapcsolatos szerződések;
- a regisztrációval kapcsolatos valamennyi információ, beleértve
  - a *Tanúsítványkérelem*mel együtt benyújtott valamennyi irat;
  - a személyes azonosítás során bemutatott dokumentum(ok) azonosító adatai;
  - Szolgáltatási szerződés(ek);
  - egyéb előfizetői jognyilatkozatok;
  - a kérelmet elbíráló regisztrációs ügyintéző azonosítója;
  - a kérelem elbírálásának körülményei és eredménye;
- a *Tanúsítvány*okkal kapcsolatos valamennyi információ a teljes életciklusra vonatkozóan;
- valamennyi elektronikus és papíralapú naplóbejegyzés.

5.5.2. Az archívum megőrzési időtartama

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;

5.5.3. Az archívum védelme

A *Hitelesítés-szolgáltató* valamennyi archivált adatot két példányban, két egymástól fizikailag elkülönült helyszínen őrzi. Az egyetlen hiteles példányban rendelkezésre álló papíralapú dokumentumról hiteles papíralapú, vagy elektronikus másolatot készít a vonatkozó jogszabályok betartásával.

A két helyszín mindegyike teljesíti az archiválással szemben támasztott biztonsági és egyéb követelményeket.

Az archivált adatok megőrzése során a *Hitelesítés-szolgáltató* gondoskodik az archivált adatok

- sértetlenségének megőrzéséről;
- illetéktelen megismerés elleni védelméről;
- rendelkezésre állásáról;
- hitelességének megőrzéséről.

Az archivált elektronikus adatokat legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel és minősített *Időbélyegző*vel látja el.

5.5.4. Az archívum mentési folyamatai

A *Hitelesítés-szolgáltató* a papír alapú dokumentumok eredeti példányáról hiteles elektronikus másolatot készít a vonatkozó jogszabályok betartásával.

Az elektronikus másolatokat a többi védendő elektronikus dokumentummal azonos szabályok szerint tárolja.

A *Hitelesítés-szolgáltató* a hiteles elektronikus másolatok archiválása után az eredeti papír alapú dokumentumokat megsemmisítheti.

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi elektronikus naplóbejegyzés tartalmaz időjelzést, amelyen legalább másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

Az időpontot a *Hitelesítés-szolgáltató* belső órája adja, amelyet a *Hitelesítés-szolgáltató* két egymástól független Stratum-1 UTC referencia időforrással szinkronizál:

- az egyik pontos idő forrás a műhold alapú GPS jelet használja;
- a másik pontos idő forrás a hosszúhullámú pontos idő szolgáltatásra (DCF77) támaszkodik.

A *Hitelesítés-szolgáltató* a fenti két független Stratum-1 időforráshoz 0,1 másodperc pontossággal szinkronizálja saját belső óráját. E szinkronizációt a *Hitelesítés-szolgáltató* naponta legalább négy alkalommal elvégzi.

A *Hitelesítés-szolgáltató* a belső óra pontosságának ilyen szinten tartásával garantálja, hogy valamennyi időjelzés pontossága legfeljebb 1 másodperccel tér el az UTC időalaptól.

A *Hitelesítés-szolgáltató* a napi naplóállományokat minősített *Időbélyegző*vel látja el.

Az archivált adatok megőrzése során szükség esetén (pl. algoritmusváltás, az eredeti *Időbélyegző* érvényességének lejárata) a *Hitelesítés-szolgáltató* gondoskodik az adatok hitelességének megőrzéséről.

5.5.6. Az archívum gyűjtési rendszere

A *Hitelesítés-szolgáltató* védett informatikai rendszerén belül keletkeznek a naplóbejegyzések, onnan csak az elektronikusan aláírt, minősített *Időbélyegző*vel védett naplóállományok kerülhetnek ki.

A szolgáltatás nyújtása során keletkezett papíralapú iratok egy eredeti példányát a *Hitelesítés-szolgáltató* az általa működtetett belső adattárban tárolja és őrzi.

5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

A *Hitelesítés-szolgáltató* a naplóállományok előállítását automatikusan végzi, a hitelesített naplóállományokat naponta állítja elő.

Az archivált adatállományokat védi a jogosulatlan hozzáféréstől.

Az arra jogosultaknak biztosítja az archivált adatokhoz való ellenőrzött hozzáférést:

- az *Ügyfel*ek jogosultak a róluk tárolt adatok megtekintésére;
- jogi eljárásokban bizonyíték nyújtása céljából biztosítani kell a szükséges adatokat.

5.6. Szolgáltatói kulcs cseréje

A *Hitelesítés-szolgáltató* gondoskodik arról, hogy az általa használt *Hitelesítő egység*ek folyamatosan rendelkezzenek a működéshez szükséges, érvényes kulccsal és Tanúsítvánnyal. A szolgáltatói *Tanúsítvány*ok lejárta illetve a hozzájuk kapcsolódó kulcsok használati idejének lejárta előtt elegendő idővel új kulcspárt generál a *Hitelesítő egység* számára, és arról időben értesíti *Ügyfel*eit. Az új szolgáltatói kulcsot a jelen szabályzatnak megfelelően generálja és kezeli.

Amennyiben a *Hitelesítés-szolgáltató* megváltoztatja végfelhasználói *Tanúsítvány*okat kibocsátó bármely szolgáltatói tanúsítványának kulcsait, az alábbiak szerint jár el:

- publikálja az érintett *Tanúsítvány*ait és nyilvános kulcsait a 2.2 fejezetben meghatározott előírásoknak megfelelően;
- a szolgáltatói kulcscsere után a kibocsátandó végfelhasználói *Tanúsítvány*okat már csak az új szolgáltatói kulcsok felhasználásával írja alá;
- megőrzi a régi szolgáltatói *Tanúsítvány*ait és nyilvános kulcsait, valamint lehetővé teszi az aláírások érvényességének ellenőrzését mindaddig, amíg a régi szolgáltatói kulccsal aláírt valamennyi aláíró *Tanúsítvány* érvényességi ideje lejár.

5.7. Kompromittálódást és katasztrófát követő helyreállítás

A *Hitelesítés-szolgáltató* katasztrófa esetén minden szükséges intézkedést meghoz annak érdekében, hogy a szolgáltatáskiesésből eredő károkat minimalizálja és a szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa.

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

A hiba elhárítása után az eseményt jelenti a Nemzeti Média- és Hírközlési Hatóságnak, mint felügyeleti szervnek.

5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások

A *Hitelesítés-szolgáltató* rendelkezik üzletmenet folytonossági tervvel.

A *Hitelesítés-szolgáltató* kialakított és folyamatosan üzemben tart egy teljes értékű tartalékrendszert, amely az elsődleges helyszíntől biztonságos távolságra, földrajzilag különböző helyszínen található és önállóan is alkalmas a szolgáltatások teljes körű ellátására.

A *Hitelesítés-szolgáltató* folyamatosan teszteli a tartalékrendszer működését és évente felülvizsgálja az üzletmenet folytonossági terveit.

A *Hitelesítés-szolgáltató* megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik a hardver és szoftver meghibásodások valamint az adatsérülések okozta szolgáltatáskiesés minimalizálása érdekében. A szolgáltatások helyreállíthatóságát a *Hitelesítés-szolgáltató* háttérszerződései és saját tartalék eszközei garantálják.

5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

A *Hitelesítés-szolgáltató* informatikai rendszereit megbízható hardver és szoftver komponensekből építette fel. A kritikus funkciókat redundáns rendszerelemek alkalmazásával valósította meg úgy, hogy azok egy elem meghibásodása esetén is képesek legyenek a további működésre.

A *Hitelesítés-szolgáltató* naponta teljes mentést készít az adatbázisairól és a keletkezett naplózási eseményekről.

A *Hitelesítés-szolgáltató* olyan gyakorisággal készít teljes rendszermentést, amely biztosítja, hogy abból katasztrófa esetén a teljes szolgáltatás helyreállítható legyen.

A *Hitelesítés-szolgáltató* üzletmenet folytonossági terve pontos előírásokat tartalmaz a kritikus rendszerkomponensek meghibásodásának esetén végrehajtandó feladatokra.

A *Hitelesítés-szolgáltató* a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leghamarabb újraindítja a szolgáltatásait.

A szolgáltatások helyreállítása során elsőbbséget élveznek a tanúsítvány állapot információkat szolgáltató rendszerek.

5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások

A *Hitelesítés-szolgáltató* katasztrófa elhárítási terve a szolgáltatói magánkulcsok kompromittálódása esetére akciótervvel rendelkezik. Az akcióterv a szolgáltatói nyilvános kulcs és a hozzá tartozó *Tanúsítvány* visszavonása mellett feltárja a kompromittálódás körülményeit, intézkedik valamennyi *Érintett fél* értesítéséről, megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen és szükség esetén új kulccsal látja el a szolgáltatói egységet és a kompromittálódás által érintett végfelhasználókat. A *Hitelesítés-szolgáltató* valamely hitelesítő egység kulcsának kompromittálódása esetén haladéktalanul megszünteti az adott kulcs használatát.

Amennyiben az adott hitelesítő egység számára – jogszabály vagy hitelesítés szolgáltatók közötti szerződés vagy megegyezés alapján – másik hitelesítés szolgáltató is bocsátott ki *Tanúsítvány*t, és felül- vagy kereszthitelesítette a *Hitelesítés-szolgáltató* ezen hitelesítő egységét, a *Hitelesítés-szolgáltató* az adott kulcs kompromittálódása esetén haladéktalanul értesíti ezen másik hitelesítés szolgáltatót, és kezdeményezi az érintett kulcshoz tartozó *Tanúsítvány* visszavonását.

A szolgáltatói nyilvános kulcsok visszavonásáról *Hitelesítés-szolgáltató* az 1.3.1. fejezetnek megfelelően értesítést tesz közzé.

5.7.4. Működés folyamatosságának biztosítása katasztrófát követően

A *Hitelesítés-szolgáltató* üzletmenet folytonossági tervében meghatározta a természeti vagy egyéb katasztrófa miatt bekövetkezett szolgáltatás leállás esetén végrehajtandó feladatokat.

A katasztrófa bekövetkezése esetén haladéktalanul életbe lépteti a rendelkezéseket és megkezdi a károk elhárítását, a szolgáltatások helyreállítását.

A másodlagos szolgáltatási helyszín az elsődleges telephelytől olyan távolságra található, hogy egy valószínűsíthető katasztrófa ne érhesse mindkét helyszínt egyszerre.

A *Hitelesítés-szolgáltató* a lehető legrövidebb időn belül köteles értesíteni az érintett felhasználókat a katasztrófa bekövetkezéséről.

A szolgáltatások helyreállítása után a *Hitelesítés-szolgáltató* a lehető legrövidebb időn belül helyreállítja a katasztrófa során tönkrement eszközeit és az eredeti szolgáltatás biztonsági szintet.

5.8. A hitelesítés-szolgáltató vagy a regisztráló szervezet leállítása

A *Hitelesítés-szolgáltató* a szolgáltatások valamelyikének tervezett megszüntetése esetén legkevesebb 60 nappal a szolgáltatás leállítását megelőzően értesíti a végfelhasználókat és a Nemzeti Média- és Hírközlési Hatóságot.

A hitelesítés-szolgáltatás és online tanúsítvány-állapot szolgáltatás leállítása

A *Hitelesítés-szolgáltató* a szolgáltatás leállítására vonatkozó bejelentéssel egyidejűleg leállítja a következő szolgáltatásait:

- regisztráció,
- *Tanúsítvány* előállítás,
- *Tanúsítvány* kibocsátás,
- *Tanúsítvány* megújítás,
- *Tanúsítvány* módosítás,
- kulcscsere.

A *Hitelesítés-szolgáltató* a tervezett leállás előtt legalább 20 nappal de az *Ügyfel*ek értesítését követően legalább 14 nappal:

- Intézkedik valamennyi érvényes végfelhasználói *Tanúsítvány* visszavonásáról;
- leállítja a *Tanúsítvány* visszavonás kezelés szolgáltatást;
- leállítja a rendszeres *Tanúsítvány visszavonási lista* kibocsátását;
- kibocsát egy záró *Tanúsítvány visszavonási list*át.

A leállás időpontjával egyidejűleg a *Hitelesítés-szolgáltató* a következő szolgáltatásokat állítja le:

- információ szolgáltatás,
- *Tanúsítvány* közzététel,
- *Tanúsítvány* visszavonási állapot közzététele,
- online tanúsítvány-állapot szolgáltatás.

A *Hitelesítés-szolgáltató* a tervezett megszűnés előtt tárgyalásokat kezd más vele azonos besorolású szolgáltatókkal szolgáltatásainak átvételéről. Nyilvántartásait a bizalmas felhasználói adatokkal együtt a 9.3 fejezet szerint mindenképpen átadja egy ilyen szolgáltatónak, vagy megállapodás hiányában a Nemzeti Média- és Hírközlési Hatóságnak, egyéb szolgáltatásait a tárgyalások eredményétől függően átadja vagy átadás nélkül megszünteti.

A szolgáltatói *Tanúsítvány*ok visszavonásáról (és a magánkulcsok megsemmisítéséről) – a tárgyalások eredményétől függően – a *Hitelesítés-szolgáltató* fokozatosan intézkedik a 60 napos időszakban.

A *Hitelesítés-szolgáltató* a tárgyalások végeredményéről tájékoztatja az *Ügyfel*eket és a Nemzeti Média- és Hírközlési Hatóságot. A *Hitelesítés-szolgáltató* az *Ügyfel*eket elektronikus levélben, az *Érintett felek*et a honlapján történő közzététel útján tájékoztatja.

A *Hitelesítés-szolgáltató* a "Microsec e-Szigno Root CA 2009" és az "e-Szigno Root CA 2017" *Tanúsítvány*ának visszavonását 5 nappal megelőzően a 2.2. fejezetnek megfelelően hirdetményt tesz közzé.

A *Hitelesítés-szolgáltató* a szolgáltatás befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, minősített *Időbélyegző*vel ellátott mentést készít.

A *Hitelesítés-szolgáltató* biztosítja, hogy a visszavont *Tanúsítvány*ok nyilvántartásában szereplő adatokat szükség esetén az arra jogosult *Érintett felek* értelmezhessék.

A *Hitelesítés-szolgáltató* – annak érdekében, hogy adatait átadhassa egy másik szolgáltatónak – az adatokat az új szolgáltató által fogadni képes médián és formátumban helyezi el vagy biztosítja az új szolgáltató számára az adatok eredeti formátumban történő feldolgozásának lehetőségét, amelyekhez átadja a megfelelő eszközöket, dokumentációkat és ismereteket.

6. Műszaki biztonsági óvintézkedések

A *Hitelesítés-szolgáltató* módosítás ellen védett, megbízható, biztonságtechnikailag értékelt termékekből álló informatikai rendszereket használ szolgáltatásai nyújtásához. A *Hitelesítés-szolgáltató* a szolgáltatói kriptográfiai kulcsokat teljes életciklusuk alatt megfelelő tanúsítással rendelkező *HSM eszköz*ökben kezeli.

Mind a *Hitelesítés-szolgáltató*, mind a rendszert szállító és kivitelező vállalkozók jelentős tapasztalatokkal rendelkeznek hitelesítés-szolgáltatás kiépítésében és nemzetközileg elismert technológiát alkalmaznak.

A *Hitelesítés-szolgáltató* folyamatosan nyomon követi a kapacitás igényeket és a trendek felállításával becslést ad a jövőbeni várható kapacitás igényekre. Igény esetén gondoskodik a szűkös kapacitások bővítéséről, ezáltal biztosítja a szükséges feldolgozási és tárolási kapacitások folyamatos rendelkezésre állását.

6.1. Kulcspár előállítása és telepítése

A *Hitelesítés-szolgáltató* gondoskodik valamennyi általa – saját maga illetve egyes szervezeti egységei (pl. *Tanúsítványtár*, *Regisztráló szervezet*ek) számára – generált magánkulcs biztonságos, a hatályos jogszabályi előírásoknak és az ipari szabványoknak megfelelő előállításáról és kezeléséről.

6.1.1. Kulcspár előállítása

A *Hitelesítés-szolgáltató* a kulcspárok generálásához mindenkor csak olyan kulcsgenerálási algoritmusokat használ, amelyek megfelelnek az alábbi normatívákban megfogalmazott követelményeknek:

- ETSI TS 119 312 [18];
- CABF Baseline Requirements ajánlás [34];

- az Eüt. [8] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

A *Hitelesítés-szolgáltató* saját kulcspár előállítása esetén biztosítja, hogy:

- A szolgáltatói magánkulcs előállítását fizikailag védett környezetben (lásd 5.1 pont), legalább két, bizalmi szerepkört (lásd 5.2.1 pont) betöltő, erre feljogosított személy együttes részvételével, más illetéktelen személyek jelenlétét kizárva végzi.
- A szolgáltatói magánkulcs előállítását olyan eszközön belül hajtja végre, amely:
  - megfelel az ISO/IEC 19790 [21] követelményeinek, vagy
  - megfelel a FIPS 140-2 [35] 3-as, illetve annál magasabb szintű követelményeinek, vagy
  - megfelel a CEN 14167-2 [36] munkacsoport egyezmény követelményeinek, vagy
  - olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [20] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint EAL 4-es vagy magasabb értékelési garancia szinten van értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előirányzaton kell alapulnia.
- A szolgáltatói magánkulcs előállítását egy kulcsgenerálási forgatókönyv alapján végzi.
- Szolgáltatói gyökér hitelesítő egység magánkulcsának előállítása esetén jelen van egy külső auditor. A külső auditor igazolja, hogy a kulcs generálása a forgatókönyv szerint történt.

A *Hitelesítés-szolgáltató* soha nem állít elő kulcspárokat a végfelhasználói *Tanúsítvány*okhoz.
Az *Igénylő* által előállított kulcspár esetén:

- a kulcsok előállítását az *Igénylő* felügyelete alatt álló, megfelelően biztonságos környezetben kell végezni;
- az *Igénylő*nek kell gondoskodnia a generált magánkulcs megfelelő védelméről;
- a *Hitelesítés-szolgáltató*nak meg kell győződnie arról, hogy az előállított kulcspár megfelel a 6.1.5 és 6.1.6 fejezetekben meghatározott követelményeknek és a nyilvános kulcs nem egy ismert gyenge kulcspár tagja.

Szolgáltatói gyökér és köztes *Tanúsítvány* előállítása esetén a *Hitelesítés-szolgáltató*nak egy kulcselőállítási jegyzőkönyvet kell felvennie, amely igazolja, hogy az eljárás az előre rögzített folyamat szerint zajlott, amely biztosítja a generált kulcsok integritását és bizalmasságát. A jegyzőkönyvet alá kell írnia:

- szolgáltatói gyökér hitelesítő egység magánkulcsának előállítása esetén a *Hitelesítés-szolgáltató* kulcsmenedzsmentért felelős bizalmi tisztviselőjének és tanúként egy a *Hitelesítés-szolgáltató* üzemeltetésétől független megbízható személynek (pl. közjegyző, auditor) akik igazolják, hogy a jegyzőkönyvben rögzítettek megfelelnek a végrehajtott folyamatnak;
- köztes szolgáltatói hitelesítő egység magánkulcsának előállítása esetén a *Hitelesítés-szolgáltató* kulcsmenedzsmentért felelős bizalmi tisztviselőjének, aki igazolja, hogy a jegyzőkönyvben rögzítettek megfelelnek a végrehajtott folyamatnak.

6.1.2. Magánkulcs eljuttatása az igénylőhöz

A *Hitelesítés-szolgáltató* soha nem állít elő kulcspárokat a végfelhasználói *Tanúsítvány*okhoz.

6.1.3. A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

Amennyiben a kulcspárt az *Igénylő* generálja, be kell tartani az alábbi rendelkezéseket:

- a nyilvános kulcsot olyan módon kell eljuttatni a *Hitelesítés-szolgáltató*hoz, hogy az egyértelműen az *Igénylő*höz rendelhető legyen;
- a *Tanúsítványkérelem* folyamatának bizonyítania kell, hogy az *Igénylő* valóban rendelkezik a nyilvános kulcshoz tartozó magánkulccsal.

Az *Igénylő* által előállított végfelhasználói kulcsok esetén az *Igénylő* egy PKCS#10 formátumú *Tanúsítványkérelmet* juttat el a *Hitelesítés-szolgáltató*hoz, amit a *Tanúsítvány*ba kerülő nyilvános kulcshoz tartozó magánkulccsal hitelesít. A PKCS#10 formátumú *Tanúsítványkérelem* tartalmazza az *Igénylő* által előállított nyilvános kulcsot és az *Alany Tanúsítvány*ba kerülő azonosító adatait, ezáltal mindkét követelmény teljesül.

6.1.4. A szolgáltatói nyilvános kulcs közzététele

A *Hitelesítés-szolgáltató* a következő módszerekkel teszi elérhetővé az *Érintett felek* részére az általa működtetett hitelesítő egységek, valamint az online tanúsítvány-állapot szolgáltatásban részt vevő egységek *Tanúsítvány*ait:

- A *Hitelesítés-szolgáltató* honlapján közzéteszi az összes gyökér és köztes szolgáltatói tanúsítványt tartalmazó teljes szolgáltatói tanúsítvány hierarchiát, ahonnan valamennyi aktuális szolgáltatói *Tanúsítvány* letölthető (lásd a "Szolgáltatói tanúsítványok" pontban a

  `https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/szolgaltatoi-tanusitvanyok`

  címen).
- A gyökér és köztes hitelesítő egységek megnevezését és a *Gyökér tanúsítvány*ok lenyomatát tartalmazza a *Szolgáltatási szabályzat* 1.3.1 fejezete.
- A köztes hitelesítő egységek *Tanúsítvány*ai publikálásra kerülnek a Nemzeti Média- és Hírközlési Hatóság által az európai közös szabályozás [37] keretében karbantartott és publikált magyar megbízható hitelesítés szolgáltatói listán [38]. A lista tartalmazza valamennyi szolgáltatói *Tanúsítvány*t (a lejártakat, visszavontakat is).
- Az online tanúsítvány-állapot válaszokat aláíró válaszadók számára a *Hitelesítés-szolgáltató* – a legjobb nemzetközi gyakorlatnak megfelelően – rendkívül rövid érvényességi idejű *Tanúsítvány*okat bocsát ki, ezzel kiküszöbölve azt, hogy a *Tanúsítvány*ok visszavonási állapotát ellenőrizni kelljen. Az aktuális *Tanúsítvány*ok folyamatosan elérhetők a *Hitelesítés-szolgáltató* honlapján a

  `https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/szolgaltatoi-tanusitvanyok`

  címen.

A *Hitelesítés-szolgáltató* a következő módszerekkel teszi elérhetővé az *Érintett felek* részére az általa működtetett hitelesítő egységek, valamint az online tanúsítvány-állapot szolgáltatásban részt vevő egységek *Tanúsítvány*aival kapcsolatos állapot információkat:

- A gyökér hitelesítő egységek *Tanúsítvány*ainak állapotváltozásával kapcsolatos információk elérhetőek a *Hitelesítés-szolgáltató* honlapján.
- A köztes (nem gyökér) hitelesítő egységek tanúsítványainak állapotváltozását a *Hitelesítés-szolgáltató* nyilvánosságra hozza a *Tanúsítvány visszavonási list*ákon, saját honlapján, valamint az online tanúsítvány-állapot válasz szolgáltatás keretében.
- Az online tanúsítvány-állapot válaszokat aláíró válaszadók számára a rendkívül rövid érvényességi idejű *Tanúsítvány*ok használata következtében nincs szükség a *Tanúsítvány*ok visszavonási állapotának ellenőrzésére. A *Hitelesítés-szolgáltató* garantálja, hogy kulcs kompromittálódás vagy bármilyen egyéb probléma esetén az OCSP válaszokat aláíró régi szolgáltatói magánkulcshoz nem bocsát ki újabb *Tanúsítvány*t. A *Hitelesítés-szolgáltató* az OCSP válaszadói *Tanúsítvány*okat ezt követően új, biztonságos magánkulcshoz bocsátja ki.

Az állapot információk közlésének módszereit illetően lásd még a 4.10. fejezetet.

6.1.5. Kulcsméretek

A *Hitelesítés-szolgáltató* mindenkor csak olyan kriptográfiai algoritmusokat és minimális kulcsméreteket használ, amelyek megfelelnek az alábbi normatívákban megfogalmazott követelményeknek:

- ETSI TS 119 312 [18];
- CABF Baseline Requirements ajánlás [34];
- az Eüt. [8] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

A *Hitelesítés-szolgáltató* valamennyi jelenleg aktív gyökér és köztes szolgáltatói *Tanúsítvány*ában, az *Időbélyegző egység*ek és OCSP válaszadók *Tanúsítvány*aiban egyaránt legalább 2048 bites RSA kulcsot vagy 256 bites ECC kulcsot használ.

6.1.6. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A *Hitelesítés-szolgáltató* a kulcsok generálását a 6.1.1. fejezetben leírtak szerint végzi.

Hardveres/szoftveres kulcselőállítás

A *Hitelesítés-szolgáltató Tanúsítvány*ok kibocsátására használt kulcsainak generálása olyan *HSM eszköz*zel történik, amely rendelkezik FIPS 140-2 Level 3 szerinti tanúsítással.

Az egyéb – a *Hitelesítés-szolgáltató* belső működéséhez szükséges – kulcsokat a *Hitelesítés-szolgáltató* vagy *HSM eszköz*ön, vagy biztonságos környezetben üzemelő számítógépen generálja.

A paraméterek megfelelőségének ellenőrzése

A kulcsgenerálás paramétereinek megfelelőségét két szempontból ellenőrzi a rendszer:

- a paraméterekhez felhasznált véletlen szám generálás megfelelőségének ellenőrzése (statisztikailag kellőképpen véletlenszerű-e a generálás),
- a paraméterekre vonatkozó előírások teljesülésének ellenőrzése.

A rendszerben használt valamennyi *HSM eszköz* képes az általa generált bitsorozat egyenletességének és függetlenségének statisztikai tesztelésére. A modulok lehetővé teszik a tesztek meghívását egy szabványos interfészen keresztül.

6.1.7. A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)

A *Hitelesítés-szolgáltató* gyökér hitelesítő egységének magánkulcsa csak az alábbi célokra használható:

- a gyökér hitelesítő egység saját maga által aláírt *Tanúsítvány*ának kibocsátására,
- köztes hitelesítő egységek *Tanúsítvány*ainak hitelesítésére,
- OCSP válaszadó *Tanúsítvány*ának hitelesítésére,
- CRL-ek hitelesítésére.

A *Hitelesítés-szolgáltató* köztes hitelesítő egységeinek magánkulcsa – illetve a más szervezetek részére kibocsátott köztes hitelesítő egység magánkulcsa – csak az alábbi célokra használható:

- köztes hitelesítő egységek *Tanúsítvány*ainak hitelesítésére,
- végfelhasználói *Tanúsítvány*ok hitelesítésére,
- *Időbélyegző egység Tanúsítvány*ának hitelesítésére,
- OCSP válaszadó *Tanúsítvány*ának hitelesítésére,
- CRL-ek hitelesítésére.

A *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítvány*okban szerepelteti a "kulcshasználat" (Key Usage) kiterjesztéseket, amelyek meghatározzák a *Tanúsítvány* felhasználási területét és az X.509v3 [33] kompatibilis alkalmazásokban műszakilag is korlátozzák a kulcsok felhasználhatóságát. A mező tartalmára vonatkozó megkötések a 7.1.2 fejezetben szerepelnek.

Az *Igénylő* a *Tanúsítvány*ához tartozó magánkulcsát kizárólag webszerver azonosításra használhatja, más felhasználás nem engedélyezett.

6.2. A magánkulcsok védelme

A *Hitelesítés-szolgáltató* gondoskodik a birtokában lévő magánkulcsok biztonságos kezeléséről, megakadályozza a magánkulcsok felfedését, lemásolását, törlését, módosítását, jogosulatlan használatát. A *Hitelesítés-szolgáltató* csak addig őrzi a magánkulcsokat, ameddig azt a szolgáltatás nyújtása feltétlenül megköveteli.

A *Hitelesítés-szolgáltató* a gyökér hitelesítő egység magánkulcsait a normál szolgáltatás eszközeitől fizikailag elkülönítve tárolja és használja oly módon, hogy azokat csak megfelelő jogosultságokkal rendelkező bizalmi tisztviselők tudják aktiválni.

A *Hitelesítés-szolgáltató* a hitelesítő szervezet *Tanúsítvány*ok kibocsátására használt magánkulcsait fizikailag biztonságos helyszínen, biztonságos *HSM eszköz*ben tárolja.

A *Hitelesítés-szolgáltató* a használatból kivont *HSM eszköz*ökben tárolt magánkulcsokat kitörli az eszköz használati útmutatójában meghatározott módon, ami után gyakorlatilag lehetetlen a kulcsok visszaállítása.

A *Hitelesítés-szolgáltató* nem generál magánkulcsokat az *Igénylő* részére, így nem kell gondoskodnia a végfelhasználói magánkulcsok megőrzéséről.

6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

A *Hitelesítés-szolgáltató* *Tanúsítvány*okat, OCSP válaszokat, CRL listákat kibocsátó rendszerei az elektronikus aláírás vagy bélyegző létrehozásához használt magánkulcsokat olyan biztonságos hardver eszközökben tárolják, amelyek:

- megfelelnek az ISO/IEC 19790 [21] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [35] 3-as, illetve annál magasabb szintű követelményeknek,
- vagy megfelelnek a CEN 14167-2 [36] munkacsoport egyezmény követelményeinek,
- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [20] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten vannak értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előirányzaton kell alapulnia.

A *Hitelesítés-szolgáltató* a szolgáltatói magánkulcsokat a *HSM eszköz*ön kívül csak kódolt formában tárolja. A kódoláshoz csak az Eüt. [8] 92. § (1) b) szerint kiadott aktuális Nemzeti Média- és Hírközlési Hatóság határozat szerinti algoritmusokat és kulcsparamétereket használ, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

A *Hitelesítés-szolgáltató* a szolgáltatói magánkulcsokat kódolt formában is fizikailag biztonságos helyszínen tárolja az *Adatközpont* páncélszekrényében, ahol azokhoz csak az arra jogosultak férhetnek hozzá.

A *Hitelesítés-szolgáltató* a kriptográfiai algoritmusok vagy kulcsparaméterek gyengülése esetén a kódolt kulcsokat megsemmisíti vagy erősebb védelmet biztosító algoritmus és kulcsparaméterek felhasználásával tovább kódolja.

6.2.2. Magánkulcs többszereplős (n-ből m) használata

A *Hitelesítés-szolgáltató* alkalmazza az "n-ből m" ellenőrzést a magánkulcsokkal kapcsolatos kulcsgondozási funkciók aktivizálásánál. A paraméterek úgy lettek meghatározva, hogy a szolgáltatói magánkulcsaival végzett kritikus műveletek végrehajtásához legalább kettő, bizalmi szerepkört betöltő munkatárs egyidejű jelenlétére legyen szükség.

6.2.3. Magánkulcs letétbe helyezése

A *Hitelesítés-szolgáltató* a gyökér tanúsítványaihoz tartozó magánkulcsait titkosított formában CD-re másolva, zárt borítékban letétbe helyezte egy banki trezorban.

A *Hitelesítés-szolgáltató* a gyökér tanúsítványok kulcsain túlmenően más szolgáltatói magánkulcsát nem helyezi letétbe.

A *Hitelesítés-szolgáltató* a webszerver azonosításához használt magánkulcsokhoz nem nyújt letéti szolgáltatást, azokat semmilyen körülmények között sem tárolja.

6.2.4. Magánkulcs mentése

A *Hitelesítés-szolgáltató* minden szolgáltatói magánkulcsáról biztonsági másolatot készít még a magánkulcs használatbavételét megelőzően a 6.2.1. fejezetben leírtak szerint védett környezetben, legalább két bizalmi szerepkört betöltő személy együttes jelenlétében, más személyek kizárásával. A mentés során a magánkulcs titkosított formában hagyja el a modult, e titkosított kulcsot később másik modulba be lehet tölteni. Mind a mentés, mind a visszatöltés csakis a 6.2.2. fejezetben leírt védelmi mechanizmus mellett végezhető.

A *Hitelesítés-szolgáltató* a biztonsági másolatot két példányban tárolja, ebből legalább az egyik példányt a szolgáltatás nyújtásától eltérő helyszínen.

A biztonsági másolatok kezelésére és megőrzésére ugyanolyan szigorú biztonsági előírások vonatkoznak, mint az éles rendszer üzemeltetésére.

A weboldal hitelesítésre szolgáló magánkulcsokról a *Hitelesítés-szolgáltató* nem készít másolatot.

6.2.5. Magánkulcs archiválása

A *Hitelesítés-szolgáltató* nem archiválja magánkulcsait és a végfelhasználói magánkulcsokat.

6.2.6. Magánkulcs bejuttatása hardver kriptográfiai eszközbe, vagy onnan történő exportja

A *Hitelesítés-szolgáltató* valamennyi szolgáltatói magánkulcsát a követelményeknek megfelelő *HSM eszköz*ben állítja elő.

A magánkulcsok nem léteznek nyílt formában a *HSM eszköz*ön kívül.

A *Hitelesítés-szolgáltató* a magánkulcsot csak biztonsági másolat készítése céljából exportálja a *HSM eszköz*ből.

A magánkulcs *HSM eszköz*ök közötti szállítása csak biztonsági másolat formájában engedélyezett.

A szolgáltatói magánkulcsok exportálása vagy betöltése minden esetben a 6.2.2. fejezetben leírt módon történik.

6.2.7. Magánkulcs tárolása hardver kriptográfiai eszközben

A *Hitelesítés-szolgáltató* a szolgáltatás nyújtásához használt magánkulcsait a 6.2.1. fejezet szerinti kriptográfiai modulokban tartja.

A *HSM eszköz*ben a magánkulcsokat az eszköz tanúsításában meghatározott módon tárolja és használja a vonatkozó kezelési utasítások maradéktalan betartásával.

6.2.8. A magánkulcs aktiválásának módja

A *Hitelesítés-szolgáltató* szolgáltatói magánkulcsait biztonságos *HSM eszköz*ben tárolja, a használat során betartja a *HSM eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott követelményeket. A *HSM eszköz*t csak a hozzá tartozó operátori kártyákkal lehet aktiválni, a *HSM eszköz*ben lévő magánkulcsokat a modul aktiválása előtt nem lehet használni. A *HSM eszköz*höz tartozó operátori kártyákat a *Hitelesítés-szolgáltató* biztonságos környezetben tárolja és e kártyákat kizárólag a *Hitelesítés-szolgáltató* erre jogosult munkatársai érhetik el.

A *Hitelesítés-szolgáltató* biztosítja, hogy a gyökér hitelesítő egység magánkulcsával csak az erre megfelelő felhatalmazással rendelkező bizalmi tisztviselő által közvetlenül kiadott parancs esetén lehet aláírást vagy bélyegzőt létrehozni.

Az *Igénylő* által előállított magánkulcs esetén a magánkulcs biztonságos kezelése teljes mértékben az *Igénylő* felelőssége.

6.2.9. A magánkulcs deaktiválásának módja

Szolgáltatói magánkulcsok

A *Hitelesítés-szolgáltató* által használt hardver kriptográfia eszközök által kezelt magánkulcs akkor deaktiválódik, ha az eszköz (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetekben következik be:

- a felhasználó deaktiválja a kulcsot,
- az eszköz áramellátása megszakad (kikapcsolás vagy tápellátási probléma),
- az eszköz hibaállapotba kerül.

Az így deaktivált magánkulcs mindaddig nem használható, amíg a modul ismét aktív állapotba nem kerül.

Végfelhasználói magánkulcsok

A szoftver alapú magánkulcsok megfelelően biztonságos használata az *Igénylő* felelőssége.

6.2.10. A magánkulcs megsemmisítésének módja

Szolgáltatói magánkulcsok

A *Hitelesítés-szolgáltató* használatból kivont, lejárt érvényességű vagy kompromittálódott szolgáltatói magánkulcsait olyan módon semmisíti meg, amely lehetetlenné teszi a magánkulcs további használatát.

A *Hitelesítés-szolgáltató* a hitelesítő szervezet biztonságos *HSM eszköz*ében tárolt szolgáltatói magánkulcsok megsemmisítését a felhasznált *HSM eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően végzi a *Hitelesítés-szolgáltató* két munkatársának (egy infrastruktúra adminisztrátor és egy biztonsági tisztviselő) együttes jelenlétében más személyek jelenlétének kizárásával.

A *Hitelesítés-szolgáltató* dokumentált módon megsemmisíti a magánkulcsról készült minden mentett példányt olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon.

Végfelhasználói magánkulcsok

A használatból kivont weboldal hitelesítő magánkulcsokat javasolt megsemmisíteni.

6.2.11. A hardver kriptográfiai eszközök értékelése

A 6.2.1 fejezet előírásaival összhangban a *Hitelesítés-szolgáltató* valamennyi szolgáltatói magánkulcsát olyan *HSM eszköz*ben tárolja, amely:

- rendelkezik ISO/IEC 19790 [21] szerinti tanúsítással,
- vagy rendelkezik FIPS 140-2 Level 3 [35] szerinti tanúsítással,
- vagy rendelkezik a CEN 14167-2 [36] munkacsoport egyezmény követelményeinek való megfelelést igazoló Common Criteria alapú tanúsítvánnyal,
- vagy rendelkezik a Nemzeti Média- és Hírközlési Hatóság által vagy az Európai Unió valamely tagállamában nyilvántartásba vett, elektronikus aláírási termékek értékelésére jogosult független tanúsító szervezet által erre a célra kiadott igazolással.

6.3. A kulcspár kezelés egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

A *Hitelesítés-szolgáltató* minden, a hitelesítő szervezete által előállított *Tanúsítvány*t archivál az érvényesség lejártától számított legalább 10 évig, illetve a Tanúsítvánnyal kapcsolatban felmerült jogvita jogerős lezárásáig.

A *Hitelesítés-szolgáltató* ugyanezen időtartamig megőriz olyan eszközöket, amelyekkel a *Tanúsítvány* tartalma megállapítható.

6.3.2. A tanúsítványok és kulcspárok használatának periódusa

A gyökér hitelesítő egységek tanúsítványai és kulcsai

A *Hitelesítés-szolgáltató* gyökér hitelesítő egységeinek *Tanúsítvány*ai és a hozzájuk tartozó magánkulcsok érvényességi ideje nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozata szerint biztonságosan felhasználhatók.
A *Hitelesítés-szolgáltató* gyökér hitelesítő egységek kulcsainak és tanúsítványainak érvényességi ideje:

- a "Microsec e-Szigno Root CA" gyökér hitelesítő egység kulcsa 2017.04.06-ig volt érvényes;
- a "e-Szigno OCSP CA" gyökér hitelesítő egység kulcsa 2017.04.26-ig volt érvényes;
- a "Microsec e-Szigno Root CA 2009" gyökér hitelesítő egység kulcsa 2029.12.30-ig érvényes.
- az "e-Szigno Root CA 2017" gyökér hitelesítő egység kulcsa 2042.08.22-ig érvényes;

A köztes hitelesítő egységek tanúsítványai és kulcsai

A *Hitelesítés-szolgáltató* köztes hitelesítő egységeinek tanúsítványai és a hozzájuk tartozó magánkulcsok érvényességi ideje:

- 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 az adott köztes szolgáltatói *Tanúsítvány*t kibocsátó gyökér vagy köztes szolgáltatói *Tanúsítvány* érvényességi idejét.

A *Hitelesítés-szolgáltató* köztes (nem gyökér) hitelesítő egységeinek kulcsai a hozzájuk tartozó *Tanúsítvány*ok érvényességi idejének lejáratáig érvényesek.

A végfelhasználói tanúsítványok

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

- legfeljebb a kibocsátástól számított 825 nap ($\doteq$27 hónap);
- 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.

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

A *Hitelesítés-szolgáltató* a felhasznált *HSM eszköz* felhasználói útmutatójában és az eszköz tanúsítványban megfogalmazott eljárásoknak, követelményeknek megfelelő aktiváló módszereket alkalmaz szolgáltatói magánkulcsainak védelmére.

Jelszó alapú aktivizáló adatok használata esetén a jelszavak kellően bonyolultak a megkívánt védelmi szint biztosítása érdekében.

A *Hitelesítés-szolgáltató* sosem generál szoftveres végfelhasználói magánkulcsot.

Az *Igénylő* által előállított magánkulcsok aktivizáló adatainak előállítása és telepítése az *Igénylő* feladata.

6.4.2. Az aktivizáló adatok védelme

A *Hitelesítés-szolgáltató* alkalmazottai a magánkulcsok aktiválásához szükséges eszközöket, aktivizáló adatokat biztonságosan kezelik, műszaki és szervezési intézkedések segítségével védik, a jelszavakat csak kódolt formában tárolják.

Az *Igénylő* által előállított magánkulcsok aktivizáló adatainak védelme az *Igénylő* feladata és felelőssége.

6.4.3. Az aktivizáló adatok kezelésének egyéb szempontjai

Nincs megkötés.

6.5. Informatikai biztonsági előírások

6.5.1. Speciális informatikai biztonsági műszaki követelmények

A *Hitelesítés-szolgáltató* informatikai rendszereinek konfigurálása és üzemeltetése során biztosítja az alábbi követelmények teljesülését:

- a rendszerhez vagy alkalmazáshoz való hozzáférés engedélyezése előtt a felhasználó azonosságát többfaktoros azonosítással ellenőrzi kártyán tárolt VPN tanúsítvány felhasználásával;
- a felhasználókhoz szerepköröket rendel és biztosítja, hogy minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezzen;
- minden tranzakcióról naplóbejegyzést állít elő és a naplóbejegyzéseket archiválja;
- a biztonságkritikus folyamatok részére biztosítja, hogy a *Hitelesítés-szolgáltató* belső hálózati tartományai kellően védettek legyenek a jogosulatlan hozzáféréstől;
- megfelelő eljárásokat alkalmaz a kulcsvesztés vagy rendszerhiba után a szolgáltatás visszaállítása érdekében.

6.5.2. Az informatikai biztonság értékelése

A Microsec kiemelten fontosnak tartja *Ügyfel*ei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a *Hitelesítés-szolgáltató* ISO 9001 szabványnak megfelelő minőségirányítási rendszert üzemeltet 2002. január 23. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A Microsec nagy figyelmet fordít az általa üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a ISO/IEC 27001-nek megfelelő információbiztonság-irányítási rendszert (korábban BS 7799) üzemeltet 2003. május 19. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A minőségirányítási rendszer és az információbiztonság-irányítási rendszer hatóköre kiterjed a Microsec által nyújtott bizalmi szolgáltatásokra is.

A Microsec kétszintű kockázatelemzése az információ technológiai kockázatokon túlmenően kiterjed a teljes szervezetre és az üzleti kockázatokra is. A kockázatelemzés legalább évente felülvizsgálatra kerül. A kockázatelemzés eredménye alapján a *Hitelesítés-szolgáltató*

- intézkedéseket hoz a feltárt sérülékenységek megszüntetésére, és/vagy
- elfogadja az azonosított maradvány kockázatokat a döntés indokainak rögzítésével.

6.6. Életciklusra vonatkozó műszaki előírások

6.6.1. Rendszerfejlesztési előírások

A *Hitelesítés-szolgáltató* az éles szolgáltatást nyújtó informatikai rendszereiben csak olyan eszközöket, alkalmazásokat használ, amelyek:

- kereskedelmi dobozos szoftverek, amelyeket dokumentált tervezési módszertan szerint terveztek és fejlesztettek;
- a *Hitelesítés-szolgáltató* saját maga által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használt;
- a *Hitelesítés-szolgáltató* részére megbízható fél által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használtak;
- olyan nyílt forráskódú szoftverek, amelyek teljesítik a biztonsági követelményeket és amelyek megfelelőségét szoftver verifikáció, strukturált fejlesztés és életciklus menedzsment biztosítja.

Az informatikai eszközök beszerzése a hardver és szoftver komponensek módosítását kizáró módon történik, megbízható és rendszeresen minősített szállítók felhasználásával.

A *Hitelesítés-szolgáltató* a szolgáltatások nyújtásához használt kritikus informatikai eszközöket más célra nem használja.

A *Hitelesítés-szolgáltató* megfelelő védelmi intézkedésekkel megakadályozza, hogy kártékony szoftver kerülhessen a hitelesítés-szolgáltatás nyújtása körében használt eszközökbe.

A hardver és szoftver komponenseket az első használat előtt és azt követően rendszeresen ellenőrzi kártékony kódok után kutatva.

A *Hitelesítés-szolgáltató* a programfrissítések vásárlása vagy fejlesztése során ugyanolyan gondossággal jár el, mint az első verzió beszerzésekor.

A *Hitelesítés-szolgáltató* megbízható, megfelelően képzett személyzetet alkalmaz a szoftverek és eszközök telepítése során.

A *Hitelesítés-szolgáltató* csak a szolgáltatás nyújtásához szükséges szoftvereket telepíti a szolgáltatást nyújtó informatikai berendezéseire.

A *Hitelesítés-szolgáltató* rendelkezik változáskövető rendszerrel, amelyben az informatikai rendszer minden lényeges változtatása dokumentálásra kerül.

A *Hitelesítés-szolgáltató* a jogosulatlan változások észlelése érdekében automatikus monitorozó rendszert üzemeltet, amely rögzíti minden állomány változását és a figyelt állományok változása esetén naplóbejegyzést generál vagy figyelmeztető jelzést küld a rendszer üzemeltetőknek.

6.6.2. Biztonságkezelési előírások

A *Hitelesítés-szolgáltató* változáskövető rendszert használ a szolgáltatásban használt rendszerek telepítésének, konfigurációjának dokumentálására, üzemeltetésére, ellenőrzésére, monitorozására és karbantartására, beleértve a módosításokat és továbbfejlesztéseket is. A változáskövető rendszer alkalmas arra, hogy észleljen a rendszerben történt bármilyen jogosulatlan változtatást, adatbevitelt, amely érinti a szolgáltatásban használt rendszert, a tűzfalakat, routereket, programokat és egyéb komponenseket. A szolgáltatásban használt program telepítésekor a *Hitelesítés-szolgáltató* minden esetben meggyőződik arról, hogy a telepítendő program a megfelelő verziójú és mentes mindenféle jogosulatlan módosítástól. A *Hitelesítés-szolgáltató* rendszeresen ellenőrzi a szolgáltatói rendszereiben használt programok integritását.

A *Hitelesítés-szolgáltató* által alkalmazott valamennyi *HSM eszköz* ellenőrzésre, bevizsgálásra és értékelésre került. A *Hitelesítés-szolgáltató* ellenőrzi a modulok sértetlenségét:

- az eszközök beszerzését követően az átvétel során,
- a használatbavételt közvetlenül megelőzően,
- rendszeresen az üzemeltetés során.

A használatból véglegesen vagy időlegesen kivont *HSM eszköz*ből a *Hitelesítés-szolgáltató* törli a szolgáltatói kulcsokat.

A *Hitelesítés-szolgáltató* a használaton kívüli *HSM eszköz*öket fizikailag védett helyszínen tárolja.

6.6.3. Életciklusra vonatkozó biztonsági előírások

A *Hitelesítés-szolgáltató* gondoskodik a felhasznált *HSM eszköz*ök védelméről azok teljes életciklusa alatt.

A szolgáltatások nyújtásához használt informatikai eszközök, rendszerek üzemeltetése során a *Hitelesítés-szolgáltató* figyelembe veszi az eszközök életciklusára vonatkozó biztonsági szempontokat, melyek szerint:

- megfelelő tanúsítással rendelkező *HSM eszköz*t használ rendszereiben;
- a *HSM eszköz* átvételekor a minőség ellenőrzése során meggyőződik róla, hogy a szállítás folyamán biztosították a *HSM eszköz*ök feltörés elleni védelmét;
- a *HSM eszköz*öket biztonságos helyen tárolja, a tárolás során biztosítja a *HSM eszköz*ök feltörés elleni védelmét;
- az üzemeltetés során folyamatosan betartja a *HSM eszköz* biztonsági előirányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket;
- a használatból kivont *HSM eszköz*ökben tárolt magánkulcsokat olyan módon törli, hogy lehetetlené válik a kulcsok visszaállítása.

6.7. Hálózati biztonsági előírások

A *Hitelesítés-szolgáltató* szigorú ellenőrzés alatt tartja az alkalmazott IT rendszereinek konfigurációját, minden változást dokumentál, beleértve a legkisebb módosítást, fejlesztést, szoftverfrissítést is. A *Hitelesítés-szolgáltató* megfelelő eljárásokat használ az IT rendszereiben bekövetkezett tetszőleges hardver vagy szoftver változás észlelésére, a rendszer telepítésére, karbantartására. A *Hitelesítés-szolgáltató* minden szoftverkomponens első betöltésekor ellenőrzi a komponens eredetiségét, integritását.

A *Hitelesítés-szolgáltató* megfelelő hálózatbiztonsági intézkedéseket alkalmaz, mint például:

- IT rendszereit jól elválasztott biztonsági zónákra osztja;
- elkülöníti az IT rendszer üzemeltetését támogató rendszereit az éles szolgáltatást nyújtó rendszereitől;
- elkülöníti az éles szolgáltatást nyújtó rendszereit a fejlesztésre és tesztelésre szolgáló rendszerektől;
- az elkülönített megbízható rendszerek között csak olyan megbízható kommunikációs csatornákon keresztül létesít kapcsolatot, amelyek logikailag el vannak választva más kommunikációs csatornáktól, megbízható végponti azonosítást használnak és védik a csatornákon küldött adatokat a módosítástól és a felfedéstől;
- az éles szolgáltatást nyújtó IT rendszereit biztonságos hálózati zónában üzemelteti;
- a zónákhoz való hozzáférést és a zónák közötti kommunikációt csak a szolgáltatás nyújtásához szükségesre korlátozza;
- letiltja a nem használt protokollokat és felhasználókat;
- letiltja a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtat.
- a használt szabályrendszert rendszeresen felülvizsgálja.

A *Hitelesítés-szolgáltató* sérülékenységvizsgálatot végez vagy végeztet a *Hitelesítés-szolgáltató* nyilvános és privát IP címein:

- a CA/Browser Forum kérésétől számított egy héten belül;
- a *Hitelesítés-szolgáltató* által jelentősnek minősített rendszer vagy hálózati változtatás után;
- legalább minden három (3) hónapban.

A *Hitelesítés-szolgáltató* legalább 3 havonta ellenőrzi a helyi hálózati eszközök (pl. router) konfigurációjának megfelelőségét a *Hitelesítés-szolgáltató* által meghatározott követelményeknek.

A *Hitelesítés-szolgáltató* évente illetve az informatikai rendszerén történt minden jelentős változás után sebezhetőségvizsgálatot végeztet egy külső, független szakemberrel, aki rendelkezik az ilyen vizsgálat elvégzéséhez szükséges képességekkel, szakértelemmel, eszközökkel és etikai kódexekkel.

6.8. Időbélyegzés

A *Hitelesítés-szolgáltató* a naplóbejegyzések és egyéb archiválandó elektronikus állományok hitelesítésére az e-Szignó Hitelesítés Szolgáltató által kibocsátott minősített elektronikus *Időbélyegző*ket használja.

7. Tanúsítvány, CRL és OCSP profilok

7.1. Tanúsítvány profil

A *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*ok illetve az azokat kibocsátó tanúsítvány láncban található gyökér és köztes hitelesítő egységek *Tanúsítvány*ai megfelelnek az alábbi ajánlásoknak, specifikációknak:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [33];
- IETF RFC 5280 [27];
- IETF RFC 6818 [29];
- IETF RFC 6962 [32];
- ETSI EN 319 412-1 [14];
- ETSI EN 319 412-4 [17];

7.1.1. Verzió szám(ok)

A *Hitelesítés-szolgáltató* által használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítvány*ai és a *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*ok az X.509 specifikáció [33] szerinti "v3" *Tanúsítvány*ok.

A *Tanúsítvány*ok alapmezői a következők:

- Verzió (Version)
  A *Tanúsítvány* az X.509 specifikáció [33] szerinti "v3" *Tanúsítvány*oknak felel meg, így a mezőbe a "2" érték kerül.

- Sorozatszám (Serial Number)
  A *Tanúsítvány*t kibocsátó hitelesítő egység által generált egyedi azonosító.

  A végfelhasználói *Tanúsítvány*ok esetében a "Serial Number" mező legalább 8 bájt entrópiájú véletlen számot tartalmaz.

- Algoritmus azonosító (Algorithm Identifier)
  A *Tanúsítvány*t hitelesítő elektronikus bélyegző készítéséhez használt kriptográfiai algoritmuskészlet azonosítója (OID). A *Hitelesítés-szolgáltató* a következő kriptográfiai algoritmust használja:

  – "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  – "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)

- Aláírás (Signature)
  A *Hitelesítés-szolgáltató* által készített, a *Tanúsítvány*t hitelesítő elektronikus bélyegző, amelyet a *Hitelesítés-szolgáltató* az "Algoritmus azonosító" -ban megadott algoritmuskészlettel hozott létre.

- Kibocsátó (Issuer)
  A *Tanúsítvány*t kibocsátó *Hitelesítő egység* megkülönböztetett neve egyedi X.501 név formátum szerint (lásd: 3.1. fejezet).

- Érvényesség (Valid From & Valid To)
  A *Tanúsítvány* érvényességének kezdete és vége.

  Az időpontok UTC szerint és az IETF RFC 5280-nak megfelelő kódolásban kerülnek rögzítésre.

- Az *Alany* azonosítója (Subject)
  Az *Alany* megkülönböztetett neve egyedi X.501 név formátum szerint(lásd: 3.1. fejezet). Mindig kitöltésre kerül.

- Az *Alany* nyilvános kulcsának algoritmus-azonosítója (Subject Public Key Algorithm Identifier)

  A *Hitelesítés-szolgáltató* az RSA és az ECC algoritmusokat támogatja a végfelhasználói *Tanúsítvány*okban.

  A mezőbe kerülő érték:

  – "rsaEncryption" (1.2.840.113549.1.1.1)
  – "ecPublicKey" (1.2.840.10045.2.1)

- Az *Alany* nyilvános kulcsa (Subject Public Key Value)
  Az *Alany* nyilvános kulcsa.

- Kibocsátó egyedi azonosító (Issuer Unique Identifier)
  Nem kitöltött.

- Az *Alany* egyedi azonosítója (Subject Unique Identifier)
  Nem kitöltött.

7.1.2. Tanúsítvány kiterjesztések

A *Hitelesítés-szolgáltató* csak az alábbi, X.509 specifikáció [33] szerinti tanúsítvány kiterjesztéseket használja:

Gyökér hitelesítési egység tanúsítványa

- Hitelesítési rendek (Certificate Policies) – nem kritikus
  OID: 2.5.29.32
  Nem szerepel ez a mező.

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
  OID: 2.5.29.35
  A *Tanúsítvány*t hitelesítő elektronikus bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.

  A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata. Önaláírt gyökér hitelesítési egység tanúsítvány esetében az értéke megegyezik a *Alany* kulcsazonosító mező értékével.

- *Alany* kulcsazonosító (Subject Key Identifier) – nem kritikus
  OID: 2.5.29.14
  Az *Alany* nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.
  A mező értéke: a nyilvános kulcs SHA-1 lenyomata.

  Mindig kitöltésre kerül.

- *Alany* alternatív nevei (Subject Alternative Names) – nem kritikus
  OID: 2.5.29.17

  Kitöltése a 3.1.1. fejezetben leírtak szerint történik.

- Alapvető megkötések (Basic Constraints) – kritikus
  OID: 2.5.29.19
  Annak megadása, hogy a *Tanúsítvány* hitelesítő egység számára lett-e kibocsátva.

  A kiterjesztés kitöltése kötelező és az értéke: CA = "TRUE".

  A gyökér *Tanúsítvány*ban nem szerepel a "pathLenConstraint" mező.

- Kulcshasználat (Key Usage) – kritikus
  OID: 2.5.29.15
  A kulcs engedélyezett használati körének meghatározása.

  A beállított értékek:

  – "keyCertSign",
  – "cRLSign".

- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus
  OID: 2.5.29.37
  A kulcs további engedélyezett használati körének meghatározása.

  Nem szerepel.

A fenti mezők mindig kitöltésre kerülnek. Más tanúsítvány kiterjesztés nem kerül kitöltésre.

Köztes hitelesítési egység tanúsítványa

- Hitelesítési rendek (Certificate Policies) – nem kritikus
  OID: 2.5.29.32

  Ez a mező korlátozhatja a köztes *Tanúsítvány*t tartalmazó tanúsítványláncban használható *Hitelesítési rend*eket. A köztes hitelesítési egység alá tartozó alrendszerekben csak olyan végfelhasználói *Tanúsítvány* adható ki, amely megfelel az itt felsorolt *Hitelesítési rend*ek közül legalább egynek.

  Minden esetben kitöltésre kerül. A *Hitelesítés-szolgáltató* saját köztes hitelesítési egységei számára kibocsátott *Tanúsítvány*ok esetében szerepelhet "anyPolicy" Identifier ebben a mezőben.

  A vonatkozó *Szolgáltatási szabályzat* hivatkozása megadható ebben a mezőben.

  Más *Hitelesítés-szolgáltató* számára kibocsátott köztes hitelesítési egység *Tanúsítvány*ainak esetében csak olyan azonosító szerepelhet ebben a mezőben, amely olyan *Hitelesítési rend*re vonatkozik, amely megfelel a kibocsátó *Hitelesítés-szolgáltató* által alkalmazott valamely *Hitelesítési rend*nek, és nem lehet benne "anyPolicy" azonosító.

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
  OID: 2.5.29.35
  A *Tanúsítvány*t hitelesítő elektronikus bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.

  Minden esetben kitöltésre kerül.

  A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata.

- *Alany* kulcsazonosító (Subject Key Identifier) – nem kritikus
  OID: 2.5.29.14
  Az *Alany* nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.
  A mező értéke: a nyilvános kulcs SHA-1 lenyomata.

  Minden esetben kitöltésre kerül.

- *Alany* alternatív nevei (Subject Alternative Names) – nem kritikus
  OID: 2.5.29.17

  Kitöltése a 3.1.1. fejezetben leírtak szerint történik.

- Alapvető megkötések (Basic Constraints) – kritikus
  OID: 2.5.29.19
  Annak megadása, hogy a *Tanúsítvány* hitelesítő egység számára lett-e kibocsátva.

  A kiterjesztés kitöltése kötelező, és az értéke: CA = "TRUE".

  A *Tanúsítvány*ban nem szerepel a "pathLenConstraint" mező.

- Kulcshasználat (Key Usage) – kritikus
  OID: 2.5.29.15
  A kulcs engedélyezett használati körének meghatározása.
  A beállított értékek:
  - "keyCertSign",
  - "cRLSign".
- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus
  OID: 2.5.29.37
  A kulcs további engedélyezett használati körének meghatározása.

  A 2019-01-01 után kiadandó *Weboldal-hitelesítő tanúsítvány*okat kiadó köztes szolgáltatói *Tanúsítvány*okban kötelezően szereplő értékek:
  - Server Authentication (1.3.6.1.5.5.7.3.1)
  - Client Authentication (1.3.6.1.5.5.7.3.2)
  - OCSP Signing (1.3.6.1.5.5.7.3.9)
- CRL szétosztási pont (CRL Distribution Points) – nem kritikus
  OID: 2.5.29.31
  A mező tartalmazza a CRL elérhetőségét http és/vagy LDAP protokollon keresztül.
  Mindig kitöltésre kerül.
- Szolgáltatói információ elérése (Authority Information Access) – nem kritikus
  OID: 1.3.6.1.5.5.7.1.1
  A *Hitelesítés-szolgáltató* által rendelkezésre bocsátott, a *Tanúsítvány* használatához kapcsolódó egyéb szolgáltatásainak leírása.

  Kötelező a kitöltése, és a mező tartalmazza a következő adatokat:
  - A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást nyújt. Ez az elérhetőség szerepel itt.
  - A tanúsítványlánc felépítésének megkönnyítésére a *Hitelesítés-szolgáltató* megadja a *Tanúsítvány*t kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.

A fenti mezők a megadott szabályok szerint mindig kitöltésre kerülnek. Más tanúsítvány kiterjesztés nem kerül kitöltésre.

Végfelhasználói tanúsítvány

- Hitelesítési rendek (Certificate Policies) – nem kritikus
  OID: 2.5.29.32
  E mező tartalmazza a *Tanúsítvány* kiadása és használata során érvényes *Hitelesítési rend* (lásd 1.2.1.fejezet) azonosítóját, valamint a *Tanúsítvány* alkalmazhatóságára vonatkozó egyéb információkat.

  Végfelhasználói *Tanúsítvány* esetében a *Hitelesítés-szolgáltató* minden esetben kitölti ezt a mezőt a következő adatok megadásával:

- a *Hitelesítési rend* azonosítója (1.2.1 fejezet szerinti OID) ;
- a *Szolgáltatási szabályzat* elérhetősége;
- szöveges figyelmeztetés angol és magyar nyelven, amelyből megállapítható, hogy II. vagy III. hitelesítési osztályú *Tanúsítvány*ról van-e szó, azaz regisztrációkor történt-e személyes azonosítás, illetve hogy a *Tanúsítvány* alanya természetes személy-e;
- az ETSI EN 319 411-1 [13] által meghatározott hitelesítési rend azonosítója (OID), amelynek a *Tanúsítvány* megfelel az alábbiak szerint:
  - DVCP *Tanúsítvány* esetében OID 0.4.0.2042.1.6,
  - OVCP *Tanúsítvány* esetében OID 0.4.0.2042.1.7,
  - IVCP *Tanúsítvány* esetében OID 0.4.0.2042.1.8.
- A CA/Browser Forum által meghatározott hitelesítési rend azonosítója az alábbiak szerint:
  - DVCP *Tanúsítvány* esetében OID 2.23.140.1.2.1,
  - OVCP *Tanúsítvány* esetében OID 2.23.140.1.2.2,
  - IVCP *Tanúsítvány* esetében OID 2.23.140.1.2.3.

A "Certificate Policies" mezőt nem tartalmazó végfelhasználói *Tanúsítvány*t teszt *Tanúsítvány*nak kell tekinteni. A teszt *Tanúsítvány* kizárólag tesztelési célra használható, valós tranzakciók esetén el kell utasítani.

A vonatkozó *Szolgáltatási szabályzat* hivatkozása megadható ebben a mezőben.

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
  OID: 2.5.29.35
  A *Tanúsítvány*t hitelesítő elektronikus bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.

  Mindig kitöltésre kerül.

  A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata.

- *Alany* kulcsazonosító (Subject Key Identifier) – nem kritikus
  OID: 2.5.29.14
  Az *Alany* nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.
  A mező értéke: a nyilvános kulcs SHA-1 lenyomata.

  Mindig kitöltésre kerül.

- *Alany* alternatív nevei (Subject Alternative Names) – nem kritikus
  OID: 2.5.29.17
  Lásd: 3.1.1. fejezet.

- Alapvető megkötések (Basic Constraints) – kritikus
  OID: 2.5.29.19
  Annak megadása, hogy a *Tanúsítvány* hitelesítő egység számára lett-e kibocsátva.

  A kiterjesztés alapértelmezett értéke CA = "FALSE", ezért ez a kiterjesztés nem szerepel a végfelhasználói *Tanúsítvány*okban.

  A "pathLenConstraint" mező nem szerepel a végfelhasználói *Tanúsítvány*okban.

- Kulcshasználat (Key Usage) – kritikus
  OID: 2.5.29.15
  A kulcs engedélyezett használati körének meghatározása.

  A *Weboldal-hitelesítő tanúsítvány*okban kötelezően beállítandó és kizárólagosan megadandó érték:

  – "digitalSignature" és
  – RSA esetében "keyEncipherment",
  – ECC esetében "keyAgreement".

  Ugynezek az értékek szerepelnek a Szerver autentikációs *Tanúsítvány*okban is, mint pl. a CISCO VPN szerver, domén kontroller, SCEP szerver, VPN szerver autentikációs *Tanúsítvány*.

- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus
  OID: 2.5.29.37
  A kulcs engedélyezett használati körének további meghatározása.

  A *Weboldal-hitelesítő tanúsítvány*okban beállított érték:

  – "serverAuth (1.3.6.1.5.5.7.3.1)"

  A *Weboldal-hitelesítő tanúsítvány*okban alapértelmezetten szereplő, de az *Igénylő* kérésére elhagyható további érték:

  – "clientAuth (1.3.6.1.5.5.7.3.2)"

  A Szerver autentikációs *Tanúsítvány*okban az alábbi táblázatban feltüntetett kiterjesztett kulcshasználati bitek kerülnek feltüntetésre:

Tanúsítvány típus	ExtKeyUsage
Cisco VPN Server	serverAuth (1.3.6.1.5.5.7.3.1), ipsecEndSystem (1.3.6.1.5.5.7.3.5), ipsecIntermediateSystem (1.3.6.1.5.5.8.2.2)
DomainController	clientAuth (1.3.6.1.5.5.7.3.2), serverAuth (1.3.6.1.5.5.7.3.1)
RDP Gateway	serverAuth (1.3.6.1.5.5.7.3.1)
SCEP szerver	

- CRL szétosztási pont (CRL Distribution Points) – nem kritikus
  OID: 2.5.29.31
  A mező tartalmazza a Tanúsítvánnyal kapcsolatban releváns CRL elérhetőségét http és/vagy LDAP protokollon keresztül.

  A *Tanúsítvány*ra vonatkozó CRL elérhetősége kerül ide (url).

- Szolgáltatói információ elérése (Authority Information Access) – nem kritikus
  OID: 1.3.6.1.5.5.7.1.1
  A *Hitelesítés-szolgáltató* által rendelkezésre bocsátott, a *Tanúsítvány* használatához kapcsolódó egyéb szolgáltatásainak leírása.

  Végfelhasználói *Tanúsítvány*ok esetében a mező tartalmazza a következő adatokat:

– A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást nyújt. Ez az elérhetőség szerepel itt.

– A tanúsítványlánc felépítésének megkönnyítésére a *Hitelesítés-szolgáltató* megadja a *Tanúsítvány*t kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.

A mezőben a *Hitelesítés-szolgáltató* több szolgáltatás illetve hitelesítési egység *Tanúsítvány* elérhetőségi adatait is megadhatja.

- Minősített tanúsítvánnyal kapcsolatos állítások (Qualified Certificate Statements) – nem kritikus
  OID: 1.3.6.1.5.5.7.1.3
  A mező a minősített *Tanúsítvány*okkal kapcsolatos állítások jelzésére szolgál, azonban van olyan mezője is, amely a nem minősített *Tanúsítvány* esetében is használható.

  A QCType mező kitöltésre kerülhet a használati célnak megfelelően.

- Beágyazott aláírt tanúsítványok időbélyegzőinek listája - nem kritikus
  OID: 1.3.6.1.4.1.11129.2.4.2
  A mező a Certificate Transparency naplószolgáltatók által aláírt SCT-ket tartalmazza.

  Kitöltése opcionális és az *Igénylő* engedélyéhez kötött.

A fenti mezők a megadott szabályok szerint mindig kitöltésre kerülnek, kivéve a Beágyazott aláírt tanúsítványok időbélyegzőinek listáját.
Más tanúsítvány kiterjesztés nem kerül kitöltésre.

7.1.3. Az algoritmus objektum azonosítója

Annak a kriptográfiai algoritmusnak a megnevezése, amellyel a *Tanúsítvány* hitelesítésre került.
A *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítvány*ok bélyegzésére a következő kriptográfiai algoritmust használja:

- "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
- "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)

7.1.4. Névformák

A *Hitelesítés-szolgáltató* a jelen *Hitelesítési rend*ek alapján kibocsátott *Tanúsítvány*okban egy – az IETF RFC 5280 szabványban [27] illetve az ETSI EN 319 412-2, -3, -4 szabványokban [15], [16], [17] meghatározott attribútumokból összeállított – megkülönböztetett nevet használ az *Alany* azonosítására.

A *Tanúsítvány* tartalmazza az *Alany* szolgáltatói egyedi azonosítóját is a 3.1.1. fejezetben meghatározottak szerint kitöltve.

A *Tanúsítvány* "Issuer DN" mezőjében szereplő érték megegyezik a kibocsátó *Tanúsítvány*ának "Subject DN" mezőjében szereplő értékkel.

7.1.5. Névhasználati megkötöttségek

A *Hitelesítés-szolgáltató* nem használ névhasználati megkötéseket a "nameConstraints" mező felhasználásával.

7.1.6. A Hitelesítési rend objektum azonosítója

A *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*okba felveszi a nem kritikus (Hitelesítési Rend) kiterjesztést a 7.1.2. fejezet előírásai szerint.

7.1.7. A Hitelesítési rend megkötöttségek kiterjesztés használata

Nincs előírás.

7.1.8. A Hitelesítési rend jellemzők szintaktikája és szemantikája

A *Hitelesítés-szolgáltató* a Hitelesítési rend (Certificate Policy) kiterjesztés Irányelv minősítő (Policy Qualifier) mezejében rövid információt helyezhet el a *Tanúsítvány* felhasználhatóságával kapcsolatban. A mező tartalmazza a *Szolgáltatási szabályzat* online elérhetőségét (URI).

7.1.9. A kritikus Hitelesítési rend kiterjesztések feldolgozási szemantikája

Nincs megkötés.

7.2. Tanúsítvány visszavonási lista (CRL) profil

7.2.1. Verziószám(ok)

A *Hitelesítés-szolgáltató* az IETF RFC 5280 [27] specifikáció szerinti "v2" verziójú *Tanúsítvány visszavonási list*ákat bocsát ki.

7.2.2. Tanúsítvány visszavonási lista kiterjesztések

A *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány visszavonási list*ák kötelezően tartalmazzák az alábbi mezőket:

- Verzió (Version)
  A mező értéke kötelezően "1".
- Algoritmus azonosító (Signature Algorithm Identifier)
  A *Tanúsítvány visszavonási list*át hitelesítő elektronikus bélyegző készítéséhez használt kriptográfiai algoritmuskészlet azonosítója (OID). A *Hitelesítés-szolgáltató* által használt kriptográfiai algoritmusok neve és azonosítója:
  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)

- Aláírás (Signature)
  A *Hitelesítés-szolgáltató* visszavonási listát hitelesítő elektronikus bélyegzője. A *Tanúsítvány visszavonási list*át az adott hitelesítő egység a *Tanúsítvány*ok bélyegzésére használt kulcsával hitelesíti.

- Kibocsátó (Issuer)
  A *Tanúsítvány visszavonási list*át kibocsátó hitelesítő egység egyedi azonosítója.

- Hatálybalépés (thisUpdate)
  A *Tanúsítvány visszavonási lista* hatálybalépésének kezdete. UTC szerinti érték az IETF RFC 5280 [27] szerinti kódolással. A *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány visszavonási list*ák esetében ez megegyezik a kibocsátás idejével.

- Következő kibocsátás (nextUpdate)
  A következő *Tanúsítvány visszavonási lista* kibocsátásának ideje (lásd: 4.10. fejezet). UTC szerinti érték az IETF RFC 5280 [27] szerinti kódolással.

- Visszavont *Tanúsítvány*ok (Revoked Certificates)
  A visszavont *Tanúsítvány*ok listája a *Tanúsítvány* sorozatszámával és a visszavonás idejével.

A *Hitelesítés-szolgáltató* által kötelező jelleggel használt *Tanúsítvány visszavonási lista* kiterjesztés:

- CRL sorozatszám (CRL number) – nem kritikus
  OID: 2.5.29.20
  Ebbe a mezőbe a *Tanúsítvány visszavonási list*ák egyesével növekvő sorozatszámai kerülnek.

A *Hitelesítés-szolgáltató* által feltételesen használt *Tanúsítvány visszavonási lista* kiterjesztés:

- expiredCertsOnCRL – nem kritikus
  OID: 2.5.29.60
  A *Hitelesítés-szolgáltató* az X.509 specifikáció szerinti szabványos jelöléssel jelzi, hogy a lejárt *Tanúsítvány*okat nem távolítja el a CRL-ről. (Lásd: 4.10. fejezet.)

A *Hitelesítés-szolgáltató* által használható *Tanúsítvány visszavonási lista* bejegyzési kiterjesztések:

- Visszavonás oka (Reason Code) – nem kritikus
  OID: 2.5.29.21
  Ebbe a mezőbe a visszavonás oka kerül.

- Érvénytelenség ideje (Invalidity Date) – nem kritikus
  Ebbe a mezőbe a magánkulcs megbízhatatlanná válásának ideje kerülhet.

  A *Hitelesítés-szolgáltató* nem tölti ki kötelező jelleggel ezt a mezőt.

- Útmutató a felfüggesztett *Tanúsítvány*okhoz (Hold Instruction) – nem kritikus
  Ebbe a mezőbe a felfüggesztett *Tanúsítvány* kezelése kerülhet.

  A *Hitelesítés-szolgáltató* nem tölti ki ezt a mezőt.

A *Hitelesítés-szolgáltató* a kiterjesztéseket nem köteles kitölteni.

7.3. Online tanúsítvány-állapot válasz (OCSP) profil

A *Hitelesítés-szolgáltató* az IETF RFC 6960 [31] szerinti online tanúsítvány-állapot szolgáltatást üzemeltet.

A *Hitelesítés-szolgáltató* által kibocsátott OCSP válaszok az alábbi mezőket tartalmazzák:

- Algoritmus azonosító (signatureAlgorithm)
  Az OCSP választ hitelesítő digitális aláírás készítéséhez használt algoritmuskészlet azonosítója (OID). A *Hitelesítés-szolgáltató* által használt kriptográfiai algoritmuskészletek neve és azonosítója:
  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
- Aláírás (Signature)
  A *Hitelesítés-szolgáltató* OCSP választ hitelesítő digitális aláírása.
- Válaszadó azonosítója (responderID)
  Az OCSP választ kibocsátó hitelesítő egység egyedi azonosítója.
- Hatálybalépés (thisUpdate)
  Az OCSP válasz hatálybalépésének ideje. UTC szerinti érték az IETF RFC 5280 [27] szerinti kódolással.
- Következő kibocsátás (nextUpdate)
  A következő OCSP válasz kibocsátásának legkésőbbi ideje. UTC szerinti érték az IETF RFC 5280 [27] szerinti kódolással.

  Kötelezően kitöltendő, értéke a kibocsátás időpontja + 12 óra.
- *Tanúsítvány* állapot válasz (SingleResponse)
  A válasz tartalmazza a *Tanúsítvány* azonosítóját (CertID) és a *Tanúsítvány* visszavonási állapotát (CertStatus).

  A *Hitelesítés-szolgáltató* a CABF BR követelményeinek megfelelő pozitív OCSP választ nyújt, vagyis a válasz csak akkor tartalmazza a "good" értéket, ha az adott *Tanúsítvány* megtalálható a *Hitelesítés-szolgáltató Tanúsítványtár*ában és nincs visszavont állapotban.

7.3.1. Verziószám(ok)

A *Hitelesítés-szolgáltató* támogatja az IETF RFC 6960 [31] szerinti "v1" verziójú online tanúsítvány-állapot kéréseket és válaszokat.

Mivel a Verzió (Version) mező alapértelmezett értéke a "v1", a mező nem szerepel az OCSP válaszokban.

7.3.2. OCSP kiterjesztések

A *Hitelesítés-szolgáltató* által feltételesen használt OCSP kiterjesztés:

- ArchiveCutoff – nem kritikus
  A *Hitelesítés-szolgáltató* az IETF RFC 6960 [31] specifikáció szerinti szabványos jelöléssel jelezheti, ha a lejárt *Tanúsítvány*okra is szolgáltat visszavonási állapot információt. (Lásd: 4.10. fejezet.)

A *Hitelesítés-szolgáltató* által használható OCSP bejegyzési kiterjesztések:

- Visszavonás oka (Reason Code) – nem kritikus
  Ebbe a mezőbe a visszavonás oka kerül.

8. A megfelelőség vizsgálata

A *Hitelesítés-szolgáltató* rendszeres időközönként megvizsgáltatja működését külső független auditorral. Az audit során felülvizsgálatra kerül, hogy a *Hitelesítés-szolgáltató* működése megfelel-e 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 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [12]
- 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 [13]

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: 1.3.1. fejezet).

8.1. Az ellenőrzések körülményei és gyakorisága

A *Hitelesítés-szolgáltató* évente külső megfelelőségértékelési auditot hajt végre a szolgáltatások nyújtását végző informatikai rendszerén.

A *Hitelesítés-szolgáltató* gondoskodik belső folyamatainak rendszeres ellenőrzéséről, ennek részleteit belső szabályzataiban rögzíti. Legalább évente egyszer egy átfogó audit során ellenőrzi a működés megfelelőségét.

A *Hitelesítés-szolgáltató* negyedévente szúrópróbaszerűen ellenőrzi az előző ellenőrzés óta kibocsátott *Weboldal-hitelesítő tanúsítvány*ok legalább 3% -át, hogy megfelelnek-e a vonatkozó *Hitelesítési rend*nek és *Szolgáltatási szabályzat*nak.

Más szervezet által felügyelt hitelesítési egység számára kibocsátott szolgáltatói *Tanúsítvány* esetében a külső hitelesítési egység működését évente auditálja.

8.2. Az auditor és szükséges képesítése

A *Hitelesítés-szolgáltató* a belső auditokat a független rendszervizsgáló szerepkörrel felruházott alkalmazottai segítségével rendszeresen végzi.

Az eIDAS és ETSI követelményeknek való megfelelőséget igazoló vizsgálatot olyan szervezet végzi el, amely rendelkezik egy EU tagállam nemzeti akkreditációs szervezete által kiadott erre feljogosító felhatalmazással.

8.3. Az auditor és az auditált rendszerelem függetlensége

A külső auditot olyan személy végzi:

- aki független a vizsgált *Hitelesítés-szolgáltató* tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- aki független a vizsgált szervezettől, vagyis sem saját maga, sem közvetlen hozzátartozója nincs munkaviszonyban vagy üzleti kapcsolatban a *Hitelesítés-szolgáltató*val;
- akinek díjazása nem függ az audit során végzett tevékenységének megállapításaitól.

8.4. Az auditálás által lefedett területek

Az átvizsgálás lefedi az alábbi területeket:

- hatályos jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;
- *Hitelesítési rend*(ek)nek és *Szolgáltatási szabályzat*(ok)nak való megfelelés;
- az alkalmazott folyamatok megfelelősége;
- a dokumentálás;
- a fizikai biztonság;

- a személyi állomány megfelelősége;
- az IT biztonság;
- az adatvédelmi szabályok betartása.

Amennyiben a *Hitelesítés-szolgáltató* bocsátott ki más szervezet hitelesítési egysége számára szolgáltatói *Tanúsítvány*t, akkor a vizsgálat az érintett külső szervezetek tevékenységére is kiterjed.

8.5. A hiányosságok kezelése

A független auditor az átvizsgálás eredményét egy részletes átvilágítási jelentésben foglalja össze, amely kitér a vizsgált rendszerelemekre, folyamatokra, tartalmazza az átvilágítás során felhasznált bizonyítékokat és vizsgálói megállapításokat. A jelentésben külön fejezetben rögzíti a vizsgálat során feltárt eltéréseket és az elhárításukra kitűzött határidőket. A független auditor a vizsgálat során feltárt eltérések, hiányosságok súlyossága alapján a jelentésben rögzíthet:

- opcionálisan figyelembe vehető módosítási javaslatokat;
- kötelezően elhárítandó eltéréseket.

8.6. Az eredmények közzététele

A *Hitelesítés-szolgáltató* a vizsgálat eredményét összefoglaló jelentést nyilvánosságra hozza honlapján az alábbi linken:

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

A feltárt hiányosságok részleteit nem publikálja, azokat bizalmas információként kezeli.

9. Egyéb üzleti és jogi kérdések

9.1. Díjak

A szolgáltatási díjakat és árakat a *Hitelesítés-szolgáltató* a honlapján közzéteszi és kérelemre nyomtatott formában ügyfélszolgálati irodájában is biztosítja olvashatóságát.

A *Hitelesítés-szolgáltató* az árlistát egyoldalúan módosíthatja. Az árlista módosítását a hatálybalépése előtt 30 nappal a *Hitelesítés-szolgáltató* a honlapján közzéteszi. Az *Ügyfél* számára kedvező változások a 30 naposnál rövidebb határidővel is bevezethetők. Az előre kifizetett szolgáltatások árát a módosítás nem érinti.

A díjak kifizetésével és visszatérítésével kapcsolatos rendelkezéseket a Szolgáltatási szerződés és mellékletei – különösen az Általános szerződési feltételek – tartalmazzák.

9.1.1. Tanúsítvány kibocsátás és megújítás díjai

Lásd: 9.1. fejezet.

9.1.2. Tanúsítvány hozzáférés díja

A *Hitelesítés-szolgáltató* ingyenes hozzáférést biztosít az *Érintett felek* részére az online *Tanúsítványtár*hoz.

9.1.3. Visszavonási állapot információ hozzáférés díja

A *Hitelesítés-szolgáltató* ingyenes online CRL és OCSP információt szolgáltat az *Érintett felek* részére valamennyi általa kibocsátott végfelhasználói és köztes szolgáltatói *Tanúsítvány* visszavonási állapotáról.

9.1.4. Egyéb szolgáltatások díjai

Lásd: 9.1. fejezet.

9.1.5. Visszatérítési politika

Lásd: 9.1. fejezet.

9.2. Anyagi felelősségvállalás

A *Hitelesítés-szolgáltató* megbízhatósága érdekében anyagi felelősséget vállal a jelen *Hitelesítési rend*ben, a vonatkozó *Szolgáltatási szabályzat*ban valamint az *Ügyfél*lel kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért.

9.2.1. Pénzügyi követelmények

A *Hitelesítés-szolgáltató* rendelkezik a szolgáltatások nyújtásával valamint a megszűnésével kapcsolatos költségek biztosításához szükséges anyagi erőforrásokkal.

9.2.2. További követelmények

Nincs megkötés.

9.2.3. Felelősségbiztosítás

- A *Hitelesítés-szolgáltató* a megbízhatóság biztosítása érdekében felelősségbiztosítással rendelkezik.
- A felelősségbiztosítási szerződés kiterjed az alábbi, a *Hitelesítés-szolgáltató* által a szolgáltatások nyújtásával összefüggésben okozott károkra:
  - a bizalmi szolgáltatási *Ügyfél*nek a Szolgáltatási szerződés megszegésével összefüggésben okozott károkra;
  - a bizalmi szolgáltatási *Ügyfél*nek és harmadik személynek szerződésen kívüli okozott károkra;

  - a Nemzeti Média- és Hírközlési Hatóságnak a bizalmi szolgáltatási tevékenységet befejező *Hitelesítés-szolgáltató* által okozott költségekre;
  - az eIDAS Rendelet [1] 17. cikk (4) bekezdés e) pontja alapján a Nemzeti Média- és Hírközlési Hatóság által felkért megfelelőségértékelő szervek eljárásának költségeire, ha azt a Nemzeti Média- és Hírközlési Hatóság eljárási költségként érvényesíti.

- A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként legalább 3.000.000 forint. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.

- A felelősségbiztosítás a meghatározott összeg erejéig fedezetet nyújt a károsultnak a szolgáltató károkozó magatartásával összefüggésben keletkező teljes kárára, függetlenül attól, hogy a kárt szerződésszegéssel vagy szerződésen kívül okozták.

- Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

9.3. Bizalmasság

A *Hitelesítés-szolgáltató* az *Ügyfel*ek adatait a jogszabályoknak megfelelően kezeli. A *Hitelesítés-szolgáltató* rendelkezik adatkezelési szabályzattal (lásd 9.4 fejezet), amely a személyes adatok kezelésével kiemelten foglalkozik.

Az *Ügyfél* a *Tanúsítvány* igénylésével, illetve a Szolgáltatási szerződés aláírásával hozzájárul ahhoz, hogy a személyes adatait a *Hitelesítés-szolgáltató* (az adatkezelési szabályzatnak megfelelő módon) tárolja és kezelje. A hozzájárulás vonatkozik a törvény által meghatározott és nyilvántartásba vett információk harmadik félhez történő továbbítására a *Hitelesítés-szolgáltató* szolgáltatásainak leállítása esetén, valamint – kizárólag a szolgáltatással összefüggő feladatok elvégzése céljából – a *Hitelesítés-szolgáltató* alvállalkozóinak való továbbításra. A Szolgáltatási szerződéshez tartozó tanúsítványkérelem űrlapon az *Igénylő* nyilatkozik arról, hogy hozzájárul a *Tanúsítvány* nyilvánosságra hozatalához. A *Hitelesítés-szolgáltató* az *Ügyfel*ek adatait kizárólag a szolgáltatásaival összefüggésben használja fel.

Az *Alany* és a *Képviselt szervezet* *Tanúsítvány*ban szereplő adatait a *Hitelesítés-szolgáltató* a Tanúsítvánnyal együtt nyilvánosságra hozza, amennyiben az *Igénylő* ehhez hozzájárul. A *Tanúsítvány*ba nem kerülő adatokat a *Hitelesítés-szolgáltató* védett módon tárolja az *Alany* személyazonosságának, a *Képviselt szervezet* szervezeti azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

A *Hitelesítés-szolgáltató* a tudomására jutott adatokat a jogszabályi követelményeknek megfelelően, az előírt időtartamig megőrzi. A *Hitelesítés-szolgáltató* az adatok megőrzése során gondoskodik az információk sértetlenségéről, bizalmasságáról és biztonságos tárolásáról. Az információkhoz való hozzáférést csak azon személyeknek engedélyezi, akik feladata azt indokolja.

A *Hitelesítés-szolgáltató* az *Ügyfel*ek adatainak továbbítása során gondoskodik a nem nyilvános információk bizalmasságáról és sértetlenségéről.

9.3.1. Bizalmas információk köre

A *Hitelesítés-szolgáltató* bizalmas információként kezeli:

- az *Ügyfel*ek minden adatát, kivéve azokat, amelyeket a 9.3.2. fejezetben nem bizalmasnak tekintett információnak minősít;
- az *Ügyfel*ek adatain kívül:
  - a magánkulcsokat és aktivizáló kódokat;
  - a tanúsítványigényléseket és Szolgáltatási szerződéseket;
  - a tranzakciós és naplóadatokat;
  - a nem nyilvános szabályzatokat;
  - minden olyan adatot, amelynek nyilvánosságra hozatala a szolgáltatás biztonságát előnytelenül befolyásolná.

9.3.2. Bizalmas információk körén kívül eső adatok

A *Hitelesítés-szolgáltató* nyilvánosnak tekint miden olyan adatot, amely nyilvánosan elérhető forrásból beszerezhető, vagy amely nyilvánosságra hozatalához az *Előfizető* előzetesen írásban hozzájárult.

Amennyiben az *Igénylő* ehhez hozzájárul, a *Hitelesítés-szolgáltató* nem bizalmas információként kezeli mindazon adatokat, amelyet a *Tanúsítvány*ba belefoglal. Ezek az adatok a Szolgáltatási szerződéshez kapcsolódó tanúsítványkérelem űrlapon egyértelmű jelöléssel szerepelnek.

A *Hitelesítés-szolgáltató* az általa kibocsátott valamennyi végfelhasználói és szolgáltatói köztes *Tanúsítvány* visszavonási állapotát nyilvános információként kezeli és ezt korlátozás nélkül elérhetővé teszi az *Érintett felek* részére *Tanúsítvány visszavonási lista* (CRL) publikálásával és online tanúsítvány-állapot szolgáltatás (OCSP) nyújtásával. A közzétett információ tartalmazza a *Tanúsítvány* sorszámát, a visszavonás időpontját és opcionálisan a visszavonás okát. Bővebb információ a 7.2. és 7.3. alfejezetekben található.

9.3.3. Bizalmas információ védelme

A *Hitelesítés-szolgáltató* felelősséggel tartozik az általa kezelt bizalmas adatok védelméért.

A *Hitelesítés-szolgáltató* szerződésben vagy titoktartási nyilatkozat aláírásával kötelezi alkalmazottait, alvállalkozóit, szerződött partnereit a bizalmas adatok védelmére.

A *Hitelesítés-szolgáltató* a birtokába jutott bizalmas adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [6] rendelkezéseinek megfelelően kezeli, és kizárólag az alábbi esetekben fedi fel azokat:

- **Információszolgáltatás a hatóságok részére**

  A *Hitelesítés-szolgáltató* az Eüt. [8] 90. § (1) bekezdésének megfelelően az általa nyújtott bizalmi szolgáltatások

felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén – a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak díjmentesen továbbítja az érintett személyazonosságát igazoló, valamint a *Hitelesítés-szolgáltató* által egyeztetett adatokat.

A *Hitelesítés-szolgáltató* rögzíti az adatátadás tényét, de arról nem tájékoztatja az érintett *Ügyfel*eket.

- **Információszolgáltatás polgári eljárás keretében**

  A *Hitelesítés-szolgáltató* a *Tanúsítvány* érvényességét érintő polgári peres, illetve nem peres eljárás során – az érintettség igazolása esetén – az *Alany* személyazonosságát igazoló, vagy a *Hitelesítés-szolgáltató* által egyeztetett adatokat átadhatja az ellenérdekű félnek vagy képviselőjének, illetve azokat közölheti a megkereső bírósággal.

  A *Hitelesítés-szolgáltató* rögzíti az adatátadás tényét, és arról tájékoztatja az érintett *Ügyfel*et.

- **A tulajdonos kérésére történő felfedés**

  A *Hitelesítés-szolgáltató* az *Ügyfél* személyes kérése vagy az általa hivatalosan, írásban adott felhatalmazása alapján tárja fel a rá vonatkozó bizalmas felhasználói információkat harmadik fél részére.

- **Egyéb információ-közzétételt eredményező körülmények**

  A *Hitelesítés-szolgáltató* köteles az Eüt. [8] 88. § (6) bekezdésének megfelelően a bizalmi szolgáltatás nyújtásának megszüntetése esetén az átvevő bizalmi szolgáltatónak a hozzáférési kötelezettség alá eső nyilvántartási adatokat átadni, ideértve a személyes adatokat is.

9.4. Személyes adatok védelme

A *Hitelesítés-szolgáltató* gondoskodik az általa kezelt személyes adatok védelméről, működése és szabályzatai megfelelnek az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [6] és a 2016/679 EU általános adatvédelmi rendelet [2] rendelkezéseinek.

A *Hitelesítés-szolgáltató* az *Ügyfél*ről nyilvántartott személyes adatokat és információkat a jogszabályi előírásoknak megfelelően

- megőrzi,
- azokat a megőrzési kötelezettség lejártával – amennyiben az *Ügyfél* erről másképpen nem rendelkezik – az ügyfél adatbázisból törli.

A *Hitelesítés-szolgáltató* nyilvántartásában azonosító adatokat, az *Alany*ról a *Tanúsítvány*ban szereplő adatokat, az *Előfizető*ről kizárólag a szolgáltatás igénybevételéhez, azonosításhoz, valamint a szerződéskötéshez és a számlázáshoz szükséges információkat tárolja.

A *Hitelesítés-szolgáltató* kizárólag olyan esetben adja át harmadik félnek az *Ügyfél* adatait, ha ezt jogszabály előírja vagy ha az *Ügyfél* ebbe írásban beleegyezett.

9.4.1. Adatkezelési szabályzat

A *Hitelesítés-szolgáltató* rendelkezik adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a személyes adatok kezelésére. Az adatkezelési szabályzat megtalálható az e-Szignó Hitelesítés Szolgáltató honlapján az alábbi linken:

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

9.4.2. Személyes adatok

A *Hitelesítés-szolgáltató* védi az érintettel kapcsolatba hozható, vagy az érintettre vonatkozó következtetést tartalmazó minden olyan személyes adatot, amely nem érhető el nyilvánosan a *Tanúsítvány*ból vagy más nyilvános adatforrásból.

9.4.3. Személyes adatnak nem minősülő adatok

A *Hitelesítés-szolgáltató* az *Igénylő* írásbeli hozzájárulása alapján nyilvánosságra hozhatja az *Alany*ok *Tanúsítvány*ban szereplő adatait.

A *Tanúsítvány*ban a *Hitelesítés-szolgáltató* feltünteti az *Alany*hoz rendelt szolgáltatói egyedi azonosítót.

9.4.4. Személyes adatok védelme

A *Hitelesítés-szolgáltató* biztonságosan tárolja és védi a *Tanúsítvány* kiadással kapcsolatos és a *Tanúsítvány*ban nem szereplő személyes adatokat. Az adatokat megfelelő intézkedésekkel védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, valamint nyilvánosságra hozatal ellen.

9.4.5. Személyes adatok felhasználása

A *Hitelesítés-szolgáltató* csak a *Tanúsítvány*okban szereplő személyes adatokat hozza nyilvánosságra az *Ügyfél* írásbeli engedélyének birtokában.

9.4.6. Adatkezelés

A *Hitelesítés-szolgáltató* az *Ügyfél* értesítése nélkül is kiadhatja az *Ügyfél*ről tárolt személyes adatokat a vonatkozó jogszabályok által meghatározott esetekben.

9.4.7. Egyéb adatvédelmi követelmények

Nincs előírás.

9.5. Szellemi tulajdonjogok

A *Hitelesítés-szolgáltató* működése során nem sértheti meg harmadik személy szellemi tulajdonjogait.

A *Hitelesítés-szolgáltató* által ügyfelei részére kibocsátott magán- és nyilvános kulcs tulajdonosa az *Előfizető*, teljes jogú felhasználója pedig az *Igénylő*, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

A *Hitelesítés-szolgáltató* által ügyfelei részére kibocsátott *Tanúsítvány* tulajdonosa a *Hitelesítés-szolgáltató*, a *Tanúsítvány*ok teljes jogú felhasználója pedig az *Előfizető*.

A *Hitelesítés-szolgáltató* az általa kibocsátott végfelhasználói *Tanúsítvány*okat a benne szereplő nyilvános kulccsal együtt a kikötéseiben és feltételeiben ismertetett módon közzéteheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti.

A *Hitelesítés-szolgáltató* tulajdonát képezi a tanúsítvány visszavonási állapot információ, amit a *Hitelesítés-szolgáltató* nyilvánosságra hoz a 7.2. és 7.3. alfejezetekben meghatározott módon.

A *Hitelesítés-szolgáltató* által az *Ügyfel*ek részére kibocsátott szolgáltatói egyedi azonosító a *Hitelesítés-szolgáltató* tulajdonát képezi, amit a *Hitelesítés-szolgáltató* nyilvánosságra hoz a *Tanúsítványtár*ban a *Tanúsítvány* részeként.

A *Tanúsítvány*ban szereplő azonosító (amely a *Tanúsítvány* alanyát azonosítja) használatára az *Ügyfél* jogosult.

A jelen *Szolgáltatási szabályzat* a *Hitelesítés-szolgáltató* kizárólagos tulajdonát képezi. Az *Ügyfel*ek és egyéb *Érintett felek* a dokumentumot csak a jelen *Szolgáltatási szabályzat* előírásainak megfelelően jogosultak felhasználni, minden egyéb kereskedelmi vagy egyéb célú felhasználás szigorúan tilos.

A jelen *Szolgáltatási szabályzat* szabadon terjeszthető, de csak változatlan formában, teljes terjedelemben és az eredet feltüntetésével.

A *Hitelesítés-szolgáltató* által a szolgáltatás igénybevételéhez biztosított szoftverek használatának szabályait a szoftver leírásában vagy magában a szoftverben elérhető illetve ott meghivatkozott helyen található felhasználói útmutató tartalmazza.

9.6. Tevékenységért viselt felelősség és helytállás

9.6.1. A szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

A *Hitelesítés-szolgáltató* felelősségét jelen *Szolgáltatási szabályzat*, a vonatkozó *Hitelesítési rend*, valamint az *Ügyfél*lel kötött Szolgáltatási szerződés és annak mellékletei tartalmazzák, melyek szerint:

- a *Hitelesítés-szolgáltató* felelősséget vállal azért, hogy megfelelő eljárásokkal ellenőrizte, hogy az *Igénylő* jogosult a *Tanúsítvány*ban feltüntetett domén nevek és IP címek használatára, vagy azok felett a gyakorlatban ellenőrzéssel bír;

- a *Hitelesítés-szolgáltató* felelősséget vállal az általa támogatott *Hitelesítési rend*(ek)ben leírt eljárásoknak való megfelelésért;

- a *Hitelesítés-szolgáltató* sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- a *Hitelesítés-szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfel*ekkel szemben a Polgári Törvénykönyv [7] a szerződésszegésért való felelősség szabályai szerint felelős;
- a *Hitelesítés-szolgáltató* a vele szerződéses jogviszonyban nem álló harmadik személlyel (ilyen az *Érintett fél*) szemben a Polgári Törvénykönyv [7] általános felelősségi szabálya szerint felelős;
- a *Hitelesítés-szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött Szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 9.8. fejezet);
- ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

A *Hitelesítés-szolgáltató* nem felelős:

- az *Alany*ok magánkulccsal kapcsolatos tevékenységeiért,
- az *Érintett felek* tanúsítvány ellenőrzési és felhasználási tevékenységeiért,
- az *Érintett felek* vagy mások által kibocsátott szabályzatokért.

A Szolgáltató kötelezettsége

A *Hitelesítés-szolgáltató* alapvető kötelezettsége, hogy a szolgáltatásokat a *Hitelesítési rend*del, a *Szolgáltatási szabályzat*tal és egyéb nyilvános szabályzatokkal, a szerződéses feltételekkel, továbbá a vállalati és biztonsági belső szabályzatokkal összhangban nyújtsa. Ezen alapvető kötelezettségek a következők:

- a szolgáltatásnak megfelelő jogi-, szabályozási-, anyagi-, szerződéses stb. keretek megteremtése;
- magas színvonalú és biztonságos szolgáltatások nyújtása a vonatkozó szabályzatok szerint;
- a szolgáltatásokhoz kapcsolódó szervezetek (hitelesítő szervezet, ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése;
- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése;
- a szolgáltatások biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket;
- a publikus nyilvántartások és saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az interneten keresztül.

A hitelesítő szervezet felelőssége

A hitelesítő szervezet feladata a hitelesítő egységek, valamint az online tanúsítvány-állapot szolgáltatáshoz szükséges egységek (lásd: 1.3.1) felállítása és működtetése, a tanúsítványtár és a visszavonási-állapot információ gondozása, valamint a szabályzatok menedzselése.

A hitelesítő szervezet belső működtetését a *Hitelesítés-szolgáltató* belső, operatív szabályzatai határozzák meg. A hitelesítő egységek által kibocsátott szolgáltatói tanúsítványok kezelése (például regisztrációs munkatársak, ügyeletesek számára) az operatív szabályzatok előírásainak megfelelően történik. Jelen szabályzat csak a nyilvános szolgáltatói és végfelhasználói tanúsítványokkal kapcsolatban tartalmaz előírásokat.

A szabályzatok menedzselése keretében ellátandó feladatok:

- az alkalmazott tanúsítványfajták specifikálása, jóváhagyása és karbantartása;
- a szolgáltatások nyilvános szabályzatainak és a belső (nem nyilvános) előírásoknak előkészítése, egyeztetése a jogszabályokkal és a belső (nem nyilvános) szabályzatokkal, továbbá az aktualizálások elvégzése;
- a szolgáltatásokra vonatkozó szabályzatokkal kapcsolatos észrevételek rögzítése és javaslatok elbírálása.

Az e-Szignó Hitelesítés Szolgáltató felelős:

- az általa kibocsátott *Tanúsítvány*ok hitelességéért, pontosságáért;
- az általa kibocsátott szabályzatokért, azok jogszabályi megfelelőségéért és betartásáért;
- az általa generált kulcspárok megfelelőségéért, a magánkulcs-nyilvános kulcs és a *Tanúsítvány* összetartozásáért;
- általában a kötelezettségei betartásáért.

9.6.2. A regisztráló szervezet felelőssége és helytállása

Az ügyfélszolgálati iroda feladata a *Hitelesítés-szolgáltató* képviselete a szolgáltatások kapcsán a végfelhasználónál. Ennek keretében a következő feladatokat látja el:

- közreműködik a szolgáltatások értékesítésében;
- elvégzi az *Alany* regisztrációját;
- a különböző tanúsítvány műveletekre vonatkozó kérelmeket fogadja (visszavonás, visszaállítás, tanúsítvány módosítás, kulcscsere stb.);
- fogadja és kezeli az adatmódosítási bejelentéseket;
- közreműködik a visszavonási állapot közzétételében;
- tájékoztatást ad az *Ügyfel*ek és az *Érintett felek* részére a *Hitelesítés-szolgáltató* által nyújtott szolgáltatásokkal kapcsolatban;

A *Regisztráló szervezet* felelős:

- az *Igénylő* személyazonosságának megállapításáért;
- a *Képviselt szervezet* szervezeti azonosságának megállapításáért, a *Képviselt szervezet* nevében eljáró személy személyazonosságának és képviseleti jogosultságának megállapításáért;
- a felvett regisztrációs adatok valódiságáért;
- a Szolgáltatási szerződés megkötését megelőzően a szolgáltatások igénybe vevőjének tájékoztatásáért a *Hitelesítési rend* és a *Szolgáltatási szabályzat* tartalmáról és elérhetőségéről, a szolgáltatás igénybevételének feltételeiről;
- általában kötelezettségeinek maradéktalan betartásáért.

9.6.3. 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 vagy IP címek 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 vagy IP címen 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.

9.6.4. 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.

9.6.5. Egyéb szereplők tevékenységéért viselt felelősség és helytállás

A Képviselt Szervezet felelőssége

A *Képviselt szervezet* kizárólag az általa kiadott igazolásokért felel. Különösen azon igazolásokért, amelyben igazolja, hogy az *Igénylő* jogosult a *Szervezet* nevét is tartalmazó *Tanúsítvány* használatára, illetve jogosult a *Képviselt szervezet* *Tanúsítvány*ában szerepelni. Amennyiben a *Képviselt szervezet* által kiállított valamely igazolásban szereplő információ megváltozik, a *Képviselt szervezet* felelőssége ezt haladéktalanul jelenteni a *Hitelesítés-szolgáltató*nak.

A Képviselt Szervezet jogai

- A *Hitelesítés-szolgáltató* kizárólag a *Képviselt szervezet* hozzájárulásával bocsát ki olyan *Tanúsítvány*t, amelyben a *Képviselt szervezet* neve is feltüntetésre kerül.
- A *Képviselt szervezet* jogosult azon *Tanúsítvány*okat visszavonatni, amelyekben a *Képviselt szervezet* neve is feltüntetésre került.

9.7. Helytállás érvénytelenségi köre

A *Hitelesítés-szolgáltató* kizárja felelősségét, amennyiben:

- az *Igénylő*k nem tartják be a magánkulcs kezelésével kapcsolatos előírásokat;
- az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozat által elfogadott kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8. 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.

Pénzügyi felelősség

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 káreseményenként 4.000.000,-Ft. Ha egy káreseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra káreseményenként a fenti korlátozás szerint meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a korlátozás szerint meghatározott összeghez viszonyított arányában történik.

9.9. Kártérítési kötelezettség

9.9.1. A szolgáltató kártérítési kötelezettsége

A *Hitelesítés-szolgáltató* kártérítési kötelezettségének részletes szabályait jelen szabályzat (lásd: 9.8. fejezet), a Szolgáltatási szerződés és az *Ügyfel*ekkel kötött szerződések tartalmazzák.

9.9.2. Az előfizető kártérítési kötelezettsége

Az *Előfizető* kártérítési felelősséggel tartozik a *Hitelesítés-szolgáltató*nak azokért a veszteségekért és károkért, amelyeket kötelezettségei és a rá vonatkozó ajánlások be nem tartásával okoz számára.

9.9.3. Az érintett felek kártérítési kötelezettsége

Lásd: 9.8. fejezet

9.10. Érvényesség és megszűnés

9.10.1. Érvényesség

A *Szolgáltatási szabályzat* adott verziója hatálybalépésének napja a dokumentum címlapján kerül meghatározásra.

9.10.2. Megszűnés

A *Szolgáltatási szabályzat* visszavonásig illetve a *Szolgáltatási szabályzat* újabb verziójának hatályba lépéséig hatályos időbeli korlátozás nélkül.

A *Szolgáltatási szabályzat* 9. fejezete érvényben marad a *Szolgáltatási szabályzat* hatályának megszűnését követően is (a hatályosság megszűnésének módjától függetlenül) mindazon *Tanúsítvány*okkal kapcsolatosan, amelyet a *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzat* hatálya alatt bocsátott ki.

9.10.3. A megszűnés következményei

A *Szolgáltatási szabályzat* visszavonása esetén a *Hitelesítés-szolgáltató* honlapján közzéteszi a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket.

A *Hitelesítés-szolgáltató* garantálja, hogy a *Szolgáltatási szabályzat* visszavonása esetén is érvényben maradnak a bizalmas adatok védelmére vonatkozó előírások.

9.11. A felek közötti kommunikáció

A *Hitelesítés-szolgáltató* az *Ügyfel*ekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát működtet.

Az *Ügyfel*ek jognyilatkozataikat a *Hitelesítés-szolgáltató* felé kizárólag írásban, aláírt módon tehetik meg. Szervezet képviseletében történő aláírás csak a képviseleti jogosultság igazolásával együtt érvényes.

A kibocsátott *Tanúsítvány*ok SMS küldésével is visszavonhatók.

Egyéb jellegű értesítés írásban, elektronikus levél vagy fax formájában is megtehető.

Az e-Szignó Hitelesítés Szolgáltató elektronikus levélben tájékoztatja *Ügyfel*eit vagy tájékoztatását honlapján teszi közzé.

9.12. Módosítások

A *Hitelesítés-szolgáltató* fenntartja magának a jogot, hogy a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén szabályozott módon megváltoztassa a *Szolgáltatási szabályzat*ot.

9.12.1. Módosítási eljárás

A *Hitelesítés-szolgáltató* nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyezteti. A *Hitelesítés-szolgáltató* több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen *Szolgáltatási szabályzat* több ilyet is megemlít). A 8.4. fejezetben leírt eljárások ezeket a dokumentumokat is vizsgálják.

A *Hitelesítés-szolgáltató* hitelesítő szervezetén belül működik egy olyan szervezeti egység, amely felelős a szabályzatok és dokumentációk karbantartásáért. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz. A szabályzatot az e-Szignó Hitelesítés Szolgáltató igazgatója hagyja jóvá.

A változtatásokat gyűjtve a csoport belső, nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. A *Hitelesítés-szolgáltató* törekszik arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A *Hitelesítés-szolgáltató* évi rendszerességgel illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja a *Szolgáltatási szabályzat*ot és elvégzi a szükségesnek tartott változtatásokat. A dokumentum a legkisebb változtatás után is új verziószámot kap és az elfogadási procedúra időigényét figyelembe véve meghatározásra kerül a tervezett hatálybalépés időpontja is.

Hitelesítés-szolgáltató a jóváhagyott dokumentumot a tervezett hatálybalépés előtt publikálja honlapján.

9.12.2. Értesítések módja és határideje

A *Hitelesítés-szolgáltató* a 9.12.1. pontban leírtak szerint értesíti az *Érintett felek*et az új dokumentum verziók kibocsátásáról.

9.12.3. Az OID megváltoztatása

A *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzat* legkisebb változtatása esetén is új verziószámot ad ki, ami része a dokumentum azonosítónak (OID), így a dokumentum minden változása az OID változását eredményezi, vagyis két eltérő tartalmú – hatályba léptetett – dokumentumnak nem lehet azonos OID azonosítója.

9.13. 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.

9.14. 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.

9.15. Az érvényben lévő jogszabályoknak való megfelelés

A vonatkozó jogszabályok:

- 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];
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [6];
- 2013. évi V. törvény a Polgári Törvénykönyvről [7].
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól [8];
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről [9];
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről [10];
- 470/2017. (XII. 28.) Kormányrendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről [11];

9.16. Vegyes rendelkezések

9.16.1. Teljességi záradék

Nincs megkötés.

9.16.2. Átruházás

A jelen *Szolgáltatási szabályzat* alapján nyújtott szolgáltatásokba bevont alvállalkozók vagy egyéb együttműködő partnerek csak a *Hitelesítés-szolgáltató* előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3. Részleges érvénytelenség

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

9.16.4. Igényérvényesítés

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

9.16.5. Vis maior

A *Hitelesítés-szolgáltató* nem felelős a *Hitelesítési rend*ben és a *Szolgáltatási szabályzat*ban megfogalmazott kötelezettség hibás vagy késedelmes teljesítéséért, illetve nem teljesítéséért, amennyiben a hiba vagy késedelem oka a *Hitelesítés-szolgáltató* ellenőrzési körén kívül eső, előre nem látható elháríthatatlan külső ok.

9.17. Egyéb rendelkezések

Nincs megkötés.

A. A rövid hitelesítési rend azonosítók képzési szabályai

A *Hitelesítés-szolgáltató* az egyszerűbb kezelhetőség érdekében minden *Hitelesítési rend*hez rendel egy öt karakteres rövid nevet (azonosítót), amelyben az egyes karakterek meghatározzák az adott rend egyes paramétereit az alábbi szabályok szerint:

- Az első karakter [?....]
  - M: minősített *Tanúsítvány Hitelesítési rend*
  - H: nem minősített, III. hitelesítési osztályú *Tanúsítvány Hitelesítési rend*
  - K: nem minősített, II. hitelesítési osztályú *Tanúsítvány Hitelesítési rend*
  - A: nem minősített, automatikus kibocsátású *Tanúsítvány Hitelesítési rend*
- A második karakter [.?...]
  - A: Aláírás célú *Tanúsítvány Hitelesítési rend*
  - B: Bélyegző létrehozása célú *Tanúsítvány Hitelesítési rend*
  - W: *Weboldal-hitelesítő tanúsítvány Hitelesítési rend*
  - K: *Kódaláíró tanúsítvány Hitelesítési rend*
  - E: Egyéb célú *Tanúsítvány Hitelesítési rend*
- A harmadik karakter [..?..]
  - T: természetes személynek kibocsátott *Tanúsítvány Hitelesítési rend*
  - J: jogi személynek kibocsátott *Tanúsítvány Hitelesítési rend*
  - x: nincs megkötés, tetszőleges *Alany* részére kiadható
- A negyedik karakter [...?.]
  - B: *Minősített elektronikus aláírást létrehozó eszköz*ön kibocsátott *Tanúsítvány Hitelesítési rend*
  - H: *Hardver kriptográfiai eszköz*ön kibocsátott *Tanúsítvány Hitelesítési rend*
  - S: Szoftveresen kibocsátott *Tanúsítvány Hitelesítési rend*
  - x: nincs megkötés, tetszőleges hordozón kiadható
- Az ötödik karakter [....?]
  - A: álneves *Tanúsítvány Hitelesítési rend*
  - N: álnevet kizáró *Tanúsítvány Hitelesítési rend*

B. 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) 2016/679 RENDELETE (2016. április 27.) 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 (általános adatvédelmi rendelet) .

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

[4] 2001. évi XXXV. törvény az elektronikus aláírásról (hatályon kívül helyezve 2016. július 1-től) .

[5] 2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról .

[6] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról .

[7] 2013. évi V. törvény a Polgári Törvénykönyvről .

[8] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól .

[9] 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről .

[10] 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről .

[11] 470/2017. (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről .

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

[13] 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.

[14] ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

[15] ETSI EN 319 412-2 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;.

[16] ETSI EN 319 412-3 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

[17] ETSI EN 319 412-4 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.

[18] ETSI TS 119 312 V1.3.1 (2019-02); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[19] ISO 3166-1:2013, Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.

[20] MSZ/ISO/IEC 15408-2002 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai, 2002 december .

[21] ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules".

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

[23] IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.

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

[25] IETF RFC 4043: Internet X.509 Public Key Infrastructure - Permanent Identifier, May 2005.

[26] IETF RFC 5019: The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environment, September 2007.

[27] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.

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

[29] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.

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

[31] IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.

[32] IETF RFC 6962: Certificate Transparency, June 2013.

[33] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[34] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.6.6. CA/Browser Forum, `https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.6.pdf`, 2019.

[35] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.

[36] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.

[37] EU Trusted Lists of Certification Service Providers, (`https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers`.

[38] Magyarország (Hungary): Trusted List (`http://www.nmhh.hu/tl/pub/HU_TL.pdf`).

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