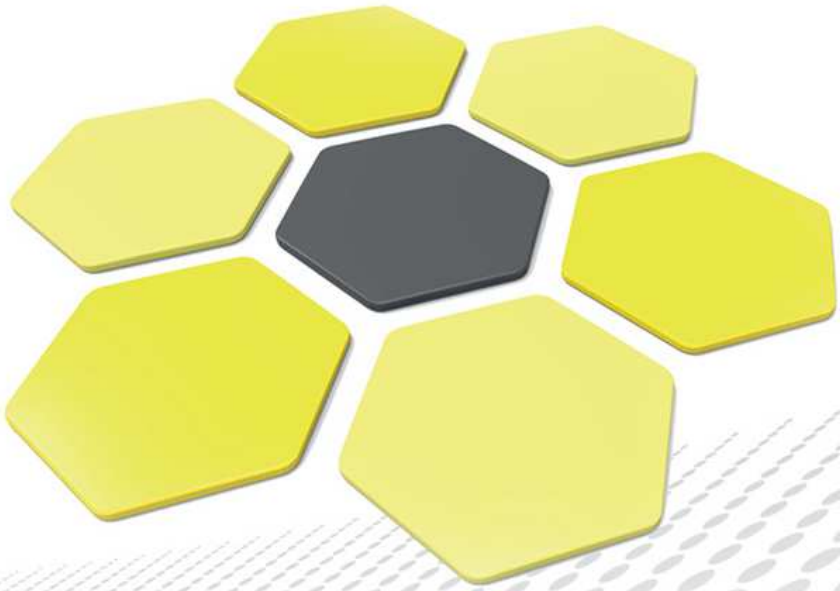
MICROSEC

e-Szignó Hitelesítés Szolgáltató

Nem minősített tanúsítvány hitelesítési rendek

ver. 4.0



Azonosító	1.3.6.1.4.1.21528.2.1.1.48.4.0, 1.3.6.1.4.1.21528.2.1.1.49.4.0, 1.3.6.1.4.1.21528.2.1.1.50.4.0, 1.3.6.1.4.1.21528.2.1.1.51.4.0, 1.3.6.1.4.1.21528.2.1.1.52.4.0, 1.3.6.1.4.1.21528.2.1.1.53.4.0, 1.3.6.1.4.1.21528.2.1.1.54.4.0, 1.3.6.1.4.1.21528.2.1.1.55.4.0, 1.3.6.1.4.1.21528.2.1.1.56.4.0
Verzió	4.0
Első verzió hatálybalépése	2006-11-19
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2015-07-01
Hatálybalépés dátuma	2015-08-01

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság
1031 Budapest, Záhony utca 7. D. épület

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Első változat OID: 1.3.6.1.4.1.21528.2.1.1.10 OID: 1.3.6.1.4.1.21528.2.1.1.11	2006-11-19	Dr. Berta István Zsolt
1.1	Hibák javítása	2006-11-19	Dr. Berta István Zsolt
1.2	Módosítás a Nemzeti Hírközlési Hatóság észrevételeinek megfelelően OID: 1.3.6.1.4.1.21528.2.1.1.10.1.2 OID: 1.3.6.1.4.1.21528.2.1.1.11.1.2	2006-12-04	Dr. Berta István Zsolt
1.3	Közjegyzői regisztráció megszüntetése. OID: 1.3.6.1.4.1.21528.2.1.1.10.1.3 OID: 1.3.6.1.4.1.21528.2.1.1.11.1.3	2007-10-28	Dr. Berta István Zsolt
1.4	Megváltozott a fogyasztóvédelem elérhetősége. OID: 1.3.6.1.4.1.21528.2.1.1.10.1.4 OID: 1.3.6.1.4.1.21528.2.1.1.11.1.4	2008-01-01	Dr. Berta István Zsolt
1.5	Változás a II. hitelesítési osztály követelményeiben. OID: 1.3.6.1.4.1.21528.2.1.1.10.1.5 OID: 1.3.6.1.4.1.21528.2.1.1.11.1.5	2008-12-20	Dr. Berta István Zsolt
1.6	Változás a III. hitelesítési osztály követelményeiben. OID: 1.3.6.1.4.1.21528.2.1.1.10.1.6 OID: 1.3.6.1.4.1.21528.2.1.1.11.1.6	2009-03-09	Dr. Berta István Zsolt
2.0	A természetes személyek és az automatizmusok számára kibocsátott tanúsítványokra vonatkozó, valamint a biztonságos hardver eszközt megkövetelő rendek különválasztása. OID: 1.3.6.1.4.1.21528.2.1.1.*.2.0	2010-10-20	Dr. Berta István Zsolt

Verzió	A változás leírása	Hatálybalépés	Készítette
3.0	Cégforma változása. OID: 1.3.6.1.4.1.21528.2.1.1.*.3.0	2012-05-01	Dr. Berta István Zsolt
3.1	Normatívák változása, kisebb változtatások. OID: 1.3.6.1.4.1.21528.2.1.1.*.3.1	2014-01-31	Dr. Szőke Sándor
4.0	Teljes átdolgozás az RFC 3647 szerint. OID: 1.3.6.1.4.1.21528.2.1.1.*.4.0	2015-08-01	Szabóné Endrődi Csilla, Dr. Szőke Sándor

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec zrt. által üzemeltetett e-Szignó Hitelesítés-szolgáltató által meghatározott nem minősített hitelesítési rendeket tartalmazza.

1.1. Áttekintés

A *Hitelesítési rend* egy "szabálygyűjtemény, amely egy *Tanúsítvány* felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára". Jelen dokumentum tartalmilag és formailag megfelel az RFC 3647 [21] keretrendszer követelményeinek. Kilenc fejezetből áll, amelyek tartalmazzák a *Hitelesítés-szolgáltató* által megfogalmazott biztonsági követelményeket, folyamatokat és a szolgáltatás nyújtása során követendő gyakorlatot. Az RFC 3647 által meghatározott felépítés szigorú megtartása érdekében azok a fejezetek is szerepelnek a dokumentumban, amelyeknél a *Hitelesítési rend* nem ír elő követelményt, ilyen esetben a fejezetben a "Nincs megkötés" szöveg szerepel.

Jelen dokumentum több *Hitelesítési rend* követelményeit tartalmazza. A dokumentumban megfogalmazott követelmények túlnyomó többsége a *Hitelesítési rend*ek mindegyikére egységesen érvényes, ezt külön nem jelöljük. Az eltérően kezelendő követelmények esetén egyértelműen meghatározásra kerül, hogy az adott követelmény mely *Hitelesítési rend*(ek)re vonatkozik.

A jelen dokumentumnak megfelelően kibocsátott *Tanúsítvány*oknak tartalmazniuk kell azon *Hitelesítési rend* azonosítóját (OID), amelynek megfelelnek. Az azonosító alapján az *Érintett felek* meg tudják ítélni a *Tanúsítvány*ok alkalmazhatóságát és megbízhatóságát egy adott alkalmazás tekintetében.

A *Hitelesítési rend*ek alapvető követelményeket fogalmaznak meg a *Tanúsítvány*okkal kapcsolatban elsősorban a *Tanúsítvány*t kibocsátó *Hitelesítés-szolgáltató* részére. Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a *Hitelesítés-szolgáltató* által kibocsátott *Szolgáltatási szabályzat*nak kell tartalmaznia.

A *Hitelesítési rend* csak egyike a *Hitelesítés-szolgáltató* által kibocsátott és a nyújtott szolgáltatás feltételeit együttesen szabályozó dokumentumoknak. Egyéb fontos dokumentumok például az Általános szerződési feltételek, a *Szolgáltatási szabályzat*, a felhasználókkal és a partnerekkel kötött egyéb szerződések.

A jelen dokumentum 1.6 fejezete számos fogalmat definiál, amelyeket más területeken nem, vagy nem teljesen ilyen értelmezésben használnak. Az ilyen értelemben használandó fogalmakat a dokumentumban minden esetben nagy kezdőbetűvel írva, döntött betűk használatával jelöljük.

1.2. Dokumentum neve és azonosítója

Jelen dokumentum egy *Hitelesítési rend* gyűjtemény, amelynek főbb azonosító adatai:

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	Nem minősített tanúsítvány hitelesítési rendek
Dokumentum verziószáma	4.0
Hatályba lépés ideje	2015-08-01

A jelen dokumentum által meghatározott *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*nak hivatkoznia kell 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)	EHSZ Szolgáltatás
(1)	dokumentumok
(1)	nyilvános dokumentumok
(x)	dokumentum egyedi azonosító sorszáma
(y)	dokumentum verziója
(z)	dokumentum alverziója

Jelen dokumentum az alábbi *Hitelesítési rend*eket definiálja:

OID	MEGNEVEZÉS	RÖVID NÉV
1.3.6.1.4.1.21528.2.1.1.48.4.0	Nem minősített tanúsítványokhoz használt, III. hitelesítési osztályba tartozó, természetes személyek számára kibocsátott, kriptográfiai hardver eszköz használatát megkövetelő, álnevet kizáró hitelesítési rend.	NSzTH
1.3.6.1.4.1.21528.2.1.1.49.4.0	Nem minősített tanúsítványokhoz használt, III. hitelesítési osztályba tartozó, természetes személyek számára kibocsátott, szoftveresen kibocsátott, álnevet kizáró hitelesítési rend.	NSzTSz
1.3.6.1.4.1.21528.2.1.1.50.4.0	Nem minősített tanúsítványokhoz használt, III. hitelesítési osztályba tartozó, nem természetes személyek számára kibocsátott, kriptográfiai hardver eszköz használatát megkövetelő, álnevet kizáró hitelesítési rend.	NSzNH
1.3.6.1.4.1.21528.2.1.1.51.4.0	Nem minősített tanúsítványokhoz használt, III. hitelesítési osztályba tartozó, nem természetes személyek számára kibocsátott, szoftveresen kibocsátott, álnevet kizáró hitelesítési rend.	NSzNSz
1.3.6.1.4.1.21528.2.1.1.52.4.0	Nem minősített tanúsítványokhoz használt, III. hitelesítési osztályba tartozó, SSL tanúsítványokhoz használt, álnevet kizáró hitelesítési rend.	NSzW
1.3.6.1.4.1.21528.2.1.1.53.4.0	Nem minősített tanúsítványokhoz használt, II. hitelesítési osztályba tartozó, álnevet kizáró hitelesítési rend.	NN

1.3.6.1.4.1.21528.2.1.1.54.4.0	Nem minősített tanúsítványokhoz használt, II. hitelesítési osztályba tartozó, SSL tanúsítványokhoz használt, álnevet kizáró hitelesítési rend.	NNW
1.3.6.1.4.1.21528.2.1.1.55.4.0	Nem minősített tanúsítványokhoz használt, automatikus kibocsátás során kibocsátott, SSL tanúsítványokhoz használt, álnevet kizáró hitelesítési rend.	NAW
1.3.6.1.4.1.21528.2.1.1.56.4.0	Nem minősített tanúsítványokhoz használt álneves hitelesítési rend.	NÁ

Ezen *Hitelesítési rend*ek alapján a *Hitelesítés-szolgáltató* többféle felhasználási célra bocsáthat ki *Tanúsítvány*t.

Ezen *Hitelesítési rend*ek alapján a *Hitelesítés-szolgáltató* olyan *Tanúsítvány*okat is kibocsáthat, amelyek az Eat. [1] szerint fokozott biztonságú elektronikus aláírás létrehozására alkalmasak. A fokozott biztonságú elektronikus aláírással ellátott dokumentumok kielégítik az írásba foglalás követelményét.

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 természetes személyek számára kibocsátott *Tanúsítvány*okra vonatkozó *Hitelesítési rend*ek esetén az *Alany* minden esetben természetes személy. A nem természetes személyek számára kibocsátott *Tanúsítvány*okra vonatkozó *Hitelesítési rend*ek esetén az *Alany* jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet. A *Tanúsítvány*okban szerepeltethető az informatikai rendszer, alkalmazás vagy automatizmus megnevezése is, amely segítségével a *Tanúsítvány*t használják (*Automata tanúsítvány*).

Az álnevet kizáró *Hitelesítési rend*ek esetén a *Tanúsítvány*ban az *Alany* valódi neve szerepel, míg az álneves *Hitelesítési rend*ek esetén a *Tanúsítvány*ban minden esetben álnév szerepel.

A kriptográfiai hardver eszköz használatát megkövetelő *Hitelesítési rend*ek esetén a *Hitelesítés-szolgáltató*

a./ meggyőződik róla, hogy a *Tanúsítvány*hoz tartozó magánkulcs az alábbi tanúsítások legalább egyikével rendelkező kriptográfiai hardver eszközön helyezkedik el:

- az Európai Unió valamely tagállamában nyilvántartásba vett tanúsító szervezet által kiadott igazolás szerint *Biztonságos aláírás-létrehozó eszköz*re vonatkozó tanúsítás;

- legalább EAL-4 szintű Common Criteria [2] tanúsítás a CEN SSCD PP [3] szerint;
- FIPS 140-2, Level 2 (vagy magasabb szintű) tanúsítás [4]

vagy

b./ elfogadhatja a *Tanúsítvány* kérelmezőjének ilyen értelmű írásos nyilatkozatát, mindenkor fenntartva a mérlegelés jogát.

Az Eat. [1] 10/A §-a szerint jogszabályban meghatározott informatikai eszköz felhasználásával automatikusan, közvetlen személyi felügyelet nélkül is készíthető minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírás.

Az [NSzTH], [NSzTSz], [NSzNH] és [NSzNSz] *Hitelesítési rend*ek alapján kiállított aláíró *Tanúsítvány*ok maradéktalanul megfelelnek a 78/2010. (III.25.) kormányrendelet [17] követelményeinek, így a hozzájuk tartozó magánkulcsok a közigazgatási hatósági eljárás során felhasználhatók az ügyfelek, valamint az ügyintézésben közreműködő, kiadmányozásra nem jogosult személy (ügyintéző) által létrehozott elektronikus aláírások előállítására.

A *Hitelesítés-szolgáltató* működése a webszerver tanúsítványok kibocsátásával kapcsolatban megfelel a CA/Browser Forum által kibocsátott Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates [18] követelményrendszer aktuális verziójának, amely a https://cabforum.org/baseline-requirements-documents/ címen érhető el, az abban megfogalmazott követeményeket a *Hitelesítés-szolgáltató* magára kötelező érvényűnek tekinti. A jelen *Hitelesítési rend*ek és a Baseline Requirements ellentmondása esetén a Baseline Requirements követelményei az irányadók.

A *Hitelesítés-szolgáltató* működése megfelel az ETSI TS 102 042 [20] (Nyilvános kulcsú tanúsítványokat kibocsátó hitelesítés szolgáltatókra vonatkozó policy követelmények) specifikációban foglaltaknak. Jelen *Hitelesítési rend*ek közül az [NSzTH], az [NSzNH], az [NSzTSz] és az [NSzNSz] megfelel az [NCP] hitelesítési rendnek. Az [NN] és az [NÁ] hitelesítési rendek megfelelnek az [LCP] hitelesítési rendnek, az [NSZW], az [NNW] illetve [NAW] hitelesítési rendek megfelelnek az [OVCP] hitelesítési rendnek.

1.2.2. Hatály

Jelen *Hitelesítési rend* gyűjtemény 2015-08-01-i hatálybalépési dátumtól visszavonásáig hatályos. A *Hitelesítési rend* gyűjtemény előző (3.1) verziója továbbra is hatályos marad annak visszavonásáig.

Jelen *Hitelesítési rend* gyűjteményt és az ezen alapuló *Szolgáltatási szabályzat*okat legalább évente felül kell vizsgálni, és gondoskodni kell az esetlegesen megváltozott követelményekhez, illetve igényekhez igazodó módosításukról.

A *Hitelesítési rend* hatálya kiterjed az 1.3 alfejezetben azonosított közösség minden egyes tagjára.

A jelen *Hitelesítési rend*ek a magyar jog alapján Magyarországon tevékenykedő, elsősorban magyar *Ügyfel*ek részére, magyar nyelven nyújtott szolgáltatásokra vonatkozó konkrét követelményeket tartalmaznak. A *Hitelesítés-szolgáltató* kiterjesztheti a szolgáltatás területi hatályát, ez esetben a magyar viszonyokra alkalmazható előírásoknak megfelelő, azoknál nem enyhébb követelményeket kell alkalmaznia.

1.2.3. A *Hitelesítés-szolgáltató*

A jelen *Hitelesítési rend*nek megfelelő *Tanúsítvány*okat kibocsátó szolgáltató (a továbbiakban: *Hitelesítés-szolgáltató*) adatait, ügyfélszolgálati irodájának elérhetőségét, a *Hitelesítés-szolgáltató*val való kapcsolattartás módját és az illetékes fogyasztóvédelmi szerv elérhetőségét a *Szolgáltatási szabályzat*nak tartalmaznia kell.

1.3. PKI szereplők

1.3.1. *Hitelesítés-szolgáltató*k

Meghatározását lásd az 1.6 fejezetben.

Jelen dokumentum előírásai vonatkoznak mindazon *Hitelesítés-szolgáltató*kra, akik a *Szolgáltatási szabályzat*ukban vállalják a jelen dokumentumban szereplő *Hitelesítési rend*ek valamelyikének való megfelelést és ennek megfelelően nyújtják a szolgáltatásaikat.

1.3.2. Regisztráló szervezetek

Meghatározását lásd az 1.6 fejezetben.

A *Regisztráló szervezet* működhet a *Hitelesítés-szolgáltató* részeként de lehet önálló, független szervezet is. A *Regisztráló szervezet*nek minden esetben ki kell elégítenie a vonatkozó *Hitelesítési rend*(ek)ben, *Szolgáltatási szabályzat*(ok)ban és egyéb dokumentumokban megfogalmazott követelményeket. A választott megoldástól függetlenül a *Hitelesítés-szolgáltató* minden esetben teljes felelősséggel tartozik a *Regisztráló szervezet* előírásoknak megfelelő működéséért.

Független *Regisztráló szervezet* esetében a *Hitelesítés-szolgáltató*nak szerződésben köteleznie kell a *Regisztráló szervezet*et a vonatkozó követelmények betartására.

1.3.3. Ügyfelek

Meghatározását lásd az 1.6 fejezetben.

Az *Előfizető* határozza meg a szolgáltatást igénybe vevő *Alanyok* körét és megfizeti az ezen szolgáltatások igénybevételével kapcsolatos szolgáltatási díjakat. Az *Alany* az a természetes személy, szervezet vagy automatizmus, aki vagy amely adatai a *Tanúsítvány*ban szerepelnek.

Elektronikus aláírás célú *Tanúsítvány* esetében az *Alany Aláíró*nak is nevezhető.

1.3.4. Érintett felek

Meghatározását lásd az 1.6 fejezetben.

Az *Érintett fél* nem feltétlenül áll szerződéses viszonyban a *Hitelesítés-szolgáltató*val, tevékenységére vonatkozó ajánlásokat a *Szolgáltatási szabályzat* és az abban megnevezett egyéb szabályzatok tartalmazzák.

Érintettek továbbá azok a szoftvergyártók is, amelyek olyan internet böngészőket vagy alkalmazásokat készítenek, amelyek működésük során *Tanúsítvány*okat használnak.

1.3.5. Egyéb szereplők

Képviselt szervezet: Az a szervezet, amely neve feltüntetésre kerül egy természetes személy számára kibocsátott *Tanúsítvány*ban. A *Hitelesítés-szolgáltató* a *Képviselt szervezet*tel nem feltétlenül áll szerződéses viszonyban, de a *Hitelesítés-szolgáltató* szervezeti tanúsítványt ezen szervezet hozzájárulása nélkül nem bocsáthat ki. A *Hitelesítés-szolgáltató* a *Képviselt szervezet* kérésére felfüggesztheti illetve visszavonhatja a *Tanúsítvány*t.

1.4. A tanúsítvány felhasználhatósága

A *Tanúsítvány* felhasználhatósági területét alapvetően meghatározzák a *Tanúsítvány*ban a *Hitelesítés-szolgáltató* által beállított attribútum értékek, amelyek mellett a *Hitelesítési rend* és a *Szolgáltatási szabályzat* is tartalmazhat további megkötéseket.

1.4.1. Megfelelő tanúsítvány használat

A *Hitelesítés-szolgáltató* által jelen *Hitelesítési rend*ek valamelyike alapján kibocsátott végfelhasználói *Tanúsítvány*okhoz tartozó magánkulcsok kizárólag a *Tanúsítvány*ban a *Hitelesítés-szolgáltató* által beállított attribútum értékek, a *Hitelesítési rend* és a *Szolgáltatási szabályzat* által meghatározott célra használhatóak fel. A felhasználási cél jellemzően lehet aláírás, titkosítás vagy autentikáció, de a konkrét felhasználási céltól függően ezeken belül is lehetnek eltérések a beállított attribútum értékekben (lásd: 6.1.7. fejezet).

A jelen *Hitelesítési rend*ek alapján kiállított aláíró *Tanúsítvány* alkalmas fokozott biztonságú elektronikus aláírások létrehozására. A fokozott biztonságú elektronikus aláírással hitelesített dokumentum a magyar jog szerint megfelel az írásba foglalás követelményeinek.

1.4.2. Tiltott tanúsítvány használat

A *Tanúsítvány* kiállításával a *Hitelesítés-szolgáltató* kizárólag azt garantálja, hogy a *Tanúsítvány* kiadását megelőzően a *Hitelesítés-szolgáltató* a *Tanúsítvány*ban szereplő adatok valódiságát megfelelő biztonsággal ellenőrizte.

A jelen *Hitelesítési rend*ek alapján kibocsátott *Tanúsítvány*okat, illetve a hozzájuk tartozó magánkulcsokat a *Tanúsítvány*ban a *Hitelesítés-szolgáltató* által beállított attribútum értékek, a *Hitelesítési rend* és a *Szolgáltatási szabályzat* által meghatározottól eltérő célra felhasználni tilos.

1.5. A Hitelesítési rend adminisztrálása

1.5.1. A Hitelesítési rend adminisztrációs szervezete

Jelen *Hitelesítési rend*ek adminisztrációját ellátó szervezet adatai az alábbi táblázatban találhatók:

Szervezet neve	Microsec e-Szignó Hitelesítés Szolgáltató
Szervezet címe	Magyarország, H-1037 Budapest, Záhony utca 7. D épület
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
E-mail cím	info@e-szigno.hu

1.5.2. Kapcsolattartó személy

Jelen *Hitelesítési rend*ekkel kapcsolatos kérdésekben közvetlenül az alábbi személyhez lehet fordulni:

Kapcsolattartó	Folyamatszervezés részleg vezetője
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1037 Budapest, Záhony utca 7. D épület
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
E-mail cím	info@e-szigno.hu

1.5.3. A Szolgáltatási szabályzatok jelen Hitelesítési rendnek való megfelelőségéért felelős személy/szervezet

Egy *Szolgáltatási szabályzat*nak a benne meghivatkozott *Hitelesítési rend*(ek)nek való megfelelőségéért és az abban foglaltak szerinti szolgáltatás nyújtásáért az adott *Szolgáltatási szabályzat*ot kibocsátó *Hitelesítés-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 a megfelelőség megállapítása érdekében független auditor megállapításaira támaszkodik.

1.5.4. A Szolgáltatási szabályzat elfogadási eljárása

A jelen *Hitelesítési rend*(ek)nek való megfelelőséget kinyilatkoztató *Szolgáltatási szabályzat* elfogadási eljárását a *Hitelesítés-szolgáltató*nak ismertetnie kell az adott *Szolgáltatási szabályzat*ban.

1.6. Fogalmak és rövidítések

1.6.1. Fogalmak

II. hitelesítési osztály	Olyan *Hitelesítési rend*, amely az *Alany* távoli regisztrációja alapján is lehetővé teszi a *Tanúsítvány* kibocsátását.
III. hitelesítési osztály	Olyan *Hitelesítési rend*, amely a *Tanúsítvány* kibocsátását az *Alany* (vagy képviselője) személyes regisztrációjához köti.
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)	A *Tanúsítvány* által azonosított természetes személy, jogi személy vagy közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet vagy alkalmazás, illetve webszerver tanusítványok esetén domain név vagy IP cím. Elektronikus aláírásra szolgáló *Tanúsítvány* esetén az *Alany* megegyezik az *Aláíró*val.

Aláírás-ellenőrző adat (Signature-Verification Data)	Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), amelyet az elektronikusan aláírt elektronikus dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ. A PKI-ban a nyilvános kulcs tölti be az aláírás-ellenőrző adat szerepét. Segítségével ellenőrizhető, hogy egy adott elektronikus aláírás egy adott aláírás-létrehozó adattal készült-e.
Aláírás-létrehozó adat (Signature-Creation Data)	Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), amelyet az *Aláíró* az elektronikus aláírás létrehozásához használ. A PKI-ban a titkos kulcs (magánkulcs, aláírókulcs) tölti be az aláírás-létrehozó adat szerepét.
Aláírás-létrehozó eszköz (ALE)	Olyan hardver, illetve szoftver eszköz, amelynek segítségével az *Aláíró* az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

Aláíró (Signatory)	• az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja vagy aki a szolgáltató által üzemeltetett aláírás-létrehozó eszközön lévő aláírás-létrehozó adathoz kizárólagosan hozzáfér, és a saját vagy más személy nevében aláírásra jogosult; • az a jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet, amely az aláírás-létrehozó eszközt birtokolja vagy aki a szolgáltató által üzemeltetett aláírás-létrehozó eszközön lévő aláírás-létrehozó adathoz kizárólagosan hozzáfér, és akinek a nevében az őt képviselő természetes személy az elektronikus aláírást az elektronikus dokumentumon elhelyezi, valamint • aki meghatározza, hogy a nevében jogszabályban meghatározott feltételeknek megfelelő informatikai eszköz elektronikus aláírást elektronikusan dokumentumon elhelyezzen.
Autentikáció	Nyilvános kulcsú tanúsítvány alapú autentikáció alatt azt a folyamatot értjük, amikor egy Érintett fél ellenőrzi a Tanúsítvány Alanyának (természetes személy, szervezet vagy alkalmazás, weboldal, szolgáltatás, szerver) azonosságát egy erre szolgáló eljárás segítségével, amelyben az azonosítandó Alanynak a magánkulcsát kell használnia, és azonossága a Tanúsítványa alapján ellenőrizhető.
Automata tanúsítvány	Olyan *Tanúsítvány*, amelyben az *Alany* adatai között feltüntetésre kerül az informatikai eszköz (alkalmazás, rendszer) elnevezése is, amely segítségével az *Alany* a *Tanúsítvány*t használja.

Érintett fél (Relying Party)	Elektronikus aláírás esetében az elektronikus dokumentum fogadója, aki egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el. Titkosítás esetében az a fél, aki a címzett számára az elektronikus dokumentumot titkosítja. Autentikáció esetében az a fél, aki egy erre szolgáló eljárás során ellenőrzi a magát azonosítani kívánó fél azonosságát.
Elektronikus aláírás (Electronic Signature)	Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.
Előfizető (Subscriber)	A *Hitelesítés-szolgáltató*val valamely szolgáltatás igénybevétele érdekében szolgáltatási szerződést kötő személy vagy szervezet.
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.
Fokozott biztonságú elektronikus aláírás (Advanced Electronic Signature)	Elektronikus aláírás, amely • alkalmas az *Aláíró* azonosítására, • egyedülállóan az *Aláíró*hoz köthető, • olyan eszközökkel hozták létre, amelyek kizárólag az *Aláíró* befolyása alatt állnak, • a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően a dokumentumon tett – módosítás érzékelhető.
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 – tanúsítványban szereplő – aláírás-ellenőrző adattal ellenőrizhető.

Hardver kriptográfiai eszköz (HSM: Hardware Security Modul)	Egy olyan hardver alapú biztonságos eszköz, mely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására. Lehetséges példák ilyen eszközre: PC bővítő kártya, intelligens kártya, USB token.
Hatóság	Az elektronikus aláírással kapcsolatos szolgáltatásokat és az azokat nyújtó szolgáltatókat felügyelő hatóság, a Nemzeti Média- és Hírközlési Hatóság.
Hitelesítés-szolgáltató	Olyan természetes személy, jogi személy vagy jogi személyiség nélküli szervezet, aki/amely a hitelesítés-szolgáltatás keretében azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat nyilvános kulcsokat és a tanúsítvány aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.
Hitelesítési rend	Olyan szabálygyűjtemény, amelyben a *Hitelesítés-szolgáltató*, igénybe vevő vagy más személy (szervezet) valamely tanúsítvány felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.
Hitelesítő egység	A *Hitelesítés-szolgáltató* rendszerének egy egysége, amely *Tanúsítvány*ok aláírását végzi. Egy hitelesítő egységhez mindig egy aláírás-létrehozó adat (aláírókulcs) tartozik. Előfordulhat, hogy egy *Hitelesítés-szolgáltató* egyszerre több hitelesítő egységet is működtet.
Kódaláíró tanúsítvány (CodeSigning certificate)	Olyan tanúsítvány, amely alkalmazások eredetének és sértetlenségének igazolására használható.

Időbélyegző (Time Stamp)	Egy elektronikus dokumentumhoz végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegző elhelyezésének időpontjában változatlan formában létezett.
Képviselt szervezet	Amennyiben a *Tanúsítvány* egy *Szervezet* képviseletében történő aláírásra vagy tevékenységének érdekében történő felhasználás céljából kerül kibocsátásra az *Alany* részére, akkor a *Képviselt szervezet* a szóban forgó *Szervezet*, amely szintén megjelölésre kerül a *Tanúsítvány*ban.
Kompromittálódás	Egy kriptográfiai kulcs akkor kompromittálódott, ha illetéktelen személyek is hozzáférhettek.
Köztes hitelesítő egység	Olyan hitelesítő egység, amely *Tanúsítvány*át a *Hitelesítés-szolgáltató* által üzemeltetett hitelesítő egység bocsátotta ki.
Kriptográfiai kulcs (Key)	Olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete titkosításhoz és dekódoláshoz, illetve elektronikus aláírás előállításához, és ellenőrzéséhez szükséges.
Kulcsgondozás (Key Management)	A kriptográfiai kulcsok előállítása, a felhasználókhoz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, szoros kapcsolatban az alkalmazott biztonsági eljárásmóddal.
Magánkulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az Alanynak szigorúan titokban kell tartania. Elektronikus aláírás esetében az Aláíró a magánkulcsa segítségével hozza létre az aláírást. Titkosítás esetében a címzettnek a magánkulcsára van szüksége ahhoz, hogy a számára titkosított dokumentumot vissza tudja fejteni. Autentikáció esetében az azonosítandó félnek a magánkulcsát kell használnia az azonosságát ellenőrző eljárás során.

Nyilvános kulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. Elektronikus aláírás esetében az aláírást létrehozó fél nyilvános kulcsa szükséges ahhoz, hogy az aláírás hitelességét ellenőrizzük (ez az Aláírás-ellenőrző adat). Titkosítás esetében a címzett fél nyilvános kulcsa szükséges ahhoz, hogy számára titkosított dokumentumot készítsünk. Autentikáció esetében az azonosítandó fél nyilvános kulcsa szükséges ahhoz, hogy az azonosságát ellenőrizni lehessen.
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	Az elektronikus aláírás létrehozására és ellenőrzésére valamint titkosításra és dekódolásra szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.
Regisztrációs igény	A *Tanúsítvány kérelem* és a szolgáltatói szerződés előkészítése céljából az *Ügyfél* által a *Hitelesítés-szolgáltató*nak előzetesen megadott adatok és nyilatkozatok, amelyben többek között felhatalmazza a *Hitelesítés-szolgáltató*t az adatok kezelésére.
Regisztráló szervezet (Registration Authority)	*Szervezet*, amely ellenőrzi a *Tanúsítvány Alany*a adatainak valódiságát, illetve ellenőrzi, hogy a *Tanúsítvány kérelem* hiteles-e, és azt egy arra jogosult személy nyújtotta-e be. A *Regisztráló szervezet* működhet a *Hitelesítés-szolgáltató* részeként, de lehet önálló, független szervezet is. Egy *Hitelesítés-szolgáltató* több ilyen szervezettel is együttműködhet.
Rendkívüli üzemeltetési helyzet	Olyan, a *Hitelesítés-szolgáltató* üzemmenetében zavart okozó rendkívüli helyzet, amikor a *Hitelesítés-szolgáltató* rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
Személyes tanúsítvány	Olyan *Tanúsítvány*, amely természetes személy számára lett kibocsátva, és az *Alany* azonosító adatai között nem kerül feltüntetésre *Szervezet* neve (azaz nem Szervezeti Tanúsítvány).

Szervezet	Jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet.
Szervezeti tanúsítvány	Olyan *Tanúsítvány*, amelyben felüntetésre kerül a *Szervezet* neve (azaz nem Személyes tanúsítvány). Szervezeti tanúsítvány kibocsátható természetes személynek a szóban forgó *Szervezet* kérésére, illetve Szervezeti tanúsítványnak nevezzük azt a *Tanúsítvány*t is, amikor az *Alany* maga a *Szervezet*.
Szervezeti ügyintéző	Olyan természetes személy, aki jogosult az általa képviselt *Szervezet*hez kapcsolódó *Tanúsítvány*ok igénylése esetén a kibocsáthatóságot a *Szervezet* részéről engedélyezni, illetve a kibocsátott *Tanúsítvány*okat felfüggesztetni, visszaállíttatni és visszavonatni. Szervezeti ügyintéző kijelölése nem kötelező minden *Szervezet*nek, ha nincs kijelölve, akkor a *Szervezet* törvényes képviselője látja el a fenti feladatokat.
Szolgáltatási szabályzat (Certificate Practice Statement)	A *Hitelesítés-szolgáltató* tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.
Tanúsítvány (Certificate)	A *Hitelesítés-szolgáltató* által kibocsátott igazolás, amely egy Nyilvános kulcsot egy *Alany*hoz kapcsol, és igazolja e *Tanúsítvány*ban közzétett adatok valódiságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget.
Tanúsítvány kérelem	Az *Alany* (*Szervezet Alany* esetében annak képviselője) által, a *Hitelesítés-szolgáltató* számára a *Tanúsítvány* kibocsátás érdekében benyújtott adatok és nyilatkozatok, amelyekben többek között az *Alany* (vagy képviselője) megerősíti a *Tanúsítvány*ba kerülő adatok valódiságát.

Tanúsítványtár	Különböző *Tanúsítvány*okat tartalmazó adattár. Tanúsítványtára van egy *Hitelesítés-szolgáltató*nak is, amelyben az általa kibocsátott *Tanúsítvány*okat publikálja, de Tanúsítványtárnak nevezzük az *Alany* számítógépén a használt alkalmazás számára elérhető *Tanúsítvány*okat tartalmazó rendszert is.
Titkosítás	Nyilvános kulcsú titkosítás alatt azt a folyamatot értjük, amikor a feladó a címzett nyilvános kulcsának segítségével kódolja a dokumentumot, amely ekkor csak a címzett fél magánkulcsával fejthető vissza.
Tranzakciós korlát, pénzügyi tranzakciós korlát, tranzakciós limit	Az a *Tanúsítvány*ban feltüntetett értékhatár, amely korlátozza a Tanúsítvánnyal hitelesített tranzakcióban a vállalható kötelezettség mértékét.
Ügyfél	Az *Előfizető* és a hozzá tartozó összes *Alany* 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 nyilvántartás a felfüggesztett, illetőleg a visszavont *Tanúsítvány*okról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját.
Webszerver tanúsítvány	Olyan *Tanúsítvány*, amelyben szereplő *Alany* IP cím vagy domain név.

1.6.2. Rövidítések

CA	(Certification Authority)	Hitelesítés-szolgáltató
CP	(Certificate Policy)	Hitelesítési rend

CPS	(Certification Practice Statement)	Hitelesítés-szolgáltatási szabályzat
CRL	(Certificate Revocation List)	Tanúsítvány visszavonási lista
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	(Obejct Identifier)	Objektum azonosító
PKI	(Public Key Infrastructure)	Nyilvános kulcsú infrastruktúra
QCP	(Qualified Certificate Policy)	Minősített hitelesítési rend
RA	(Registration Authority)	Regisztráló szervezet
TSA	(Time Stamping Authority)	Időbélyegzés szolgáltató

2. Közzétételre és tanúsítványtárra vonatkozó felelősségek

2.1. Adatbázisok - tanúsítványtárak

A *Hitelesítés-szolgáltató* a honlapján és LDAP protokollon keresztül is tegye közzé azon *Tanúsítvány*okat, amelyek közzétételéhez az *Alany* 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* biztosítsa, hogy szolgáltatói tanúsítványait, 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.

2.2. A tanúsítványokra vonatkozó információk közzététele

A *Hitelesítés-szolgáltató* tegye közzé a honlapján a szolgáltatói tanúsítványait, valamint tegye közzé a végfelhasználói *Tanúsítvány*okat az *Érintett felek* részére, amennyiben a tanúsítványhoz tartozó *Alany* ehhez hozzájárul.

A *Hitelesítés-szolgáltató* tegye közzé az általa működtetett hitelesítő egységek, valamint az online tanúsítvány-állapot szolgáltatásban részt vevő egységek tanúsítványával kapcsolatos állapot-információkat a következő módszerekkel:

- A gyökér hitelesítő egységek megnevezését, illetve gyökértanúsítványaik lenyomatát a *Szolgáltatási szabályzat*ban . Az állapotváltozásukkal kapcsolatos információk legyenek elérhetőek a szolgáltató honlapján.

- A köztes (nem gyökér) hitelesítő egységek tanúsítványainak állapotváltozását hozza nyilvánosságra a visszavonási listákon, 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 *Tanúsítvány*t bocsásson ki, ezzel kiküszöbölve a tanúsítvány visszavonási állapot ellenőrzésének szükségességét. E *Tanúsítvány* visszavonási állapotát a *Hitelesítés-szolgáltató* kizárólag olyan módon tegye közzé, hogy kulcs kompromittálódás vagy bármilyen egyéb probléma esetén az OCSP válaszokat aláíró régi magánkulcshoz ne kerüljön kibocsátásra újabb *Tanúsítvány*. A *Hitelesítés-szolgáltató* az OCSP válaszadói tanúsítványokat ezt követően új, biztonságos magánkulcshoz bocsássa ki.

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

- a visszavonási listákon,
- az online tanúsítvány-állapot válasz szolgáltatás keretében.

A végfelhasználói *Tanúsítvány* visszavonását és felfüggesztését a *Hitelesítés-szolgáltató* hozza nyilvánosságra, ehhez nem szükséges az *Alany* hozzájárulása. Az állapot-információk közlésének módszereit illetően lásd még a 4.10. fejezetet.

2.2.1. Szolgáltatói információ közzététele

A *Hitelesítés-szolgáltató* hozza nyilvánosságra szerződéses feltételeit és szabályzatait a honlapján elektronikus formában. A honlapon legalább 30 nappal a hatálybalépés előtt kerüljenek publikálásra a bevezetésre váró új dokumentumok. A honlapon az érvényben levő dokumentumokon kívül legyen elérhető valamennyi dokumentum összes korábbi verziója is.

A *Hitelesítés-szolgáltató* értesítse *Ügyfel*eit a regisztrációkor megadott elérhetőségek valamelyikén az Általános szerződési feltételek tervezett változásáról a hatálybalépést megelőzően 30 nappal.

2.3. A közzététel időpontja vagy gyakorisága

2.3.1. Kikötések és feltételek közzétételi gyakorisága

A *Hitelesítési rend*del kapcsolatos új verziók közzététele a 2.2.1. 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 késlekedés nélkül tegye közzé a jogszabályi előírásoknak megfelelően, illetve ennek hiányában amikor szükséges.

2.3.2. Tanúsítványok nyilvánosságra hozatalának gyakorisága

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

- Az általa működtetett gyökér hitelesítő egységek *Tanúsítvány*ait a szolgáltatás megkezdését, vagy az új *Tanúsítvány* kibocsátását követő 10 munkanapon belül tegye közzé.
- Az általa működtetett köztes hitelesítő egységek *Tanúsítvány*ait a kibocsátást követően 5 munkanapon belül hozza nyilvánosságra.
- A *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítvány*okat a kibocsátást követően haladéktalanul jelenítse meg a *Tanúsítványtár*ban az *Alany* hozzájárulása esetén.

2.3.3. A megváltozott visszavonási állapot közzétételének gyakorisága

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

A *Tanúsítvány*ok állapotára vonatkozó információk a *Tanúsítványtár*ban a tanúsítvány-visszavonási listákon is jelenjenek meg. A tanúsítvány visszavonási listák kibocsátási gyakoriságával kapcsolatos előírásokat a 4.10. fejezet tárgyalja.

2.4. A tanúsítványtár elérésének szabályai

A *Hitelesítés-szolgáltató* által közzétett *Tanúsítvány*ok és állapot információk nyilvános információk, olvasás céljából bárki számára biztosítani kell a hozzáférési lehetőséget a közzététel sajátosságainak megfelelően.

A *Hitelesítés-szolgáltató* által közölt információkat kizárólag csak 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 a jelen *Hitelesítési rend*eknek megfelelően, a végfelhasználók számára kibocsátott *Tanúsítvány*okba kerülő adatokkal kapcsolatban tartalmaz követelményeket.

A *Tanúsítvány* alapmezői között található Kibocsátó azonosító (Issuer), illetve *Alany* azonosító (Subject) mezők feleljenek meg az RFC 5280 [5] illetve RFC 6818 [6] ajánlások szerinti egyedi név formátum előírásainak, ezen kívül a *Hitelesítés-szolgáltató* támogassa a kiterjesztések között található Alternatív név mezők (Subject Alternative Names), (Issuer Alternative Names) kitöltését is.

3.1.1. Név típusok

Az *Alany* megnevezése

Jelen hitelesítési rend a következőket írja elő a *Tanúsítvány* alanyának azonosítójával (Subject mező) kapcsolatban:

- Common Name (CN) – OID: 2.5.4.3

  Az *Alany* neve. Kitöltése kötelező.

  Természetes személy esetén a természetes személy neve kerüljön ebbe a mezőbe valamely közhiteles nyilvántartásban szereplő alakkal megegyező formában.

  Szervezet esetében a szervezet teljes vagy rövid elnevezése kerüljön ebbe a mezőbe, a megfelelő közhiteles nyilvántartásban (vagy ennek híján az alapító okiratban) szereplő alakkal megegyező formában.

  Webszerver tanúsítványok esetében a kért domain név vagy IP cím kerül ide. Webszerver tanúsítványok esetében csak ebben a mezőben, illetve a Subject Alternative Names mezőben szerepelhet domain név vagy IP cím.

  Az *Alany* kérésére ebben a mezőben feltüntethető az automatizmus neve is, amely segítségével a *Tanúsítvány*t használni kívánja (*Automata tanúsítvány*).

  Ha a *Tanúsítvány*ban álnév szerepel, akkor az "álneves tanúsítvány" szöveg (vagy ennek idegen nyelvű megfelelője) szerepeljen e mezőben, magát az álnevet pedig a pseudonym (PSEUDO) mező tartalmazza.

  Webszerver tanúsítvány nem lehet álneves.

- Pseudonym (PSEUDO) – OID: 2.5.4.65

Kizárólag álneves tanúsítvány esetén kerülhet kitöltésre, ebben a mezőben kell szerepeltetni az *Alany* által szabadon választott álnevet. Az álnevet a *Hitelesítés-szolgáltató*nak semmilyen szempontból sem kell ellenőriznie vagy jóváhagynia.

Ha a Pseudonym mező kitöltésre kerül, akkor a "CN" mezőben jelölni kell, hogy a *Tanúsítvány* álnevet tartalmaz.

Webszerver tanúsítvány nem lehet álneves.

- Serial Number – OID: 2.5.4.5

  Az *Alany* egyedi azonosítója az RFC 4043 [7] ajánlás szerint. A *Tanúsítvány*ban legalább egy "Serial Number" kötelezően szerepel.

- Organization (O) – OID: 2.5.4.10

  *Szervezet*i *Tanúsítvány* esetében az "O" mezőben kell, hogy szerepeljen a szervezet teljes vagy rövid neve, az alapító okirat vagy valamely közhiteles nyilvántartás szerint.

  Webszerver tanúsítványok számára kibocsátott *Tanúsítvány* esetében is csak akkor kerül kitöltésre, ha a *Tanúsítvány* szervezethez kapcsolódik.

  Hitelesítés-szolgáltató számára kibocsátott *Tanúsítvány* esetében az "O" mező kitöltése kötelező, és a hitelesítés szolgáltatást nyújtó szervezet valódi nevének kell szerepelnie benne.

- Organizational unit (OU) – OID:

  *Szervezet*i egység elnevezése, védjegy, vagy egyéb információ kerülhet ebbe a mezőbe. Csak olyan adat kerülhet bele, amelyet a *Hitelesítés-szolgáltató* ellenőrzött, és amire az adott cégnek használati joga van.

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

- Country (C) – OID: 2.5.4.6

  *Szervezet*i tanúsítvány esetén az "O" mezőben szereplő *Szervezet* székhelye szerinti ország kétbetűs kódja, *Szervezet*hez nem kapcsolódó természetes személy *Alany* esetében az *Alany* állandó lakcíme szerinti ország kétbetűs kódja.

  Webszerver tanúsítvány esetén a domainhez vagy IP címhez kapcsolódó ország, ha ez nem egyértelműen eldönthető, akkor az igénylő országa kerüljön ide. Kitöltése kötelező. Magyarország esetében a "C" mező értéke: "HU".

- Subject Street Address (SA) – OID: 2.5.4.9

  Szervezeti tanúsítvány esetében a szervezet székhelye szerinti cím. Kitöltése opcionális, amennyiben kitöltésre kerül, akkor csak ellenőrzött információ tüntethető fel.

  Szervezethez nem kapcsolódó *Tanúsítvány*ok esetében a használata tilos.

- Subject Locality Name(L) – OID: 2.5.4.7

  Szervezetei tanúsítvány esetében a szervezet székhelye szerinti helység neve, szervezethez nem kapcsolódó természetes személy *Alany* esetében az *Alany* állandó lakcíme szerinti helység neve kerüljön ebbe a mezőbe.

  Kitöltése kötelező.

  Webszerver tanúsítványok esetében a "Subject Locality Name":

  – nem lehet kitöltve, ha az "O" mező nincs kitöltve;
  – kötelező kitölteni, ha az "O" mező ki van töltve és a "Subject State or Province Name" nincs kitöltve;
  – opcionális, ha az "O" mező és a "Subject State or Province Name" is ki van töltve.

- State or Province Name – OID: 2.5.4.8

  Szervezeti tanúsítvány esetében a *Szervezet* székhelye szerinti tagállam, megye vagy tartomány neve, szervezethez nem kapcsolódó természetes személy *Alany* esetében az *Alany* állandó lakcíme szerinti tagállam, megye vagy tartomány neve kerüljön ebbe a mezőbe. Kitöltése opcionális.

  Webszerver tanúsítványok esetében a "Subject State or Province Name":

  – nem lehet kitöltve, ha az "O" mező nincs kitöltve;
  – kötelező kitölteni, ha az "O" mező ki van töltve és a "Subject Locality Name" nincs kitöltve;
  – opcionális, ha az "O" mező és a "Subject Locality Name" is ki van töltve.

- Postal Code – OID: 2.5.4.17

  Szervezeti tanúsítvány esetében a *Szervezet* székhelye szerinti postai irányítószám, szervezethez nem kapcsolódó természetes személy *Alany* esetében az *Alany* állandó lakcíme szerinti postai irányítószám kerüljön ebbe a mezőbe.

  Kitöltése opcionális, amennyiben kitöltésre kerül, akkor csak ellenőrzött információ tüntethető fel.

  Webszerver tanúsítványok esetében a "Subject Postal Code":

  – nem lehet kitöltve, ha az "O" mező nincs kitöltve;
  – opcionális kitölteni, ha az "O" mező ki van töltve.

- Title (T) – OID: 2.5.4.12

  Az *Alany* szerepe, beosztása vagy hivatása.

Meghatározza, hogy az *Alany* az adott szervezethez kapcsolódó milyen szerepkörben használja a *Tanúsítvány*át. A mező csak szervezeti tanúsítvány esetén tartalmazhat értéket, azaz csak akkor, ha az "O" mező is kitöltésre kerül.

A *Hitelesítés-szolgáltató*nak – a képviselt szervezet által kiállított hivatalos dokumentum alapján – ellenőriznie kell a mezőbe írandó érték valódiságát és hitelességét.

Webszerver tanúsítvány esetében nem lehet kitöltve.

- E-mail address (EMAIL) – OID: 1.2.840.113549.1.9.1

  Az *Alany* e-mail címe.

  Ha kitöltésre kerül, akkor meg kell egyeznie az *Alany* alternatív neve mezőben szereplő "RFC822name" mezőben szereplő e-mail címmel.

  Webszerver tanúsítvány esetében nem lehet kitöltve.

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

Az Alany alternatív nevei

Az Alany alternatív nevei nem kritikus mező.

A kitöltésére a következő szabályok vonatkoznak:

Nem webszerver *Tanúsítvány*ok esetében:

Az *Alany* kérésére ide (jellemzően a "Subject Alternative Names" "CN" mezejébe) kerülhet a "Subject DN / Common Name" mezőben szereplőtől eltérő írásmóddal írott neve. E név egyaránt szerepelhet ékezetes vagy ékezet nélküli írásmóddal. A *Hitelesítés-szolgáltató* jogosult jelölni a feltüntetett név jellegét is.

A *Hitelesítés-szolgáltató*nak ellenőriznie kell a "Subject Alternative Names" mezőbe kerülő neveket is.

Az *Alany* alternatív nevei mező "rfc822Name" mezőjében kerülhet megadásra az *Alany* e-mail címe. Amennyiben a *Tanúsítvány*ban szerepel e-mail cím, akkor e mező mindenképpen kerüljön kitöltésre. Ugyanez az e-mail cím opcionálisan megjelenhet a *Tanúsítvány* "EMAIL" mezejében is.

Webszerver tanúsítványok esetében:

Az *Alany* alternatív nevei mezőben legalább egy domain névnek vagy IP címnek kell benne szerepelnie és kitöltése kötelező. Ebben a mezőben minden domaint / IP címet fel kell sorolni (azt is, ami a CN-ben benne volt), a "domain" mezőben. Csak teljesen minősített domain név (FQDN:

Fully Qualified Domain Name) szerepelhet itt, illetve nem szerepelhet lefoglalt tartománybeli IP cím.

A *Tanúsítvány*ban csak itt, illetve a "Subject" mező "CN"-jében szerepelhet domain név.

3.1.2. A nevek értelmezhetősége

A "SubjectDN" mezőre a következő szabályokat kell alkalmazni:

- az azonosítónak értelmezhetőnek kell lennie;
- a *Tanúsítvány*ban szereplő személynevet a közhiteles nyilvántartásban szereplő írásmóddal kell feltüntetni;
- a *Tanúsítvány*ban szereplő *Szervezet* nevét a közhiteles nyilvántartásban – annak hiányában az alapító okiratban – szereplő írásmóddal kell feltüntetni.

Álneves *Tanúsítvány* esetén egyedül a "Pseudonym" mező tartalmazhat álnevet, a többi mezőt a *Hitelesítés-szolgáltató*nak a nem álneves *Tanúsítvány*oknál alkalmazottal megegyező módon kell ellenőriznie.

3.1.3. Álnevek használata

Lásd 3.1.1 . fejezetet.

3.1.4. A különböző elnevezési formák értelmezési szabályai

Az azonosítók értelmezése érdekében az *Érintett felek*nek a jelen dokumentumban leírtak alapján kell 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, hogy jogszabály ezt nem írja elő – nem adhat, csak a *Tanúsítvány*ban feltüntetett adatok értelmezését segítő információt szolgáltathatja.

3.1.5. A nevek egyedisége

Az *Alany*nak a *Hitelesítés-szolgáltató Tanúsítványtár*ában egyedi névvel kell rendelkeznie. Az egyediség biztosítása érdekében a *Hitelesítés-szolgáltató* adjon minden *Alany*nak egy – a *Hitelesítés-szolgáltató* nyilvántartásában egyedi – azonosítót (OID), amelyet szerepeltessen az *Alany* egyedi azonosítója "Subject DN Serial Number" mezőben.

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

Kérésre a *Tanúsítvány*ban a *Hitelesítés-szolgáltató* más egyedi azonosítót (pl. személyi igazolvány szám, adószám, szervezeten belüli azonosító) is feltüntethet.

Eljárások a nevekre vonatkozó vitás kérdések megoldására

A *Hitelesítés-szolgáltató* győződjön meg 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 *Előfizető* által igényelt végfelhasználói *Tanúsítvány* mezőiben előfordulhatnak védjegyek, ezek jogos használatáról a *Hitelesítés-szolgáltató*nak meg kell győződnie, illetve reklamáció esetén jogosult a *Tanúsítvány* visszavonására.

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 dönthet az igényelt *Tanúsítvány* kiadásának megtagadásáról.

3.2.1. A magánkulcs birtoklásának igazolása

A *Tanúsítvány* kiállítása előtt a *Hitelesítés-szolgáltató*nak biztosítania kell illetve meg kell győződnie arról, hogy a *Tanúsítvány*t kérelmező valóban birtokolja a *Tanúsítvány*ba kerülő nyilvános kulcshoz tartozó magánkulcsot. A követelmény teljesítésének módját rögzíteni kell a *Szolgáltatási szabályzat*ban.

A III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetében a *Hitelesítés-szolgáltató*nak személyes találkozás során kell meggyőződnie arról, hogy az *Alany* valóban birtokolja a *Tanúsítvány*ba kerülő nyilvános kulcshoz tartozó magánkulcsot.

A II. hitelesítési osztályba tartozó *Tanúsítvány*ok esetében személyes találkozásra nincs szükség. A *Hitelesítés-szolgáltató* távolról is azonosíthatja az *Alany*t és elfogadhatja az *Alany* magánkulcs birtoklására vonatkozó nyilatkozatát.

3.2.2. Szervezet és domain azonosságának hitelesítése

Szervezet azonosságának hitelesítése

Szervezeti tanúsítványok kibocsátása előtt a *Hitelesítés-szolgáltató*nak megbízható harmadik fél vagy közhiteles nyilvántartás alapján meg kell győződnie a *Tanúsítvány*ba kerülő szervezeti adatok valódiságáról.

A Szervezeti tanúsítványokban szerepelnie kell legalább a *Szervezet* nevének a 3.1.1 fejezetben meghatározottak szerint.

A szervezeti tanúsítványt a *Hitelesítés-szolgáltató* kizárólag a *Szervezet* hozzájárulásával bocsáthatja ki. A *Szervezet* nevében eljáró természetes személynek megfelelő meghatalmazással kell rendelkeznie, a meghatalmazott természetes személy azonosságát a 3.2.3 fejezetben meghatározott követelmények szerint kell ellenőrizni.

A *Szolgáltatási szabályzat*nak meg kell határoznia a részletes eljárásrendet.

Domain azonosságának hitelesítése

Webszerver tanúsítványok kibocsátása előtt a *Hitelesítés-szolgáltató*nak megbízható harmadik fél vagy közhiteles nyilvántartás alapján meg kell győződnie a *Tanúsítvány*ba kerülő domain név vagy IP cím valódiságáról.

A Webszerver tanúsítványokban szerepelnie kell legalább egy domain névnek vagy IP címnek. A domain név és IP cím használati jogosultságát ellenőrizni kell.

A *Szolgáltatási szabályzat*nak meg kell határoznia a domain nevek és IP címek ellenőrzésének részletes eljárásrendjét.

3.2.3. Természetes személy azonosságának hitelesítése

A természetes személy azonosságát igazolni kell az alábbi esetekben:

- amennyiben a kibocsátandó *Tanúsítvány* alanya a természetes személy;
- amennyiben a természetes személy egy jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet nevében jár el szervezeti tanúsítvány kérelmezése céljából.

A III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetében a természetes személy azonosításának követelményei:

- a/ a természetes személynek a regisztráció elvégzéséhez személyesen meg kell jelennie a regisztrációt végző szervezet előtt;
- b/ a regisztráció során a természetes személy azonosságát ellenőrizni kell egy személyazonosító igazolvány alapján;

- c/ Webszerver tanúsítvány igénylése esetén a regisztráció során a természetes személy lakcímét is ellenőrizni kell a lakcím azonosítására szolgáló igazolvány alapján;
- d/ a regisztráció és a személyazonosság ellenőrzésére szolgáló adatok helyességét a természetes személynek nyilatkozatban, saját kezű aláírással ellátva igazolnia kell;
- e/ elektronikus aláírás létrehozására szolgáló *Tanúsítvány* igénylése esetén a b/ pont szerinti igazolvány adatainak helyességét és az igazolvány érvényességét a regisztrációs szervezetnek megbízható harmadik fél vagy közhiteles nyilvántartás segítségével ellenőriznie kell.

Az utolsó személyes azonosítást követően legfeljebb 39 hónapig, kizárólag a szolgáltatás nyújtása időtartama alatt a *Hitelesítés-szolgáltató* lehetőséget biztosíthat az *Alany* számára újabb *Tanúsítvány kérelem* esetén a személyes azonosításkor egyeztetett adatok alapján az új *Tanúsítvány* kibocsátására. A kérelem hitelességét, a *Tanúsítvány*ba kerülő adatok pontosságát és a kérelmet benyújtó személy azonosságát ebben az esetben is ellenőrizni kell. A *Szolgáltatási szabályzat*ban pontosan meg kell határozni az ellenőrzés folyamatát.

A személyes azonosítás helyett a *Hitelesítés-szolgáltató* elfogadhat más, azzal azonos biztonságot nyújtó azonosító módszert is. Ilyen például, ha az *Alany* már rendelkezik egy európai szabályozás szerinti minősített *Hitelesítés-szolgáltató*tól származó *Biztonságos aláírás-létrehozó eszköz*re kiadott, érvényes, személyes azonosítást megkövetelő minősített hitelesítési rend alapján kibocsátott, nem álneves aláíró tanúsítvánnyal, és azzal aláírva nyújtja be a *Tanúsítvány* kérelmét.

A II. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a természetes személy azonosításához személyes találkozásra nincs szükség, ilyen esetben a *Hitelesítés-szolgáltató* távolról is azonosíthatja az *Alany*t. Ennek egyik lehetséges módja, hogy az *Alany* eljuttatja a *Hitelesítés-szolgáltató*nak valamely személyazonosság igazolására alkalmas hatósági igazolványának fénymásolatát. Elektronikus aláírás létrehozására szolgáló *Tanúsítvány* igénylése esetén az *Alany* adatainak helyességét a regisztrációs szervezetnek megbízható harmadik fél vagy közhiteles nyilvántartás segítségével ekkor is ellenőriznie kell.

A *Szolgáltatási szabályzat*ban pontosan meg kell határozni az azonosítás folyamatát.

3.2.4. Nem ellenőrzött *Alany* információk

A *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány*ba csak olyan adatok kerülhetnek, amelyeket a *Hitelesítés-szolgáltató* ellenőrzött, vagy amelyek valódiságáról az *Alany* írásban, büntetőjogi felelősségének tudatában nyilatkozott.

3.2.5. Jogok, felhatalmazások ellenőrzése

Szervezeti tanúsítvány kiállítása előtt a jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet nevében eljáró természetes személy azonosságát igazolni kell a 3.2.3

fejezet előírásai szerint.

Ellenőrizni kell a természetes személy képviseleti jogosultságát.

A *Szolgáltatási szabályzat*ban pontosan meg kell határozni az ellenőrzés folyamatát.

A *Szervezet* kijelölhet egy szervezeti ügyintézőt, aki jogosult az általa képviselt *Szervezet*hez kapcsolódó Szervezeti tanúsítványok igénylése esetén a kibocsáthatóságot a szervezet részéről engedélyezni, illetve a kibocsátott *Tanúsítvány*okat felfüggesztetni, visszaállíttatni és visszavonatni.

Szervezeti ügyintéző kijelölése nem kötelező, amennyiben nincs kijelölve, a *Szervezet* törvényes képviselője látja el a fenti feladatokat.

3.2.6. Együttműködési képességre vonatkozó követelmények

A *Hitelesítés-szolgáltató* a szolgáltatás nyújtása során együttműködhet más *Hitelesítés-szolgáltató*kkal, akik magukra kötelező érvényűnek ismerik el jelen *Hitelesítési rend*ek követelményeinek betartását.

Az együttműködő *Hitelesítés-szolgáltató*knak a *Szolgáltatási szabályzat*okban részletesen ismertetniük kell az együttműködés módját.

Az együttműködés eredményeképpen semmilyen módon nem csorbulhatnak az *Ügyfel*ek jogai, nem csökkenhet a szolgáltatás színvonala.

A *Hitelesítés-szolgáltató*nak közzé kell tennie minden általa kért vagy elfogadott kereszthitelesített tanúsítványát.

3.3. Azonosítás és hitelesítés kulcscsere kérelem esetén

3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

Amennyiben az *Alany* rendelkezik egy még érvényes, ugyanezen *Hitelesítés-szolgáltató* által kibocsátott aláíró tanúsítvánnyal, akkor az ehhez tartozó magánkulccsal aláírt kulcscsere kérelmet minden további vizsgálat nélkül automatikusan elfogadhatja a *Hitelesítés-szolgáltató*. Amennyiben az *Alany* nem rendelkezik ilyen aláíró Tanúsítvánnyal, vagy nem kívánja azt használni, a 3.2.3 fejezetben ismertetett folyamat szerint történik az új *Tanúsítvány* kibocsátásához szükséges azonosítás.

3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

A *Hitelesítés-szolgáltató* kizárólag a szolgáltatás nyújtásának időtartama alatt elfogadhat kulcscsere kérelmeket visszavont vagy felfüggesztett *Tanúsítvány*ok esetén is . A kérelmet benyújtó személy azonosságát a 3.2.3 fejezetben ismertetett folyamat szerint kell ellenőrizni.

3.4. Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási kérelem esetén

A *Hitelesítés-szolgáltató*nak a felfüggesztési és visszavonási kérelmek gyors teljesítése mellett biztosítania kell, hogy a kérelmeket csak az arra jogosult felektől fogadja el. A kérelmeket benyújtó személyek azonosságát, a kérelmek hitelességét ellenőrizni kell.

4. A tanúsítványok életciklusára vonatkozó követelmények

4.1. Tanúsítvány kérelem

Minden új *Tanúsítvány* kiadásához *Tanúsítvány kérelem* benyújtására van szükség. A *Tanúsítvány kérelem* benyújtását megelőzően az *Alany Regisztrációs igény*t kell, hogy benyújtson a *Hitelesítés-szolgáltató*nak, ez történhet a *Hitelesítés-szolgáltató* honlapján keresztül is. A *Regisztrációs igény*ben az *Alany* meg kell adja a *Tanúsítvány*ba kerülő adatait, meg kell nevezze, hogy pontosan milyen *Tanúsítvány*t igényel, és fel kell hatalmazza a *Hitelesítés-szolgáltató*t a személyes adatainak kezelésére.

A *Hitelesítés-szolgáltató* mindaddig nem tekintheti a *Regisztrációs igény*ben szereplő adatokat hitelesnek, amíg az *Alany Tanúsítvány kérelem*ben meg nem erősíti azokat.

Amennyiben új szolgáltatási szerződés megkötésére van szükség, a *Hitelesítés-szolgáltató* a *Regisztrációs igény*ben megadott adatok alapján előkészítheti az *Előfizető*vel kötendő szolgáltatási szerződést.

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

Amennyiben az *Alany* nem azonos az *Előfizető*vel, akkor az *Alany* számára is meg kell adni a fenti tájékoztatást.

A tájékoztatást tartalmazó dokumentumokat közérthető módon megfogalmazva, elektronikusan letölthető formában, kérés esetén nyomtatott formában is elérhetővé kell tenni.

A *Tanúsítvány kérelem*nek tartalmaznia kell legalább a következő adatokat:

- az *Alany – Szervezet* esetében a *Szervezet* képviselőjének – személyes azonosító adatai (teljes név, személyazonosító okmány száma);
- az *Alany – Szervezet* esetében a *Szervezet* képviselőjének – elérhetőségei (telefonszám, e-mail cím);
- szervezeti tanúsítvány igénylése esetében a *Szervezet* adatai (teljes neve);
- az *Előfizető* adatai (számlázási adatok);

- a *Tanúsítvány*ba kerülő adatok (pl. név, cím, *Szervezet* neve, város, ország, e-mail cím, webszerver tanúsítvány esetében domain név vagy IP cím).

A *Tanúsítvány kérelem*mel együtt a *Hitelesítés-szolgáltató*nak be kell kérnie illetve meg kell tekintenie legalább a következő okmányokat, igazolásokat, meghatalmazásokat illetve nyilatkozatokat (távoli azonosítás esetén ezek másolatát, az *Alany* által hitelesítve):

- az *Alany* – *Szervezet* esetében a *Szervezet* képviselőjének – azonosításához szükséges okmányokat a 3.2.3 fejezetnek megfelelően;
- szervezeti tanúsítvány igénylése esetén a *Szervezet* azonosításához szükséges okmányokat a 3.2.2 fejezetnek megfelelően;
- amennyiben az *Alany* szervezet, a *Szervezet* által kiadott igazolást vagy meghatalmazást arról, hogy az igénylő személy jogosult a *Szervezet* képviseletére;
- amennyiben az *Alany* természetes személy, de a *Tanúsítvány*ban kéri egy *Szervezet*hez való tartozás feltüntetését, akkor a *Szervezet* igazolását arról, hogy ehhez hozzájárul;
- amennyiben a kért *Tanúsítvány*ban szerepel márkanév vagy védjegy, akkor annak igazolását, hogy az *Alany* jogosult annak használatára.

4.1.1. Ki nyújthat be tanúsítvány kérelmet

Tanúsítvány kérelmet azok az *Alany*ok nyújthatnak be, akik *Előfizető*ivel előzetesen a *Hitelesítés-szolgáltató* szerződéses kapcsolatot létesített.

A III. tanúsítási osztályba tartozó *Tanúsítvány*ok esetén a *Tanúsítvány kérelmet* az *Alany* – *Szervezet* esetében a *Szervezet* képviselője – a következő módokon nyújthatja be:

- személyesen azonosítását követően kézi aláírásával hitelesítve a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely külső *Regisztráló szervezet* regisztrációs munkatársa előtt;
- amennyiben rendelkezik egy európai szabályozás szerinti minősített *Hitelesítés-szolgáltató*tól származó *Biztonságos aláírás-létrehozó eszköz*re kiadott, érvényes, személyes azonosítást megkövetelő minősített *Hitelesítési rend* alapján kibocsátott, nem álneves aláíró tanúsítvánnyal, akkor azzal aláírva nyújthatja be a *Tanúsítvány kérelmet*;
- amennyiben a *Hitelesítés-szolgáltató*nak korábbi ügyfele és a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában (vagy a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely *Regisztráló szervezet*énél) korábban már megjelent személyes azonosításon, akkor az azonosítása távolról is megtörténhet és a kézi aláírásával hitelesített *Tanúsítvány kérelmet* postai úton is beküldheti.

A II. tanúsítási osztályba tartozó *Tanúsítvány*ok esetén az *Ügyfél* az aláírt *Tanúsítvány kérelmet* és az aláírt szolgáltatási szerződést postai úton juttatja el a *Hitelesítés-szolgáltató*hoz. A kérelemhez mellékelni kell minden szükséges, a *Hitelesítés-szolgáltató* által előírt dokumentumot (lásd: 3.2.3.). Amennyiben az *Előfizető* és az *Alany* (*Szervezet* esetén annak vagy képviselője) rendelkezik legalább fokozott biztonságú, érvényes aláíró tanúsítvánnyal, akkor az ahhoz tartozó magánkulccsal aláírva elektronikusan is eljuttathatja a *Hitelesítés-szolgáltató*hoz ezen dokumentumokat. A *Hitelesítés-szolgáltató* ezek kézhezvétele után, a szükséges ellenőrzések elvégeztét követően kiállítja az igényelt *Tanúsítvány*(oka)t. Webszerver tanúsítvány igénylése esetén ellenőrizni kell egy másik – megbízható – csatornán, hogy a kérelem valóban attól a személytől érkezett-e, akinek az adatai (igazolványai) az igénylésben szerepelnek.

Az *Előfizető*nek és az *Alany*nak – *Szervezet* esetében annak képviselőjének – a *Tanúsítvány* igénylése során meg kell adniuk azon elérhetőségi adataikat, melyek alapján a későbbiekben fel lehet velük venni a kapcsolatot.

4.1.2. A bejegyzés folyamata és a résztvevők felelőssége

A kérelem feldolgozása során a *Hitelesítés-szolgáltató* (vagy a *Regisztráló szervezet*) regisztrációs munkatársának meg kell győződnie a *Tanúsítvány kérelmet* benyújtó személy azonosságáról. Amennyiben az *Alany* szervezet, vagy a *Tanúsítvány*ban feltüntetésre kerül egy *Szervezet* neve is (Szervezeti tanúsítvány), akkor a *Szervezet*et is azonosítani kell, illetve meg kell győződni arról, hogy a megjelent személy jogosult a *Szervezet* képviseletére illetve a *Szervezet*hez kapcsolódó *Tanúsítvány* igénylésére. Az *Előfizető* határozza meg, hogy mely *Alany* mely *Hitelesítési rend* szerinti *Tanúsítvány*t jogosult igényelni.

Az *Alany* – *Szervezet* esetében annak képviselője – meg kell adjon minden szükséges információt az azonosítási eljárások lefolytatásához.

A *Hitelesítés-szolgáltató*nak nyilvántartásba kell vennie az *Alany*, illetve *Szervezet* azonosságára vonatkozó, a szolgáltatás nyújtásához és a kapcsolattartáshoz szükséges minden információt.

A *Hitelesítés-szolgáltató*nak nyilvántartásba kell vennie 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*nak nyilvántartásba kell vennie az *Alany* – *Szervezet* esetén annak képviselője – által aláírt *Tanúsítvány kérelmet*, amelynek tartalmaznia kell a következőket:

- annak megerősítését, hogy a *Tanúsítvány kérelem*ben megadott adatok pontosak;
- Aláírás-létrehozó eszköz átadása esetén az *Alany* nyilatkozatát arra vonatkozóan, hogy a részére átadott eszköz használatával kapcsolatos kötelezettségeit megismerte és azok betartását vállalja;
- azt, hogy hozzájárul-e a *Tanúsítvány* közzétételéhez;

- nyilatkozatot arról, hogy az igényelt *Tanúsítvány*ban nem szerepel márkanév vagy védjegy, vagy hogy szerepel és annak jogos felhasználója.

A fenti nyilvántartásokat meg kell őrizni legalább a hatályos jogszabályokban előírt időtartamig.

4.2. A tanúsítvány kérelem feldolgozása

4.2.1. Az igénylő azonosítása és hitelesítése

A *Hitelesítés-szolgáltató*nak az igénylőt a 3.2 fejezetnek megfelelően kell azonosítania.

4.2.2. A tanúsítvány kérelem elfogadása vagy visszautasítása

A *Hitelesítés-szolgáltató*nak a *Tanúsítvány* kibocsátása előtt ellenőriznie kell a *Tanúsítvány kérelem*ben megadott, a *Tanúsítvány*ba kerülő valamennyi információ hitelességét.

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

A *Tanúsítvány kérelem* elutasítása esetén az elutasítás tényéről tájékoztatni kell az *Alany*t és az *Előfizető*t, de a *Hitelesítés-szolgáltató* nem köteles döntését megindokolni.

A *Hitelesítés-szolgáltató* alakítson ki olyan folyamatokat, amelyek során azonosítja a magas kockázatú webszerver tanúsítvány kérelmeket, amelyeket szigorúbban kell ellenőrizni. A gyanús kérelmek azonosításának folyamatát és a szigorúbb ellenőrzés folyamatát dokumentálni kell a *Szolgáltatási szabályzat*ában.

4.2.3. A tanúsítvány kérelem feldolgozásának időtartama

A *Hitelesítés-szolgáltató*nak a *Szolgáltatási szabályzat*ban meg kell határoznia, hogy milyen határidőn belül vállalja a benyújtott *Tanúsítvány kérelem* elbírálását.

4.3. A tanúsítvány kibocsátása

A *Hitelesítés-szolgáltató* csak a *Tanúsítvány kérelem* elfogadása után állíthatja ki a *Tanúsítvány*t az *Alany* részére. A kiállított *Tanúsítvány* csak az *Alany Tanúsítvány kérelem*ben megadott és az elbírálás során a *Hitelesítés-szolgáltató* által ellenőrzött adatait tartalmazhatja.

4.3.1. A Hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során

A *Tanúsítvány*ok kibocsátásának megfelelően biztonságos módon kell történnie.

4.3.2. Az Ügyfél értesítése a tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* a *Tanúsítvány* kibocsátásáról értesítse az *Alany*t és az *Előfizető*t, valamint tegye lehetővé az *Alany* 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 *Alany*nak – *Szervezet* esetében a *Szervezet* képviselőjének – a *Tanúsítvány* átvétele előtt ellenőriznie kell a *Tanúsítvány*ban szereplő adatainak helyességét és erről írásbeli nyilatkozatot kell tennie. A nyilatkozat aláírásával az *Alany* – *Szervezet* esetében a *Szervezet* képviselője – igazolja a *Tanúsítvány* átvételét.

A II. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén az *Alany*nak (vagy képviselőjének) nem kell külön nyilatkoznia a kiállított *Tanúsítvány* átvételéről. A szolgáltatási szerződés aláírásával az *Előfizető*, a *Tanúsítvány* kérelem aláírásával az *Alany* 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* átadása után a *Hitelesítés-szolgáltató* köteles nyilvánosságra hozni a kiadott *Tanúsítvány*t.

A *Tanúsítvány* nyilvánosságra hozatalának feltétele az érintett *Alany* hozzájárulása.

4.4.3. További szereplők értesítése a tanúsítvány kibocsátásról

Amennyiben a *Tanúsítvány*t olyan céllal bocsátották ki, hogy az *Alany* más személy vagy *Szervezet* nevében hozhasson létre elektronikus aláírást, a *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell a *Képviselt szervezet* vagy személy kapcsolattartóját is.

4.5. A kulcspár és a tanúsítvány használata

4.5.1. A magánkulcs és a tanúsítvány használata

Az *Alany* a *Tanúsítvány*ához tartozó magánkulcsát kizárólag a *Tanúsítvány*ban szereplő kulcshasználatnak megfelelően használhatja, más felhasználás nem engedélyezett.

Az *Alany* köteles gondoskodni magánkulcsának és az aktivizáló adatának (PIN kód vagy jelszó) 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 végrehajtott műveletek (pl. elektronikus aláírás elfogadása, távoli fél azonosítása, címzett számára dokumentum titkosítása) végrehajtása során a *Hitelesítés-szolgáltató* által garantált biztonsági szint megtartásához szükséges, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, és feleljen meg a *Szolgáltatási szabályzat*ban leírt követelményeknek, különös tekintettel az alábbiakra:

- a nyilvános kulcsokat csak olyan alkalmazásokban fogadja el, amelyek összhangban vannak a *Tanúsítvány* "kulcshasználat" és "kiterjesztett kulcshasználat" mezőinek tartalmával;
- ellenőrizze a *Tanúsítvány* érvényességét, visszavonási, felfüggesztési állapotát;
- vegyen figyelembe minden korlátozást, amely a *Tanúsítvány*ban vagy a *Tanúsítvány*ban meghivatkozott szabályzatokban szerepel.

Amennyiben az *Érintett fél* nem az ott leírtaknak megfelelően jár el, az ebből eredő károkért a *Hitelesítés-szolgáltató* nem vállal felelősséget.

A *Hitelesítés-szolgáltató* tegyen elérhetővé 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.

A *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzat*ában korlátozhatja a tanúsítvány megújításba bevont tanúsítvány típusok körét.

4.6.1. A tanúsítvány megújítás körülményei

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

- a megújítandó *Tanúsítvány* még érvényes (nem járt le);
- a megújítandó *Tanúsítvány* nincs felfüggesztve vagy 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 fogadhat el. A *Tanúsítvány* megújítása során tájékoztatni kell az *Alany*t arról, ha a korábbi *Tanúsítvány* kibocsátása óta változtak a *Tanúsítvány* használatával kapcsolatos kikötések illetve feltételek. Amennyiben az *Alany* nem azonos az *Előfizető*vel, akkor az *Előfizető* számára is meg kell adni a fenti tájékoztatást.

4.6.2. Ki kérelmezheti a tanúsítvány megújítást

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

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.

4.6.3. A tanúsítvány megújítási kérelmek feldolgozása

A tanúsítvány megújítási kérelem elbírálása során a *Hitelesítés-szolgáltató*nak ellenőriznie kell, 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 megújítandó *Tanúsítvány* még érvényes (nem járt le);
- a megújítandó *Tanúsítvány* nincs felfüggesztve vagy visszavonva;
- az aktuálisan elérhető információk alapján a kiadandó *Tanúsítvány* tervezett érvényessége alatt a felhasznált kriptográfiai algoritmusok még használhatók lesznek.

4.6.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* értesítse az *Alany*t és az *Előfizető*t az új *Tanúsítvány* kibocsátásáról.

4.6.5. A megújított tanúsítvány elfogadása

Nincs megkötés.

4.6.6. A megújított tanúsítvány közzététele

A *Hitelesítés-szolgáltató*nak az eredeti *Tanúsítvány* kibocsátásával megegyező módon kell publikálnia a megújított *Tanúsítvány*t.

4.6.7. További szereplők értesítése a tanúsítvány kibocsátásáról

Amennyiben a *Tanúsítvány*t olyan céllal bocsátották ki, hogy az *Alany* más személy vagy *Szervezet* nevében hozhasson létre elektronikus aláírást, a *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell a *Képviselt szervezet* vagy személy kapcsolattartóját 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 az *Alany* azonosító adatai nem változnak, viszont 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.

4.7.1. A kulcscsere körülményei

A kulcscsere szükségessé válik az alábbi esetekben:

- az *Alany* magánkulcsa elveszett vagy kompromittálódott;
- a megújítandó *Tanúsítvány* visszavonásra került.

Kulcscsere az *Ügyfél* kérésére is végrehajtható.

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

A kulcscsere során tájékoztatni kell az *Alany*t arról, ha a korábbi *Tanúsítvány* kibocsátása óta változtak a *Tanúsítvány* használatával kapcsolatos kikötések illetve feltételek. Amennyiben az *Alany* nem azonos az *Előfizető*vel, akkor az *Előfizető* számára is meg kell adni a fenti tájékoztatást.

4.7.2. Ki kérelmezheti a kulcscserét

A kulcscserét olyan személy kezdeményezheti, aki a kérelem benyújtásának időpontjában jogosult lenne új *Tanúsítvány kérelem* benyújtására is az *Alany* nevében.

4.7.3. A kulcscsere kérelmek feldolgozása

Az *Alany* által vagy az *Alany* nevében benyújtott kulcscsere kérelem elbírálása során a *Hitelesítés-szolgáltató*nak ellenőriznie kell, hogy

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

4.7.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* értesítse az *Alany*t és az Előfizetőt az új *Tanúsítvány* kibocsátásáról.

4.7.5. A kulcscserével megújított tanúsítvány elfogadása

Nincs megkötés.

4.7.6. A kulcscserével megújított tanúsítvány közzététele

A *Hitelesítés-szolgáltató*nak az eredeti *Tanúsítvány* kibocsátásával megegyező módon kell publikálnia a megújított *Tanúsítvány*t.

4.7.7. További szereplők értesítése a tanúsítvány kibocsátásáról

Amennyiben a *Tanúsítvány*t olyan céllal bocsátották ki, hogy az *Alany* egy *Szervezet* nevében hozhasson létre elektronikus aláírást, a *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell a *Képviselt szervezet* kapcsolattartóját 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.

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

A tanúsítvány módosítás feltételei:

- a megújítandó *Tanúsítvány* még érvényes (nem járt le);
- a megújítandó*Tanúsítvány* nincs felfüggesztve vagy visszavonva;
- a *Tanúsítvány*hoz tartozó magánkulcs nem kompromittálódott.

Tanúsítvány módosítási kérelmet a *Hitelesítés-szolgáltató* csak a szolgáltatási szerződés hatálya alatt fogadhat el.

Az új *Tanúsítvány* kibocsátása során tájékoztatni kell az *Alany*t arról, ha a korábbi *Tanúsítvány* kibocsátása óta változtak a *Tanúsítvány* használatával kapcsolatos kikötések illetve feltételek. Amennyiben az *Alany* nem azonos az *Előfizető*vel, akkor az *Előfizető* számára is meg kell adni a fenti tájékoztatást.

4.8.2. Ki kérelmezheti a tanúsítvány módosítást

A tanúsítvány módosítást olyan személy kezdeményezheti, aki a kérelem benyújtásának időpontjában jogosult lenne új *Tanúsítvány kérelem* benyújtására is az *Alany* nevében.

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

4.8.3. A tanúsítvány módosítási kérelmek feldolgozása

Az *Alany* által vagy az *Alany* nevében benyújtott tanúsítvány módosítási kérelem elbírálása során a *Hitelesítés-szolgáltató*nak ellenőriznie kell, hogy

- a benyújtott kérelem hiteles;

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

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

4.8.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* értesítse az *Alany*t és az *Előfizető*t az új *Tanúsítvány* kibocsátásáról.

4.8.5. A módosított tanúsítvány elfogadása

Nincs megkötés.

4.8.6. A módosított tanúsítvány közzététele

A *Hitelesítés-szolgáltató*nak az eredeti *Tanúsítvány* kibocsátásával megegyező módon kell publikálnia a módosított *Tanúsítvány*t.

4.8.7. További szereplők értesítése a tanúsítvány kibocsátásáról

Amennyiben a *Tanúsítvány*t olyan céllal bocsátották ki, hogy az *Alany* más személy vagy *Szervezet* nevében hozhasson létre elektronikus aláírást, a *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell a *Képviselt szervezet* vagy személy kapcsolattartóját 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.

A tanúsítvány felfüggesztés alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* egy még érvényes *Tanúsítvány* érvényességét átmenetileg megszünteti az eredetileg tervezett érvényességi idő lejárta előtt. A tanúsítvány felfüggesztés egy átmeneti állapot, a felfüggesztett *Tanúsítvány* visszavonható, vagy a *Tanúsítvány* eredeti érvényességi idejének lejárta előtt a felfüggesztés visszavonásával újra érvényessé tehető. A felfüggesztés visszavonása esetén a *Tanúsítvány* érvényessé válik visszamenőleges hatállyal, mintha a felfüggesztés meg sem történt volna.

4.9.1. A tanúsítvány visszavonás körülményei

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

- a *Tanúsítvány* módosítása az *Alany*ra vonatkozó adatok változása miatt;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban foglalt adatok nem felelnek meg a valóságnak;
- az *Alany* vagy az *Előfizető* értesíti a *Hitelesítés-szolgáltató*t arról, hogy az eredeti *Tanúsítvány kérelmet* nem hagyta jóvá, és utólag sem ad erre jóváhagyást;
- az *Alany* vagy az *Előfizető* írásban kéri a *Tanúsítvány* visszavonását;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem az *Alany* kizárólagos birtokában van ;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t jogellenesen használták;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy az *Előfizető* nem teljesítette valamely anyagi kötelezettségét a vonatkozó szolgáltatási szerződésnek megfelelően;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő domain név vagy IP cím használati jogosultsága megszűnt (pl. bíróság visszavonta a domain használati jogát, vagy a tulajdonos nem hosszabbította meg a domain regisztrációját);
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a wildcard tanúsítványt megtévesztő domain név hitelesítésére használták;
- 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 nem a vonatkozó *Hitelesítési rend* illetve *Szolgáltatási szabályzat* szerint bocsátották ki;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t kibocsátó hitelesítő egység magánkulcsa kompromittálódhatott;
- 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* már nem lenne jogosult *Tanúsítvány*okat kibocsátani és a meglevő *Tanúsítvány*okra vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;

- a *Hitelesítés-szolgáltató* tevékenységét befejezte;
- a visszavonást jogszabály kötelezővé teszi;

A *Szolgáltatási szabályzat* előírhat a fentieken kívül egyéb feltételeket is, amelyek esetén a *Hitelesítés-szolgáltató* a *Tanúsítvány*t visszavonja.

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

- a *Tanúsítvány* módosítása a hitelesítési egységre, vagy a *Hitelesítés-szolgáltató*ra vonatkozó adatok változása miatt;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem a kizárólagos birtokában van;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t jogellenesen használták;
- 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;
- 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);
- 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;
- 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 *Hitelesítés-szolgáltató* a tevékenységét befejezte;
- a visszavonást jogszabály kötelezővé teszi.

A *Szolgáltatási szabályzat* előírhat a fentieken kívül egyéb feltételeket is, amelyek esetén a *Hitelesítés-szolgáltató* a *Tanúsítvány*t visszavonja.

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

- a *Tanúsítvány* módosítása a hitelesítési egységre, vagy az azt üzemeltető *Hitelesítés-szolgáltató*ra a vonatkozó adatok változása miatt;

- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban foglalt adatok nem felelnek meg a valóságnak;
- 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 köztes hitelesítő egységet üzemeltető *Hitelesítés-szolgáltató* írásban kéri a *Tanúsítvány* visszavonását;
- 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*t jogellenesen használták;
- 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;
- 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 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 rendnek vagy *Szolgáltatási szabályzat*nak;
- 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 hitelesítési egységet működtető *Hitelesítés-szolgáltató* vagy a *Tanúsítvány*át kibocsátó *Hitelesítés-szolgáltató* a tevékenységét befejezte;
- a visszavonást jogszabály kötelezővé teszi.

A *Szolgáltatási szabályzat* előírhat a fentieken kívül egyéb feltételeket is, amelyek esetén a *Hitelesítés-szolgáltató* a *Tanúsítvány*t visszavonja.

4.9.2. Ki kérelmezheti a visszavonást

A *Tanúsítvány* visszavonását kezdeményezhetik:

- az *Alany*;
- szervezeti tanúsítvány esetén a *Szervezet* nevében eljárásra jogosult természetes személy;
- a szolgáltatási szerződésben megjelölt kapcsolattartó;
- a *Hitelesítés-szolgáltató*.

4.9.3. A visszavonási kérelemre vonatkozó eljárás

A *Hitelesítés-szolgáltató* tanúsítvány visszavonási kérelmet csak az arra jogosult személyek érvényes aláírásával ellátott papír alapú vagy legalább fokozott biztonságú elektronikus aláírással ellátott elektronikus dokumentumon fogadhat be. Ez alól kivételt képeznek a webszerver tanúsítványok, amelyek esetében a *Hitelesítés-szolgáltató*nak lehetővé kell tennie a telefonos ügyfélszolgálatán illetve a honlapján történő visszavonást is. A *Hitelesítés-szolgáltató* a tanúsítvány visszavonási kérelem benyújtására legalább az alábbi lehetőségeket biztosítsa:

- a kérelem személyes benyújtása a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában ügyfélszolgálati időben;
- a papíralapú kérelem eljuttatása a *Hitelesítés-szolgáltató* címére postai küldeményként;
- elektronikus kérelem elküldése a *Hitelesítés-szolgáltató* ügyfélszolgálati e-mail címére.
- Webszerver tanúsítványok esetében a visszavonás kérhető még a 4.9.15 -ben megadott módokon is, 0-24 órában minden nap (ebben az esetben a leírt eljárás lefolytatása nem felfüggesztést, hanem visszavonást eredményez).

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

4.9.4. A visszavonási kérelemre vonatkozó kivárási idő

Nincs megkötés.

4.9.5. A visszavonási eljárás maximális hossza

A visszavonási kérelmeket a *Hitelesítés-szolgáltató* legkésőbb a kérelem beérkezését követő munkanap végéig dolgozza fel.

A *Hitelesítés-szolgáltató* a webszerver *Tanúsítvány*okkal kapcsolatos problémabejelentéseket 24 órán belül vizsgálja ki és döntsön a további szükséges lépésekről.

A *Hitelesítés-szolgáltató* a webszerver *Tanúsítvány*okat a 4.9.1-ben meghatározott feltételek bekövetkezését követően legkésőbb 24 órán belül vonja vissza.

A *Hitelesítés-szolgáltató* a webszerver *Tanúsítvány*okat kibocsátó köztes hitelesítési egységek *Tanúsítvány*ait a 4.9.1-ben meghatározott feltételek bekövetkezését követően legkésőbb 7 napon belül vonja vissza.

4.9.6. Az Érintett felek kötelezettsége 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 ellenőrzés terjedjen ki 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* legalább naponta egyszer bocsásson ki új tanúsítvány visszavonási listát a végfelhasználói *Tanúsítvány*okat kibocsátó hitelesítési egységeire.

Az ilyen kibocsátott tanúsítvány visszavonási listák érvényességi ideje legfeljebb 25 óra lehet.

A *Hitelesítés-szolgáltató* legalább évente egyszer, de visszavonás esetén 24 órán belül bocsásson ki új tanúsítvány visszavonási listát a köztes hitelesítési egységeire. Az ilyen kibocsátott tanúsítvány visszavonási listák érvényességi ideje legfeljebb 12 hónap lehet.

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

A visszavonási lista (CRL) előállítása és közzététele között legfeljebb 5 perc telhet el.

4.9.9. Valós idejű tanúsítvány állapot ellenőrzés lehetősége

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

4.9.10. A valós idejű tanúsítvány állapot ellenőrzésre vonatkozó követelmények

A valós idejű tanúsítvány állapot szolgáltatás feleljen meg a 4.10 fejezet követelményeinek.

4.9.11. A visszavonási hirdetmények egyéb elérhető formái

Nincs megkötés.

4.9.12. A kulcs kompromittálódásra vonatkozó speciális követelmények

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

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

4.9.13. A felfüggesztés körülményei

A *Hitelesítés-szolgáltató* a kockázatok csökkentése érdekében nyújtson lehetőséget a *Tanúsítvány*ok használhatóságának ideiglenes megszüntetésére arra az esetre, ha feltételezhető, hogy a *Tanúsítvány* visszavonását megalapozó okok valamelyike fennáll.

Ez alól kivételt képeznek a webszerver tanúsítványok, amelyek esetében a felfüggesztés nem alkalmazható, azoknál bármilyen gyanú fennállása esetén vissza kell vonni a tanúsítványt.

4.9.14. Ki kérelmezheti a felfüggesztést

A tanúsítvány felfüggesztésre a tanúsítvány visszavonásnak megfelelő – a 4.9.2 fejezet szerinti – követelmények vonatkoznak.

4.9.15. A felfüggesztési kérelemre vonatkozó eljárás

A *Hitelesítés-szolgáltató* tegye lehetővé a honlapján keresztül történő felfüggesztés kezdeményezését.

A *Hitelesítés-szolgáltató* tartson fenn 24 órás telefonos ügyeletet, amelyen keresztül az *Ügyfel*ek a *Tanúsítvány*ok felfüggesztését kérhetik.

A *Hitelesítés-szolgáltató* tegye lehetővé a felfüggesztési kérelmek benyújtását a visszavonási kérelmek benyújtásával azonos módon is, a 4.9.3 fejezet előírásai szerint.

A *Hitelesítés-szolgáltató* ügyeleti telefonján fogadott tanúsítvány felfüggesztési kérelmeket a *Hitelesítés-szolgáltató* ügyintézőjének a hívás időtartama alatt el kell bírálnia, döntéséről szóban értesíteni kell a kérelmezőt.

A *Hitelesítés-szolgáltató* honlapján benyújtott tanúsítvány felfüggesztési kérelmeket a *Hitelesítés-szolgáltató* informatikai rendszerének azonnal el kell bírálnia, az elbírálás eredményéről az oldalon tájékoztatnia kell a kérelem benyújtóját.

A felfüggesztési kérelem elfogadása esetén az állapotváltozást haladéktalanul rögzíteni kell a *Hitelesítés-szolgáltató* tanúsítvány állapot nyilvántartásában.

Az egyéb kommunikációs csatornán keresztül fogadott felfüggesztési kérelmek feldolgozására a tanúsítvány visszavonásnak megfelelő, a 4.9.3 és a 4.9.5 fejezet szerinti követelmények vonatkoznak.

Webszerver tanúsítványok esetében a felfüggesztés nem alkalmazható, azoknál a fenti eljárás lefolytatása a tanúsítvány visszavonását kell, hogy maga után vonja.

4.9.16. A felfüggesztés maximális hossza

A *Hitelesítés-szolgáltató* korlátozhatja a felfüggesztési állapot időtartamát, ezt a *Szolgáltatási szabályzat*ban egyértelműen ismertetni kell. Az időtartam elteltét követően a *Hitelesítés-szolgáltató* külön értesítés nélkül jogosult a felfüggesztett *Tanúsítvány* visszavonására.

4.10. Tanúsítvány állapot szolgáltatások

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

- OCSP – online tanúsítvány visszavonási állapot lekérdezési szolgáltatás,
- CRL – visszavonási lista.

A visszavonási listában kerüljenek feltüntetésre a visszavont és felfüggesztett *Tanúsítvány*ok.

A felfüggesztett *Tanúsítvány*ok a visszaállítás (felfüggesztés visszavonása) hatására kerüljenek ki a visszavonási listából.

A visszavont *Tanúsítvány*ok a *Tanúsítvány* érvényességének lejárta után se törlődjenek a visszavonási listából. A *Hitelesítés-szolgáltató* a visszavonási listában tüntesse fel ezt a tényt az "expiredCertsOnCRL" opcionális kiterjesztés használatával.

Felfüggesztés, visszaállítás és visszavonás esetén a folyamat sikeres lezárását követően a *Tanúsítvány* új állapota azonnal jelenjen meg a *Hitelesítés-szolgáltató* visszavonási nyilvántartásában. Ettől a pillanattól kezdve a *Hitelesítés-szolgáltató* által nyújtott OCSP válaszok már a *Tanúsítvány* új visszavonási állapotát tartalmazzák.

A visszavonási lista használata esetén az állapotváltozás legkésőbb a következő visszavonási listában kerüljön publikálásra.

Kulcs kompromittálódás miatti tanúsítvány felfüggesztés vagy visszavonás esetén, az állapotváltozás bejegyzése után a *Hitelesítés-szolgáltató* bocsásson ki rendkívüli visszavonási listát.

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.

A *Hitelesítés-szolgáltató* más visszavonási állapotváltozás hatására is bocsáthat ki rendkívüli visszavonási listát, ennek szabályait ismertesse a *Szolgáltatási szabályzat*ában.

4.10.1. Működési jellemzők

Nincs megkötés.

4.10.2. A szolgáltatás rendelkezésre állása

A *Hitelesítés-szolgáltató*nak biztosítania kell 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*nak biztosítania kell a visszavonási nyilvántartások és a visszavonás kezelési szolgáltatás éves szinten legalább 99% -os rendelkezésre állását, ahol az eseti szolgáltatáskiesések időtartama legfeljebb 24 óra.

A visszavonási nyilvántartások válaszideje normál terhelés esetén legyen 10 másodpercnél kevesebb.

4.10.3. Opcionális lehetőségek

Nincs megkötés.

4.11. Az előfizetés vége

Az *Előfizető*vel kötött szerződés megszűnése esetén a *Hitelesítés-szolgáltató* vonja vissza a végfelhasználói *Tanúsítvány*t.

4.12. Magánkulcs letétbe helyezése és visszaállítása

A *Hitelesítés-szolgáltató* az aláíró és autentikációs tanúsítványhoz tartozó magánkulcshoz nem nyújthat kulcsletét szolgáltatást.

A *Hitelesítés-szolgáltató* a titkosító *Tanúsítvány*okhoz tartozó magánkulcshoz nyújthat kulcsletét szolgáltatást. A szolgáltatás igénybevételének módját és a szolgáltatás nyújtásának részteleit a *Szolgáltatási szabályzat*ban kell meghatározni.

4.12.1. Kulcsletét és visszaállítás rendje és szabályai

Az aláíró tanúsítványhoz tartozó magánkulcs nem helyezhető letétbe.

4.12.2. Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Nincs megkötés.

5. Elhelyezési, eljárásbeli és üzemeltetési előírások

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

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

5.1. Fizikai követelmények

A *Hitelesítés-szolgáltató*nak gondoskodnia kell 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 kell megvalósítani. A biztosított védelem mértéke legyen megfelelő a *Hitelesítés-szolgáltató* által végzett kockázatelemzésben megállapított fenyegetettség mértékének.

5.1.1. A telephely elhelyezése és szerkezeti felépítése

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

5.1.2. Fizikai hozzáférés

A *Hitelesítés-szolgáltató*nak védenie kell a szolgáltatás nyújtásában részt vevő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében. A Szolgáltatónak biztosítania kell, hogy

- a CA gépterembe történő minden belépés regisztrálásra kerül;
- a CA gépterembe 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 kell tartani;
- a bejelentkezett terminálokat nem szabad felügyelet nélkül hagyni;
- nem szabad olyan munkafolyamatot végezni, amely során bizalmas adatok felfedésre kerülhetnek.

A gépterem elhagyásakor az adminisztrátornak ellenőriznie kell, hogy

- a CA minden berendezése a 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 fizikai biztonsági vizsgálatok rendszeres elvégzésére felelősöket kell kijelölni. A vizsgálatok eredményét megfelelő naplóbejegyzésekben kell rögzíteni.

5.1.3. Áramellátás és légkondicionálás

A *Hitelesítés-szolgáltató Adatközpont*jában olyan szünetmentes áramellátó rendszert kell alkalmazni, 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 szűrőrendszerrel kell biztosítani, amely kiszűri a levegőből a különféle szennyeződéseket (por, szennyező anyagok, korrozív anyagok, mérgező vagy gyúlékony anyagok). A szellőző rendszernek megfelelő szűrés mellett biztosítania kell az operátorok biztonságos munkavégzéséhez szükséges mennyiségű friss levegőt (oxigént).

A levegő nedvességtartalmát az informatikai rendszerek által megkívánt szintre kell csökkenteni.

Megfelelő teljesítményű hűtő rendszereket kell használni a szükséges üzemi hőmérséklet biztosítása, az informatikai eszközök túlhevülésének megakadályozása érdekében.

5.1.4. Beázás és elárasztódás veszély kezelése

A *Hitelesítés-szolgáltató Adatközpont*ját megfelelően védeni kell a víz betöréstől és az elárasztódástól.

5.1.5. Tűz megelőzés és tűzvédelem

A *Hitelesítés-szolgáltató Adatközpont*ját füst- és tűzérzékelőkkel kell felszerelni. Minden helyiségben jól látható helyen el kell helyezni a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készüléket.

5.1.6. Adathordozók tárolása

A *Hitelesítés-szolgáltató*nak védenie kell valamennyi adathordozóját a jogosulatlan hozzáféréstől és a véletlen rongálódástól. Valamennyi audit és archív adatot duplikáltan kell létrehozni. A két példányt egymástól fizikailag elkülönítve kell tárolni, egymástól biztonságos távolságra lévő helyszíneken. A tárolt adathordozókat védeni kell a káros környezeti behatásoktól, mint pl. alacsony vagy magas hőmérséklet, szennyeződés, nedvesség, napfény, erős mágneses tér, erős sugárzás.

5.1.7. Hulladék megsemmisítése

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

Az ilyen eszközöket, adathordozókat a *Hitelesítés-szolgáltató* alkalmazottainak személyes felügyelete alatt, a széleskörűen elfogadott módszereknek megfelelően kell véglegesen törölni vagy használhatatlanná tenni.

5.1.8. A mentési példányok fizikai elkülönítése

A *Hitelesítés-szolgáltató*nak legalább heti rendszerességgel elő kell állítania olyan mentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható. A mentéseket - legalább az utolsó teljes

mentést is beleértve - egy olyan külső helyszínen kell tárolni, amelynek a fizikai és működési védelme azonos az elsődleges helyszínével. Az elsődleges és a tartalék helyszínek között meg kell oldani az adatok biztonságos továbbítását.

5.2. Eljárásbeli előírások

A *Hitelesítés-szolgáltató*nak gondoskodnia kell 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 biztosítsa 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 különüljenek el egymástól a fejlesztési és üzemeltetési folyamatok. A rendszer megfelelő működését a független rendszervizsgáló és a *Hitelesítés-szolgáltató* belső folyamatainak rendszeres ellenőrzése biztosítsa.

5.2.1. Bizalmi szerepkörök

A *Hitelesítés-szolgáltató*nak feladatai ellátásához bizalmi szerepköröket (a rendelet szövegezésében munkaköröket) kell létrehoznia a 3/2005. (III. 18.) IHM rendelet [8] előírásainak megfelelően. A jogosultságokat és funkciókat oly módon kell megosztani az egyes bizalmi szerepkörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére.

A megvalósítandó bizalmi szerepkörök:

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

- regisztrációs felelős: a végtanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.

A bizalmi szerepkörök ellátására *Hitelesítés-szolgáltató* biztonságért felelős vezetőjének formálisan ki kell nevezni a *Hitelesítés-szolgáltató* munkatársait.

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

A bizalmi szerepkörökről naprakész nyilvántartást kell vezetni, amit változás esetén haladéktalanul be kell jelenteni a Nemzeti Média- és Hírközlési Hatóságnak.

5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

A *Hitelesítés-szolgáltató* biztonsági és üzemeltetési szabályzataiban elő kell írni, 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 felhasználóknak egyedi azonosító adatokkal kell rendelkezniük, 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 adatokat a felhasználói jogosultságok megszűnésekor haladéktalanul vissza kell vonni.

5.2.4. Egymást kizáró szerepkörök

A *Hitelesítés-szolgáltató* munkatársai egyidejűleg több bizalmi szerepkört is betölthetnek, de a *Hitelesítés-szolgáltató* köteles biztosítani, 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.

5.3. Személyzetre vonatkozó előírások

A *Hitelesítés-szolgáltató* gondoskodjon 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 foglalkozzon a személyi biztonsággal, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését. Valamennyi bizalmi szerepkör esetén a felvételre jelentkezőknek a jelentkezéskor még 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 biztosítsa 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

A *Hitelesítés-szolgáltató* valamennyi dolgozójának rendelkeznie kell a munkaköre ellátásához szükséges végzettséggel, gyakorlattal és szakmai tapasztalattal. Már a munkaerő felvétel során a leendő dolgozók kiválasztásánál különös hangsúlyt kell fektetni a személyiségi jegyekre, csak megbízható személyek vehetők fel a bizalmi szerepkörbe.

A *Hitelesítés-szolgáltató*nál bizalmi szerepkört csak olyan személy tölthet be,

- akiknek a befolyásmentességét és szakértelmét a *Hitelesítés-szolgáltató* igazolni tudja.

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* vezetői munkakörben illetve bizalmi szerepkörben csak olyan alkalmazottakat foglalkoztathat, akik büntetlen előélettel rendelkeznek és ellenük nincs folyamatban olyan eljárás, amely a büntetlenséget befolyásolhatja. A büntetlen előéletet a felvételi eljárás során a dolgozónak 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolnia.

A *Hitelesítés-szolgáltató*nak a felvételi eljárás során ellenőriznie kell a jelentkező önéletrajzában megadott releváns információk valódiságát.

5.3.3. Képzési követelmények

A *Hitelesítés-szolgáltató* az újonnan felvett alkalmazottakat ki kell képezze, 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.

A regisztrációban közreműködő munkatársakat ki kell képezni:

- 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 dokumentálni kell.

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

5.3.4. Továbbképzési gyakoriságok és követelmények

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

Továbbképzést kell tartani, ha a *Hitelesítés-szolgáltató* folyamataiban vagy informatikai rendszerében változás áll be.

A továbbképzést megfelelően dokumentálni kell, amelyből egyértelműen megállapítható a továbbképzés tematikája és a résztvevő dolgozók köre.

5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

Nincs előírás.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

A *Hitelesítés-szolgáltató*nak a dolgozókkal kötendő munkaszerződésben kell szabályoznia a dolgozók felelősségrevonásának lehetőségeit a dolgozó által elkövetett mulasztások, hibák, vétlen vagy szándékos károkozások esetére. A szankció lehet például fegyelmi eljárás, elbocsátás, kinevezés visszavonása, büntetőjogi felelősségrevonás.

5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

A *Hitelesítés-szolgáltató* által szerződéses viszonyban foglalkoztatott dolgozókra ugyanolyan szabályokat kell alkalmazni, mint a munkavállalókra.

A bizalmi szerepkört betöltő személynek munkaviszonyban kell állnia a *Hitelesítés-szolgáltató*val.

5.3.8. A személyzet számára biztosított dokumentációk

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

5.4. Naplózási eljárások

A *Hitelesítés-szolgáltató*nak a biztonságos informatikai környezet fenntartása érdekében a teljes informatikai rendszerét átfogó eseménynaplózó és ellenőrző rendszert kell megvalósítania és üzemeltetnie.

5.4.1. A tárolt események típusai

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

- 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 kell tenni a független rendszervizsgálók részére, akik a *Hitelesítés-szolgáltató* működésének megfelelőségét vizsgálják.

Naplózni kell minimálisan az alábbi eseményeket:

- 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 (pl. jelszó alapúról PKI alapúra).
- KULCSKEZELÉS:
  - a szolgáltatói kulcsok teljes életciklusára vonatkozó valamennyi esemény (kulcsgenerálás, betöltés, elmentés stb.);
  - a felhasználói kulcsok generálásával, kezelésével kapcsolatos események;
  - a *Hitelesítés-szolgáltató* által bármilyen célból tárolt felhasználói magánkulcsok kezelésével kapcsolatos minden esemény.
- TANÚSÍTVÁNY KEZELÉS:

  - minden kérés, beleértve a *Tanúsítvány* kibocsátást, kulcscserét, megújítást, felfüggesztést és 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;
  - tanúsítvány kérelmek 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;
  - időbélyeg 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*nak biztosítania kell a keletkezett naplóállományok rendszeres kiértékelését.

A keletkezett napi naplóállományokat lehetőség szerint a következő munkanapon, de legkésőbb 1 héten belül ki kell értékelni.

A naplóállományok kiértékelését csak a megfelelő szakértelemmel, jogosultságokkal és kinevezéssel rendelkező független rendszervizsgáló végezheti el.

A *Hitelesítés-szolgáltató* használhat automatizált eszközöket az elektronikus naplóállományok kiértékelésének segítésére.

A kiértékelés során meg kell győződni a vizsgált naplóállományok hitelességéről és sértetlenségéről.

A kiértékelés során elemezni kell a rendszerek által generált hibaüzeneteket.

Statisztikai módszerekkel elemezni kell a forgalmi adatokban bekövetkezett jelentős változásokat.

A vizsgálat tényét, a vizsgálat eredményeit és az esetleges feltárt hiányosságok elhárítása érdekében meghozott intézkedéseket megfelelően dokumentálni kell.

5.4.3. A naplófájl megőrzési időtartama

Az on-line rendszerből való kitörlés előtt a naplóállományokat archiválni kell és gondoskodni kell azok biztonságos megőrzéséről az 5.5.2 fejezetben meghatározott ideig.

5.4.4. A naplófájl védelme

A *Hitelesítés-szolgáltató*nak meg kell védenie a keletkezett naplóállományokat az előírt megőrzési ideig. A megőrzési idő teljes időtartama alatt biztosítania kell a naplóadatok

- védelmét az illetéktelen felfedés ellen: a naplóállományokhoz csak az arra jogosultak – elsősorban a független rendszervizsgálók – férhessenek hozzá;
- rendelkezésre állását: a jogosultak számára biztosítani kell a naplóállományokhoz való hozzáférést;
- integritását: meg kell akadályozni a naplóállományokban bármilyen adat módosítását, törlését, bejegyzések sorrendjének megváltoztatását stb.

5.4.5. A naplófájl mentési eljárásai

Az üzemeltetés során az egyes rendszerekben folyamatosan keletkező naplóbejegyzésekből napi naplóállományokat kell előállítani. A napi naplóállományokat a kiértékelés után 2 példányban archiválni kell és a példányokat egymástól fizikailag elkülönülő helyszíneken az előírt ideig meg kell őrizni. A mentések pontos menetét a *Szolgáltatási szabályzat*ban elő kell írni.

5.4.6. A naplózás adatgyűjtési rendszere

A *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzat*ában írja elő a naplózási folyamatainak működését.

A *Hitelesítés-szolgáltató* használhat automatikus vizsgáló és naplózó rendszereket is, amennyiben biztosítani tudja, hogy azok a rendszer indításakor már aktívak és a rendszer leállásáig folyamatosan működnek.

Amennyiben az automatikus vizsgáló és naplózó rendszerek működésében bármilyen rendellenesség lép fel, a *Hitelesítés-szolgáltató* működését fel kell függeszteni az üzemzavar elhárításáig.

5.4.7. Az eseményeket kiváltó alanyok értesítése

A feltárt hiba esetén a *Hitelesítés-szolgáltató* saját hatáskörében dönthet, hogy értesíti-e a hibáról az azt kiváltó személyt, szerepkört, eszközt vagy alkalmazást.

5.4.8. Sebezhetőség felmérése

A *Hitelesítés-szolgáltató*nak évente sebezhetőség vizsgálatot kell végeznie, amely segítségével feltérképezi 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.

Fel kell térképezni továbbá az egyes fenyegetettségek bekövetkezésének valószínűségét és a bekövetkezés esetén várható kárt is.

Rendszeresen értékelnie kell az alkalmazott folyamatokat, védelmi intézkedéseket, informatikai rendszereket, hogy azok megfelelően képesek-e ellenállni a feltárt fenyegetettségeknek.

A feltárt hibák kiértékelése után szükség szerint módosítani kell a védelmi rendszereken, hogy a hasonló hibák a jövőben megakadályozhatók legyenek.

5.5. Adatok archiválása

5.5.1. Az archivált adatok típusai

A *Hitelesítés-szolgáltató*nak fel kell készülnie elektronikus és papíralapú dokumentumok megfelelően biztonságos, hosszú idejű archiválására.

A *Hitelesítés-szolgáltató*nak az alábbi jellegű információt kell archiválnia:

- 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 *Tanúsítvány kérelem*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;
- az *Aláírás-létrehozó eszköz*ök megszemélyesítésével kapcsolatos információk;
- valamennyi elektronikus és papíralapú naplóbejegyzés.

A *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzat*ában meghatározhatja az archiválandó adatok bővebb körét is.

5.5.2. Az archívum megőrzési időtartama

A *Hitelesítés-szolgáltató* köteles megőrizni az archivált adatokat az alábbi időtartamokig:

- a *Tanúsítvány*okkal kapcsolatos valamennyi elektronikus és/vagy papír alapú információt legalább
  - a *Tanúsítvány* érvényességének lejáratától számított 10 évig;
  - a tanúsítvánnyal előállított elektronikus aláírással kapcsolatos jogvita jogerős lezárásáig.
- a *Szolgáltatási szabályzat*ot a hatályon kívül helyezéstől számított 10 évig;
- az összes többi archivált adat megőrzési idejét a *Szolgáltatási szabályzat*ban kell meghatározni.

5.5.3. Az archívum védelme

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

A két helyszín mindegyikének teljesítenie kell az archiválással szemben támasztott biztonsági és egyéb követelményeket.

Az archivált adatok megőrzése során gondoskodni kell az archivált adatok

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

Az archivált elektronikus adatokat legalább fokozott biztonságú elektronikus aláírással és minősített időbélyeggel kell ellátni.

5.5.4. Az archívum mentési folyamatai

Az archivált adatok másodpéldányát a *Hitelesítés-szolgáltató* telephelyétől fizikailag eltérő helyszínen kell tárolni az 5.1.8 fejezet előírásainak megfelelően.

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi elektronikus naplóbejegyzést el kell látni időjellel, amelyen legalább másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

A *Hitelesítés-szolgáltató*nak biztosítania kell, hogy a szolgáltatást nyújtó rendszerein a gépidő maximum 1 másodpercre térjen el a referenciaidőtől.

A napi naplóállományokat minősített időbélyeggel kell ellátni.

Az archivált adatok megőrzése során szükség esetén (pl. algoritmusváltás, az eredeti időbélyeg érvényességének lejárata) gondoskodni kell az adatok hitelességének megőrzéséről.

5.5.6. Az archívum gyűjtési rendszere

A *Hitelesítés-szolgáltató* védett informatikai rendszerén belül kell keletkeznie a naplóbejegyzéseknek, onnan csak az elektronikusan aláírt, minősített időbélyeggel védett naplóállományok kerülhetnek ki.

5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

A *Hitelesítés-szolgáltató* a naplóállományok előállítását manuálisan vagy automatikusan is elvégezheti. Automatikus naplózó rendszer alkalmazása esetén a hitelesített naplóállományokat naponta kell előállítani.

Az archivált adatállományokat védeni kell a jogosulatlan hozzáféréstől.

Az arra jogosultaknak biztosítani kell az archivált adatokhoz való ellenőrzött hozzáférést

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

5.6. Kulcscsere

A *Hitelesítés-szolgáltató* gondoskodjon arról, hogy az általa használt hitelesítési egységek folyamatosan rendelkezzenek a működéshez szükséges, érvényes kulccsal és Tanúsítvánnyal. Ennek érdekében a *Tanúsítvány*uk lejárta illetve a hozzájuk kapcsolódó kulcsok használati idejének lejárta előtt elegendő idővel generáljon új kulcspárt a hitelesítő egység számára, és arról időben értesítse *Ügyfel*eit. Az új szolgáltatói kulcsot a jelen szabályzatnak megfelelően kell generálni és kezelni.

Amennyiben a *Hitelesítés-szolgáltató* megváltoztatja a végfelhasználói *Tanúsítvány*okat kibocsátó bármely szolgáltatói tanúsítványának kulcsait, be kell tartania az alábbi előírásokat:

- publikálnia kell 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 írhatja alá;
- meg kell őriznie a régi szolgáltatói *Tanúsítvány*ait és nyilvános kulcsait, valamint lehetővé kell tennie az aláírások érvényességének ellenőrzését mindaddig, amíg a régi szolgáltatói kulccsal aláírt valamennyi *Tanúsítvány* érvényességi ideje lejár.

5.7. Kompromittálódást és katasztrófát követő helyreállítás

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

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

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

5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások

A *Hitelesítés-szolgáltató*nak rendelkeznie kell üzletmenet folytonossági tervvel.

A *Hitelesítés-szolgáltató*nak ki kell alakítania és fenn kell tartania egy teljes értékű tartalék CA rendszert, amely az elsődleges helyszíntől biztonságos távolságra, földrajzilag különböző helyszínen található és önállóan is alkalmas a szolgáltatások teljes körű ellátására. A *Hitelesítés-szolgáltató*nak évente tesztelnie kell a tartalék rendszerre való átállást és felül kell vizsgálnia az üzletmenet folytonossági terveit.

Katasztrófa esetén a lehető legrövidebb időn belül helyre kell állítani a szolgáltatások elérhetőségét.

5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

A *Hitelesítés-szolgáltató* informatikai rendszereit megbízható hardver és szoftver komponensekből kell felépíteni.

A kritikus funkciókat redundáns rendszerelemek alkalmazásával kell megvalósítani úgy, hogy azok egy elem meghibásodása esetén is képesek legyenek a további működésre.

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

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

A *Hitelesítés-szolgáltató* üzletmenet folytonossági terve tartalmazzon pontos előírásokat a kritikus rendszer komponensek meghibásodásának esetén végrehajtandó feladatokra.

A *Hitelesítés-szolgáltató* a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leghamarabb indítsa újra a szolgáltatásait. A szolgáltatások helyreállítása során elsőbbséget kell élvezzenek a tanúsítvány állapot információkat szolgáltató rendszerek.

5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások

A *Hitelesítés-szolgáltató* magánkulcsának kompromittálódása esetén haladéktalanul meg kell tenni az alábbi lépéseket:

- vissza kell vonni a *Hitelesítés-szolgáltató* összes érintett *Tanúsítvány*át;
- új szolgáltatói magánkulcsokat kell generálni a szolgáltatások helyreállításához;
- vissza kell vonni az összes webszerver tanúsítványt, amelyet az érintett magánkulcsokkal írtak alá;
- nyilvánosságra kell hozni a visszavont szolgáltatói tanúsítványok adatait a 2.2 fejezetben szabályozott módon;

- a visszavont webszerver tanúsítványok helyett új *Tanúsítvány*okat kell kibocsátani az új szolgáltatói kulcsok felhasználásával.

5.7.4. Működés folyamatosságának biztosítása katasztrófát követően

A *Hitelesítés-szolgáltató* üzletmenet folytonossági tervében meg kell határozni a természeti vagy egyéb katasztrófa miatt bekövetkezett szolgáltatás leállás esetén végrehajtandó feladatokat. A katasztrófa bekövetkezése esetén haladéktalanul életbe kell léptetni a rendelkezéseket és meg kell kezdeni a károk elhárítását, a szolgáltatások helyreállítását.

A másodlagos szolgáltatási helyszínt az elsődleges telephelytől olyan távol kell elhelyezni, 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 állítsa helyre a katasztrófa során tönkrement eszközeit és állítsa helyre az eredeti szolgáltatás biztonsági szintet.

5.8. A hitelesítés szolgáltató vagy a regisztrációs szervezet leállítása

A *Hitelesítés-szolgáltató*nak a szolgáltatás megszüntetésekor teljesítenie kell a jogszabályokban megfogalmazott követelményeket ([1], [8]).

A leállítás során kiemelten kezelendő feladatok:

- a tervezett leállásról időben értesíteni kell a Nemzeti Média- és Hírközlési Hatóságot és az érintett partnereket, *Előfizető*ket;
- a *Hitelesítés-szolgáltató* tegyen meg mindent annak érdekében, hogy legkésőbb a szolgáltatás leállításáig egy másik szolgáltató átvegye nyilvántartásait és szolgáltatási kötelezettségeit;
- be kell szüntetni az új *Tanúsítvány*ok kiadását;
- vissza kell vonni a szolgáltatói *Tanúsítvány*okat és meg kell semmisíteni a szolgáltatói magánkulcsokat;
- a szolgáltatás megszüntetése után egy teljes rendszermentést és archiválást kell végeznie;
- át kell adni az archivált adatokat a szolgáltatást átvállaló szolgáltatónak vagy a Nemzeti Média- és Hírközlési Hatóságnak.

6. Műszaki biztonsági óvintézkedések

A *Hitelesítés-szolgáltató*nak módosítás ellen védett, megbízható rendszereket és termékeket kell használnia a kriptográfiai kulcsok és aktivizáló adataik kezelésére a teljes életciklus alatt.

6.1. Kulcspár előállítása és telepítése

A *Hitelesítés-szolgáltató*nak gondoskodnia kell az általa generált valamennyi magánkulcs biztonságos, az ipari szabványoknak és a hatályos jogszabályi előírásoknak megfelelő előállításáról és kezeléséről.

6.1.1. Kulcspár előállítása

Valamennyi kulcspárt az Eat. [1] 18. § szerint kiadott aktuális NMHH határozatban megfogalmazott követelményeknek megfelelő algoritmussal kell létrehozni.

A *Hitelesítés-szolgáltató* saját kulcspár előállítása esetén:

- 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 kell végezni.
- A szolgáltatói magánkulcs előállítását egy kulcsgenerálási forgatókönyv alapján kell végezni.
- Szolgáltatói gyökér hitelesítő egység magánkulcsának előállítása esetén legyen jelen egy külső auditor, vagy készüljön videofelvétel az eseményről. A külső auditor igazolása szükséges arról, hogy a kulcs generálása a forgatókönyv szerint történt.
- A szolgáltatói magánkulcs előállítását olyan eszközön belül kell végrehajtani, amely:
  - megfelel a FIPS 140-2 [4] 3-as, illetve annál magasabb szintű követelményeinek, vagy
  - megfelel a CEN 14167-2 [19] munkacsoport egyezmény követelményeinek, vagy
  - olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [9] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten van értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előirányzaton kell alapulnia.

A *Hitelesítés-szolgáltató* által más felek (pl. bizalmi szerepkört betöltő saját munkatársai és az *Alany*ok) számára előállított kulcspár előállítása esetén:

- A kulcsok előállítását fizikailag védett környezetben kell végezni, kizárólag bizalmi szerepkört betöltő személyek részvételével.

- A kriptográfiai hardver eszköz használatát előíró *Hitelesítési rend*ek esetén a *Hitelesítés-szolgáltató* a magánkulcsot csak a szolgáltatást igénybe vevő *Alany* kriptográfiai hardver eszközén generálhatja, ami lehetetlenné teszi a magánkulcs felfedését.
- Az előállított magánkulcsokat a *Hitelesítés-szolgáltató*nak a kulcs átadásáig megfelelően biztonságos környezetben kell tárolnia a felfedés megakadályozása érdekében. Az aláíró és autentikációs magánkulcs *Alany*nak történő dokumentált átadása után a *Hitelesítés-szolgáltató* köteles haladéktalanul megsemmisíteni az átadott magánkulcs általa tárolt minden példányát olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon. 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.

Az *Alany* által előállított kulcspár esetén:

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

6.1.2. Magánkulcs eljuttatása az alanyhoz

Amennyiben a *Hitelesítés-szolgáltató* állította elő az *Alany* magánkulcsát, akkor az alábbi követelményeknek kell megfelelni:

- A *Hitelesítés-szolgáltató*nak az általa az *Alany*ok részére generált magánkulcsokat és aktivizáló adatokat a kulcsok átadásáig biztonságos módon kell tárolnia, amely megakadályozza a kulcsok felfedését, lemásolását, módosítását, sérülését, illetéktelenek általi használatát.
- A *Hitelesítés-szolgáltató*nak biztosítania kell, hogy a magánkulcsokat és aktivizáló adataikat csak az arra jogosult *Alany* vehesse át.
- A *Hitelesítés-szolgáltató*nak megfelelő bizonyítékot kell szereznie a magánkulcs *Alany* részére történő átadásáról, az átadás pontos időpontjáról.
- Az aláíró és autentikációs magánkulcs *Alany* részére történő átadása után a *Hitelesítés-szolgáltató* nem őrizhet meg másolatot az aláíró magánkulcsból.

6.1.3. A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

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

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

6.1.4. A szolgáltatói nyilvános kulcs közzététele

A *Hitelesítés-szolgáltató*nak olyan módszerrel kell elérhetővé tennie legfelsőbb szintű szolgáltatói tanúsítványainak nyilvános kulcsait az *Érintett felek* részére, amely lehetetlenné teszi a kulcsok megváltoztatására irányuló támadásokat. Ennek keretében a *Hitelesítés-szolgáltató* legalább

- a honlapján tegye közzé a szolgáltatói *Tanúsítvány*ait.

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

- A gyökér hitelesítő egységek megnevezését, illetve gyökértanúsítványaik lenyomatát tartalmazza a *Szolgáltatási szabályzat*. Az állapotváltozásukkal kapcsolatos információk legyenek elérhetőek a *Hitelesítés-szolgáltató* honlapján.
- A köztes (nem gyökér) hitelesítő egységek tanúsítványainak állapotváltozását hozza nyilvánosságra a visszavonási listákon, 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 *Tanúsítvány*t bocsásson ki, ezzel kiküszöbölve azt, hogy a *Tanúsítvány* visszavonási állapotát ellenőrizni kelljen. E *Tanúsítvány* visszavonási állapotát a *Hitelesítés-szolgáltató* kizárólag olyan módon tegye közzé, hogy kulcs kompromittálódás vagy bármilyen egyéb probléma esetén az OCSP válaszokat aláíró régi magánkulcshoz ne kerüljön kibocsátásra újabb *Tanúsítvány*. A *Hitelesítés-szolgáltató* az OCSP válaszadói *Tanúsítvány*okat ezt követően új, biztonságos magánkulcshoz bocsássa ki.

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

6.1.5. Kulcsméretek

A *Hitelesítés-szolgáltató* mindenkor a Nemzeti Média- és Hírközlési Hatóságnak az Eat. 18. § [1] szerinti felhatalmazása alapján kibocsátott határozata által engedélyezett algoritmusokat és minimális kulcsméreteket használhat.

6.1.6. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A kulcsparaméterek előállítására vonatkozó követelményeket a 6.1.1. fejezet tartalmazza.

A kulcsok előállításához használt, megfelelő tanúsítvánnyal rendelkező eszközöket a tanúsításban meghatározott követelmények szigorú betartásával kell üzemeltetni a generált kulcsparaméterek minőségének biztosítása érdekében.

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

A *Hitelesítés-szolgáltató* a végfelhasználói tanúsítványokban szerepeltesse a "kulcshasználat" (Key Usage) kiterjesztéseket, amelyek meghatározzák a tanúsítvány felhasználási területét és az X.509v3 [22] kompatibilis alkalmazásokban műszakilag is korlátozzák a kulcsok felhasználhatóságát. A mező tartalmára vonatkozó megkötések a 7.1.2 fejezetben szerepelnek. Az *Alany* a *Tanúsítvány*ához tartozó magánkulcsát kizárólag a *Tanúsítvány*ban szereplő kulcshasználatnak megfelelően használhatja, más felhasználás nem engedélyezett.

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

- a gyökér hitelesítő egység saját önaláírt tanúsítványának kibocsátására,
- köztes hitelesítő egységek tanúsítványainak aláírására,
- OCSP válaszadó tanúsítványának aláírására,
- időbélyegző egység tanúsítványának aláírására,
- CRL-ek aláírására.

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

- végfelhasználói tanúsítványok aláírására,
- köztes hitelesítő egységek tanúsítványainak aláírására,

- időbélyegző egység tanúsítványának aláírására,
- OCSP válaszadó tanúsítványának aláírására,
- CRL-ek aláírására.

6.2. A magánkulcsok védelme

A *Hitelesítés-szolgáltató*nak gondoskodnia kell a birtokában lévő saját és a végfelhasználói magánkulcsok biztonságos kezeléséről, meg kell akadályoznia a magánkulcsok felfedését, lemásolását, törlését, módosítását, jogosulatlan használatát.

A *Hitelesítés-szolgáltató* csak addig őrizheti a saját és végfelhasználói magánkulcsait, ameddig azt a szolgáltatás nyújtása feltétlenül megköveteli.

6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

A *Hitelesítés-szolgáltató* tanúsítvány kibocsátó és az OCSP válaszokat, CRL listákat aláíró rendszerei az aláírás létrehozásához használt magánkulcsokat olyan biztonságos hardver eszközökben kell tárolja, amelyek rendelkeznek az Eat. 7. § (5)-(6) szerinti igazolással [1], illetve FIPS 140-2 Level 3 szerinti tanúsítással [4].

A szolgáltatói magánkulcsok a kriptográfiai modulon kívül csak kódolt formában tárolhatók. A kódoláshoz csak az Eat. [1] 18. § szerint kiadott aktuális NMHH határozat szerinti algoritmusok és kulcsparaméterek használhatók, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

6.2.2. Magánkulcs többszereplős (n-ből m) használata

A *Hitelesítés-szolgáltató*nak biztosítania kell, hogy a magánkulcsaival végzett kritikus műveletek végrehajtásához legalább kettő, bizalmi szerepkört betöltő munkatárs egyidejű jelenlétére legyen szükség.

6.2.3. Magánkulcs letétbe helyezése

A *Hitelesítés-szolgáltató* nem helyezheti letétbe a szolgáltatói aláíró magánkulcsait.

A végfelhasználói aláíró és autentikációs magánkulcsok nem helyezhetők letétbe, azok másolása, többszörös használata nem engedélyezett.

6.2.4. Magánkulcs mentése

A *Hitelesítés-szolgáltató*nak biztonsági másolatokat kell készítenie szolgáltatói magánkulcsairól, ebből legalább egy példányt a szolgáltatás nyújtásától eltérő helyszínen kell tárolni.

A biztonsági másolatok készítése csak védett környezetben, legalább két bizalmi szerepkört betöltő személy együttes jelenlétében, más személyek kizárásával történhet.

A biztonsági másolatok kezelésére és megőrzésére legalább ugyanolyan szigorú biztonsági előírásokat kell alkalmazni, mint az éles rendszer üzemeltetésére.

A végfelhasználók aláíró és autentikációs magánkulcsairól a *Hitelesítés-szolgáltató* nem készíthet semmilyen másolatot.

6.2.5. Magánkulcs archiválása

A *Hitelesítés-szolgáltató* nem archiválhatja magánkulcsait és a végfelhasználói aláíró és autentikációs magánkulcsokat.

6.2.6. Magánkulcs bejuttatása kriptográfiai modulba, vagy onnan történő exportja

A *Hitelesítés-szolgáltató* valamennyi szolgáltatói magánkulcsát a követelményeknek megfelelő kriptográfiai modulban kell előállítani.

A magánkulcsok nem létezhetnek nyílt formában a kriptográfiai modulon kívül.

A *Hitelesítés-szolgáltató* a magánkulcsot csak biztonsági másolat készítése céljából exportálhatja a kriptográfiai modulból.

A magánkulcs kriptográfiai modulok közötti szállítása csak biztonsági másolat formájában engedélyezett.

6.2.7. Magánkulcs tárolása kriptográfiai modulban

A *Hitelesítés-szolgáltató*nak a jelen *Hitelesítési rend*ek szerinti szolgáltatás nyújtásához használt magánkulcsait kriptográfiai modulban kell tartania.

A kriptográfiai modulon belüli tárolási formára vonatkozóan nincs előírás.

6.2.8. A magánkulcs aktiválásának módja

A *Hitelesítés-szolgáltató* szolgáltatói magánkulcsait a felhasznált kriptográfiai modul felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell aktiválni.

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

A *Hitelesítés-szolgáltató* által előállított végfelhasználói magánkulcsok esetén a *Hitelesítés-szolgáltató*nak gondoskodnia kell róla, hogy a magánkulcsokat és a magánkulcsok aktiváló adatait

megfelelően biztonságos módon állítsa elő és kezelje, amely kizárja a magánkulcsok illetéktelen használatának lehetőségét.

A *Hitelesítés-szolgáltató* által az *Alany* részére intelligens kártyán vagy tokenen átadott magánkulcsok esetén az intelligens eszközt úgy kell konfigurálni és az *Alany* részére átadni, hogy

- egyértelműen megállapítható legyen, hogy az eszközt az átadás előtt nem használták ;
- a magánkulcs használata előtt előtt az *Alany*nak azonosítania kelljen magát a kriptográfiai hardver eszköz felé.

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

6.2.9. A magánkulcs deaktiválásának módja

Szolgáltatói magánkulcsok

A *Hitelesítés-szolgáltató* szolgáltatói magánkulcsait a felhasznált kriptográfiai modul felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell deaktiválni.

Végfelhasználói magánkulcsok

A kriptográfiai hardver eszköz használatát megkövetelő *Hitelesítési rend*ek esetén a magánkulcsokat az alkalmazott hardver eszköz használati útmutatójában és az eszköz tanúsítvány tanúsítási mellékletében megfogalmazott követelményeknek megfelelően kell használni.

Az intelligens kártyán vagy tokenen átadott magánkulcsok esetén az eszköznek biztosítania kell, hogy az magánkulcsok deaktiválódnak az alábbi esetekben:

- az eszköz áramellátása bármely okból megszűnik;
- az *Alany* kilép az magánkulcsot használó alkalmazásból;
- az *Alany* deaktiváló (kilépés) utasítást ad az alkalmazásból az eszköznek.

A deaktivált kulcs illetve kriptográfiai hardver eszköz csak az *Alany* újbóli azonosítása után használható .

A kriptográfiai hardver eszköz használatát nem megkövetelő Hitelesítési rendek esetén a magánkulcsok megfelelően biztonságos használata az *Alany* felelőssége.

6.2.10. A magánkulcs megsemmisítésének módja

Szolgáltatói magánkulcsok

A *Hitelesítés-szolgáltató* használatból kivont, lejárt érvényességű vagy kompromittálódott szolgáltatói magánkulcsait olyan módon kell megsemmisíteni, ami lehetetlenné teszi a magánkulcs további használatát.

A szolgáltatói magánkulcsok megsemmisítését a felhasznált kriptográfiai modul felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell elvégezni.

Végfelhasználói magánkulcsok

A kriptográfiai hardver eszköz használatát megkövetelő *Hitelesítési rend*ek esetén a feleslegessé vált magánkulcsokat az alkalmazott hardver eszköz használati útmutatójában és az eszköz tanúsítvány tanúsítási mellékletében megfogalmazott követelményeknek megfelelően kell megsemmisíteni.

Az *Alany* részére kriptográfiai hardver eszközön (pl. intelligens kártyán vagy tokenen) kiadott, használatból kivont magánkulcsok megsemmisítése az eszköz fizikai megsemmisítésével lehetséges, ami az *Alany* felelőssége.

A kriptográfiai hardver eszköz használatát nem megkövetelő *Hitelesítési rend*ek esetén a magánkulcsok megfelelően biztonságos megsemmisítése az *Alany* felelőssége.

A végfelhasználók használatból kivont aláíró és autentikációs magánkulcsait javasolt megsemmisíteni, azonban a titkosító magánkulcsokat javasolt megőrizni annak érdekében, hogy a korábban titkosított dokumentumok később is visszafejthetők legyenek.

6.2.11. A kriptográfiai modulok értékelése

A 6.2.1 fejezet előírásaival összhangban a *Hitelesítés-szolgáltató* valamennyi magánkulcsát olyan kriptográfiai modulban kell tárolni, amely

- rendelkezik FIPS 140-2 Level 3 szerinti tanúsítással [4], vagy
- rendelkezik a CEN 14167-2 [19] munkacsoport egyezmény követelményeinek való megfelelést igazoló Common Criteria alapú tanúsítvánnyal, vagy
- rendelkezik az Eat. 7. § (5) és (6) bekezdései szerint [1], 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*nak archiválnia kell valamennyi általa kibocsátott *Tanúsítvány*t.

6.3.2. A tanúsítványok és kulcspárok használatának periódusa

A *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*ok érvényességi ideje legfeljebb a kibocsátástól számított 2 év, de nem haladhatja meg

- azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Nemzeti Média- és Hírközlési Hatóság Eat. 18. § [1] szerint kibocsátott határozata értelmében biztonságosan felhasználhatók;
- a *Tanúsítvány*t kibocsátó szolgáltatói tanúsítvány hátralevő érvényességi idejét.

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

A *Hitelesítés-szolgáltató* a felhasznált kriptográfiai modul felhasználói útmutatójában és a tanúsítványban megfogalmazott eljárásoknak, követelményeknek megfelelő aktiváló módszereket kell alkalmazzon szolgáltatói magánkulcsainak védelmére.

Jelszó alapú aktivizáló adatok használata esetén a jelszavaknak kellően bonyolultnak kell lenniük a megkívánt védelmi szint biztosítása érdekében.

A *Hitelesítés-szolgáltató* által az *Alany* részére kibocsátott kriptográfiai hardver eszközök esetén a *Hitelesítés-szolgáltató*nak

- az aktivizáló adatokat megfelelő minőségű véletlenszám-generátor segítségével, fizikailag biztonságos körülmények között kell előállítania és a kriptográfiai hardver eszközre telepítenie;
- az aktivizáló adatokat biztonságos módszer felhasználásával kell az *Alany* részére átadni.

A *Hitelesítés-szolgáltató* által az *Alany* részére előállított, szoftveresen átadott magánkulcsok esetén:

- a *Hitelesítés-szolgáltató*nak az aktivizáló adatokat megfelelő minőségű véletlenszám-generátor segítségével, fizikailag biztonságos körülmények között kell előállítania és a magánkulcshoz rendelnie;

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

6.4.2. Az aktivizáló adatok védelme

A *Hitelesítés-szolgáltató* alkalmazottainak a magánkulcsok aktiválásához szükséges eszközöket, aktivizáló adatokat biztonságosan kell tárolniuk, a jelszavak csak kódolt formában tárolhatók.

A *Hitelesítés-szolgáltató* által az *Alany*ok részére kibocsátott kriptográfiai hardver eszközök illetve az *Alany* számára generált szoftveres magánkulcsok esetén:

- a *Hitelesítés-szolgáltató* az aktivizáló adatokat csak abból a célból rögzítheti, hogy azt az *Alany* részére átadhassa;
- a *Hitelesítés-szolgáltató*nak az aktivizáló adatokat biztonságos módszer felhasználásával kell az *Alany*ok részére szétosztani.

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

6.4.3. Az aktivizáló adatok 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 biztosítani kell az alábbi követelmények teljesülését:

- a rendszerhez vagy alkalmazáshoz való hozzáférés engedélyezése előtt a felhasználó azonosságát ellenőrizni kell;
- a felhasználókhoz szerepköröket kell rendelni és biztosítani kell, hogy minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezzen;
- minden tranzakcióról naplóbejegyzést kell előállítani és a naplóbejegyzéseket archiválni kell;
- a biztonságkritikus folyamatok részére biztosítani kell, hogy a *Hitelesítés-szolgáltató* belső hálózati tartományai kellően védettek legyenek a jogosulatlan hozzáféréstől;
- megfelelő eljárásokat kell alkalmazni a kulcsvesztés vagy rendszerhiba utáni szolgáltatás visszaállítás biztosítása érdekében.

6.5.2. Az informatikai biztonság értékelése

Az informatikai biztonság és a szolgáltatás minőségének biztosítása érdekében a *Hitelesítés-szolgáltató* nemzetközileg elfogadott módszertanok szerinti irányítási rendszert kell alkalmazzon, ezek megfelelőségét független tanúsító szervezet által kiállított tanúsítvánnyal kell igazolnia.

6.6. Életciklusra vonatkozó műszaki előírások

6.6.1. Rendszerfejlesztési előírások

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

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

A beszerzést a hardver és szoftver komponensek módosítását kizáró módon kell elvégezni.

A szolgáltatás nyújtásához használt hardver és szoftver komponensek más célra nem használhatók.

A *Hitelesítés-szolgáltató* megfelelő védelmi intézkedésekkel akadályozza meg, hogy kártékony szoftver kerülhessen a hitelesítés szolgáltatásban használt eszközökbe.

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

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

Megbízható, megfelelően képzett személyzetet kell alkalmazni a szoftverek és eszközök telepítése során.

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

A *Hitelesítés-szolgáltató*nak rendelkeznie kell egy változáskövető rendszerrel, amelyben minden változást dokumentálni kell.

A *Hitelesítés-szolgáltató* alkalmazzon eljárásokat a jogosulatlan változások észlelésére.

6.6.2. Biztonságkezelési előírások

A *Hitelesítés-szolgáltató* alkalmazzon eljárásokat a hitelesítés szolgáltatásban használt rendszerek telepítésének, konfigurációjának dokumentálására, üzemeltetésére, ellenőrzésére, monitorozására és karbantartására, beleértve a módosításokat és továbbfejlesztéseket is. A változás követő rendszernek észlelnie kell a rendszerben történt bármilyen jogosulatlan változtatást, adatbevitelt, ami érinti a hitelesítés szolgáltatásban használt rendszert, a tűzfalakat, routereket, programokat és egyéb komponenseket. A hitelesítés szolgáltatásban használt program telepítésekor a *Hitelesítés-szolgáltató* győződjön meg róla, hogy a telepítendő program a megfelelő verziójú és mentes mindenféle jogosulatlan módosítástól. A *Hitelesítés-szolgáltató* ellenőrizze rendszeresen a hitelesítés szolgáltatásban használt rendszereiben használt programok integritását.

6.6.3. Életciklusra vonatkozó biztonsági előírások

Nincs megkötés.

6.7. Hálózati biztonsági előírások

A *Hitelesítés-szolgáltató* tartsa szigorú ellenőrzés alatt az alkalmazott IT rendszereinek konfigurációját, dokumentáljon minden változást, beleértve a legkisebb módosítást, fejlesztést, szoftverfrissítést is. A *Hitelesítés-szolgáltató* vezessen be megfelelő eljárásokat az IT rendszereiben bekövetkezett tetszőleges hardver vagy szoftver változás észlelésére, a rendszer telepítésére, karbantartására. A *Hitelesítés-szolgáltató* ellenőrizze minden szoftverkomponens első betöltésekor a komponens eredetiségét, integritását.

A *Hitelesítés-szolgáltató* alkalmazzon megfelelő hálózatbiztonsági intézkedéseket, mint például

- tiltsa le a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtasson.

6.8. Időbélyegzés

A *Hitelesítés-szolgáltató*nak a Nemzeti Média- és Hírközlési Hatóság szolgáltatói nyilvántartásában szereplő minősített időbélyeg szolgáltató által biztosított időbélyegeket kell használnia.

7. Tanúsítvány, CRL és OCSP profilok

7.1. Tanúsítvány profil

A *Hitelesítés-szolgáltató* által kibocsátott tanúsítványok feleljenek meg az RFC 5280 [5], RFC 6818 [6] és az ETSI TS 101 862 [10] X.509 specifikációknak.

7.1.1. Verzió szám(ok)

A *Hitelesítés-szolgáltató* az X.509 specifikáció [22] szerinti "v3" *Tanúsítvány*okat bocsásson ki.

7.1.2. Tanúsítvány kiterjesztések

A *Hitelesítés-szolgáltató* az X.509 specifikáció [22] szerinti tanúsítvány kiterjesztéseket használhat, saját maga által definiált kritikus kiterjesztések használata nem megengedett.

A tanúsítvány kiterjesztéssel kapcsolatos konkrét előírások:

- 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) megnevezését, valamint a tanúsítvány alkalmazhatóságára vonatkozó egyéb információkat.

  Végfelhasználói tanúsítvány esetében a *Hitelesítés-szolgáltató* minden esetben töltse ki ezt a mezőt a következő adatok megadásával:

  – a *Hitelesítési rend* azonosítója (OID);
  – a *Szolgáltatási szabályzat* elérhetősége.

  A végfelhasználói tanúsítványoknál minden esetben meg kell adni legalább egy olyan hitelesítési rendet, amely szerint a *Hitelesítés-szolgáltató* a *Tanúsítvány*t kibocsátotta, és amely hitelesítési rend szerint később a tanúsítvánnyal kapcsolatban eljár. A *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*okban tüntesse fel legalább egy ilyen hitelesítési rend azonosítóját (OID) és a hozzá kapcsolódó *Szolgáltatási szabályzat* elérhetőségét (URL).

  A "Certificate Policies" mezőt nem tartalmazó végfelhasználói *Tanúsítvány*t teszt tanúsítványnak kell tekinteni. A teszt *Tanúsítvány* kizárólag tesztelési célra használható, valós tranzakciók esetén el kell utasítani.

  Gyökér hitelesítési egység tanúsítványában ne szerepeljen ez a mező.

  Köztes hitelesítési egység tanúsítványban a mező kitöltése kötelező és nem lehet kritikus. A *Hitelesítés-szolgáltató* saját köztes hitelesítési egységei számára kibocsátott tanúsítványok

esetében szerepelhet anyPolicy Identifier ebben a mezőben. A vonatkozó *Szolgáltatási szabályzat* hivatkozása megadható ebben a mezőben.

Más *Hitelesítés-szolgáltató* számára kibocsátott köztes hitelesítési egység tanúsítványainak esetében csak olyan azonosító szerepelhet ebben a mezőben, amely olyan hitelesítési rendre vonatkozik, amely megfelel a kibocsátó *Hitelesítés-szolgáltató* által alkalmazott valamely hitelesítési rendnek, és nem lehet benne anyPolicy Identifier.

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
  OID: 2.5.29.35
  A *Tanúsítvány*t hitelesítő elektronikus aláírás létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója. Használata kötelező.
  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. Használata kötelező.

- *Alany* alternatív nevei (Subject Alternative Names) – nem kritikus
  OID: 2.5.29.17
  Lásd: 3.1.1. fejezet.

  Végfelhasználói tanúsítvány esetében az *Alany* neve a "CN" -ben feltüntetettől eltérő írásmóddal, illetve e-mail cím kerülhet ide. Kitöltése opcionális.

  Gyökér és köztes hitelesítő egység tanúsítványában a *Hitelesítés-szolgáltató* központi e-mail címe kerülhet ide. Kitöltése opcionális.

- Alapvető megkötések (Basic Constraints) – kritikus
  OID: 2.5.29.19
  Annak megadása, hogy a *Tanúsítvány* hitelesítő egység számára lett-e kibocsátva.

  A kiterjesztés default értéke CA = "FALSE", ezért ezt a kiterjesztést nem szabad beleírni a végfelhasználók, OCSP válaszadók és időbélyegző egységek számára kibocsátott tanúsítványokba.

  Gyökér és köztes hitelesítő egységek tanúsítványai esetében a kiterjesztés kitöltése kötelező, és az értéke: CA = "TRUE".

  A "pathLenConstraint" mező nem szerepelhet a végfelhasználói tanúsítványokban.

  Köztes és gyökér hitelesítő egység tanúsítványban szerepelhet a PathLenConstraint mező.

- Kulcshasználat (Key Usage) – kritikus
  OID: 2.5.29.15
  A kulcs engedélyezett használati körének meghatározása.

A különböző felhasználási célú tanúsítványok esetében a következő kulcshasználati bitek kerüljenek beállításra (más érték nem megengedett):

Tanúsítvány típus	keyUsage (kritikus)	ExtKeyUsage
autentikációs	digitalSignature, keyAgreement	clientAuth (1.3.6.1.5.5.7.3.2)
aláírói	nonRepudiation, digitalSignature	emailProtection (1.3.6.1.5.5.7.3.4)
Cisco VPN client	digitalSignature, keyAgreement, keyEncipherment	clientAuth (1.3.6.1.5.5.7.3.2), ipsecEndSystem (1.3.6.1.5.5.7.3.5), 1.3.6.1.5.5.8.2.2,
Cisco VPN Server	digitalSignature, keyAgreement, keyEncipherment	serverAuth (1.3.6.1.5.5.7.3.1), 1.3.6.1.5.5.7.3.5, 1.3.6.1.5.5.8.2.2
kódaláírói	nonRepudiation, digitalSignature	1.3.6.1.5.5.7.3.3, 1.3.6.1.4.1.311.2.1.22
DomaiController	digitalSignature, keyEncipherment	clientAuth (1.3.6.1.5.5.7.3.2), serverAuth (1.3.6.1.5.5.7.3.1)
Titkosító	keyEncipherment, dataEncipherment	emailProtection (1.3.6.1.5.5.7.3.4)
RDP Gateway	keyEncipherment, dataEncipherment	serverAuth (1.3.6.1.5.5.7.3.1)
SCEP server	digitalSignature, keyEncipherment, dataEncipherment	
Smartcardlogon	digitalSignature, keyEncipherment	clientAuth (1.3.6.1.5.5.7.3.2),1.3.6.1.4.1.311.20.2.2
VPN Server	digitalSignature, keyAgreement, keyEncipherment	1.3.6.1.5.5.7.3.1
Webserver	digitalSignature, keyEncipherment, keyAgreement	serverAuth (1.3.6.1.5.5.7.3.1)
Hitelesítő egység (CA)	keyCertSign, cRLSign	
Időbélyegző egység (TSA)	nonRepudiation, digitalSignature	timeStamping (1.3.6.1.5.5.7.3.8)
OCSP válaszadó		ocspsigning (1.3.6.1.5.5.7.3.9)

- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus
  A kulcs engedélyezett használati körének további meghatározása.

A különböző felhasználási célú tanúsítványok esetében az előző táblázatban feltüntetett kiterjesztett kulcshasználati bitek kerüljenek beállításra (más érték nem megengedett). Gyökér és köztes hitelesítő egységek tanúsítványaiban nem szerepelhet.

- CRL szétosztási pont (CRL Distribution Points) – nem kritikus
  OID: 2.5.29.31
  Végfelhasználói tanúsítványok és köztes hitelesítő egységek tanúsítványai esetében kötelező a kitöltése és a mező tartalmazza a tanúsítvánnyal kapcsolatban releváns CRL elérhetőségét http és/vagy ldap protokollon keresztül. Gyökér hitelesítő egységek esetében a mező kitöltése opcionális.

- 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 tanúsítványok és köztes hitelesítő egységek tanúsítványai esetében 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 kell nyújtson. Ennek elérhetőségét kell itt szerepeltetni.
  - A tanúsítványlánc felépítésének megkönnyítésére a *Hitelesítés-szolgáltató* adja meg a *Tanúsítvány*t kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.
    Gyökér hitelesítő egységek esetében a mező kitöltése opcionális.

- Minősített tanúsítvánnyal kapcsolatos állítások (Qualified Certificate Statements) – Kritikus
  OID: 1.3.6.1.5.5.7.1.3
  A mező ne szerepeljen a végfelhasználói *Tanúsítvány*okban, illetve a gyökér és köztes hitelesítő egységek *Tanúsítvány*aiban.

Más tanúsítvány kiterjesztés nem kerülhet kitöltésre.

7.1.3. Az algoritmus objektum azonosítója

Annak az algoritmusnak a megnevezése, amellyel a tanúsítvány hitelesítésre került. Csak olyan aláíró algoritmus használható, amely megfelel a Nemzeti Média- és Hírközlési Hatóságnak az Eat. 18. § [1] szerinti felhatalmazása alapján kibocsátott, engedélyezett algoritmusokat és minimális kulcsméreteket meghatározó határozatának. A *Hitelesítés-szolgáltató* által használható algoritmusokat a Szolgáltatási szabályzatban fel kell sorolni.

7.1.4. Névformák

A *Hitelesítés-szolgáltató* a jelen *Hitelesítési rend*ek alapján kibocsátott *Tanúsítvány*okban egy – az RFC 5280 szabványban [5] meghatározott attribútumokból összeállított – megkülönböztetett nevet kell használjon az *Alany* azonosítására. A *Tanúsítvány*nak tartalmaznia kell az *Alany* globálisan egyedi azonosítóját is (OID), a 3.1.1 -es fejezetben meghatározottak szerint kitöltve.

A tanúsítvány Issuer DN mezőjében szereplő értéknek meg kell egyeznie a kibocsátó tanúsítványának Subject DN mezőjében szereplő értékkel.

7.1.5. Névhasználati megkötöttségek

A *Hitelesítés-szolgáltató* igény esetén használhat névhasználati megkötéseket a "nameConstraints" mező felhasználásával. Ebben az esetben ezt a mezőt kritikusnak kell megjelölni.

7.1.6. A Hitelesítési rend objektum azonosítója

A *Hitelesítés-szolgáltató*nak a jelen *Hitelesítési rend*ek alapján kibocsátott *Tanúsítvány*okba fel kell vennie 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 mezőnek tartalmaznia kell a *Szolgáltatási szabályzat* on-line 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 RFC 5280 [5] specifikáció szerinti "v2" verziójú tanúsítvány visszavonási listákat bocsásson ki.

7.2.2. Tanúsítvány visszavonási lista kiterjesztések

A *Hitelesítés-szolgáltató* által kibocsátott tanúsítvány visszavonási listák kötelezően tartalmazzák az alábbi mezőket:

- Verzió (Version)
  A mező értéke kötelezően "1" legyen.
- Algoritmus azonosító (Signature Algorithm Identifier)
  A visszavonási listát hitelesítő elektronikus aláírás készítéséhez használt algoritmuskészlet azonosítója (OID). A minimálisan támogatandó algoritmuskészletek:
  - " sha256WithRSAEncryption".
- Aláírás (Signature)
  A *Hitelesítés-szolgáltató* visszavonási listát hitelesítő elektronikus aláírása.
- Kibocsátó (Issuer)
  A visszavonási listát kibocsátó hitelesítő egység egyedi azonosítója. A visszavonási listát az adott hitelesítő egység a *Tanúsítvány*ok aláírására használt kulcsával kell hitelesítse.
- Hatálybalépés (Effective Date)
  A visszavonási lista hatálybalépésének kezdete. UTC szerinti érték az RFC 5280 [5] szerinti kódolással.
- Következő kibocsátás (Next Update)
  A következő visszavonási lista kibocsátásának ideje (lásd: 4.10. fejezet). UTC szerinti érték az RFC 5280 [5] szerinti kódolással.
- Visszavont *Tanúsítvány*ok (Revoked Certificates)
  A felfüggesztett vagy visszavont *Tanúsítvány*ok listája a *Tanúsítvány* sorozatszámával és a felfüggesztés vagy visszavonás idejével.

A *Hitelesítés-szolgáltató* által kötelező jelleggel kitöltendő visszavonási lista kiterjesztések:

- CRL sorozatszám (CRL number) – nem kritikus
  Ebbe a mezőbe a visszavonási listák egyesével növekvő sorozatszámai kerüljenek.
- expiredCertsOnCRL – nem kritikus
  A *Hitelesítés-szolgáltató* az X.509 specifikáció szerinti szabványos jelöléssel jelezze, ha 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
  Ebbe a mezőbe a visszavonás oka kerülhet.

  Felfüggesztett *Tanúsítvány* esetén kötelezően kitöltendő mező,

  az értéke: "certificateHold (6)".

- Érvénytelenség ideje (Invalidity Date) – nem kritikus
  Ebbe a mezőbe a magánkulcs megbízhatatlanná válásának ideje kerülhet.

- Útmutató a felfüggesztett *Tanúsítvány*okhoz (Hold Instruction) – nem kritikus
  Ebbe a mezőbe a felfüggesztett *Tanúsítvány* kezelése kerülhet.

A *Hitelesítés-szolgáltató* a kiterjesztéseket nem köteles kitölteni.

7.3. Online tanúsítvány-állapot válasz (OCSP) profil

A *Hitelesítés-szolgáltató*nak az RFC 2560 [11] és RFC 6960 [12] szerinti online tanúsítvány-állapot szolgáltatást kell üzemeltetnie.

7.3.1. Verziószám(ok)

A *Hitelesítés-szolgáltató*nak támogatnia kell az RFC 2560 [11] és RFC 6960 [12] szerinti "v1" verziójú online tanúsítvány-állapot kéréseket és válaszokat.

7.3.2. OCSP kiterjesztések

Nincs megkötés.

8. A megfelelőség vizsgálata

A *Hitelesítés-szolgáltató* tevékenységét az Európai Uniós szabályozással összhangban a Nemzeti Média- és Hírközlési Hatóság felügyeli. A Nemzeti Média- és Hírközlési Hatóság minimum éves rendszerességgel helyszíni szemlét tart a *Hitelesítés-szolgáltató* telephelyén, a helyszíni szemle előtt a *Hitelesítés-szolgáltató* köteles külső auditor igénybevételével átvilágíttatni üzemeltetését és az átvilágításról készült részletes jelentést a Nemzeti Média- és Hírközlési Hatóság számára előzetesen megküldeni. Az átvizsgálás során azt kell megállapítani, hogy a *Hitelesítés-szolgáltató* működése megfelel-e az alkalmazott *Hitelesítési rend*(ek)ben és az ennek megfelelő *Szolgáltatási szabályzat*(ok)ban támasztott követelményeknek.

Az átvilágítás tematikája és módszertana feleljen meg az alábbi szabványoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 1999/93/EK IRÁNYELVE (1999. december 13.) az elektronikus aláírással kapcsolatos közösségi keretrendszerről (hatályon kívül helyezve 2016. július 1-től) [13];
- 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 [14];
- A webszerver tanúsítványok kibocsátása vonatkozásában a CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [18];
- ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates V2.4.1 (2013-02) [20];

Az átvilágítás eredménye bizalmas dokumentum, csak az arra jogosultak számára hozzáférhető.

A Microsec fenntartja a jogot, hogy a jelen *Hitelesítési rend*ek alapján működő szolgáltatók tevékenységét tetszőleges időpontban független szakértő bevonásával átvizsgálja a követelmények betartásának ellenőrzése érdekében.

8.1. Az ellenőrzések körülményei és gyakorisága

A *Hitelesítés-szolgáltató* évente köteles elvégeztetni az átvilágítást.

Amennyiben a *Hitelesítés-szolgáltató* külső Regisztrációs szervezettel működik együtt, akkor annak folyamatait évente auditálni kell.

Más *Hitelesítés-szolgáltató* által felügyelt hitelesítési egység számára kibocsátott *Tanúsítvány* esetében a külső hitelesítés-szolgáltató működését évente auditálni kell.

8.2. Az auditor és szükséges képesítése

A *Hitelesítés-szolgáltató* a belső auditokat a független rendszervizsgáló szerepkörrel felruházott alkalmazottai segítségével is elvégezheti.

A külső auditot csak olyan személy végezheti, aki

- szerepel a Nemzeti Média- és Hírközlési Hatóság által vezetett és a weboldalán publikált független PKI szakértői névjegyzékben;
- rendelkezik valamelyik neves IT biztonsági vizsgáló testület érvényes tanúsítványával (pl. CISA);
- képes a 8. fejezetben megadott követelményrendszerek szerinti audit elvégzésére.

8.3. Az auditor és az auditált rendszerelem függetlensége

A külső auditot csak olyan személy végezheti, aki

- független a vizsgált *Hitelesítés-szolgáltató* tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- független a vizsgált szervezettől, vagyis sem saját maga, sem közvetlen hozzátartozója nincs munkaviszonyban vagy üzleti kapcsolatban a *Hitelesítés-szolgáltató*val.

8.4. Az auditálás által lefedett területek

Az átvizsgálásnak le kell fednie minimálisan 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* külső *Regisztráló szervezet*tel együttműködik, illetve ha bocsátott ki más *Hitelesítés-szolgáltató* hitelesítési egysége számára *Tanúsítvány*t, akkor a felsorolt területeket ezeknél a külső szervezeteknél is meg kell vizsgálni.

8.5. A hiányosságok kezelése

A független auditor az átvizsgálás eredményét egy részletes átvilágítási jelentésben kell összefoglalja, amely kitér a vizsgált rendszerelemekre, folyamatokra, tartalmazza az átvilágítás során felhasznált bizonyítékokat és vizsgálói megállapításokat. A jelentésben külön fejezetben kell rögzíteni 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 veendő módosítási javaslatokat;

- kötelezően elhárítandó eltéréseket.

A független auditornak a feltárt súlyos eltéréseket haladéktalanul jelentenie kell a Nemzeti Média- és Hírközlési Hatóságnak, aki jogosult meghozni a szükséges intézkedéseket.

A *Hitelesítés-szolgáltató* köteles a független vizsgáló által felvetett problémákra írásban válaszolni, az elhárításukra tett intézkedésekről a következő hatósági szemle alkalmával beszámolni.

A független auditornak a vizsgálati jelentést minden esetben meg kell küldenie a Nemzeti Média- és Hírközlési Hatóságnak.

8.6. Az eredmények közzététele

A *Hitelesítés-szolgáltató* nem köteles a független rendszervizsgálat során feltárt hiányosságok publikálására, azokat bizalmas információként kezelheti.

Az Nemzeti Média- és Hírközlési Hatóság által kiállított tanúsítási igazolást nyilvánosságra kell hozni a vizsgálat lezárását követően 3 hónapon belül.

8.7. Belső ellenőrzések

A *Hitelesítés-szolgáltató* gondoskodjon belső folyamatainak rendszeres ellenőrzéséről, ennek részleteit a *Szolgáltatási szabályzat*ban illetve belső szabályzataiban rögzítse. Legalább évente egyszer egy átfogó audit során ellenőrizze a működés megfelelőségét.

Negyedévente ellenőrizni kell szúrópróbaszerűen, az előző ellenőrzés óta kibocsátott webszerver tanúsítványok legalább 3 % -át, hogy megfelel-e a vonatkozó hitelesítési rendnek és szolgáltatási szabályzatnak.

9. Egyéb üzleti és jogi kérdések

9.1. Díjak

A *Hitelesítés-szolgáltató* által alkazmazható díjakat a vonatkozó szabályzásnak megfelelően nyilvánosan elérhetővé kell tenni az *Előfizető*k részére.

9.1.1. Tanúsítvány kibocsátás és megújítás díjai

A *Hitelesítés-szolgáltató* díjat állapíthat meg a *Tanúsítvány*ok kibocsátásával, megújításával, módosításával és a kulcscserével kapcsolatos tevékenységéért.

9.1.2. Tanúsítvány hozzáférés díja

A *Hitelesítés-szolgáltató* ingyenesen köteles az *Érintett felek* részére on-line hozzáférést biztosítani a *Tanúsítványtár*hoz.

9.1.3. Visszavonási állapot információ hozzáférés díja

A *Hitelesítés-szolgáltató* ingyenesen köteles az *Érintett felek* részére on-line CRL és OCSP információt szolgáltatni a kibocsátott *Tanúsítvány*ok visszavonási állapotáról.

9.1.4. Egyéb szolgáltatások díjai

A *Hitelesítés-szolgáltató* szolgáltatási díjat állapíthat meg az *Előfizető*k részére nyújtott egyéb szolgáltatásokért.

9.1.5. Visszatérítési politika

Nincs megkötés.

9.2. Anyagi felelősségvállalás

A *Hitelesítés-szolgáltató*nak az elektronikus aláírások ellenőrzése céljából kibocsátott *Tanúsítvány*ok kibocsátásával kapcsolatos tevékenysége nyújtása során meg kell felelnie a 3/2005. IHM rendeletben [8] meghatározott felelősségvállalásra vonatkozó követelményeket.

9.2.1. Pénzügyi követelmények

Nincs megkötés.

9.2.2. További követelmények

Nincs megkötés.

9.2.3. Felelősségbiztosítás

A 3/2005. IHM rendelet [8] 11. § rendelkezései szerint az elektronikus aláírások ellenőrzése céljából kibocsátott *Tanúsítvány*ok esetén:

- A *Hitelesítés-szolgáltató*nak a megbízhatóság biztosítása érdekében felelősségbiztosítással kell rendelkeznie.

- A felelősségbiztosítási szerződésnek ki kell terjednie az alábbi, a szolgáltató által a szolgáltatások nyújtásával összefüggésben okozott károkra:
  - az elektronikus aláírással, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra;
  - az elektronikus aláírással, illetve az ezzel ellátott elektronikus dokumentummal szerződésszegéssel okozott károkra;
  - az Eat. [1] 16. §-ának (4) bekezdésében foglaltak megszegésével a Nemzeti Média- és Hírközlési Hatóságnak okozott károkra.
- A felelősségbiztosítási szerződésnek egy biztosítási esemény vonatkozásában káreseményenként a *Tanúsítvány*ban, illetve a *Szolgáltatási szabályzat*ban vállalt felelősségvállalási érték legalább háromszorosáig kell fedezetet biztosítania az összes károsultnak okozott károkra. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.
- A felelősségbiztosításnak a 3/2005. IHM rendelet [8] 11. § (3) bekezdésben meghatározott összeg erejéig fedezetet kell nyújtania 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*nak az *Ügyfel*ek adatait a jogszabályoknak megfelelően kell kezelnie.

9.3.1. Bizalmas információk köre

A *Hitelesítés-szolgáltató*nak a *Szolgáltatási szabályzat*ában pontosan meg kell határoznia, hogy mely adatok minősülnek bizalmas információnak.

9.3.2. Bizalmas információk körén kívül eső adatok

A *Hitelesítés-szolgáltató* nyilvánosnak tekinthet miden olyan adatot, amely nem szerepel a bizalmas adatok felsorolásában a *Szolgáltatási szabályzat*ban. Nyilvános adatnak tekintendők például

- a *Tanúsítvány*ban szereplő valamennyi adat,
- a *Tanúsítvány*ok állapotával kapcsolatos adatok.

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 kell kötelezze alkalmazottait, alvállalkozóit, szerződött partnereit a bizalmas adatok védelmére.

A *Hitelesítés-szolgáltató Szolgáltatási szabályzat*ában tételesen meg kell határozni azon eseteket, amikor a *Hitelesítés-szolgáltató* felfedheti a bizalmas adatokat. Ilyen esetek például:

- kötelező információszolgáltatás a felügyelő hatóság részére,
- információszolgáltatás polgári peres eljárás keretében,
- az érintett kérésére történő adatszolgáltatás.

9.4. Személyes adatok védelme

A *Hitelesítés-szolgáltató*nak gondoskodnia kell az általa kezelt személyes adatok védelméről. Működésének és szabályzatainak meg kell felelniük az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [15] rendelkezéseinek.

A *Hitelesítés-szolgáltató* köteles az *Ügyfél*ről nyilvántartott személyes adatokat és információkat a jogszabályi előírásoknak megfelelően

- megőrizni,
- a szolgáltatási szerződés megszűnésekor az *Ügyfél* kérésére az ügyfél adatbázisából törölni.

Az *Ügyfél* olyan adatok törlését kérheti, amelyek megőrzését nem írja elő vonatkozó jogszabály.

9.4.1. Adatkezelési szabályzat

A *Hitelesítés-szolgáltató*nak rendelkeznie kell Adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a személyes információk kezelésére. Az Adatkezelési szabályzatot nyilvánosságra kell hozni a *Hitelesítés-szolgáltató* honlapján.

9.4.2. Személyes adatok

A *Hitelesítés-szolgáltató*nak védenie kell 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.

Az Eat. [1] 11. § (1) szerint a *Hitelesítés-szolgáltató* csak az *Alany*tól közvetlenül, vagy annak egyértelmű előzetes hozzájárulásával gyűjthet személyes adatokat és csak olyan mértékben, ami a *Tanúsítvány* kiadásához szükséges.

9.4.3. Személyes adatnak nem minősülő adatok

A *Hitelesítés-szolgáltató* az *Alany*ok írásbeli hozzájárulása alapján nyilvánosságra hozhatja az *Alany*ok *Tanúsítvány*ban szereplő adatait. A *Tanúsítvány*ban a *Hitelesítés-szolgáltató* feltünteti az *Alany* személyéhez rendelt globálisan egyedi azonosítót (OID-et).

9.4.4. Adatbiztonság

A *Hitelesítés-szolgáltató* köteles biztonságosan tárolni és védeni a tanúsítvány kiadással kapcsolatos és a *Tanúsítvány*ban nem szereplő személyes adatokat. Az adatokat megfelelő intézkedésekkel védeni kell 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 hozhatja 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 az Eat. [1] 11. §-ában meghatározott esetekben.

9.4.7. Egyéb adatvédelmi követelmények

Nincs előírás.

9.5. Szellemi tulajdonjogok

A *Hitelesítés-szolgáltató* működése során nem sértheti meg harmadik személyek szellemi tulajdonjogait.

A *Hitelesítés-szolgáltató* által ügyfelei részére kibocsátott magán- és nyilvános kulcs tulajdonosa az *Előfizető*, teljes jogú felhasználója pedig az *Alany*, 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 *Alany*. A *Hitelesítés-szolgáltató* az általa kibocsátott végfelhasználói tanúsítványokat 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 hozhat a *Szolgáltatási szabályzat*ban meghatározott módon.

A *Hitelesítés-szolgáltató* által az *Ügyfel*ek részére kibocsátott egyedi azonosító (OID) a *Hitelesítés-szolgáltató* tulajdonát képezi, amit a *Hitelesítés-szolgáltató* nyilvánosságra hozhat a *Tanúsítvány* részeként.

A *Tanúsítvány*ban szereplő azonosító (amely a *Tanúsítvány* alanyát azonosítja) használatára a megnevezett *Alany*, illetve *Ügyfél* jogosult.

A jelen *Hitelesítési rend* a Microsec kizárólagos tulajdonát képezi. Az *Ügyfel*ek, *Alany*ok és egyéb *Érintett felek* a dokumentumot csak a *Hitelesítési rend* előírásainak megfelelően jogosultak felhasználni, minden egyéb kereskedelmi vagy egyéb célú felhasználás szigorúan tilos. A *Hitelesítési rend* szabadon terjeszthető, de csak változatlan formában, teljes terjedelemben és az eredet feltüntetésével.

A *Hitelesítés-szolgáltató* által a szolgáltatás igénybevételéhez biztosított szoftverek használatának szabályait a *Szolgáltatási szabályzat*ban kell meghatározni.

9.6. Tevékenységért viselt felelősség és helytállás

9.6.1. A Hitelesítés-szolgáltató felelőssége és helytállása

A *Hitelesítés-szolgáltató* felel a jelen *Hitelesítési rend*ben, a vonatkozó *Szolgáltatási szabályzat*ban valamint az *Ügyfél*lel kötött szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért.

A *Hitelesítés-szolgáltató* sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért.

A *Hitelesítés-szolgáltató* a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a Polgári Törvénykönyv [16] általános felelősségi szabálya szerint, az Alannyal szemben pedig a szerződésszegésért való felelősség szabályai szerint felelős a minősített elektronikus aláírással, illetve az elektronikusan aláírt elektronikus dokumentummal okozott kárért az Eat-ban [1] meghatározott szabályok megszegése esetén.

A *Hitelesítés-szolgáltató* a felelősségi körében keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel kötött szolgáltatási szerződésben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása).

9.6.2. A regisztrációs szervezet felelőssége és helytállása

A *Hitelesítés-szolgáltató* megköveteli a vele együttműködő *Regisztráló szervezet*ektől a jelen *Hitelesítési rend* és a vonatkozó *Szolgáltatási szabályzat* előírásainak maradéktalan betartását.

A *Regisztráló szervezet* felelőssége:

- az *Alany*ok személyazonosságának megállapítása;
- a *Képviselt szervezet* szervezeti azonosságának, a *Képviselt szervezet* nevében eljáró személy személyazonosságának és képviseleti jogosultságának megállapítása;
- a felvett regisztrációs adatok valódiságának garantálása;
- a szolgáltatási szerződés megkötését megelőzően a szolgáltatások igénybe vevőjének tájékoztatása a *Hitelesítési rend* és a *Szolgáltatási szabályzat* tartalmáról és elérhetőségéről, a szolgáltatás igénybevételének feltételeiről;
- általában kötelezettségeinek maradéktalan betartása.

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* kötelessége a *Hitelesítés-szolgáltató* szerződéses feltételeinek és szabályzatainak megfelelően eljárni a hitelesítés-szolgáltatás igénybevétele során, beleértve a *Tanúsítvány*ok és magánkulcsok igénylését és alkalmazását. Az *Előfizető* kötelezettségeit a jelen *Hitelesítési rend*, a szolgáltatási szerződés és annak mellékletei – különösen az általános szerződési feltételek – és a *Szolgáltatási szabályzat* írja le.

Az *Alany* felelőssége

Az *Alany* felelős:

- a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért;

- a *Tanúsítvány*ában szereplő adatok ellenőrzéséért,
- az adataiban bekövetkezett változások haladéktalan bejelentéséért;
- magánkulcsának, *Aláírás-létrehozó eszköz*ének és *Tanúsítvány*ának a szabályzatoknak megfelelő felhasználásáért;
- magánkulcsának és aktivizáló kódjának biztonságos kezeléséért;
- az *Aláírás-létrehozó eszköz*e biztonságos kezeléséért ;
- a *Hitelesítés-szolgáltató* haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyekben;
- általában a kötelezettségei betartásáért.

Az *Alany* kötelezettségei

Az *Alany* köteles:

- a szolgáltatás igénybevétele előtt megismerni a jelen *Hitelesítési rend*et és a *Szolgáltatási szabályzat*ot;
- a *Hitelesítés-szolgáltató* által kért, a szolgáltatás igénybevételéhez szükséges adatokat hiánytalanul megadni, a valóságnak megfelelő adatokat szolgáltatni;
- amennyiben az *Alany* 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* felfüggesztését vagy visszavonását és
  - megszüntetni a *Tanúsítvány* használatát;
- a szolgáltatást kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a hivatkozott szabályzatokban, a hivatkozott dokumentumokban foglaltaknak megfelelően használni;
- Webszerver tanúsítvány esetében a *Tanúsítvány*t kizárólag olyan szerverre telepíteni, amely a *Tanúsítvány*ban szereplő domain néven 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, a szolgáltatással kapcsolatos elektronikus aláírással, illetve 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;
- amennyiben az *Alany* magánkulcsa, *Aláírás-létrehozó eszköz*e vagy az eszköz aktiválásához szükséges titkos kódok illetéktelen kezekbe kerültek vagy megsemmisültek, az *Alany* ezt köteles haladéktalanul jelezni a *Hitelesítés-szolgáltató*nak, kezdeményezni a *Tanúsítvány*ok felfüggesztését vagy visszavonását és megszüntetni a *Tanúsítvány* használatát;
- kulcs kompromittálódás vagy nem jogszerű használat gyanújának felmerülése esetében a *Hitelesítés-szolgáltató* megkereséseire az *Alany* köteles a *Hitelesítés-szolgáltató* által megadott időn belül reagálni;
- tudomásul venni, hogy az *Előfizető* jogosult a *Tanúsítvány* visszavonását vagy felfüggesztését kérni;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a *Tanúsítvány*t a *Szolgáltatási szabályzat*ban leírt meghatározott módon, az ott leírt ellenőrzési lépések elvégeztével 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 az aláírás-létrehozó adat nem az *Alany* kizárólagos birtokában vagy használatában van, és ebben az esetben az *Alany* köteles a *Tanúsítvány* használatát beszüntetni;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* jogosult a *Tanúsítvány*t felfüggeszteni, illetve 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 felfüggeszteni illetve visszavonni, amennyiben az *Előfizető* megszegi a szolgáltatási szerződést vagy a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t illegális tevékenységhez (pl. adathalászat, csalás, kártékony programok terjesztése) használták.

A *Szolgáltatási szabályzat* további kötelezettségeket tartalmazhat az *Alany* számára.

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 jelen *Hitelesítési rend*ben és a vonatkozó *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 figyelembe vétele, amely a *Tanúsítvány*ban, a *Hitelesítési rend*ben és a *Szolgáltatási szabályzat*ban szerepel.

9.6.5. Egyéb szereplők tevékenységéért viselt felelősség és helytállás

A *Képviselt szervezet* felelősséggel tartozik az általa kiadott igazolásokért, különös tekintettel azon igazolásokra, amelyben azt igazolja, hogy az *Alany* jogosult a *Szervezet* nevét is tartalmazó *Tanúsítvány* használatára .

9.7. Helytállás érvénytelenségi köre

A *Hitelesítés-szolgáltató* kizárja felelősségét, amennyiben

- az *Érintett fél* nem körültekintően jár el a *Tanúsítvány*ok felhasználása vagy ellenőrzése során, azaz nem a jelen *Hitelesítési rend*, a *Szolgáltatási szabályzat* vagy a hatályos jogszabályok szerint jár el;
- az *Alanyok* nem tartják be a magánkulcs, illetve aláírás-létrehozó eszköz kezelésével kapcsolatos előírásokat;

- az *Érintett felek* vagy mások által kibocsátott szabályzatok nem felelnek meg a jelen *Hitelesítési rend*nek vagy a *Szolgáltatási szabályzat*nak;
- 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 által elfogadott kriptográfai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8. A felelősség korlátozása

A *Hitelesítés-szolgáltató* korlátozhatja a kártérítési felelősségét

- *Tanúsítvány*onként,
- a tanúsítvánnyal egy alkalommal vállalható kötelezettség legmagasabb mértékében (tranzakciós limit),
- összességében az összes tanúsítvánnyal és káreseménnyel kapcsolatban.

9.9. Kártérítési kötelezettség

9.9.1. A *Hitelesítés-szolgáltató* kártérítési kötelezettsége

A *Hitelesítés-szolgáltató* kártérítési kötelezettségének részletes szabályait a *Szolgáltatási szabályzat*, a szolgáltatási szerződés vagy az *Ügyfel*ekkel kötött szerződések tartalmazzák.

9.9.2. Az *Előfizető* kártérítési kötelezettsége

A *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzat*ban és a szolgáltatási szerződésben szabályozza az *Előfizető*kkel szemben támasztott kártérítési igényeit.

9.9.3. Az *Érintett felek* kártérítési kötelezettsége

A *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzat*ban szabályozza az *Érintett felek*kel szemben támasztott kártérítési igényeit.

9.10. Érvényesség és megszűnés

9.10.1. Érvényesség

A *Hitelesítési rend* adott verziója hatályba lépésének napja a *Hitelesítési rend* címlapján kerül meghatározásra.

9.10.2. Megszűnés

A *Hitelesítési rend* visszavonásig érvényes időbeli korlátozás nélkül.

9.10.3. A megszűnés következményei

A *Hitelesítési rend* 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 *Hitelesítési rend* 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 működtessen ügyfélszolgálati irodát.

9.12. Módosítások

A Microsec fenntartja magának a jogot, hogy a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén szabályozott módon megváltoztassa a *Hitelesítési rend*et.

Rendkívüli esetben (pl. kritikus biztonsági intézkedések meghozatalának szükségessége) a változások azonnali hatállyal is életbe léptethetők.

9.12.1. Módosítási eljárás

A Microsec évi rendszerességgel illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja a *Hitelesítési rend*et és elvégzi a szükségesnek tartott változtatásokat. A *Hitelesítési rend* a legkisebb változtatás után is új verziószámot kap és az elfogadási procedúra időigényét figyelembe véve meghatározásra kerül a tervezett hatálybalépés időpontja is.

A jóváhagyott dokumentum legalább 30 nappal a tervezett hatálybalépés előtt publikálásra kerül a Microsec honlapján és megküldésre kerül véleményezésre a Nemzeti Média- és Hírközlési Hatóság részére. Érdemi változtatást igénylő észrevétel esetén a dokumentum változtatásra kerül és újra indul az elfogadási folyamat.

9.12.2. Értesítések módja és határideje

A Microsec 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 *Hitelesítési rend* 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 dokumentumnak nem lehet azonos OID azonosítója.

9.13. Vitás kérdések rendezése

A *Hitelesítés-szolgáltató* törekedjen a működése során felmerülő vitás kérdések békés, tárgyalásos rendezésére. A rendezés során a fokozatosság elvét kell követni.

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 jelen *Hitelesítési rend* megfelel az alábbi jogszabályoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 1999/93/EK IRÁNYELVE (1999. december 13.) az elektronikus aláírással kapcsolatos közösségi keretrendszerről (hatályon kívül helyezve 2016. július 1-től) [13];
- 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 [14];
- 2001. évi XXXV. törvény az elektronikus aláírásról;
- 78/2010. (III. 25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól;
- 45/2005 (III. 11) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól;
- 4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról;
- 9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról;

- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről;
- 7/2002 (IV.26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről;
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról;
- 2013. évi V. törvény a Polgári Törvénykönyvről.

9.16. Vegyes rendelkezések

9.16.1. Teljességi záradék

Nincs megkötés.

9.16.2. Átruházás

A jelen *Hitelesítési rend*(ek)nek megfelelően működő szolgáltatók csak a Microsec zrt. előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3. Részleges érvénytelenség

A jelen *Hitelesítési rend* 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 *Hitelesítési rend* 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 követelmény hibás vagy késedelmes teljesítéséért, amennyiben a hiba vagy késedelem oka a *Hitelesítés-szolgáltató* ellenőrzési körén kívül eső körülmény volt.

9.17. Egyéb rendelkezések

Nincs megkötés.

A. Hivatkozások

[1] 2001. évi XXXV. törvény az elektronikus aláírásról.

[2] Common Criteria for Information Technology Security Evaluation, Part 1 - 3.

[3] CEN CWA 14169: Secure signature-creation devices "EAL 4+", March 2004.

[4] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.

[5] RFC 5280: X.509 Internet Public Key Infrastructure – Certificate and Certificate revocation List (CRL) Profile, May 2008.

[6] RFC 6818 (Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile).

[7] RFC 4043: Internet X.509 public Key Infrastructure - permanent Identifier, May 2005.

[8] 3/2005. (III.18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.

[9] MSZ/ISO/IEC 15408 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai, 2002 december.

[10] ETSI TS 101 862 Qualified Certificate Profile V1.3.3 (2006-01).

[11] RFC 2560: X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol (OCSP), June 1999.

[12] RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.

[13] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 1999/93/EK IRÁNYELVE (1999. december 13.) az elektronikus aláírással kapcsolatos közösségi keretrendszerről (hatályon kívül helyezve 2016. július 1-től).

[14] 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.

[15] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

[16] 2013. évi V. törvény a Polgári Törvénykönyvről.

[17] 78/2010. (III. 25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól.

[18] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.0. CA/Browser Forum, `https://cabforum.org/wp-content/uploads/CAB-Forum-BR-1.3.0.pdf`, 2015.

[19] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.

[20] ETSI TS 102 042; Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates V2.4.1 (2013-02).

[21] RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.

[22] ITU X.509 Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks.