MICROSEC

e-Szignó Hitelesítés Szolgáltató

Nem minősített elektronikus aláírás hitelesítés szolgáltatásra és aláírás-létrehozó eszközön aláíró adat elhelyezése szolgáltatásra vonatkozó Szolgáltatási szabályzat

ver. 1.0

Hatályba lépés: 2015-10-05

Azonosító	1.3.6.1.4.1.21528.2.1.1.65.1.0
Verzió	1.0
Első verzió hatálybalépése	2015-10-05
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2015-09-23
Hatálybalépés dátuma	2015-10-05

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

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Új dokumentum az Rfc 3647 szerint. OID: 1.3.6.1.4.1.21528.2.1.1.65.1.0	2015-10-05	Szabóné Endrődi Csilla, Dr. Szőke Sándor

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zrt. (továbbiakban: Microsec vagy *Hitelesítés-szolgáltató*) által üzemeltetett e-Szignó Hitelesítés Szolgáltató nem minősített hitelesítés és eszköz szolgáltatására vonatkozó *Szolgáltatási szabályzat*a.

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

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

1.1. Áttekintés

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

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

Jelen dokumentum feladata továbbá, hogy segítségével a *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány*ok, tanúsítvány visszavonási listák, online tanúsítvány-állapot válaszok használói és elfogadói egyértelműen meg tudják állapítani azok kezelésének módját, az általuk garantált biztonság mértékét, valamint a rájuk vonatkozó technikai, üzleti és pénzügyi garanciákat és jogi felelősségvállalásokat.

Jelen dokumentum tartalmilag és formailag megfelel az RFC 3647 [26] 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 *Hitelesítés-szolgáltató* nem ír elő követelményt, ilyen esetben a fejezetben a "Nincs megkötés" szöveg szerepel.

Felhívjuk a végfelhasználók figyelmét, hogy az igénybe vett szolgáltatással kapcsolatos tevékenységükre vonatkozó előírásokat jelen *Szolgáltatási szabályzat*on kívül az általános szerződési feltételek, a szolgáltatóval kötött szolgáltatási szerződés, a *Hitelesítés-szolgáltató* által

alkalmazott *Hitelesítési rend*ek (lásd: 1.2.1. fejezet), az *Időbélyegzési rend* [1] illetve egyéb, a *Hitelesítés-szolgáltató*tól független szabályzat illetve dokumentum is tartalmazhat.

1.2. Dokumentum neve és azonosítója

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	Nem minősített elektronikus aláírás hitelesítés szolgáltatásra és aláírás-létrehozó eszközön aláíró adat elhelyezése szolgáltatásra vonatkozó Szolgáltatási szabályzat
Dokumentum verziószáma	1.0
Hatályba lépés ideje	2015-10-05

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

1.2.1. Hitelesítési rendek

A *Hitelesítés-szolgáltató* által kibocsátott valamennyi *Tanúsítvány* hivatkozik arra a *Hitelesítési rend*re, amely alapján a kibocsátás történt. A *Hitelesítési rend*eket azonosító OID első hét száma a Microsec egyedi azonosítója az alábbiak szerint:

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

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

(1.3.6.1.4.1.21528)	MICROSEC Ltd.
(2)	EHSZ Szolgáltatás
(1)	dokumentumok

(1)	nyilvános dokumentumok
(x)	dokumentum egyedi azonosító sorszáma
(y)	dokumentum verziója
(z)	dokumentum alverziója

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

OID	MEGNEVEZÉS	RÖVID NÉV
1.3.6.1.4.1.21528.2.1.1.49.1.0	Nem minősített elektronikus aláírás létrehozására és ellenőrzésére szolgáló, III. hitelesítési osztályba tartozó, természetes személyek számára *Hardver kriptográfiai eszköz*ön kibocsátott tanúsítványokat szabályozó, álnevet kizáró hitelesítési rend.	NASzTH
1.3.6.1.4.1.21528.2.1.1.50.1.0	Nem minősített elektronikus aláírás létrehozására és ellenőrzésére szolgáló, III. hitelesítési osztályba tartozó, természetes személyek számára szoftveresen kibocsátott tanúsítványokat szabályozó, álnevet kizáró hitelesítési rend.	NASzTSz
1.3.6.1.4.1.21528.2.1.1.51.1.0	Nem minősített elektronikus aláírás létrehozására és ellenőrzésére szolgáló, III. hitelesítési osztályba tartozó, nem természetes személyek számára *Hardver kriptográfiai eszköz*ön kibocsátott tanúsítványokat szabályozó, álnevet kizáró hitelesítési rend.	NASzNH
1.3.6.1.4.1.21528.2.1.1.52.1.0	Nem minősített elektronikus aláírás létrehozására és ellenőrzésére szolgáló, III. hitelesítési osztályba tartozó, nem természetes személyek számára szoftveresen kibocsátott tanúsítványokat szabályozó, álnevet kizáró hitelesítési rend.	NASzNSz

1.3.6.1.4.1.21528.2.1.1.53.1.0	Nem minősített elektronikus aláírás létrehozására és ellenőrzésére szolgáló, II. hitelesítési osztályba tartozó tanúsítványok kibocsátását szabályozó, álnevet kizáró hitelesítési rend.	NAN
1.3.6.1.4.1.21528.2.1.1.54.1.0	Nem minősített elektronikus aláírás létrehozására és ellenőrzésére szolgáló tanúsítványok kibocsátását szabályozó, álneves hitelesítési rend.	NAÁ

A felsorolt *Hitelesítési rend*ek részletes követelményeit az "e-Szignó Hitelesítés-Szolgáltató - Nem minősített aláíró tanúsítvány hitelesítési rendek ver. 1.0." [2] dokumentum tartalmazza.

Ezen *Hitelesítési rend*ek alapján a *Hitelesítés-szolgáltató* olyan *Tanúsítvány*okat bocsát ki, amelyek az Eat. [3] 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 *Hardver kriptográfiai 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 *Hardver kriptográfiai eszköz*ön 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 [21] tanúsítás a CEN SSCD PP [23] 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 [NASzTH], [NASzTSz], [NASzNH] és [NASzNSz] *Hitelesítési rend*ek alapján kiállított aláíró *Tanúsítvány*ok maradéktalanul megfelelnek a 78/2010. (III.25.) kormányrendelet [20] 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* a jogszabályi előírásoknak megfelelően biztosítja ezen *Tanúsítvány*ok esetében a személy azonosításához szükséges adatok elektronikus ellenőrizhetőségének lehetőségét (Lásd 4.13 fejezet).

A *Hitelesítés-szolgáltató* működése megfelel az ETSI TS 102 042 [24] (Nyilvános kulcsú tanúsítványokat kibocsátó hitelesítés szolgáltatókra vonatkozó policy követelmények) specifikációban foglaltaknak.

Jelen *Hitelesítési rend*ek közül az [NASzTH], az [NASzNH], az [NASzTSz] és az [NASzNSz] megfelel az ETSI TS 102 042-ben [24] definiált [NCP+] hitelesítési rendnek és az összes jelen *Hitelesítési rend* megfelel az [NCP] hitelesítési rendnek. Az [NAN] és az [NAÁ] hitelesítési rendek megfelelnek az [LCP] hitelesítési rendnek.

1.2.2. Hatály

Tárgyi hatály

A *Szolgáltatási szabályzat* az 1.3.1. fejezetben ismertetett szolgáltatások nyújtását és igénybevételét foglalja magában.

Időbeli hatály

A *Szolgáltatási szabályzat* jelen verziója a dokumentum címlapján feltüntetett hatálybalépési dátumtól visszavonásig hatályos. A hatályosság automatikusan megszűnik a szolgáltatások beszüntetésekor.

Jelen *Szolgáltatási szabályzat* hatályba lépésével egyidejűleg visszavonásra kerül az alábbi dokumentum:

"e-Szignó Hitelesítés Szolgáltató nem minősített elektronikus aláírás hitelesítés szolgáltatásra és nem minősített időbélyegzés szolgáltatásra vonatkozó szolgáltatási szabályzat ver. 4.3."

Személyi hatály

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

Területi hatály

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

1.3. PKI szereplők

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

- a Microsec e-Szignó Hitelesítés Szolgáltató,
- a Microsec e-Szignó Hitelesítés Szolgáltatóval szerződéses kapcsolatban álló *Regisztráló szervezet*ek,
- a Microsec e-Szignó Hitelesítés Szolgáltató *Ügyfel*ei (*Előfizető*k és *Aláíró*k),
- *Érintett felek*,
- egyéb szereplők.

1.3.1. Hitelesítés-szolgáltató

A *Hitelesítés-szolgáltató* adatai

Név:	Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság
Cégjegyzékszám:	01-10-047218 Fővárosi Törvényszék Cégbírósága
Székhely:	1031 Budapest, Záhony utca 7. D. épület
Telefonszám:	(+36-1) 505-4444
Telefax szám:	(+36-1) 505-4445
Internet cím:	`https://www.microsec.hu`, `https://www.e-szigno.hu`
LDAP címe:	`ldap://ldap.e-szigno.hu`

A szolgáltató egység neve:	e-Szignó Hitelesítés Szolgáltató
Ügyfélszolgálati iroda:	1031 Budapest, Záhony u. 7., Graphisoft Park, D épület
Ügyfélszolgálati iroda nyitvatartási ideje:	munkanapokon 9:00-16:30 között
Ügyfélszolgálati iroda telefonszáma:	(+36-1) 505-4444
Ügyfélszolgálati iroda e-mail címe:	`info@e-szigno.hu`
A szolgáltatással kapcsolatos információk elérése:	`https://www.e-szigno.hu`
Panaszok bejelentésének helye:	Microsec zrt. 1031 Budapest, Záhony u. 7., Graphisoft Park, D épület
Illetékes fogyasztóvédelmi felügyelőség:	Budapest Főváros Kormányhivatal Fogyasztóvédelmi Felügyelőség 1052 Budapest, Városház u. 7. 1364 Budapest, Pf. 144.

A *Hitelesítés-szolgáltató* bemutatása

A Microsec zrt. (illetve jogelődje, a Microsec Kft.) 2002. május 30. óta szerepel a Nemzeti Média- és Hírközlési Hatóság (illetve annak jogelődje, a továbbiakban: Hatóság) nyilvántartásában nem minősített szolgáltatóként a 2001. évi XXXV. törvényben meghatározott elektronikus aláírás hitelesítés-szolgáltatás, időbélyegzés és aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatás vonatkozásában. Regisztrációs szám: MH 6834 1/2002.

A Microsec 2005. május 15. óta minősített szolgáltatóként is szerepel a Hatóság nyilvántartásában elektronikus aláírás hitelesítés-szolgáltatás, időbélyegzés és eszköz szolgáltatás vonatkozásában.

A Microsec minősített elektronikus archiválás szolgáltatást nyújtó szolgáltatóként is szerepel a Hatóság nyilvántartásában. A nyilvántartásba vételről szóló határozat ügyiratszáma: HL-3549-2/2007, az elektronikus archiválás szolgáltatás indításának időpontja 2007. február 1.

Minőség és információbiztonság

A Microsec kiemelten fontosnak tartja *Ügyfel*ei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a *Hitelesítés-szolgáltató* ISO 9001 szabványnak megfelelő minőségirányítási rendszert üzemeltet 2002. január 23. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította. A Microsec nagy figyelmet szentel az általa üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a ISO/IEC 27001-nek megfelelő információbiztonság-

irányítási rendszert (korábban BS 7799) üzemeltet 2003. május 19. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A *Hitelesítés-szolgáltató* önkéntes akkreditációs rendszer keretében nem lett tanúsítva, mert ilyen rendszer Magyarországon még nem működik.

Hitelesítés szolgáltatást nyújtó üzletág

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

Szolgáltatások

A *Hitelesítés-szolgáltató* az alábbi Eat. [3] által meghatározott szolgáltatásokat nyújthatja az *Előfizető* számára jelen *Szolgáltatási szabályzat* keretében:

- nem minősített elektronikus aláírás hitelesítés szolgáltatás,
- aláírás-létrehozó eszközön az aláíró adat elhelyezése (a továbbiakban eszköz szolgáltatás).

A szolgáltatásokat a *Hitelesítés-szolgáltató* jelen *Szolgáltatási szabályzat* keretében nyújtja.

Elektronikus aláírás hitelesítés-szolgáltatás

A *Hitelesítés-szolgáltató* az elektronikus aláírás hitelesítés szolgáltatás nyújtása érdekében az *Előfizető*vel szolgáltatási szerződést köt, amelynek keretében az *Előfizető* által meghatározott *Aláíró*k számára elektronikus aláírás létrehozására alkalmas *Tanúsítvány*t bocsát ki. A *Tanúsítvány* hitelesen összekapcsolja az azonosított *Aláíró* adatait és az általa birtokolt aláírás-létrehozó adathoz tartozó nyilvános aláírás-ellenőrző adatot. Egy szolgáltatási szerződés keretében több *Aláíró*nak és több *Tanúsítvány* is kibocsátható

Elektronikus aláírás hitelesítés-szolgáltatás esetén az érvényes előfizetéssel rendelkező *Aláíró* a következő műveleteket kezdeményezheti:

- az *Aláíró* elektronikus aláírás létrehozására alkalmas *Tanúsítvány*t (illetve hozzá *Aláírás-létrehozó eszköz*t) igényelhet a *Hitelesítés-szolgáltató*tól, a *Tanúsítvány* kibocsátása valamely *Hitelesítési rend* vagy rendek szerint történik;

- az *Aláíró* kérheti a *Tanúsítvány*a visszavonását;
- az *Aláíró* kérheti *Tanúsítvány*a felfüggesztését, illetve visszaállítását.

Az *Előfizető* is kérheti a hozzá tartozó *Aláíró Tanúsítvány*ának visszavonását (illetve felfüggesztését, visszaállítását). Ezen műveleteket az *Előfizető* által erre feljogosított és a *Hitelesítés-szolgáltató*nál bejelentett ún. szervezeti ügyintéző is kérheti.

A *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*ok visszavonási állapotát tartalmazó visszavonási listákat nyilvánosan elérhetővé teszi. A *Hitelesítés-szolgáltató* magát a *Tanúsítvány*t is nyilvánosságra hozza, amennyiben az *Aláíró* ehhez hozzájárul. A visszavont, a felfüggesztett és a lejárt *Tanúsítvány* érvénytelen. Az érvénytelen *Tanúsítvány* alapján létrehozott aláíráshoz nem fűződik semmilyen joghatás.

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

Tanúsítványfajták

A jelen *Szolgáltatási szabályzat*ban támogatott *Hitelesítési rend*eket az 1.2.1. fejezetben mutatjuk be. Az alkalmazott *Hitelesítési rend* azonosítója minden esetben feltüntetésre kerül a *Tanúsítvány* "Certificate Policies" mezejében.

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

- Szervezeti *Tanúsítvány*ról beszélünk, ha a *Tanúsítvány* alanya Szervezet, vagy ha a *Tanúsítvány* egy természetes személy *Alany* valamely *Szervezet*hez való tartozását mutatja. Ilyen esetben a *Tanúsítvány* "O" mezejében a *Szervezet* neve feltüntetésre kerül. Az ilyet *Tanúsítvány* kizárólag az adott *Szervezet* által meghatározott módon használható. Természetes személy számára kibocsátott szervezeti tanúsítvány esetén a "Title" mezőben további korlátozások szerepelhetnek a *Tanúsítvány* használhatóságával kapcsolatban.
- Automata *Tanúsítvány*ról beszélünk, ha a *Tanúsítvány*ban az *Alany* adatai között feltüntetésre kerül az informatikai eszköz (alkalmazás, rendszer) elnevezése is, amely segítségével az *Alany* a *Tanúsítvány*t használja.
- Álneves *Tanúsítvány*ról beszélünk, ha a *Tanúsítvány*ban nem az *Alany* közhiteles nyilvántartásban szereplő hivatalos elnevezése szerepel. Az álneves *Tanúsítvány*okban a kért elnevezés a "Pseudonym" mezőben kerül feltüntetésre, és a "CN" mezőben feltüntetésre kerül, hogy a *Tanúsítvány* álnevet tartalmaz.
- Személyes *Tanúsítvány*ról akkor beszélhetünk, ha a *Tanúsítvány* sem "O", sem "Title" mezőt nem tartalmaz. Ilyen csak természetes személyek számára kerül kibocsátásra.

Az e-Szignó Hitelesítés Szolgáltató mind természetes személyek, mind jogi személyek vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezetek számára bocsát ki *Tanúsítvány*okat. Jogi személyek vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezetek számára igényelt *Tanúsítvány*ok esetében a képviseletre jogosult természetes személynek kell eljárnia a *Tanúsítvány* ügyében.

Teszt tanúsítványok

A *Hitelesítés-szolgáltató* – egyrészt saját rendszerének tesztelése céljából, másrészt azért, hogy harmadik felek tesztelhessék a szolgáltatásokat – teszt tanúsítványokat is kibocsát. A teszt tanúsítványokhoz semmilyen joghatás nem tartozik, és a *Hitelesítés-szolgáltató* sem kibocsátásukért, sem felhasználásukért, sem a hozzájuk kapcsolódó szolgáltatások rendelkezésre állásáért nem vállal felelősséget.

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

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

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

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

Eszköz szolgáltatás

Az eszköz szolgáltatás keretében a *Hitelesítés-szolgáltató* az *Alany Tanúsítvány*okhoz kapcsolódó aláírás-létrehozó adatát *Aláírás-létrehozó eszköz*ökön helyezi el.

Hitelesítő egységek

Az alábbiakban az e-Szignó Hitelesítés Szolgáltató rendszerében megjelenő, jelen *Szolgáltatási szabályzat* hatálya alá tartozó hitelesítő egységeit mutatjuk be. A *Hitelesítés-szolgáltató* tanúsítvány-hierarchiájáról a `https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/szolgaltatoi-tanusitvanyok.html` weboldalon található további információ.

A *Hitelesítés-szolgáltató* alábbi hitelesítő egységei bocsátanak ki *Tanúsítvány*okat:

- "Microsec e-Szigno Root CA 2009" – Gyökér hitelesítő egység, amely SHA-256 alapú *Tanúsítvány*okat bocsát ki a *Hitelesítés-szolgáltató* hitelesítő egységei részére. E hitelesítő egység önhitelesített tanúsítvánnyal (SHA-256 alapú) rendelkezik.
- "Qualified e-Szigno TSA ..." időbélyegző egységek, amelyeket a "Microsec e-Szigno Root CA 2009" hitelesít felül. Az e-Szignó Hitelesítés Szolgáltató ezen egység magánkulcsával bocsátja ki az SHA-256 alapú minősített időbélyegzőket. Ezen egység egyáltalán nem bocsát ki SHA-1 alapú időbélyeget. Az időbélyegző egységek tanúsítványai "timeStamping" kiterjesztett kulcshasználatot tartalmaznak.
- "Advanced Class 3 e-Szigno CA 2009" – Ezen egység kizárólag a III. hitelesítési osztály szerint bocsát ki *Tanúsítvány*okat természetes személyek és automaták részére. A "Microsec e-Szigno Root CA 2009" hitelesíti felül. Ezen egység nem bocsát ki álneves *Tanúsítvány*t.
- "Advanced Class 2 e-Szigno CA 2009" – Ezen egység a II. hitelesítési osztály szerint bocsát ki *Tanúsítvány*okat természetes személyek és automaták részére. A "Microsec e-Szigno Root CA 2009" hitelesíti felül. Ezen egység nem bocsát ki álneves *Tanúsítvány*t.
- "Advanced Pseudonymous e-Szigno CA 2009" – Ezen egység a II. és a III. hitelesítési osztály szerint bocsát ki *Tanúsítvány*okat természetes személyek és automaták részére. A "Microsec e-Szigno Root CA 2009" hitelesíti felül. Ezen egység álneves *Tanúsítvány*okat is kibocsát.
- "Signature KET e-Szigno CA 2009" – Ezen egység közigazgatási hitelesítési rendek szerinti *Tanúsítvány*okat bocsát ki és a KGYHSZ hitelesíti felül.
- OCSP válaszadók; minden SHA-256 alapú tanúsítvánnyal rendelkező hitelesítő egység külön, dedikált OCSP válaszadó egységet hitelesít felül, amely az adott hitelesítő egység által kibocsátott *Tanúsítvány*ok visszavonási állapotára vonatkozóan ad választ. Az OCSP válaszadó egységek neve az adott hitelesítő egység neve mögött az "OCSP Responder" szöveget tartalmazza. Az OCSP válaszadók *Tanúsítvány*ában "OCSPSigning" kiterjesztett kulcshasználat szerepel.

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

A *Hitelesítés-szolgáltató* korábban a "Microsec e-Szigno Root CA" hitelesítő egysége alatt SHA-1 alapú *Tanúsítvány*okat bocsátott ki. E hierarchia szerint a *Hitelesítés-szolgáltató* már nem bocsát ki elektronikus aláíráshoz használható *Tanúsítvány*okat és nem bocsát ki időbélyegeket. Az SHA-1 alapú hierarchiáját a *Hitelesítés-szolgáltató* a korábban készült aláírások és időbélyegek ellenőrizhetősége érdekében továbbra is fenntartja. E hierarchiában a következő hitelesítő egységek szerepelnek:

- "Microsec e-Szigno Root CA" (önhitelesített) – Gyökér hitelesítési egység, SHA-1 alapú *Tanúsítvány*okat bocsátott a *Hitelesítés-szolgáltató* hitelesítő egységei számára. E hitelesítő egység önhitelesített tanúsítvánnyal rendelkezik.
- "Advanced e-Szigno CA3" – Ezen egység kizárólag a III. hitelesítési osztály szerint bocsátott ki *Tanúsítvány*okat természetes személyek és automaták részére. Ezen egység nem bocsátott ki álneves *Tanúsítvány*t. A "Microsec e-Szigno Root CA" hitelesítette felül.
- "Advanced e-Szigno CA2"ű – Ezen egység a II. hitelesítési osztály szerint bocsátott ki *Tanúsítvány*okat természetes személyek és automaták részére. Ezen egység bocsátotta ki a III. hitelesítési osztályba tartozó álneves *Tanúsítvány*okat is. A "Microsec e-Szigno Root CA" hitelesíti felül.
- "Signature e-Szigno CA6" – Ezen egység kizárólag közigazgatási hitelesítési rendeknek megfelelő nem minősített *Tanúsítvány*okat bocsátott ki, ezen egységet a Közigazgatási Gyökér Hitelesítés Szolgáltató (KGYHSZ) hitelesítette felül.
- "Microsec e-Szigno Server CA", a gyökér hitelesítő egység, illetve a KGYHSZ hitelesítette felül. Ezen hitelesítő egység hitelesítette felül az időbélyegző egységeket, illetve közigazgatási hitelesítési rendeknek megfelelő *Tanúsítvány*okat bocsátott ki automaták számára.
- Időbélyegző egységek, amelyeket a "Microsec e-Szigno Server CA" hitelesített felül. Az e-Szignó Hitelesítés Szolgáltató ezen egységek magánkulcsaival bocsátotta ki az SHA-1 alapú nem minősített időbélyegzőket. Az időbélyegző egységek *Tanúsítvány*ai "timeStamping" kiterjesztett kulcshasználatot tartalmaznak.
- "e-Szigno OCSP CA" (önhitelesített) – Az OCSP válaszadó tanúsítványát kibocsátó hitelesítő egység.
- "Advanced e-Szigno OCSP Responder" – OCSP válaszadó – az "e-Szigno OCSP CA" hitelesíti felül.

A *Hitelesítés-szolgáltató* SHA-1 alapú rendszerének köztes hitelesítő egységei "záró CRL"-t bocsátanak ki, amelynek érvényességi ideje (`nextUpdate`) a köztes szolgáltatói *Tanúsítvány* lejártával egyezik meg. A korábban készült aláírások és időbélyegek zavartalan ellenőrizhetősége érdekében a korábban kibocsátott SHA-1 alapú *Tanúsítvány*okra 2012. december 31-éig SHA-1 alapú visszavonási információ volt elérhető. A *Hitelesítés-szolgáltató* ezen időpontig a SHA-1 alapú hierarchiájában SHA-1 alapú OCSP válaszadói *Tanúsítvány*okat használt és SHA-1 alapú OCSP válaszokat bocsátott ki. 2013. január 1-étől a *Hitelesítés-szolgáltató* a SHA-1 alapú hierarchiájában SHA-256 alapú OCSP válaszadói tanúsítványokat használ és SHA-256 alapú OCSP válaszokat bocsát ki.

A *Hitelesítés-szolgáltató* SHA-1 alapú rendszerében 2012. január 1-ét követően nem szerepel érvényes, elektronikus aláíráshoz használható végfelhasználói tanúsítvány. Ezen időpontot követően a *Hitelesítés-szolgáltató* már nem bocsát ki SHA-1 alapú időbélyeget.

A "Microsec e-Szigno Root CA" és az "e-Szigno OCSP CA" gyökér *Tanúsítvány*ának lenyomatát a *Hitelesítés-szolgáltató* a Magyar Nemzet 2005. július 21-ei számában, a "Microsec e-Szigno Root CA 2009" gyökér *Tanúsítvány*ának lenyomatát az Expressz 2010. június 17-ei számában tette közzé. Ezen gyökér *Tanúsítvány*ok az e-Szignó Hitelesítés Szolgáltató honlapján keresztül is elérhetőek.

- A "Microsec e-Szigno Root CA" gyökér *Tanúsítvány*ának SHA-1 lenyomata:
  `23 88 c9 d3 71 cc 9e 96 3d ff 7d 3c a7 ce fc d6 25 ec 19 0d`,
  ugyanezen gyökér *Tanúsítvány* SHA-256 lenyomata:
  `32 7a 3d 76 1a ba de a0 34 eb 99 84 06 27 5c b1 a4 77 6e fd ae 2f df 6d 01 68 ea 1c 4f 55 67 d0`

- Az "e-Szigno OCSP CA" gyökér *Tanúsítvány*ának SHA-1 lenyomata:
  `56 2c 85 5b 9c d9 be 0e 64 e6 f7 95 86 24 95 a1 09 3e f1 68`,
  ugyanezen gyökér *Tanúsítvány* SHA-256 lenyomata:
  `15 a9 45 a5 e4 92 c8 6c 3e 4e 0e a5 81 4c 9c 43 b0 4f 2e a6 83 1a 64 6c 37 8c d2 b1 82 05 aa 89`

- A "Microsec e-Szigno Root CA 2009" gyökér *Tanúsítvány*ának SHA-1 lenyomata[1]:
  `89 df 74 fe 5c f4 0f 4a 80 f9 e3 37 7d 54 da 91 e1 01 31 8e`,
  ugyanezen tanúsítvány SHA-256 lenyomata:
  `3c 5f 81 fe a5 fa b8 2c 64 bf a2 ea ec af cd e8 e0 77 fc 86 20 a7 ca e5 37 16 3d f3 6e db f3 78`

A "Microsec e-Szigno Root CA" és "Microsec e-Szigno Root CA 2009" gyökerek *Tanúsítvány*ait tartalmazzák illetve terjesztik az alábbi megbízható tanúsítvány tárak:

- Microsoft Windows tanúsítványtár,
- Network Security Services (NSS) tanúsítványtár,
- Google Android v2.3 (Gingerbread) változatától,

A "Microsec e-Szigno Root CA 2009" gyökér *Tanúsítvány*át ezen felül tartalmazzák illetve terjesztik az alábbi megbízható tanúsítvány tárak:

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

- Apple iOS 7.1.2 változatától.
- Apple Mac OS X 10.9.4 változatától.

A `https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/bongeszo-tamogatas.html` oldalon található további információ arról, hogy mely más böngészőprogramokban és tanúsítványtárakban szerepelnek alapértelmezetten a *Hitelesítés-szolgáltató* gyökértanúsítványai.

A *Hitelesítés-szolgáltató* többi saját *Tanúsítvány*a az önhitelesített gyökértanúsítványok alapján ellenőrizhető, ezért ezen *Tanúsítvány*okat a *Hitelesítés-szolgáltató* csak a honlapján teszi közzé. Amennyiben – jogszabály, vagy hitelesítés-szolgáltatók közötti szerződés vagy kölcsönös megegyezés keretében – a *Hitelesítés-szolgáltató* egyes hitelesítő egységei számára más hitelesítés-szolgáltató is bocsát ki *Tanúsítvány*t, a *Hitelesítés-szolgáltató* ezen *Tanúsítvány*okat is közzéteheti honlapján. A *Hitelesítés-szolgáltató* számára ilyen módon kibocsátott *Tanúsítvány*ok esetén a *Hitelesítés-szolgáltató* vállalja, hogy a *Hitelesítés-szolgáltató*t felül- vagy kereszthitelesítő másik szolgáltató hitelesítési rendjét betartja, és az ezen tanúsítvánnyal kapcsolatban benne foglaltakat magára nézve kötelezőnek ismeri el.

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

Láncolt hitelesítés-szolgáltatás

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

Ezen felülhitelesítés a következő feltételekkel történik:

- A felülhitelesített hitelesítés-szolgáltatóval a *Hitelesítés-szolgáltató* szerződést köt, a felülhitelesítés pontos feltételeit e szerződés szabályozza. A felülhitelesített hitelesítés-szolgáltató maga köt szerződést a hozzá tartozó *Ügyfel*ekkel, e szerződésben a felülhitelesített hitelesítés-szolgáltató jelenik meg hitelesítés-szolgáltatóként.
- A *Hitelesítés-szolgáltató* teljes felelősséget vállal a láncolt hitelesítés-szolgáltató tevékenységéért.
- A felülhitelesített hitelesítés-szolgáltató kizárólag valamely jól definiált kör részére bocsáthat ki *Tanúsítvány*t.
- A felülhitelesített hitelesítés-szolgáltatónak nyilvánosságra kell hoznia a hitelesítési rendjét, és e hitelesítési rend szerint kell működnie.

- A *Hitelesítés-szolgáltató* jogosult rendszeresen ellenőrizni a felülhitelesített szolgáltató működését.
- A *Hitelesítés-szolgáltató* visszavonja a felülhitelesítés során kibocsátott *Tanúsítvány*t, amennyiben a felülhitelesített hitelesítés-szolgáltató nem felel meg saját hitelesítési rendjének, vagy amennyiben a felülhitelesített hitelesítés-szolgáltató jelzi, hogy a felülhitelesített szolgáltatói kulcsa kompromittálódott.
- Amennyiben a *Hitelesítés-szolgáltató* más hitelesítés szolgáltató számára bocsát ki szolgáltatói *Tanúsítvány*t, ezt bejelenti a Nemzeti Média- és Hírközlési Hatóságnak. Amennyiben a felülhitelesített szolgáltató belföldi és nyilvános körben használható *Tanúsítvány*okat bocsát ki, a felülhitelesített szolgáltató köteles a felülhitelesítést bejelenteni a Nemzeti Média- és Hírközlési Hatóságnak, és köteles kérni a nyilvántartásba vételét (amennyiben még nem szerepel a Nemzeti Média- és Hírközlési Hatóság nyilvántartásában). Más, alárendelt szolgáltatásként nyújtott elektronikus aláírással kapcsolatos szolgáltatásokra (pl. időbélyegzés) is ennek megfelelő szabályok vonatkoznak.

1.3.2. Regisztráló szervezetek

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

Az iroda feladatai:

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

A *Hitelesítés-szolgáltató* által üzemeltetett ügyfélszolgálati iroda fogadja a különböző tanúsítvány műveletekre vonatkozó kérelmeket és kezdeményezi azok feldolgozását. A *Hitelesítés-szolgáltató* a felfüggesztés kezdeményezésére folyamatosan – a nap 24 órájában, a hét minden napján – rendelkezésre álló ügyeletet tart fenn.

A *Regisztráló szervezet* a következő helyeken végezhet regisztrációs tevékenységet:

- a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában;

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

A *Hitelesítés-szolgáltató* egyéb szervezetekkel is szerződést köthet külső regisztrációs irodák létrehozására illetve mobil regisztrációs egységek működtetésére, amelyek a központi iroda egyes feladatait külső helyszínen látják el. E külső *Regisztráló szervezet*ek is szabályozottan, jelen *Szolgáltatási szabályzat*tal összhangban működnek, a *Hitelesítés-szolgáltató* ellenőrzi e szervezetek kontrollrendszerét és működését.

1.3.3. Ügyfelek

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

- *Előfizető*:
  - szolgáltatási szerződést köt a *Hitelesítés-szolgáltató*val,
  - meghatározza a hitelesítés szolgáltatást igénybe vevő *Alany*ok körét,
  - megfizeti a hitelesítés szolgáltatás igénybe vételével kapcsolatos díjakat.
- *Alany*: a *Hitelesítés-szolgáltató* az *Alany* számára bocsátja ki a *Tanúsítvány*t.
- *Aláíró*: az elektronikus aláírás hitelesítés szolgáltatást igénybe vevő fél, aki a kibocsátott *Tanúsítvány* segítségével elektronikus aláírást hozhat létre.

Az *Alany* megegyezik az *Aláíró*val.

1.3.4. Érintett felek

- *Érintett fél*: a *Tanúsítvány* felhasználásával létrehozott elektronikus aláírással ellátott elektronikus dokumentumot befogadó fél, valamint az időbélyegzőt befogadó fél. Az *Érintett fél* nem feltétlenül áll szerződéses viszonyban a *Hitelesítés-szolgáltató*val. Tevékenységére vonatkozó ajánlásokat a *Szolgáltatási szabályzat* 4.5.2, 4.9.6, 9.6.4 és 9.9.3 fejezetei és az abban megnevezett egyéb szabályzatok tartalmaznak. A *Hitelesítés-szolgáltató* az *Érintett fél*lel elsősorban az internetes honlapon keresztül tart kapcsolatot.

1.3.5. Egyéb szereplők

- *Képviselt szervezet*: amennyiben a *Tanúsítvány* egy *Szervezet* nevében történő aláírásra vagy tevékenységének érdekében történő felhasználás céljából kerül kibocsátásra az *Alany* részére (természetes személy számára kibocsátott szervezeti tanúsítvány), akkor a *Képviselt szervezet* a szóban forgó *Szervezet*, amely szintén megjelölésre kerül a

*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 bocsát ki. A *Hitelesítés-szolgáltató* felfüggeszti, illetve visszavonja a *Tanúsítvány*t ezen *Szervezet* kérésére.

1.4. A tanúsítvány felhasználhatósága

1.4.1. Megfelelő tanúsítvány használat

A kibocsátott végfelhasználói *Tanúsítvány*okhoz kapcsolódó magánkulcsok elektronikus aláírások készítésére, míg a hozzájuk kapcsolódó, a *Tanúsítvány*ban is szereplő nyilvános kulcs, maga a *Tanúsítvány*, a *Tanúsítvány* visszavonási listák, az időbélyegzők és az online tanúsítvány-állapot válaszok az elektronikus aláírások ellenőrzésére használhatóak fel. Az időbélyeg további felhasználási célja annak igazolása, hogy az időbélyegzett dokumentum az időbélyegzés pillanatában létezett.

1.4.2. Tiltott tanúsítvány használat

Az elektronikus aláírásra használható *Tanúsítvány*okhoz kapcsolódó magánkulcsokat kizárólag elektronikus aláírás létrehozására szabad felhasználni. Egyéb más célra – különösen titkosításra, felhasználó-hitelesítésre – való felhasználásuk tilos.

1.5. A dokumentum adminisztrálása

1.5.1. A dokumentum adminisztrációs szervezete

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

Szervezet neve	Microsec e-Szignó Hitelesítés Szolgáltató
Szervezet címe	Magyarország, H-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 *Szolgáltatási szabályzat*tal 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 szabályzat 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 *Szolgáltatási szabályzat* új verziójának illetve tetszőleges módosításának megírása, elfogadása és kibocsátása egységes folyamatok szerint – a 9.12.1 fejezetben részletezett módon – történik.

1.6. Fogalmak és rövidítések

1.6.1. Fogalmak

II. hitelesítési osztály	Olyan *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. Elektronikus aláírásra szolgáló *Tanúsítvány* esetén az *Alany* megegyezik az *Aláíró*val.
Alany egyedi azonosítója	A *Hitelesítés-szolgáltató* által az *Alany* számára adott globálisan egyedi azonosító. Az azonosító OID formátumú, és megfelel az RFC 4043 [5] ajánlásnak.
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, aláíró kulcs) 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.
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.
Biztonságos aláírás-létrehozó eszköz (BALE)	Az Eat. [3] 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz. Olyan hardver, illetve szoftver eszköz, amelyet egy erre kijelölt független tanúsító szervezet megvizsgált és a biztonsági és működési követelményeknek megfelelőnek talált. Minősített elektronikus aláírás csak BALE használatával készíthető.
Érintett fél (Relying Party)	Az elektronikus dokumentum fogadója, aki egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el.

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 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 (aláíró kulcs) 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.
Időbélyegzési rend	Olyan szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely időbélyegző felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.

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.
Időbélyegző egység	A Hitelesítés-szolgáltató rendszerének egy egysége, amely az időbélyegzők aláírását végzi. Egy időbélyegző egységhez mindig egy aláírás-létrehozó adat (aláírókulcs) tartozik. Előfordulhat, hogy egy Hitelesítés-szolgáltató egyszerre több időbélyegző egységet is működtet
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.

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).
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	Az elektronikus aláírás létrehozására és ellenőrzésére 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 feltüntetésre 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	Az a természetes személy, aki jogosult az adott szervezet számára igényelt *Tanúsítvány*ok igénylése, felfüggesztése, visszaállítása és visszavonása során eljárni, valamint az adott szervezethez kapcsolódó személyes *Tanúsítvány*ok kibocsáthatóságát jóváhagyni illetve ezen *Tanúsítvány*okat visszavonatni. A Szervezeti ügyintézőt az adott szervezet képviseletére jogosult személy jelölheti ki. Szervezeti ügyintéző kijelölése nem kötelező, ha nincs kijelölve, akkor az adott szervezet képviseletére jogosult személy láthatja el ezt a feladatot.
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 az aláírás-ellenőrző adatot az Eat. [3] 9. § (3), illetőleg (4) bekezdése szerint egy meghatározott *Aláíró*hoz kapcsolja 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 aláírás-kezelő rendszer számára elérhető *Tanúsítvány*okat tartalmazó rendszert is.

Tárolt kulcsos aláírás szolgáltatás	Olyan szolgáltatás, amely során az Aláíró magánkulcsa egy megfelelően védett szerveren, egy biztonságos hardver kriptográfiai eszközben található, amelyet az Aláíró egy megfelelően biztonságos azonosítási lépést követően tud használni.
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.

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. Közzététel és tanúsítványtár

2.1. Adatbázisok - tanúsítványtárak

A *Hitelesítés-szolgáltató* a honlapján (https://www.e-szigno.hu) és LDAP protokollon (ldap://ldap.e-szigno.hu) keresztül is közzé teszi 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* biztosítja, 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* közzéteszi a honlapján a szolgáltatói tanúsítványait, valamint közzéteszi a végfelhasználói *Tanúsítvány*okat az *Érintett felek* részére, amennyiben a tanúsítványhoz tartozó *Alany* ehhez hozzájárul.

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

- A gyökér hitelesítő egységek megnevezését, illetve gyökértanúsítványaik lenyomatát a *Szolgáltatási szabályzat*ban (lásd: 1.3.1. fejezet). Az állapotváltozásukkal kapcsolatos információk elérhetőek a szolgáltató honlapján.
- A köztes (nem gyökér) hitelesítő egységek és időbélyegző egységek tanúsítványainak állapotváltozását nyilvánosságra hozza 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 (10 percig érvényes) *Tanúsítvány*t bocsát ki, ezzel kiküszöbölve azt, hogy a *Tanúsítvány* visszavonási állapotát ellenőrizni kelljen. Az OCSP válaszadói *Tanúsítvány*ok visszavonási állapotát a *Hitelesítés-szolgáltató* kizárólag olyan módon teszi közzé, hogy kulcs

kompromittálódás vagy bármilyen egyéb probléma esetén az OCSP válaszokat aláíró régi magánkulcshoz nem kerül kibocsátásra újabb *Tanúsítvány*. A *Hitelesítés-szolgáltató* az OCSP válaszadói tanúsítványokat ezt követően új, biztonságos magánkulcshoz

bocsátja ki. Az OCSP válaszok ellenőrzését bővebben az 4.5.2. fejezet tartalmazza.

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

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

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

A *Hitelesítés-szolgáltató* értesíti *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 *Szolgáltatási szabályzat*tal 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 közzé teszi a jogszabályi előírásoknak megfelelően, illetve ennek hiányában amikor szükséges.

2.3.2. Tanúsítványok nyilvánosságra hozatalának gyakorisága

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

- Az általa működtetett gyökér hitelesítő egységek *Tanúsítvány*ait a szolgáltatás megkezdését, vagy az új *Tanúsítvány* kibocsátását követő 10 munkanapon belül teszi 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 megjeleníti 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 elérhetőek.

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

2.4. A tanúsítványtár elérésének szabályai

A *Hitelesítés-szolgáltató* által közzétett *Tanúsítvány*ok és állapot információk nyilvános információk, olvasás céljából bárki számára biztosított a hozzáférési lehetőség 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 az alkalmazott *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 megfelelnek az RFC 5280 [6] illetve RFC 6818 [7] ajánlások szerinti egyedi név formátum előírásainak, ezen kívül a *Hitelesítés-szolgáltató* támogatja a kiterjesztések között található Alternatív név mezők (Subject Alternative Names), (Issuer Alternative Names) kitöltését is.

3.1.1. Név típusok

Az *Alany* megnevezése

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

- Common Name (CN) – OID: 2.5.4.3

  Az *Alany* neve. Kitöltése kötelező.

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

  Szervezet esetében a szervezet teljes vagy rövid elnevezése kerül ebbe a mezőbe, a megfelelő közhiteles nyilvántartásban – vagy ennek híján az alapító okiratban – szereplő alakkal megegyező formában. Amennyiben a *Tanúsítvány* méretkorlátja miatt a szervezetnek se a teljes, se a rövid neve nem fér ki ebbe a mezőbe, akkor a szervezet elnevezésének félre nem érthető rövidítése szerepel itt.

  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) szerepel e mezőben, magát az álnevet pedig a pseudonym (PSEUDO) mező tartalmazza.

- Pseudonym (PSEUDO) – OID: 2.5.4.65

  Kizárólag álneves tanúsítvány esetén kerül kitöltésre, ebben a mezőben szerepel az *Alany* által szabadon választott álnév.

  Az álnevet a *Hitelesítés-szolgáltató* nem ellenőrzi. Az álnév használat kizárólag a "PSEUDO" mezőt érinti, minden más mezőbe a *Hitelesítés-szolgáltató* által ellenőrzött, valós érték kerül.

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

- Serial Number – OID: 2.5.4.5

  Az *Alany* egyedi azonosítója. A *Tanúsítvány*ban legalább egy kitöltött "Serial Number" mező szerepel, amely az *Alany* RFC 4043 [5] ajánlás szerinti egyedi azonosítóját tartalmazza.

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

  A *Hitelesítés-szolgáltató* által az *Alany* számára adott, RFC 4043 [5] ajánlás szerinti egyedi azonosítók OID formátumúak: "1.3.6.1.4.1.21528.2.2.x.y"

Ebben az első számjegyek rögzítettek (1.3.6.1.4.1.21528.2.2: ez a *Hitelesítés-szolgáltató* egyedi azonosítója),

"x" a Microsec által használt belső azonosító,

"y" egy automatikusan kiosztott, az adott "x" értéken belül egyedi sorszám.

Így az "x.y" értékpár a *Hitelesítés-szolgáltató* rendszerén belül az *Alany* egyedi azonosítója.

Egy *Alany*hoz tartozhat több különböző OID, de egy OID csak egyetlen *Alany*hoz tartozhat. Az *Alany* minden esetben jogosult friss (még ki nem osztott) OID-et kérni. Álneves tanúsítványt a *Hitelesítés-szolgáltató* kizárólag friss OID-hez bocsát ki. A *Hitelesítés-szolgáltató* kizárólag akkor ad két *Tanúsítvány*nak azonos OID-et, ha meggyőződött arról, hogy a két *Tanúsítvány*hoz tartozó *Alany* azonos.

További Serial Number mezők (Név:Érték) párokat tartalmazhatnak. Például: "Szig.szam:AAAAAA"

Ügyvédek számára kibocsátott *Tanúsítvány*ok esetén a *Hitelesítés-szolgáltató* e mezőben tünteti fel azon ügyvédi kamara megnevezését, amelynek az ügyvéd tagja, valamint az ügyvédi kamara által az ügyvédhez rendelt azonosítót (lajstromszámot vagy KASZ számot).

A Serial Number mezőben a *Hitelesítés-szolgáltató* – a szabványoknak megfelelően – nem tüntet fel ékezeteket.

E további mezők is az *Alany* egyedi azonosítójának tekinthetőek, de a legelöl szereplő, OID formátumú azonosító tölti be az RFC 4043 szerinti azonosító szerepét.

- Organization (O) – OID: 2.5.4.10

  Szervezeti *Tanúsítvány* esetében az "O" mezőben szerepel a szervezet teljes vagy rövid neve, az alapító okirat vagy valamely közhiteles nyilvántartás szerint.

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

- Organizational unit (OU) – OID: 2.5.4.11

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

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

- Country (C) – OID: 2.5.4.6

  Szervezeti *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.

Kitöltése kötelező.

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

- Subject Street Address (SA) – OID: 2.5.4.9

  Nem kerül kitöltésre.

- Subject Locality Name(L) – OID: 2.5.4.7

  Szervezeti *Tanúsítvány* esetében a szervezet székhelye szerinti helység neve. Szervezethez nem kapcsolódó *Tanúsítvány* esetében nem kerül kitöltésre.

- State or Province Name – OID: 2.5.4.8

  Szervezeti *Tanúsítvány* esetében a *Szervezet* székhelye szerinti tagállam, megye vagy tartomány neve. Kitöltése opcionális.

  Szervezethez nem kapcsolódó *Tanúsítvány* esetében nem kerül kitöltésre.

- Postal Code – OID: 2.5.4.17

  Szervezeti *Tanúsítvány* esetében a *Szervezet* székhelye szerinti postai irányítószám. Amennyiben kitöltésre kerül, akkor csak ellenőrzött információ tüntethető fel. Kitöltése opcionális

  Szervezethez nem kapcsolódó *Tanúsítvány* esetében nem kerül kitöltésre.

- Title (T) – OID: 2.5.4.12

  A természetes személy *Alany* szerepe, beosztása vagy munkaköre.

  Meghatározza, hogy az *Alany* az adott szervezethez kapcsolódó milyen szerepkörben hozza létre az aláírást. A mező csak szervezeti tanúsítvány esetén tartalmaz értéket, azaz csak akkor, ha az "O" mező is kitöltésre kerül.

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

  Mivel a "Title" mező az *Alany* szerepét tartalmazza, további korlátozásokat tartalmazhat a *Tanúsítvány* felhasználhatóságával kapcsolatban.

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

  Az *Alany* e-mail címe. Ha kitöltésre kerül, akkor értéke megegyezik az *Alany* alternatív neve mezőben szereplő "RFC822name" mezőben szereplő e-mail címmel.

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

Az Alany alternatív nevei

Az "Alany alternatív nevei" nem kritikus mező.

Az *Alany* kérésére ide (jellemzően a "Subject Alternative Names" "CN" mezejébe) kerül 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* a "Subject Alternative Names" mezőbe kerülő neveket is ellenőrzi, a nevekről egyedi elbírálás alapján dönt. A döntést az alapján hozza meg, hogy az *Ügyfél* által kért elnevezés valóban az *Alany* neve-e, illetve nem vezethet-e félre másokat. Amennyiben az *Alany* a hivatása gyakorlása során nem a személyazonosításra használt okmányában szereplő nevét használja, akkor kérheti, hogy a *Hitelesítés-szolgáltató* a "Subject Alternative Names" mezőben ezen alternatív elnevezést szerepeltesse.

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 kitöltésre kerül. Ugyanez az e-mail cím opcionálisan megjelenhet a *Tanúsítvány* "EMAIL" mezejében is.

Az *Alany* alternatív nevei mezőben szerepel továbbá az RFC 4043 [5] szerinti állítás, miszerint a "Subject" mezőben szereplő első "Serial Number" érték az *Alany* permanens azonosítóját tartalmazza a *Hitelesítés-szolgáltató* rendszerének kontextusában.

A tanúsítványt kibocsátó hitelesítő egység megnevezése

A tanúsítványok kibocsátójának azonosítója (Issuer mező) a következő módon épül fel:

- Common Name (CN) – OID: 2.5.4.3
  A tanúsítványt kibocsátó hitelesítő egység angol nyelvű megnevezése (lásd: 1.3.1. fejezet).
- Organization (O) – OID: 2.5.4.10
  "Microsec Ltd."
  (A *Hitelesítés-szolgáltató* neve angolul, ékezet nélkül.)
- Organizational unit (OU) – OID: 2.5.4.11
  "e-Szigno CA"
  (A *Hitelesítés-szolgáltató* szervezeti egységének neve ékezet nélkül; SHA-256 alapú szolgáltatói tanúsítványokban nem kerül kitöltésre.)
- Locality (L) – OID: 2.5.4.7
  "Budapest"
  (A *Hitelesítés-szolgáltató* székhelye szerinti város neve ékezet nélkül.)

- Country (C) – OID: 2.5.4.6
  "HU"
  (A *Hitelesítés-szolgáltató* székhelye szerinti ország kétbetűs rövidítése.)

A végfelhasználói tanúsítvány kibocsátójának tanúsítványában, az alany azonosító mezőben ugyanezen adatok szerepelnek.

A tanúsítványt kibocsátó hitelesítő egység alternatív nevei

A végfelhasználói tanúsítványokban a kibocsátó alternatív nevei (Issuer Alternative Names) mező nem kerül kitöltésre.

A végfelhasználói tanúsítvány kibocsátójának tanúsítványában szereplő elnevezések:

- Az SHA-1 alapú szolgáltatói tanúsítványokban az aláíró (azaz a hitelesítési egység) alternatív nevei mező kitöltésre került a következők szerint:

  Subject Alternative Names – OID: 2.5.29.17 (nem kritikus)
  CN = (a kibocsátó hitelesítő egység magyar nyelvű megnevezése, lásd: 1.3.1. fejezet)
  O = Microsec Kft.
  OU = e-Szignó HSZ
  L = Budapest
  C = HU
  rfc822Name = info@e-szigno.hu

- Az SHA-256 alapú szolgáltatói tanúsítványok esetén az alternatív név mezőben csak az e-mail cím (rfc822Name) kerül kitöltésre.

3.1.2. A nevek értelmezhetősége

A "SubjectDN" mezőre a következő szabályok érvényesek:

- az azonosítónak értelmezhetőnek kell lennie;
- a *Tanúsítvány*ban szereplő személynevet a 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* a nem álneves *Tanúsítvány*oknál alkalmazottal megegyező módon ellenőrzi.

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 ad, csak a *Tanúsítvány*ban feltüntetett adatok értelmezését segítő információt szolgáltatja.

A *Hitelesítés-szolgáltató* biztosítja a személy azonosításához szükséges adatok elektronikus ellenőrizhetőségének lehetőségét, amennyiben a *Hitelesítés-szolgáltató* olyan *Hitelesítési rend* szerint bocsátotta ki a *Tanúsítvány*t, amely ezt megköveteli. Ennek részleteit a 4.13. fejezet írja le.

3.1.5. A nevek egyedisége

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

Az *Alany*ok egyedi azonosítóinak (OID) kiosztása a beérkezett tanúsítvány kérelmek elbírálásának sorrendje szerint történik, 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* meggyőződik az *Ügyfél* jogosultságáról a feltüntetett nevek használatára vonatkozóan. Jogszerűtlen név- vagy adathasználat miatt a *Hitelesítés-szolgáltató*nak jogában áll visszavonni a kérdéses *Tanúsítvány*t.

3.1.6. Márkanevek elismerése, azonosítása, szerepük

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

Amennyiben az *Ügyfél* olyan *Tanúsítvány*t igényel, amelyben egy márkanév vagy védjegy feltüntetését kéri, akkor annak használatának jogosságáról az *Ügyfél*nek kell bizonyítékot szolgáltatnia, amelyet a *Hitelesítés-szolgáltató* a Tanúsítvány kibocsátása előtt ellenőriz.

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

3.2. Kezdeti regisztráció, azonosság hitelesítése

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

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

3.2.1. A magánkulcs birtoklásának igazolása

A *Tanúsítvány* kiállítása előtt a *Hitelesítés-szolgáltató* biztosítja illetve meggyőződik arról, hogy a *Tanúsítvány*t kérelmező valóban birtokolja a *Tanúsítvány*ba kerülő nyilvános kulcshoz tartozó magánkulcsot, vagy a *Hitelesítés-szolgáltató* által üzemeltetett aláírás-létrehozó eszközön lévő aláírás-létrehozó adathoz kizárólagosan hozzáfér. Amennyiben az *Alany* számára a *Tanúsítvány*hoz tartozó magánkulcsot a *Hitelesítés-szolgáltató* saját szervezetén belül maga generálja – jellemzően a *Hardver kriptográfiai eszköz* használatát megkövetelő *Hitelesítési rend*ek esetén – , akkor nem kell külön ellenőriznie azt, hogy az *Alany* rendelkezik-e a hitelesítendő nyilvános kulcs magánkulcs-párjával.

Amennyiben az *Alany* általa biztosított kulcshoz kéri a *Tanúsítvány* kibocsátását – jellemzően szoftveres tanúsítványok esetében –, akkor a *Hitelesítés-szolgáltató* PKCS#10 formátumban fogadja a *Tanúsítvány kérelmet*, amely egyúttal igazolja, hogy valóban a magánkulcs birtokosa kért *Tanúsítvány*t az adott megnevezéshez. A *Hitelesítés-szolgáltató* ezzel egyenértékű bizonyítéknak tekinti, ha az *Alany* az igényelt *Tanúsítvány*ban szerepeltetni kívánt nyilvános kulcshoz tartozó érvényes *Tanúsítvány* felhasználásával létrehozott elektronikus aláírással ellátva nyújtja be a *Tanúsítvány kérelmet*.

3.2.2. Szervezet azonosságának hitelesítése

Szervezet azonossága ellenőrizésre kerül a következő esetekben:

- amennyiben a kibocsátandó *Tanúsítvány* alanya a szervezet;
- amennyiben a *Tanúsítvány* természetes személy számára kerül kibocsátásra, de a *Tanúsítvány*ban a szervezet neve is feltüntetésre kerül.

Ellenőrzésre kerül továbbá, hogy

- a *Szervezet* nevében eljáró természetes személy jogosult-e a *Szervezet* nevében eljárni;
- szervezethez kapcsolódó személyes tanúsítvány kibocsátása esetén azt, hogy a *Szervezet* hozzájárult-e az ilyen jellegű *Tanúsítvány* kibocsátásához.

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

- a szervezet hivatalos elnevezése és székhelye,
- a szervezeten belüli szervezeti egység neve, ha kérik ennek feltüntetését a *Tanúsítvány*ban,
- szervezethez kapcsolódó személyes tanúsítvány kibocsátása esetén az *Alany*nak a szervezetben betöltött szerepe, ha kérik ennek feltüntetését a *Tanúsítvány*ban,

A *Tanúsítvány kérelem*hez csatolni kell a következő igazolásokat illetve bizonyítékokat:

- a kérelem benyújtójának saját kezű aláírásával ellátott nyilatkozatát arról, hogy a szervezet azonosítására megadott adatok helyesek és megfelelnek a valóságnak;
- igazolás arra vonatkozóan, hogy a szervezet nevében *Tanúsítvány kérelmet* benyújtó természetes személy jogosult a kérelmet benyújtani (*),
- szervezethez kapcsolódó személyes tanúsítvány kibocsátása esetén igazolás arra vonatkozóan, hogy a szervezet hozzájárul ahhoz, hogy a természetes személy számára kibocsátandó *Tanúsítvány*ban szerepeljen a szervezet neve (*),
- a *Szervezet* képviseletére jogosult személy aláírási címpéldányát vagy más, az aláírási címpéldánnyal egyenértékű hivatalos dokumentumot, mely a szervezet képviseletére jogosult személyek nevét és aláírását tartalmazza (**),
- a *Szervezet* azonosságát hitelesítő dokumentumot (**).

(*) A felhatalmazások, jogosultságok ellenőrzésével kapcsolatos részleteket a 3.2.5. fejezet tartalmazza.

(**) Cégbíróságon bejegyzett cégek esetében a fenti iratokat a *Hitelesítés-szolgáltató* is beszerezheti.

A *Hitelesítés-szolgáltató* 3 hónapnál nem régebbi igazolásokat illetve bizonyítékokat fogad el.

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

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

Az adategyeztetés tekintetében a *Hitelesítés-szolgáltató* elfogadja:

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

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

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

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

3.2.3. Természetes személy azonosságának hitelesítése

A természetes személy azonosságát igazolni kell:

- 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 módja:

- a/ a természetes személynek a személyes azonosítás elvégzéséhez személyesen meg kell jelennie az azonosítást végző szervezet előtt;
- b/ a személyes azonosítás során a természetes személy azonossága ellenőrzésre kerül egy személyazonosító igazolvány alapján;
- c/ a személyazonosság ellenőrzésére szolgáló adatok helyességét a természetes személynek nyilatkozatban, saját kezű aláírással ellátva igazolnia kell;

- d/ a b/ pont szerinti igazolvány adatainak helyességét és az igazolvány érvényességét a *Regisztráló szervezet* megbízható harmadik fél vagy közhiteles nyilvántartás segítségével ellenőrzi.

A személyes azonosítás helyett a *Hitelesítés-szolgáltató* elfogadhat más, azzal azonos biztonságot nyújtó azonosító módszert is. Ilyen például, ha az *Alany* a *Tanúsítvány kérelmet* elektronikus formában nyújtja be egy nem álneves tanúsítványán alapuló minősített elektronikus aláírással ellátva.

Érvényes minősített elektronikus aláírással ellátott tanúsítvány kérelem esetében nincs szükség a kérelmező azonosságának további vizsgálatára. A *Tanúsítvány*ba kerülő adatok pontosságának ellenőrzése ugyanúgy történik, mint a személyes kérelem benyújtás esetében.

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. A *Hitelesítés-szolgáltató* a II. hitelesítési osztályba tartozó tanúsítványok esetén is végez adategyeztetést közhiteles nyilvántartásokkal. Az *Aláíró* választása szerint a III. hitelesítési osztály szerint is igazolhatja személyazonosságát.

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

A *Hitelesítés-szolgáltató* külföldi állampolgárok személyazonosságát útlevél, vagy más, személyazonosításra alkalmas okmány segítségével ellenőrzi, illetve ekkor az adott ország megfelelő nyilvántartásaival végez adategyeztetést, amennyiben elérhető ilyen nyilvántartás. A külföldi okmány megfelelő biztonsággal történő ellenőrzése, illetve a külföldi nyilvántartáshoz való hozzáféréshez további lépések szükségesek. Az adategyeztetés tekintetében a *Hitelesítés-szolgáltató* elfogadja:

- a külföldi ország magyarországi nagykövetsége vagy konzulátusa által kibocsátott igazolást, miszerint az adott okmány létezik és érvényes, és az adott személy, illetve szervezet létezik.
- a külföldi országban lévő magyar nagykövetség vagy konzulátus által kibocsátott igazolást, miszerint az adott okmány létezik és érvényes, és az adott személy, illetve szervezet létezik.

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

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

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

3.2.4. Nem ellenőrzött alany információk

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

3.2.5. Jogok, felhatalmazások ellenőrzése

Szervezetnek történő *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.

Egy *Szervezet* nevében eljárhat

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

A Szervezeti ügyintéző az a személy, aki jogosult az adott *Szervezet* számára igényelt *Tanúsítvány*ok igénylése, felfüggesztése, visszaállítása és visszavonása során eljárni, valamint az adott szervezethez kapcsolódó személyes *Tanúsítvány*ok kibocsáthatóságát jóváhagyni illetve ezen *Tanúsítvány*okat visszavonatni.

A Szervezeti ügyintéző kijelölhető a tanúsítvány igénylés során, vagy később is bármikor a megfelelő formanyomtatvány segítségével. Az űrlapon meg kell adni a kijelölt személy(ek) azonosító adatait, amelyek alapján a későbbi eljárás során azonosíthatóak. Az űrlapot a *Szervezet* képviselőjének (saját kezű vagy minősített elektronikus) aláírással kell ellátnia, amelyet az űrlap befogadásakor a *Hitelesítés-szolgáltató* regisztrációs munkatársai ellenőriznek. Szervezeti ügyintéző kijelölése nem kötelező, illetve egyidejűleg több szervezeti képviselő is kijelölhető. Amennyiben nincs kijelölve szervezeti ügyintéző, akkor az adott szervezet képviseletére jogosult személy láthatja el ezt a feladatot.

3.2.6. Együttműködési képességre vonatkozó követelmények

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

3.3. Azonosítás és hitelesítés kulcscsere kérelem esetén

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

A kulcscserével kapcsolatos eljárás részletei a 4.7. fejezetben olvashatóak.

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

3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

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

- papíralapon kézi aláírásával ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely külső Regisztráló szervezet regisztrációs munkatársa előtt, előzetesen egyeztetett időpontban;
- elektronikus aláírásával ellátva e-mailben,
- a *Tanúsítvány* felfüggesztési vagy visszavonási folyamata során,
- kézi aláírással ellátva postai úton az Ügyfélszolgálatnak eljuttatva.

Személyes kérelem benyújtása esetén a kérelmező azonosítása a 3.2.3-as fejezetben leírtak szerint történik.

A még érvényes aláíró *Tanúsítvány*hoz kapcsolódó magánkulccsal aláírt kulcscsere kérelem esetében nincs szükség a kérelmező azonosságának és a kérelem hitelességének további vizsgálatára.

A *Hitelesítés-szolgáltató* lehetőséget biztosít az *Alany*nak arra, hogy amennyiben a kulcscserére azért van szükség, mert a *Tanúsítvány*hoz tartozó magánkulcs kompromittálódott, akkor az *Alany* ezt a *Tanúsítvány* felfüggesztési vagy visszavonási eljárás keretében jelezze. Ebben az eseteben az *Alany* a felfüggesztési illetve visszavonási eljárás keretében kerül azonosításra, ennek részleteit a 3.6. fejezet tartalmazza.

A papíralapon, postai úton történő kulcscsere kérelem benyújtása esetében a kérelmező azonosítása és a kérelem megerősítése a kérelem benyújtását követően, személyesen találkozás során történik.

3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Kulcscsere kérelmeket – kizárólag a szolgáltatási szerződés érvényessége alatt – visszavont vagy felfüggesztett *Tanúsítvány*okhoz is elfogad a *Hitelesítés-szolgáltató*. A kérelmet benyújtó személy azonossága ugyanúgy kerül ellenőrzésre, mint a még érvényes *Tanúsítvány*hoz történő kulcscsere kérelem esetében (lásd: 3.2.3. fejezet), azzal a különbséggel, hogy az ott felsorolt lehetőségek közül nem mindegyiket tudja igénybe venni az *Ügyfél*.

3.4. Azonosítás és hitelesítés tanúsítvány megújítás esetén

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

3.4.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

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

- papíralapon kézi aláírásával ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely külső Regisztráló szervezet regisztrációs munkatársa előtt, előzetesen egyeztetett időpontban;
- elektronikus aláírásával ellátva e-mailben,
- kézi aláírással ellátva postai úton az Ügyfélszolgálatnak eljuttatva.

Személyes kérelem benyújtása esetén a kérelmező azonosítása a 3.2.3. fejezetben leírtak szerint történik.

A még érvényes aláíró *Tanúsítvány*hoz kapcsolódó magánkulccsal aláírt megújítási kérelem esetében nincs szükség a kérelmező azonosságának és a kérelem hitelességének további vizsgálatára.

A papíralapon, postai úton történő megújítási kérelem benyújtása esetében a kérelmező azonosítása és a kérelem megerősítése a kérelem benyújtását követően, személyesen találkozás során történik. Ez alól kivételt képeznek a II. hitelesítési osztályba tartozó Tanúsítványok, amelyek esetében nincs szükség személyes találkozásra.

3.4.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen *Tanúsítvány* megújítása nem kérhető.

3.5. Azonosítás és hitelesítés tanúsítvány módosítás esetén

3.5.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

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

- papíralapon kézi aláírásával ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely külső Regisztráló szervezet regisztrációs munkatársa előtt, előzetesen egyeztetett időpontban;
- elektronikus aláírásával ellátva e-mailben,
- kézi aláírással ellátva postai úton az Ügyfélszolgálatnak eljuttatva.

Személyes kérelem benyújtása esetén a kérelmező azonosítása a 3.2.3. fejezetben leírtak szerint történik.

A még érvényes aláíró *Tanúsítvány*hoz kapcsolódó magánkulccsal aláírt Tanúsítvány módosítási kérelem esetében nincs szükség a kérelmező azonosságának és a kérelem hitelességének további vizsgálatára.

A papíralapon, postai úton történő Tanúsítvány módosítási kérelem benyújtása esetében a kérelmező azonosítása és a kérelem megerősítése a kérelem benyújtását követően, személyesen találkozás során történik. Ez alól kivételt képeznek a II. hitelesítési osztályba tartozó *Tanúsítvány*ok, amelyek esetében nincs szükség személyes találkozásra.

3.5.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen *Tanúsítvány* módosítása nem kérhető.

3.6. Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási kérelem esetén

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

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

4. A tanúsítványok életciklusára vonatkozó követelmények

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

Tanúsítványcserének nevezzük azt a folyamatot, amikor egy korábban már regisztrált (és ennek során azonosított) *Alany* egy meglévő (már kibocsátott, és amelyre érvényes szolgáltatási szerződés vonatkozik) *Tanúsítvány*a helyett új *Tanúsítvány*t igényel. Tanúsítványcserére több okból is sor kerülhet:

- Ha az *Alany* meglévő *Tanúsítvány*a még érvényes, de hamarosan le fog járni, és az *Ügyfél* olyan *Tanúsítvány*t igényel, amelybe az *Alany* korábbi *Tanúsítvány*ában lévőkkel megegyező adatok kerülnek, és a két *Tanúsítvány* ugyanazon nyilvános kulcshoz kerül kibocsátásra, akkor Tanúsítvány *megújításról* beszélünk, amelynek részleteit a 4.6. fejezet írja le.
- Ha az *Alany* meglevő *Tanúsítvány*a még érvényes, de az *Alany Tanúsítvány*ban szereplő adatai megváltoztak, és ezért kéri a *Tanúsítvány* megváltoztatását, akkor Tanúsítvány *módosításról* beszélünk. A Tanúsítvány módosítás során az új *Tanúsítvány* azonos nyilvános kulcshoz kerül kibocsátásra. A Tanúsítvány módosítás részleteit a 4.8. fejezet írja le.
- Ha az *Alany* kérésére a *Hitelesítés-szolgáltató* az új *Tanúsítvány*t új nyilvános kulcshoz bocsátja ki, a folyamatot *kulcscserének* nevezzük, amelyet a 4.7. fejezet ír le. Kulcscserére jellemzően akkor kerül sor, ha az *Alany Tanúsítvány*a már nem érvényes (pl. kulcskompromittálódás miatt visszavonásra került), de még érvényes *Tanúsítvány* esetén is történhet kulcscsere (például, ha a régi kulcsok mérete már nem megfelelő).

A Tanúsítványcseréhez kapcsolódó folyamatok bizonyos pontokon egyszerűbbek, mint egy új *Tanúsítvány* igénylésének folyamata. Az új *Tanúsítvány* kibocsátásának folyamatától való eltérést – a Tanúsítványcsere mindhárom esetében – a hozzájuk kapcsolódó fejezetek (4.6., 4.7. és 4.8.) tartalmazzák.

Amennyiben egy korábbi – érvényes szolgáltatási szerződéssel rendelkező – *Ügyfél* a meglevőn kívül új *Tanúsítvány*t igényel, akkor szükséges a szolgáltatási szerződés módosítása, azonban az igénylés folyamata szintén egyszerűbb, mint az első *Tanúsítvány* igénylése esetében. Ezeket az eltéréseket az új *Tanúsítvány* kibocsátásának folyamatát leíró részben jelezzük.

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

Egy *Tanúsítvány* fenntartását kizárólag a rá vonatkozó szolgáltatási szerződés érvényessége alatt végzi a *Hitelesítés-szolgáltató*. A szolgáltatási szerződés lezárásával kapcsolatos előírást a 4.11. fejezet tartalmazza.

4.1. Tanúsítvány kérelem

Minden új *Tanúsítvány* kiadásához *Tanúsítvány kérelem* benyújtására van szükség. Az első *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 tekinti 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 előkészíti az *Előfizető*vel kötendő szolgáltatási szerződést. A szolgáltatási szerződésnek tartalmaznia kell, hogy annak keretében mely *Alany*ok milyen szolgáltatási csomag keretében, milyen típusú *Tanúsítvány*t jogosultak igényelni.

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

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

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

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

A *Tanúsítvány kérelem*ben a következő adatokat kell megadnia az *Alany*nak:

- a *Tanúsítvány*ba kerülő adatok (pl. név, cím, *Szervezet* neve, város, ország, e-mail cím).
- az *Alany – Szervezet* esetében a *Szervezet* képviselőjének – személyes azonosító adatai teljes név, személyazonosító okmány száma, anyja neve, születés helye, ideje);
- az *Alany – Szervezet* esetében a *Szervezet* képviselőjének – elérhetőségei (telefonszám, e-mail cím);
- szervezeti *Tanúsítvány* igénylése esetében a *Szervezet* adatai hivatalos elnevezése, székhelye, opcionálisan: azonosító adatai, a szervezeti egység elnevezése);
- az *Előfizető* adatai (számlázási adatok);

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

- 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 a 3.2.5. fejezetnek megfelelően;
- amennyiben az *Alany* természetes személy, de a *Tanúsítvány*ban kéri egy *Szervezet*hez való tartozás feltüntetését, akkor a *Szervezet* igazolását arról, hogy ehhez hozzájárul a 3.2.2. fejezetnek megfelelően;
- amennyiben a kért *Tanúsítvány*ban szerepel márkanév vagy védjegy, akkor annak igazolását, hogy az *Alany* jogosult annak használatára a 3.1.6. fejezetnek megfelelően.

4.1.1. Ki nyújthat be tanúsítvány kérelmet

Tanúsítvány kérelmet természetes személyek nyújthatnak be saját maguk vagy az általuk képviselt szervezet számára történő *Tanúsítvány* kibocsátása céljából. A *Tanúsítvány* kibocsátás előfeltétele az adott *Tanúsítvány* kibocsátására és fenntartására vonatkozó érvényes (az *Előfizető* és a *Hitelesítés-szolgáltató* által aláírt) szolgáltatási szerződés megléte.

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

- papíralapon kézi aláírásával ellátva a személyesen azonosítás alkalmával a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely külső *Regisztráló szervezet* regisztrációs munkatársa előtt;
- papíralapon postai úton a *Hitelesítés-szolgáltató* postacímére megküldve (ekkor a személyes azonosításra később kerül sor);
- elektronikus formában, egy nem álneves tanúsítványán alapuló minősített elektronikus aláírással ellátva, a *Hitelesítés-szolgáltató* e-mail címére megküldve.

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 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.

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 munkatársa meggyőződik a *Tanúsítvány kérelmet* benyújtó személy azonosságáról (lásd: 3.2.3. fejezet). Amennyiben az *Alany* szervezet, vagy a *Tanúsítvány*ban feltüntetésre kerül egy *Szervezet* neve is (Szervezeti tanúsítvány), akkor a *Hitelesítés-szolgáltató* (vagy a *Regisztráló szervezet*) azonosítja a *Szervezet*et (lásd: 3.2.2. fejezet) illetve meggyőződik arról, hogy az igénylő személy jogosult a *Szervezet* képviseletére lásd: 3.2.5. fejezet illetve a *Szervezet*hez kapcsolódó *Tanúsítvány* igénylésére (lásd: 3.2.2. fejezet). Az *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* adategyeztetést végez közhiteles adatbázisokkal (például a lakcímnyilvántartással vagy a cégnyilvántartással). Amely adatbázisok esetén ez megoldható, ott a *Hitelesítés-szolgáltató* az adategyeztetést elektronikusan végzi.

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

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

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

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

- annak megerősítését, hogy a *Tanúsítvány kérelem*ben megadott adatok pontosak;
- azt, hogy hozzájárul ahhoz, hogy a *Hitelesítés-szolgáltató* a kérelemben megadott adatait nyilvántartsa és kezelje;
- azt, hogy hozzájárul-e a *Tanúsítvány* közzétételéhez;

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

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

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

Amennyiben az *Alany*(szervezet esetében annak képviselőjének) személyazonossága, vagy szervezeti tanúsítvány esetében a *Szervezet* azonossága, illetve szervezethez kapcsolódó személyes tanúsítvány esetében az *Alany*nak a *Képviselt szervezet*hez való tartozása nem állapítható meg minden kétséget kizáróan, vagy valamely, a tanúsítványkérelem űrlapon feltüntetett adat nem helyes, akkor a *Hitelesítés-szolgáltató* belső szabályzatainak megfelelően lehetőséget adhat az *Ügyfél*nek a hiányos vagy hibás adatokat korrigálására, illetve a hiányzó igazolásokat átadására a Tanúsítvány kérelem benyújtásától számított 3 hónapon belül.

4.2. A tanúsítvány kérelem feldolgozása

4.2.1. Az igénylő azonosítása és hitelesítése

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

4.2.2. A tanúsítvány kérelem elfogadása vagy visszautasítása

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

Amennyiben az *Alany* e-mail címet tartalmazó *Tanúsítvány*t igényel, a *Hitelesítés-szolgáltató* a *Tanúsítvány* kibocsátása előtt ellenőrzi a *Tanúsítvány*ba kerülő e-mail címet is. Meggyőződik róla, hogy az valóban létező e-mail cím, valamint ellenőrzi, hogy az e-mail cím valóban az *Alany* e-mail címe.

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

Amennyiben az azonosításra kerülő természetes személy vagy szervezet azonossága, illetve szervezethez kapcsolódó személyes tanúsítvány esetében az *Alany*nak a *Képviselt szervezet*hez való tartozása nem állapítható meg minden kétséget kizáróan, vagy valamely, a tanúsítványkérelem

űrlapon feltüntetett adat nem helyes, és ezeket az *Ügyfél* a *Hitelesítés-szolgáltató* kérésére sem korrigálta vagy egészítette ki, akkor a *Hitelesítés-szolgáltató* elutasítja a kérelmet.

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

4.2.3. A tanúsítvány kérelem feldolgozásának időtartama

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

4.3. A tanúsítvány kibocsátása

A A III. tanúsítási osztályba tartozó *Tanúsítvány*ok esetén a *Hitelesítés-szolgáltató* csak a *Tanúsítvány kérelem* elfogadása esetén állítja 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 tartalmazza.

Amennyiben az *Alany* számára a *Hitelesítés-szolgáltató* biztosítja az *Aláírás-létrehozó eszköz*t is (eszköz-szolgáltatás keretében), akkor a folyamat részeként a kibocsátott Tanúsítvány telepítésre kerül az *Aláírás-létrehozó eszköz*re is. A magánkulcsot tartalmazó *Aláírás-létrehozó eszköz Alany*nak történő átadása ellenőrzött keretek között, a 6.1.2. fejezetben ismertetett biztonsági előírások betartása mellett történik. Amennyiben az *Alany Tanúsítvány*át és magánkulcsát tartalmazó *Aláírás-létrehozó eszköz* átvétele nem közvetlenül a tanúsítvány igényléshez kapcsolódó személyes azonosítást követően történik, akkor az *Alany* (nem természetes személy *Aláíró* esetén a képviselője) olyan személyes azonosítást követően veheti át az eszközét, amely során személyazonosításra alkalmas igazolvánnyal kell azonosítania magát. Az átadó fél ellenőrzi, hogy az *Alany* arcképe megfelel-e az igazolványában szereplő arcképnek, és az *Alany* aláírása megfelel-e az igazolványában szereplő aláírásának.

Az *Aláírás-létrehozó eszköz* átvételével egyidejűleg az *Alany* megkapja az aktiválásához szükséges, a 6.4. fejezetnek megfelelően előállított aktiváló kódokat is. E kódokat zárt borítékban kapja meg, amelyet átvételkor köteles felnyitni és ellenőrizni, hogy a kódok olvashatóak-e.

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

4.3.1. A Hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során

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

4.3.2. Az Ügyfél értesítése a tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* a *Tanúsítvány* kibocsátásáról értesíti az *Alany*t és az *Előfizető*t, valamint lehetővé teszi 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* részére kiállított *Tanúsítvány* esetén az *Alany* képviselőjének – a *Tanúsítvány* átvétele során ellenőriznie kell a *Tanúsítvány*ban szereplő adatok helyességét és erről írásbeli nyilatkozatot kell tennie. A nyilatkozatban az *Alany* vagy képviselője egyúttal igazolja a *Tanúsítvány* átvételét is.

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.

Amennyiben az *Alany* számára a *Hitelesítés-szolgáltató* biztosítja az aláírás-létrehozó eszközt is, akkor az *Alany* magánkulcsát és *Tanúsítvány*át tartalmazó aláírás-létrehozó eszköz, valamint az aktiváláshoz szükséges kód átvétele után az Alany kipróbálhatja az aláírás-létrehozó eszközét. Ezt követően az Alanynak (kézzel) alá kell írnia a kártyaátvételi nyilatkozatot, amelyben – többek között – azt igazolja, hogy a tanúsítványban szereplő adatok helyesek, az aláírás-létrehozó eszközt és a hozzá tartozó aktiváló kódokat átvette, valamint azt, hogy ismeri az eszköz használatának műszaki és jogszabályi feltételeit.

4.4.2. A tanúsítvány közzététele

A *Tanúsítvány Alany*nak történő átadását követően – amennyiben az *Alany* ehhez hozzájárult– a *Hitelesítés-szolgáltató* haladéktalanul közzéteszi a *Tanúsítvány*t a nyilvános tanúsítványtárában.

4.4.3. További szereplők értesítése a tanúsítvány kibocsátásról

Amennyiben a *Tanúsítvány*t olyan céllal bocsátották ki, hogy az *Alany* egy *Szervezet* nevében hozhasson létre elektronikus aláírást, a *Tanúsítvány* kibocsátásáról a *Hitelesítés-szolgáltató* haladéktalanul értesíti a *Képviselt szervezet* 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 elektronikus aláírás létrehozására használhatja, más felhasználás (pl. azonosítás, titkosítás) nem engedélyezett.

Lejárt érvényességű, visszavont, vagy felfüggesztett *Tanúsítvány*hoz tartozó magánkulcs nem használható elektronikus aláírás létrehozására.

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* segítségével igazolt elektronikus aláírás elfogadása során a *Hitelesítés-szolgáltató* által garantált biztonsági szint megtartásához szükséges, hogy az *Érintett fél* megfelelő körültekintéssel járjon el , különös tekintettel az alábbiakra:

- ellenőrizze a *Tanúsítvány* érvényességét, felfüggesztési és visszavonási állapotát;
- az aláíró tanúsítványokat, illetve az azokhoz tartozó nyilvános kulcsokat kizárólag elektronikus aláírás ellenőrzésére használja;
- a *Tanúsítvány*ra vonatkozó ellenőrzéseket célszerű elvégeznie a teljes tanúsítványláncra vonatkozóan;
- az elektronikus aláírás ellenőrzését megbízható alkalmazással végezze, amely megfelel az aktuális vonatkozó műszaki ajánlásoknak, és amely rugalmasan konfigurálható és megfelelően van beállítva, valamint vírusmentes környezetben fut;
- szervezethez kapcsolódó személyes *Tanúsítvány*ok esetén azt is javasolt megvizsgálni, hogy az aláíró a *Tanúsítvány* alapján megállapítható (pl. a "Title" mezőben feltüntetett) szerepe szerint jogosan írta-e alá az adott dokumentumot;
- javasolt ellenőrizni, hogy a *Tanúsítvány* a célnak megfelelő hitelesítési rend alapján lett-e kibocsátva;
- javasolt megvizsgálni az adott *Tanúsítvány*ban is feltüntetett, a tanúsítvánnyal egy alkalommal vállalható kötelezettség legmagasabb értékét (az ezen korlátokat meghaladó ügyletekben kibocsátott és aláírt elektronikus dokumentumból származó követelésekért, illetve az így okozott kárért a Hitelesítés-szolgáltató az Eat. [3] 15. § (2) bekezdése értelmében nem felel);

- vegyen figyelembe minden korlátozást, amely a *Tanúsítvány*ban vagy a *Tanúsítvány*ban meghivatkozott szabályzatokban szerepel.

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

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

4.6. Tanúsítvány megújítás

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

Tanúsítvány megújítására jellemzően akkor kerül sor, amikor az *Alany* meglévő *Tanúsítvány*a még érvényes, de hamarosan le fog járni. Ha az *Alany* a *Tanúsítvány*t a lejáíratot követően is használni szeretné, akkor kezdeményeznie kell a *Tanúsítvány* megújítását. A *Tanúsítvány* megújítás műszakilag új *Tanúsítvány* kibocsátását jelenti, amelybe az előzőben szereplővel megegyező Alanyt azonosító adatok, azonban új érvényességi időtartam kerül. A *Tanúsítvány*ban esetleg változhatnak további adatok is, mint például a CRL és OCSP hivatkozások vagy a Tanúsítvány aláírására használt szolgáltatói kulcs.

4.6.1. A tanúsítvány megújítás körülményei

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

- a 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 fogad el.

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

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

A *Tanúsítvány* megújítása során a *Hitelesítés-szolgáltató* tájékoztatja az *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 megadja a fenti tájékoztatást.

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

4.6.2. Ki kérelmezheti a tanúsítvány megújítást

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

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

- papíralapon kézi aláírásával ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely külső Regisztráló szervezet regisztrációs munkatársa előtt, előzetesen egyeztetett időpontban;
- elektronikus aláírásával ellátva e-mailben,
- kézi aláírással ellátva postai úton az Ügyfélszolgálatnak eljuttatva.

4.6.3. A tanúsítvány megújítási kérelmek feldolgozása

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

- a benyújtott tanúsítvány megújítási kérelem hiteles;
- a tanúsítvány megújítási kérelem benyújtója rendelkezik a szükséges jogosultságokkal, felhatalmazásokkal;
- a tanúsítvány megújítási kérelem benyújtója nyilatkozott a *Tanúsítvány*ba kerülő *Alany* adatok változatlanságáról és érvényességéről;
- a 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.

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

4.6.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

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

4.6.5. A megújított tanúsítvány elfogadása

Mivel a tanúsítvány megújítás során nem történik új kulcs generálása, így nem kell kulcsot átadni az *Alany* részére. A megújított *Tanúsítvány* személyes találkozás nélkül is átvehető (letölthető). Amennyiben az *Alany* magánkulcsa *Aláírás-létrehozó eszköz*ön található, akkor *Tanúsítvány*t maga telepíti az eszközre. Ehhez a *Hitelesítés-szolgáltató* írásos segédletet biztosít, illetve szükség esetén telefonos konzultációs lehetőséget is nyújt. Az *Alany* a *Tanúsítvány* használatba vételével fogadja el a *Tanúsítvány*t, nincs szükség külön nyilatkozat tételére.

4.6.6. A megújított tanúsítvány közzététele

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

4.6.7. 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 a *Hitelesítés-szolgáltató* haladéktalanul értesíti a *Képviselt szervezet* 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 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.

Kulcscserére jellemzően akkor kerül sor, ha az *Alany Tanúsítvány*a már nem érvényes (pl. kulcskompromittálódás miatt visszavonásra került), de még érvényes *Tanúsítvány* esetén is történhet kulcscsere (például, ha a régi kulcsok mérete már nem megfelelő). Kulcscserét az *Alany* külön indoklás nélkül is kérhet.

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

4.7.1. A kulcscsere körülményei

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

A kulcscsere során a *Hitelesítés-szolgáltató* tájékoztatja az *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 megadja a fenti tájékoztatást.

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

4.7.2. Ki kérelmezheti a kulcscserét

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

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

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

- papíralapon kézi aláírásával ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely külső Regisztráló szervezet regisztrációs munkatársa előtt, előzetesen egyeztetett időpontban;
- elektronikus aláírásával ellátva e-mailben,
- a *Tanúsítvány* felfüggesztési vagy visszavonási folyamata során,
- kézi aláírással ellátva postai úton az Ügyfélszolgálatnak eljuttatva.

4.7.3. A kulcscsere kérelmek feldolgozása

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

- a benyújtott kérelem hiteles;

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

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

4.7.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

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

4.7.5. A kulcscserével megújított tanúsítvány elfogadása

Amennyiben a kulcscsere során felhasznált új kulcsot a *Hitelesítés-szolgáltató* generálta egy *Aláírás-létrehozó eszköz*ön, akkor a kulcscsere folyamat részeként a kibocsátott *Tanúsítvány* telepítésre kerül az *Aláírás-létrehozó eszköz*re is. A magánkulcsot tartalmazó *Aláírás-létrehozó eszköz* *Alany*nak történő átadása ellenőrzött keretek között, a 6.1.2. fejezetben ismertetett biztonsági előírások betartása mellett történik. Az *Alany* (nem természetes személy qdefAlairo esetén a képviselője) olyan személyes azonosítást követően veheti át az eszközét, amely során személyazonosításra alkalmas igazolvánnyal kell azonosítania magát. Az átadó fél ellenőrzi, hogy az *Alany* arcképe megfelel-e az igazolványában szereplő arcképnek, és az *Alany* aláírása megfelel-e az igazolványában szereplő aláírásának. Az *Aláírás-létrehozó eszköz* átvételével egyidejűleg az *Alany* megkapja az aktiválásához szükséges, a 6.4. fejezetnek megfelelően előállított aktiváló kódokat is. E kódokat zárt borítékban kapja meg, amelyet átvételkor köteles felnyitni és ellenőrizni, hogy a kódok olvashatóak-e. Az *Alany*nak az *Aláírás-létrehozó eszköz* kipróbálása után (kézzel) alá kell írnia a kártyaátvételi nyilatkozatot, amelyben – többek között – azt igazolja, hogy a *Tanúsítvány*ban szereplő adatok helyesek, az *Aláírás-létrehozó eszköz*t és a hozzá tartozó aktiváló kódokat átvette, valamint azt, hogy ismeri az eszköz használatának műszaki és jogszabályi feltételeit.

Amennyiben a kulcscsere során felhasznált új kulcsot az *Alany* biztosította, akkor nincs szükség kulcs illetve *Aláírás-létrehozó eszköz* átadására. A kulcscsere keretében kibocsátott új *Tanúsítvány* személyes találkozás nélkül is átvehető (letölthető). Az *Alany* a *Tanúsítvány* használatba vételével fogadja el a *Tanúsítvány*t, nincs szükség külön nyilatkozat tételére.

4.7.6. A kulcscserével megújított tanúsítvány közzététele

A *Hitelesítés-szolgáltató* az eredeti *Tanúsítvány* kibocsátásával megegyező módon kell publikálja 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 a *Hitelesítés-szolgáltató* haladéktalanul értesíti 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.

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

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

4.8.1. A tanúsítvány módosítás körülményei

A tanúsítvány módosítás szükségessé válik az alábbi esetekben:

- az *Alany Tanúsítvány*ban szereplő adatai megváltoznak;
- a *Hitelesítés-szolgáltató Tanúsítvány* kibocsátó rendszerében megváltozik az adott *Tanúsítvány*t kibocsátó CA valamely a "Subject DN"-ben szereplő azonosító adata vagy a nyilvános kulcsa és így szolgáltatói *Tanúsítvány*a;
- a *Tanúsítvány*ban a *Hitelesítés-szolgáltató* által megadott, a szolgáltatásra jellemző adatok (tanúsítvány profil) megváltoznak.

A tanúsítvány módosítás feltételei:

- 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 fogad el.

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

Amennyiben az *Alany Tanúsítvány*ban szereplő adatai nem változtak, de a közelgő lejárati dátum miatt szeretne új *Tanúsítvány*t igényelni, akkor azt a Tanúsítvány megújítás (lásd: 4.6. fejezet) keretében kell igényelnie.

Az új *Tanúsítvány* kibocsátása során a *Hitelesítés-szolgáltató* tájékoztatja 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 megadja a fenti tájékoztatást.

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

4.8.2. Ki kérelmezheti a tanúsítvány módosítást

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

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

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

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

- papíralapon kézi aláírásával ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely külső Regisztráló szervezet regisztrációs munkatársa előtt, előzetesen egyeztetett időpontban;
- elektronikus aláírásával ellátva e-mailben,
- papíralapon kézi aláírással ellátva postai úton az Ügyfélszolgálatnak eljuttatva.

4.8.3. A tanúsítvány módosítási kérelmek feldolgozása

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

- a benyújtott kérelem hiteles;

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

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

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

4.8.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

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

4.8.5. A módosított tanúsítvány elfogadása

Mivel a Tanúsítvány módosítás során nem történik új kulcs generálása, így nem kell kulcsot átadni az *Alany* részére. A módosított *Tanúsítvány* személyes találkozás nélkül is átvehető (letölthető). Amennyiben az *Alany* magánkulcsa aláírás-létrehozó eszközön található, akkor *Tanúsítvány*t maga telepíti az eszközre. Ehhez a *Hitelesítés-szolgáltató* írásos segédletet biztosít, illetve szükség esetén telefonos konzultációs lehetőséget is nyújt. Az *Alany* a Tanúsítvány használatba vételével fogadja el a Tanúsítványt, nincs szükség külön nyilatkozat tételére.

4.8.6. A módosított tanúsítvány közzététele

A *Hitelesítés-szolgáltató* az eredeti *Tanúsítvány* kibocsátásával megegyező módon publikálja a módosított *Tanúsítvány*t.

4.8.7. 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 a *Hitelesítés-szolgáltató* haladéktalanul értesíti a *Képviselt szervezet* 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.

A visszavont és felfüggesztett tanúsítványhoz tartozó magánkulcs használatát azonnal meg kell szüntetni, illetve fel kell függeszteni. A visszavont tanúsítványhoz tartozó magánkulcsot a visszavonást követően azonnal meg kell semmisíteni, amennyiben ez lehetséges.

Felelősségi szabályok a felfüggesztéssel és visszavonással kapcsolatban:

- A visszavonási/felfüggesztési kérelem *Hitelesítés-szolgáltató*hoz történő megérkezéséig az *Alany*, illetve az *Előfizető* a felelős a felmerülő károkért.
- Azon pillanattól kezdve, amikor a *Hitelesítés-szolgáltató* a felfüggesztés vagy visszavonás bejelentést elfogadja, a *Hitelesítés-szolgáltató* felel a felmerülő károkért. A *Hitelesítés-szolgáltató* a kérelem elfogadását követően haladéktalanul közzéteszi a tanúsítvány megváltozott visszavonási állapotát.
- Amennyiben a *Hitelesítés-szolgáltató* már közzétette a tanúsítvány érténytelen visszavonási állapotát, a *Hitelesítés-szolgáltató* semmilyen felelősséget nem vállal azért, ha az *Érintett fél* ekkor mégis érvényesnek tekinti a tanúsítványt.

4.9.1. A tanúsítvány visszavonás körülményei

A *Hitelesítés-szolgáltató* intézkedik 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;
- ha a *Tanúsítvány*t a *Hitelesítés-szolgáltató* harmadik féltől származó dokumentum alapján állította ki, és e harmadik fél ezen igazolást írásban visszavonja;
- az *Alany* vagy az *Előfizető* írásban kéri a *Tanúsítvány* visszavonását;

- a *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem az *Alany* kizárólagos birtokában van illetve tárolt kulcsos aláírás szolgáltatás esetén nem csak az *Aláíró* fér hozzá kizárólagosan;
- 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 *Tanúsítvány* korábban felfüggesztésre került és nem került visszaállításra az erre biztosított időtartam alatt (lásd: 4.9.16. fejezet);
- a szolgáltatási szerződés megszűnik;
- 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 *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 *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-szolgáltatóra 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;
- ha a *Tanúsítvány*t a *Hitelesítés-szolgáltató* harmadik féltől származó dokumentum alapján állította ki, és e harmadik fél ezen igazolást írásban visszavonja;
- 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.

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 papíralapú vagy minősített vagy a visszavonni kívánt Tanúsítvánnyal azonos hitelesítési rendbe tartozó fokozott biztonságú elektronikus aláírással ellátott elektronikus dokumentumon fogadhat be. A *Hitelesítés-szolgáltató* a tanúsítvány visszavonási kérelem benyújtására legalább az alábbi lehetőségeket biztosítja:

- papíralapon kézi aláírásával ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, ügyfélszolgálati időben;

- minősített vagy a visszavonni kívánt Tanúsítvánnyal azonos hitelesítési rendbe tartozó fokozott biztonságú elektronikus aláírásával ellátva e-mailben,
- kézi aláírással ellátva postai úton az Ügyfélszolgálatnak eljuttatva.

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

Személyes kérelem benyújtása esetén a kérelmező azonosítása a 3.2.3-as fejezetben leírtak szerint történik.

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

A papíralapon, postai úton történő visszavonási kérelem benyújtása esetében a *Hitelesítés-szolgáltató* ellenőrzi a kérelmen található kézi aláírást, valamint a kezdeti regisztrációkor egyeztetett elérhetőségek valamelyikén felveszi a kérelmezővel a kapcsolatot a kérelem megerősítése érdekében.

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

Amennyiben a visszavonást az *Ügyfél* kéri kulcskompromittálódás miatt, akkor a *Hitelesítés-szolgáltató* lehetőséget biztosít számára a visszavonási eljárás során, hogy a visszavonandó *Tanúsítvány* helyett kulcscsere keretében új *Tanúsítvány*t igényeljen. A kulcscsere szabályait a 4.7. fejezet tartalmazza.

4.9.4. A visszavonási kérelemre vonatkozó kivárási idő

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

4.9.5. A visszavonási eljárás maximális hossza

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

A személyesen benyújtott kérelmek esetén a megérkezés időpontja az, amikor az *Ügyfél* megad minden, a visszavonáshoz szükséges adatot. A postán vagy elektronikus levélben küldött kérelmek esetén a megérkezés időpontja az, amikor a levél nyitvatartási időben a *Hitelesítés-szolgáltató* ügyfélszolgálatához, vagy a *Hitelesítés-szolgáltató* szerverén lévő postafiókba ér. A nyitvatartási időn kívül érkező levelek a legközelebbi nyitvatartási idő kezdetén tekinthetőek megérkezettnek. A *Hitelesítés-szolgáltató* kizárólag az 1.2. fejezetben megjelölt címekre küldött kérelmekre vállalja e követelmények teljesítését, más csatornákon vagy címekre – különösen a *Hitelesítés-szolgáltató*

egyes munkatársainak közvetlenül – küldött kérelmek feldolgozásával kapcsolatban semmilyen rendelkezésre állást nem vállal.

Ha az *Ügyfél* vissza kívánja vonni a tanúsítványát, és a visszavonás sürgős, vagy az *Ügyfél* nem képes személyesen bemenni a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájába, a *Hitelesítés-szolgáltató* azt javasolja, hogy a visszavonásig az *Ügyfél* függessze fel a tanúsítványt a 24 órában elérhető telefonos ügyelet segítségével (lásd: 4.9.13. fejezet). A felfüggesztett tanúsítvány visszavonásáról elég később gondoskodni, illetve a felfüggesztett *Tanúsítvány*okat a *Hitelesítés-szolgáltató* a visszaállításra rendelkezésre álló idő letelte után automatikusan visszavonja (lásd: 4.9.16. fejezet).

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

A *Tanúsítvány*ban foglalt információ elfogadását és felhasználását megelőzően a Hitelesítés-szolgáltató által garantált biztonsági szint megtartásához szükséges, hogy az *Érintett felek* megfelelően gondosan járjanak el, így különösen javasolt ellenőrizniük a tanúsítási láncban található valamennyi *Tanúsítvány* érvényességét a vonatkozó műszaki szabványoknak megfelelően. Az 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* naponta legalább egyszer, de kulcskompromittálódás miatti visszavonás vagy felfüggesztés esetén a bejelentés elfogadását követően azonnal kibocsát új tanúsítvány visszavonási listát a végfelhasználói *Tanúsítvány*okat kibocsátó hitelesítési egységeire.

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

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

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

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

4.9.9. Valós idejű tanúsítvány állapot ellenőrzés lehetősége

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

4.9.10. A valós idejű tanúsítvány állapot ellenőrzésre vonatkozó követelmények

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

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

4.9.11. A visszavonási hirdetmények egyéb elérhető formái

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

4.9.12. A kulcs kompromittálódásra vonatkozó speciális követelmények

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

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

4.9.13. A felfüggesztés körülményei

A *Hitelesítés-szolgáltató* lehetőséget nyújt az *Ügyfel*ek számára a *Tanúsítvány*ok használhatóságának ideiglenes megszüntetésére arra az esetre, ha feltételezhető, hogy a *Tanúsítvány* visszavonását megalapozó okok valamelyike fennáll.

A *Hitelesítés-szolgáltató* maga is jogosult a *Tanúsítvány* felfüggesztésére, a következő okok esetén:

- Ha az *Előfizető* a fizetési határidőig nem fizet.
- Ha a *Hitelesítés-szolgáltató* valószínűsíti, hogy a tanúsítványban szereplő adatok nem felelnek meg a valóságnak, azaz az Eat. 14. §-a (1), (2) bekezdés b), c), e), illetve f) pontjaiban meghatározott valamely körülmények esetén. Amennyiben a *Hitelesítés-szolgáltató* e körülményekről tudomást szerez, kezdeményezi a tanúsítvány felfüggesztését vagy visszavonását.
- Ha a *Hitelesítés-szolgáltató* valószínűsíti, hogy a tanúsítványhoz tartozó magánkulcs nem az *Alany* birtokában van, és ezt megalapozott bizonyítékok alátámasztják. Amennyiben a *Hitelesítés-szolgáltató* tudomására jut, hogy egy intelligens kártya illetéktelen kezekbe került, akkor a *Hitelesítés-szolgáltató* a rajta lévő összes tanúsítványt felfüggeszti.

4.9.14. Ki kérelmezheti a felfüggesztést

Egy *Tanúsítvány* felfüggesztését ugyanazok a felek kezdeményehetik, akik jogosultak az adott *Tanúsítvány* visszavonását is kérni (lásd: 4.9.2. fejezet).

4.9.15. A felfüggesztési kérelemre vonatkozó eljárás

A *Hitelesítés-szolgáltató* a következő módokon nyújt lehetőséget a felfüggesztés kezdeményezésére:

- telefonos ügyeleten keresztül;
- a honlapján keresztül;
- a visszavonási kérelmek benyújtásával azonos módon.

Felfüggesztés telefonos ügyeleten keresztül

A telefonos felfüggesztés a hét 7 napján, a nap 24 órájában működik. A *Hitelesítés-szolgáltató Ügyfel*ei ezen ügyelet segítségével jelezhetik a *Hitelesítés-szolgáltató*nak, ha kártyájuk vagy magánkulcsuk illetéktelen kezekbe került. A telefonos felfüggesztés szolgáltatás rendelkezésre állása éves szinten legalább 99% , és az eseti szolgáltatás-kiesések nem haladhatják meg a 3 órát. A telefonon megérkező kérelmeket a *Hitelesítés-szolgáltató* soron kívül dolgozza fel és haladéktalanul teljesíti.

A telefonos kérelemre a *Hitelesítés-szolgáltató* ügyeletes munkatársa válaszol. A *Hitelesítés-szolgáltató* jogosult hangfelvételt készíteni az ügyelethez megérkező felfüggesztések és visszaállítások során elhangzott párbeszédekről.

A *Hitelesítés-szolgáltató* ügyeletes munkatársa a következő információkat mindenképpen elkéri a kérelmezőtől:

- a kérelmező nevét,
- azon *Alany* nevét, akinek a *Tanúsítvány*át fel kell függeszteni,
- az *Alany* születési dátumát vagy a *Tanúsítvány*ában szereplő OID-jének utolsó három tagját (pl. 2.2.123),
- a felfüggesztési kérelem hitelességét igazoló adatot vagy adatokat:
  - a felfüggesztési jelszót, vagy
  - a felfüggesztési jelszó helyett az *Alany* személyes adatait, azaz
    - születési nevét és
    - születési idejét és

* születési helyét és
* anyja nevét.

Amennyiben a kérelmező nem adja meg a fenti listában szereplő kötelező adatok valamelyikét, vagy nem a helyes jelszót adja meg, a *Hitelesítés-szolgáltató* elutasítja a felfüggesztési kérelmet.

Amint a *Hitelesítés-szolgáltató* munkatársa a telefonbeszélgetés során sikeresen megállapította a kérelmező felfüggesztési jogosultságát, közli, hogy a kérelmet a *Hitelesítés-szolgáltató* elfogadta, és megkezdte annak feldolgozását. E pillanattól a *Hitelesítés-szolgáltató* felelősséget vállal a *Tanúsítvány* elfogadásából eredő károkért, amíg a *Tanúsítvány* új visszavonási állapota meg nem jelenik a *Hitelesítés-szolgáltató* visszavonási nyilvántartásában.

Amennyiben a kérelmező az *Ügyfél* valamely kártyájához tartozó felfüggesztési jelszót adja meg, a *Hitelesítés-szolgáltató* a kártyára kibocsátott összes tanúsítványt felfüggeszti. Amennyiben a kérelmező az *Ügyfél* valamely szoftveres *Tanúsítvány*ához tartozó felfüggesztési jelszót adja meg, a *Hitelesítés-szolgáltató* a összes szoftveres tanúsítványt felfüggeszti. Amennyiben a kérelmező az *Alany* személyes adatait adta meg, a *Hitelesítés-szolgáltató* az *Alany* valamennyi tanúsítványát felfüggeszti.

A *Hitelesítés-szolgáltató* a felfüggesztési kérelmet a hívás időtartama alatt – jellemzően néhány másodpercen belül – feldolgozza, és az esetleg megváltozott visszavonási állapot a feldolgozást követően azonnal megjelenik a *Hitelesítés-szolgáltató* visszavonási nyilvántartásában. A *Hitelesítés-szolgáltató* belső folyamatai biztosítják, hogy e művelet legfeljebb 5 percen belül lezajlik, azaz a megváltozott visszavonási állapot a felfüggesztési kérelem megérkezésétől számítva legfeljebb ennyi időn belül közzétételre kerül.

Mivel telefonon a felfüggesztési jogosultság ellenőrzése (vagyis az *Alany* azonosítása) jelszó vagy személyes adatok alapján történik. A *Hitelesítés-szolgáltató* mindenkitől elfogadja a felfüggesztést, aki meg tudja adni a helyes felfüggesztési jelszót vagy személyes adatokat.

Sikeres felfüggesztés esetén a *Hitelesítés-szolgáltató* e-mailben értesíti az *Alany*t és az *Előfizető*t a felfüggesztés tényéről.

Felfüggesztés weben keresztül

A felfüggesztés a *Hitelesítés-szolgáltató* honlapján keresztül is kérhető az alábbi címen:

`https://www.e-szigno.hu/felfuggesztes`

A *Hitelesítés-szolgáltató* honlapján keresztül az *Ügyfél*nek pontosan azon információkat kell megadnia, mint a telefonos ügyeleten keresztül. A *Hitelesítés-szolgáltató* honlapján benyújtott tanúsítvány felfüggesztési kérelmeket a *Hitelesítés-szolgáltató* informatikai rendszere azonnal kiértékeli, és az eredményéről az oldalon tájékoztatja a kérelem benyújtóját. Sikeres felfüggesztés esetén a megváltozott visszavonási állapot azonnal megjelenik a *Hitelesítés-szolgáltató* visszavonási nyilvántartásában. A *Hitelesítés-szolgáltató* belső folyamatai biztosítják,

hogy a feldolgozás az adatok megadásától számított legfeljebb 5 percen belül lezajlik, azaz a megváltozott visszavonási állapot a felfüggesztési kérelem megérkezésétől számítva legfeljebb ennyi időn belül közzétételre kerül.

A *Hitelesítés-szolgáltató* minden felfüggesztési kérelmet naplóz. Sikeres felfüggesztés esetén a *Hitelesítés-szolgáltató* e-mailben értesíti az *Alany*t és az *Előfizető*t a felfüggesztés tényéről.

A *Hitelesítés-szolgáltató* a telefonon érkező felfüggesztési kérelmekre vállal rendelkezésre állást. Amennyiben a *Hitelesítés-szolgáltató* honlapja nem érhető el, a *Hitelesítés-szolgáltató* azt javasolja az *Ügyfél*nek, hogy telefonon keresztül kezdeményezze a felfüggesztést.

Felfüggesztés a visszavonási kérelmek benyújtásával azonos módon

A *Hitelesítés-szolgáltató* lehetővé teszi a felfüggesztési kérelmek benyújtását a visszavonási kérelmek benyújtásával azonos módon, a 4.9.3 fejezet előírásai szerint. A felfüggesztési kérelemből a *Hitelesítés-szolgáltató* pontosan meg kell, hogy tudja állapítani, hogy a kérelmező pontosan melyik *Tanúsítvány* felfüggesztését kéri, és milyen jogcímen. A regisztrációs munkatárs e-mailben értesítést küld az *Alany*nak és az *Előfizető*nek.

Felfüggesztéskor meg kell adni a *Tanúsítvány* felfüggesztésének okát. Amennyiben a felfüggesztést az *Ügyfél* kéri, és a visszavonás okát nem adja meg, a *Hitelesítés-szolgáltató* úgy tekinti, hogy a felfüggesztés oka a magánkulcs kompromittálódása.

Amennyiben a felfüggesztést az *Ügyfél* kéri kulcskompromittálódás miatt, akkor a *Hitelesítés-szolgáltató* lehetőséget biztosít számára a felfüggesztési eljárás során, hogy jelezze, hogy amennyiben a *Tanúsítvány* a megadott időkorláton belül nem kerül visszaállításra (és így visszavonásra kerül), akkor helyette kulcscsere keretében új *Tanúsítvány*t igényeljen. A kulcscsere szabályait a 4.7. fejezet tartalmazza.

4.9.16. A felfüggesztés maximális hossza

Az *Alany* által kért felfüggesztés esetén egy *Tanúsítvány* egyfolytában legfeljebb 5 munkanapig lehet felfüggesztett állapotban. Ha a *Tanúsítvány* ezen idő elteltével sem kerül visszaállításra, a *Hitelesítés-szolgáltató* a tanúsítványt külön értesítés nélkül visszavonja.

A *Tanúsítvány* visszaállítása azt a folyamatot jelenti, amelynek során a felfüggesztett *Tanúsítvány* újra érvényes állapotba kerül. Egy *Tanúsítvány* visszaállítását az a személy kérheti, aki az adott *Tanúsítvány* felfüggesztését kérte. Visszaállítási kérelem kizárólag személyesen vagy minősített vagy a visszaállítani kívánt Tanúsítvánnyal azonos hitelesítési rendbe tartozó fokozott biztonságú *Tanúsítvány*on alapuló elektronikusan aláírással ellátva nyújtható be a *Hitelesítés-szolgáltató*nak. Ha ugyanarra a tanúsítványra több féltől is érkezett felfüggesztési kérelem, akkor a *Hitelesítés-szolgáltató* csak akkor állítja vissza a tanúsítványt, ha mindegyik felfüggesztő fél kéri a visszaállítást is.

Sikeres *Tanúsítvány* visszaállítás esetén a *Hitelesítés-szolgáltató* e-mailben értesíti az *Alany*t és az *Előfizető*t ennek tényéről.

4.10. Tanúsítvány állapot szolgáltatások

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

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

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

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

A *Hitelesítés-szolgáltató* a végfelhasználói tanúsítványok visszavonási állapotát a tanúsítvány lejártán túl is közzéteszi. A lejárt tanúsítványokat nem távolítja el a CRL-ről, és a lejárt tanúsítványok tekintetében is ad OCSP szolgáltatást.

A *Hitelesítés-szolgáltató* ezt a tényt az "expiredCertsOnCRL" opcionális kiterjesztés használatával tünteti fel a visszavonási listában.

Felfüggesztés, visszaállítás és visszavonás esetén a folyamat sikeres lezárását követően a *Tanúsítvány* új állapota azonnal – lásd: 4.9. fejezet – megjelenik a *Hitelesítés-szolgáltató* visszavonási nyilvántartásában. Ettől a pillanattól kezdve a *Hitelesítés-szolgáltató* által nyújtott OCSP válaszok már a *Tanúsítvány* új visszavonási állapotát tartalmazzák.

Felfüggesztés, visszaállítás és visszavonás esetén a *Hitelesítés-szolgáltató* haladéktalanul – lásd: 4.9. fejezet – új CRL-t bocsát ki.

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

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

4.10.1. Működési jellemzők

A *Hitelesítés-szolgáltató* egyes hitelesítő egységei az alábbi gyakorisággal bocsátanak ki visszavonási listát:

- A *Hitelesítés-szolgáltató* SHA-256 alapú rendszerében működtetett produktív (nem gyökér) hitelesítő egységek legfeljebb 24 óránként bocsátanak ki CRL-t.

- A *Hitelesítés-szolgáltató* SHA-1 alapú rendszerében szereplő köztes egységek záró CRL-t bocsátanak ki, amelynek érvényességi ideje ("nextUpdate") megegyezik az adott egység *Tanúsítvány*ának érvényességi idejével.
- A "Microsec e-Szigno Root CA 2009" gyökér hitelesítő egység legfeljebb 24 óránként bocsát ki CRL-t.
- A "Microsec e-Szigno Root CA" gyökér hitelesítő egység legfeljebb havonta bocsát ki CRL-t.
- Az "e-Szigno OCSP CA" gyökér hitelesítő egység legfeljebb 24 óránként bocsát ki CRL-t[2].

Az egyes *Tanúsítvány*okra vonatkozó mindenkori aktuális visszavonási listák az alábbi oldalon érhetők el: `https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/szolgaltatoi-tanusitvanyok.html`

A visszavonási listák hatályba lépésének időpontja ("thisUpdate") egyúttal azt az időpontot is jelöli, amikor a hitelesítő egység a visszavonási listát összeállította, és aláírását megkezdte. Ezt követően a visszavonási lista publikálásáig hosszú visszavonási listák esetén egy vagy két perc is eltelhet. A következő visszavonási lista megjelenése (következő frissítés, "nextUpdate") azt az időpontot jelzi, amikortól kezdve a következő lista a nyilvánosság számára elérhető. Ennek megfelelően a visszavonási lista hatályba lépési időpontja és a következő visszavonási lista megjelenési időpontja között a fenti időintervallumoknál hosszabb időintervallumok is megjelenhetnek, ez nem befolyásolja azt, hogy a visszavonási listák megjelenése között legfeljebb 24 óra, illetve (szolgáltatói tanúsítványokra vonatkozó CRL esetében) egy hónap telik el.

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

Online tanúsítvány-állapot szolgáltatás (OCSP)

A *Hitelesítés-szolgáltató* a tanúsítványok visszavonási állapotát OCSP szolgáltatás segítségével is közzéteszi. E szolgáltatáson keresztül, a legfrissebb CRL-en elérhető állapottal megegyező információ érhető el.

Az SHA-1 alapú tanúsítványok tekintetében a *Hitelesítés-szolgáltató* az RFC 2560 szerinti "trusted responder" elv szerint nyújtja az OCSP szolgáltatást, azaz OCSP válaszadói külön tanúsítvány-hierarchiában helyezkednek el. Az SHA-256 alapú tanúsítványok tekintetében a *Hitelesítés-szolgáltató* az RFC 2560 szerinti "authorized responder" elv szerint nyújtja az OCSP szolgáltatást, így minden egyes hitelesítő egysége külön OCSP válaszadót hitelesít felül, amely az adott hitelesítő egység által kibocsátott tanúsítványok állapotára vonatkozóan nyújt információt (1.3.1. fejezet).

[2]Az "e-Szigno OCSP CA" által kibocsátott CRL egyetlen *Tanúsítvány*ra sem vonatkozik, mindig üres, mert az ezen egység által kibocsátott rövid lejáratú OCSP válaszadói *Tanúsítvány*ok "ocspNoCheck" kiterjesztést tartalmaznak.

A *Hitelesítés-szolgáltató* két különböző módon nyújt OCSP szolgáltatást, az alábbiakban e két változat jellemzőit mutatjuk be.

_Ügyfel_ek részére nyújtott OCSP szolgáltatás

- Az OCSP szolgáltatás e változatát azok az *Ügyfel*ek vehetik igénybe, akik rendelkeznek *Tanúsítvány* fenntartására vonatkozó érvényes szolgáltatási szerződéssel. A *Hitelesítés-szolgáltató* lekérdezéskor *Tanúsítvány* vagy felhasználónév-jelszó páros alapján azonosíthatja az *Ügyfel*et.
- Az OCSP szolgáltatás e változata minden *Tanúsítvány* tekintetében elérhető, a válaszok mindig a *Hitelesítés-szolgáltató* visszavonási nyilvántartásában szereplő aktuális információt tartalmazzák.
- A kibocsátott OCSP válasz mindig a lekérdezés időpontjának pillanatában készül. Az OCSP válaszban szereplő "thisUpdate" és "producedAt" időpontok megegyeznek a lekérdezés időpontjával.
- A válaszban szereplő "nextUpdate" időpont vagy nincsen kitöltve, vagy a válaszadói tanúsítvány lejáratánál nem későbbi időpontot tartalmaz.
- Az *Ügyfel*ek részére nyújtott OCSP szolgáltatás segítségével mindig beszerezhető olyan bizonyíték, amely később harmadik fél felé is igazolja a *Tanúsítvány*nak a *Hitelesítés-szolgáltató* nyilvántartásában szereplő visszavonási állapotát, a lekérdezés időpontjára vonatkozóan.

Nyilvánosan és ingyenesen nyújtott OCSP szolgáltatás

- Az OCSP szolgáltatás e változata nyilvánosan és ingyenesen érhető el, a visszavonási listákhoz hasonlóan bármely *Érintett fél* igénybe veheti. Lekérdezéskor nincsen szükség autentikációra.
- Az OCSP szolgáltatás e változata a tanúsítványokban feltüntetett URL-eken érhető el.
- Az RFC 6960 "Response Pre-production" eljárása alapján, a kibocsátott OCSP válasz a lekérdezést megelőzően is létrejöhet, és nem feltétlenül tartalmaz "nonce" elemet. A *Hitelesítés-szolgáltató* egyazon választ több lekérdezésre is visszaadhatja. Az OCSP válaszban szereplő "thisUpdate" és "producedAt" időpontok megegyeznek, de ezek megelőzhetik a lekérdezés időpontját.
- A válaszban szereplő "nextUpdate" időpont vagy nincsen kitöltve, vagy a válaszadói tanúsítvány lejáratánál nem későbbi időpontot tartalmaz.

- Az OCSP válaszok mindig a *Hitelesítés-szolgáltató* visszavonási nyilvántartásában szereplő aktuális információt tartalmazzák, azonban ha az OCSP válasz "thisUpdate" időpontja korábbi, mint az az időpont, amelyre nézve az ellenőrzést végezzük — amely vagy korábbi vagy egybeesik a lekérdezés időpontjával -–, akkor az OCSP válasz nem egyértelmű bizonyíték harmadik fél számára a *Tanúsítvány* visszavonási állapotára vonatkozóan.

Az OCSP szolgáltatás fenti két változatában jelzett különbözőségek következtében a nyilvánosan és ingyenesen nyújtott szolgáltatás csak a következő esetekben tekinthető egyenértékűnek az *Ügyfel*ek számára nyújtott szolgáltatással:

- Ha nincsen szükség az OCSP válaszok tárolására, hanem azokat prompt, azonnali döntések meghozatalánál használjuk. Ekkor elfogadható, hogy az OCSP válasz utólag nem igazolja egyértelműen harmadik fél számára a *Tanúsítvány* adott időpontban vett érvényességét.
- Ha az OCSP lekérdezés időpontja között és azon időpont között, amelyre nézve az ellenőrzést végezzük, eltelt idő nagyobb, mint a tárolt OCSP válasz "nextUpdate" és "thisUpdate" időpontjainak különbsége (amely legfeljebb az OCSP válasz aláírására használt válaszadói tanúsítvány érvényességi ideje lehet). Ekkor a nyilvánosan és ingyenesen nyújtott szolgáltatás által biztosított OCSP válaszok is egyértelmű bizonyítékként fogadhatóak el harmadik fél számára, mert a bennük szereplő "thisUpdate" időpont már garantáltan későbbi lesz, mint az az időpont, amelyre nézve az ellenőrzést végezzük.
- Ha az ellenőrző fél nem maga kérdezi le az OCSP választ (hanem pl. egy archív aláíráshoz csatolt OCSP választ használ fel), nem szükséges vizsgálnia, hogy az OCSP válasz eredetileg mely forrásból származik. Elegendő azt vizsgálnia, hogy az OCSP válaszban szereplő "thisUpdate" időpont későbbi-e, mint amely időpontra nézve végzi az ellenőrzést.

Az OCSP szolgáltatás fenti két változatát a *Hitelesítés-szolgáltató* azonos rendelkezésre állással nyújtja.

4.10.2. A szolgáltatás rendelkezésre állása

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

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

A visszavonási nyilvántartások válaszideje normál terhelés esetén 10 másodpercnél kevesebb.

4.10.3. Opcionális lehetőségek

A *Hitelesítés-szolgáltató* a jelen fejezetben ismertetettek szerint többféle (CRL illetve kétféle OCSP) szolgáltatást is nyújt, amelyek keretében az *Ügyfel*ek és *Érintett felek* ellenőrizhetik a *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány*ok visszavonási állapotát. Mindezeken kívül a Hitelesítés-szolgáltató publikus tanúsítványtárában is elérhetővé teszi – az állapotuk megjelölésével – a visszavont és felfüggesztett *Tanúsítvány*okat is. Így a tanúsítványtárban keresve az *Ügyfel*ek és *Érintett felek* személyesen (alkalmazás segítsége nélkül) is ellenőrizhetik egy *Tanúsítvány* visszavonási állapotát.

4.11. Az előfizetés vége

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

4.12. Magánkulcs letétbe helyezése és visszaállítása

A *Hitelesítés-szolgáltató* az aláíró *Tanúsítvány*hoz tartozó magánkulcshoz nem nyújt kulcsletét szolgáltatást.

4.12.1. Kulcsletét és visszaállítás rendje és szabályai

Az aláíró *Tanúsítvány*hoz tartozó magánkulcs nem helyezhető letétbe.

4.12.2. Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Az aláíró *Tanúsítvány*hoz tartozó magánkulcs nem helyezhető letétbe, így ezzel kapcsolatban nem kell szimmetrikus rejtjelező kulcsokat kezelni.

4.13. Személy azonosításához szükséges adatok elektronikus ellenőrizhetőségének biztosítása

A *Hitelesítés-szolgáltató* biztosítja a jelen *Szolgáltatási szabályzat* által meghivatkozott *Hitelesítési rend*ek alapján kibocsátott *Tanúsítvány*ok esetében a személy azonosításához szükséges adatok elektronikus ellenőrizhetőségét, minden olyan fél részére, akit erre valamely jogszabály felhatalmaz.

A személy azonosításhoz szükséges adatok elektronikus ellenőrizhetőségének biztosítása a következőképpen történik:

1. A kérelmező letölti a *Hitelesítés-szolgáltató* honlapjáról az erre a célra szolgáló űrlapot. Ezt kitölti, beilleszti egy e-aktába és elektronikusan aláírja.

2. Az aláírt aktát beküldi a *Hitelesítés-szolgáltató* Ügyfélszolgálatának e-mail címére.
3. Az ügyfélszolgálati munkatárs ellenőrzi az aláírást a kérelmen, valamint a kérelmező jogosultságát.
4. Amennyiben a kérelem teljesíthető, az ügyfélszolgálati munkatárs ellenőrzi a kérelemben megadott adatokat, és a dokumentumban szereplő táblázat megfelelő részében IGEN vagy NEM választ ad. Amennyiben a kérelemben szereplő adatok alapján a keresett *Tanúsítvány* nem azonosítható, vagy a *Hitelesítés-szolgáltató* nem adott ki ilyen *Tanúsítvány*t, akkor ezt jelzi a dokumentumban.
5. A választ is tartalmazható dokumentumot elektronikusan aláírva visszaküldi a kérelmezőnek a dokumentumban megadott e-mail címre.

A *Hitelesítés-szolgáltató* mind a kérelmet, mind az arra adott választ archiválja.

5. Elhelyezési, eljárásbeli és üzemeltetési előírások

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

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

5.1. Fizikai követelmények

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

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

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

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

- A *Hitelesítés-szolgáltató* védett számítógéptermében valósítja meg a szigorúbban védendő szolgáltatásokat. Ez a számítógépterem speciálisan erre a célra lett tervezve és kialakítva,

tervezésénél különböző védelmi szempontok (a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés (beléptetés ellenőrzése és felügyelete), áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása stb.) egységes érvényesítésére került sor.

- A *Hitelesítés-szolgáltató* ügyfélszolgálati irodája úgy lett kialakítva, hogy reális költségek mellett képes legyen kielégíteni a regisztrációs szolgáltatásokkal szemben támasztott követelményeket.
- A *Hitelesítés-szolgáltató* úgy alakította ki mobil regisztrációs egységeit, hogy azok megfeleljenek a regisztrációs szolgáltatásokkal szemben támasztott követelményeknek.
- A *Hitelesítés-szolgáltató* a külső *Regisztráló szervezet*ek irodáival és mobil egységeivel szemben azt várja el, hogy biztonságuk egyenszilárdságú legyen a *Hitelesítés-szolgáltató* regisztrációs irodáinak és mobil egységeinek biztonságával. Ennek feltételeit és a *Hitelesítés-szolgáltató* ezzel kapcsolatos elvárásait a *Hitelesítés-szolgáltató* a külső *Regisztráló szervezet*tel kötött szerződésben rögzíti.
- A *Hitelesítés-szolgáltató* valamennyi kritikus szolgáltatását egy külön biztonsági zónában valósítja meg, az ehhez szükséges valamennyi eszközt egy – a biztonsági zóna részét képező – védett számítógépteremben helyezett el.

5.1.1. A telephely elhelyezése és szerkezeti felépítése

A *Hitelesítés-szolgáltató* informatikai rendszereit fizikai és logikai védelemmel ellátott, megfelelően biztonságos *Adatközpont*ban helyezte el és üzemelteti, amely megakadályozza az illetéktelen hozzáférést. Az *Adatközpont* elhelyezése és kialakítása során egymásra épülő és egymást támogató védelmi megoldásokat alkalmaz – őrzés, biztonsági zárak, behatolás érzékelők, 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* védi a szolgáltatás nyújtásában részt vevő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében. A *Hitelesítés-szolgáltató* biztosítja, 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 tartják;
- a bejelentkezett terminálokat nem hagyják felügyelet nélkül;
- nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet.

A gépterem elhagyásakor az adminisztrátornak ellenőriznie kell, hogy

- 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 felelősök lettek kijelölve. A vizsgálatok eredményét megfelelő naplóbejegyzésekben rögzítik.

5.1.3. Áramellátás és légkondicionálás

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

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

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

A levegő nedvességtartalmát az informatikai rendszerek által megkívánt szintre csökkentjük.

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

5.1.4. Beázás és elárasztódás veszély kezelése

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

5.1.5. Tűz megelőzés és tűzvédelem

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

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

5.1.6. Adathordozók tárolása

A hitelesítő szervezet operátori helyiségében egy kódzáras tűzálló páncélszekrény gondoskodik az adathordozók biztonságos tárolásáról. Az ügyfélszolgálati irodában is páncélszekrény szolgál az adathordozók biztonságos tárolására.

5.1.7. Hulladék megsemmisítése

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

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

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

5.1.8. A mentési példányok fizikai elkülönítése

A *Hitelesítés-szolgáltató* legalább heti rendszerességgel előállít olyan mentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható. A mentéseket - legalább az utolsó teljes mentést is beleértve - egy olyan külső helyszínen tárolja, amelynek a fizikai és működési védelme azonos az elsődleges helyszínével. Az elsődleges és a tartalék helyszínek között biztosítja az adatok biztonságos továbbítását.

5.2. Eljárásbeli előírások

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

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

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

5.2.1. Bizalmi szerepkörök

A *Hitelesítés-szolgáltató* feladatai ellátásához a 3/2005. (III. 18.) IHM rendelet [8] előírásainak megfelelő bizalmi szerepköröket (a rendelet szövegezésében munkaköröket) hozott létre. A jogosultságok és funkciók oly módon lettek megosztva az egyes bizalmi szerepkörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére.

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

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

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

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

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

Független rendszervizsgáló: A *Hitelesítés-szolgáltató* naplózott, illetve archivált adatállományát vizsgáló, a *Hitelesítés-szolgáltató* által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.

Regisztrációs felelős: A végfelhasználói tanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy;

Perszonalizáció területén tevékenykedő tisztviselő: Feladata az intelligens kártyák gondozása, megszemélyesítése, valamint a tanúsítványkérelmek összeállítása;

Ügyeletes tisztviselő: Feladata a 24 órás ügyelet biztosítása. Felelős az ügyelet elérhetőségéért, valamint azért, hogy a megérkező felfüggesztési és visszaállítási kérelmeket haladéktalanul feldolgozza a *Hitelesítés-szolgáltató* biztonsági szabályzata szerint.

A bizalmi szerepkörök ellátására a *Hitelesítés-szolgáltató* biztonságért felelős vezetője formálisan kinevezi 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 a *Hitelesítés-szolgáltató* naprakész nyilvántartást vezet, a változásokat haladéktalanul bejelenti a Nemzeti Média- és Hírközlési Hatóságnak.

5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

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

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

- a szolgáltatói magánkulcs aktiválása;
- a szolgáltatói magánkulcs megsemmisítése.

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

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

5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés

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

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

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

Az informatikai rendszer minden felhasználója és az adminisztratív folyamatok minden szereplője személy szerint kerül azonosításra. A fizikai hozzáférés ellenőrzéséhez a *Hitelesítés-szolgáltató* RFID kártyára épülő beléptető rendszert használ, a logikai hozzáférés ellenőrzése *Biztonságos aláírás-létrehozó eszköz*ön kiadott tanúsítványok segítségével történik. Sikeres hitelesítés előtt egyetlen biztonság kritikus feladatot sem lehet végrehajtani. A *Hitelesítés-szolgáltató* minden munkatársa pontosan annyi hozzáférési jogosultsággal rendelkezik, amennyi a feladatköre ellátásához elengedhetetlenül szükséges.

5.2.4. Egymást kizáró szerepkörök

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

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

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

5.3. Személyzetre vonatkozó előírások

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

A *Hitelesítés-szolgáltató* már a felvételi szakaszban foglalkozik a személyi biztonsággal, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését. Valamennyi bizalmi szerepkör esetén a 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 biztosítja valamennyi munkakör betöltéséhez a szükséges közös, általános, illetve az egyes szerepkörök betöltéséhez szükséges speciális szakmai ismeretek megszerzését, illetve továbbfejlesztését.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

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

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

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 foglalkoztat, akik

- büntetlen előélettel rendelkeznek és ellenük nincs folyamatban olyan eljárás, amely a büntetlenséget befolyásolhatja. A büntetlen előéletet a felvételi eljárás során a leendő dolgozónak 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolnia.
- nem állnak az elektronikus aláírással kapcsolatos szolgáltatás végzését kizáró foglalkozástól eltiltás hatálya alatt.

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

5.3.3. Képzési követelmények

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

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

A *Hitelesítés-szolgáltató* a regisztrációban közreműködő munkatársakat képzésben részesíti

- a *Tanúsítvány*ba kerülő adatok ellenőrzésével kapcsolatos veszélyekről és kockázatokról.

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

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

5.3.4. Továbbképzési gyakoriságok és követelmények

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

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

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

5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

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

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

A *Hitelesítés-szolgáltató* a dolgozókkal kötendő munkaszerződésben szabályozza a dolgozók felelősségre vonásának lehetőségeit a dolgozó által elkövetett mulasztások, hibák, vétlen vagy szándékos károkozások esetére. A szankció lehet például fegyelmi eljárás, elbocsátás, kinevezés visszavonása, büntetőjogi felelősségre vonás.

Valamennyi bizalmi munkakört betöltő munkatárs a munkakörbe kinevezéskor a foglalkoztatási dokumentumok részeként

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

Mindezek tartalmazzák azokat a munkajogi vagy büntető következményeket, melyek a különböző fegyelem- munkaköri kötelezettség- vagy törvénysértést szankcionálják. Amennyiben egy munkatárs – gondatlanságból fakadóan vagy szándékosan – megsérti a fenti szabályokat, ellene büntető intézkedések hozhatók, amelyek az elkövetés módjától és következményétől függően a jutalom megvonástól fegyelmi eljárás indításán és kártérítésen át egészen a hatósági feljelentésig terjedhetnek.

5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

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

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

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

5.3.8. A személyzet számára biztosított dokumentációk

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

Minden bizalmi munkakört betöltő munkatárs írásban megkapja a következő dokumentumokat:

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

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

5.4. Naplózási eljárások

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

5.4.1. A tárolt események típusai

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

- az esemény időpontját;

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

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

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

- 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.
  - 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* független rendszervizsgálói a keletkezett naplóbejegyzéseket minden munkanapon átvizsgálják.

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

Az informatikai rendszerek ellenőrzésére a *Hitelesítés-szolgáltató* automatizált ellenőrző rendszereket is használ, amelyek előre beállított szempontok szerint folyamatosan figyelik a keletkező naplóbejegyzéseket és szükség esetén riasztják az üzemeltetés munkatársait.

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

5.4.3. A naplófájl megőrzési időtartama

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

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

5.4.4. A naplófájl védelme

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

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

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

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

5.4.5. A naplófájl mentési eljárásai

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

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

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

5.4.6. A naplózás adatgyűjtési rendszere

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

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

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

5.4.7. Az eseményeket kiváltó alanyok értesítése

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

5.4.8. Sebezhetőség felmérése

A naplóbejegyzések napi rendszerességgel végzett feldolgozásán túl a *Hitelesítés-szolgáltató* szakemberei havonta áttekintik a rendkívüli eseményeket és a sebezhetőségre vonatkozó elemzéseket végeznek, amely alapján a *Hitelesítés-szolgáltató* szükség esetén intézkedéseket hoz a rendszer biztonságának növelésére.

Minden nagyobb jelentőségű feltárt hiányosság vagy külső fenyegetettség esetén, de legalább évente egyszer a *Hitelesítés-szolgáltató* szakemberei átfogó sebezhetőség vizsgálatot végeznek, amely segítségével feltérképezik a potenciális belső és külső fenyegetettségeket, amelyek jogosulatlan hozzáféréseket eredményezhetnek, hatással lehetnek a *Tanúsítvány* kiadási folyamatra, vagy lehetővé teszik a *Tanúsítvány*ban tárolt adatok módosítását. A vizsgálat eredményei alapján a *Hitelesítés-szolgáltató* szükség esetén továbbfejleszti folyamatait, rendszereit a szolgáltatás általános biztonságának növelése érdekében.

5.5. Adatok archiválása

5.5.1. Az archivált adatok típusai

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

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

- a *Hitelesítés-szolgáltató* akkreditációjával kapcsolatos valamennyi irat;
- a *Hitelesítési rend*(ek) és *Szolgáltatási szabályzat*(ok) valamennyi kibocsátott verziója;
- az Általános Szerződési Feltételek valamennyi kibocsátott verziója;
- a *Hitelesítés-szolgáltató* működésével kapcsolatos szerződések;
- a regisztrációval kapcsolatos valamennyi információ, beleértve
  - a *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.

5.5.2. Az archívum megőrzési időtartama

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

- 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;

5.5.3. Az archívum védelme

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

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

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

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

Az archivált elektronikus adatokat legalább fokozott biztonságú elektronikus aláírással és minősített időbélyeggel látja el.

5.5.4. Az archívum mentési folyamatai

A *Hitelesítés-szolgáltató* a papír alapú dokumentumokat egy eredeti példányban tárolja, a papír alapú eredetiről hiteles elektronikus másolatot készít a vonatkozó jogszabályok betartásával. Az elektronikus másolatokat a többi védendő elektronikus dokumentummal azonos szabályok szerint tárolja.

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

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

A *Hitelesítés-szolgáltató* biztosítja, hogy a szolgáltatást nyújtó rendszerein a gépidő maximum 1 másodpercre tér el a referenciaidőtől.

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

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

5.5.6. Az archívum gyűjtési rendszere

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

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

5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

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

Az archivált adatállományokat védi a jogosulatlan hozzáféréstől.

Az arra jogosultaknak biztosítja az archivált adatokhoz való ellenőrzött hozzáférést

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

5.6. Szolgáltatói kulcs cseréje

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

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

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

5.7. Kompromittálódást és katasztrófát követő helyreállítás

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

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

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

5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások

A *Hitelesítés-szolgáltató* rendelkezik üzletmenet folytonossági tervvel.

A *Hitelesítés-szolgáltató* kialakított és folyamatosan üzemben tart egy teljes értékű 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* folyamatosan teszteli a tartalék rendszer működését és évente felülvizsgálja az üzletmenet folytonossági terveit.

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

5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

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

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

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

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

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

5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások

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

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

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

5.7.4. Működés folyamatosságának biztosítása katasztrófát követően

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

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

A másodlagos szolgáltatási helyszínt az elsődleges telephelytől olyan távol hozta létre, hogy egy valószínűsíthető katasztrófa ne érhesse mindkét helyszínt egyszerre.

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

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

5.8. A hitelesítés-szolgáltató vagy a regisztráló szervezet leállítása

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

A hitelesítés-szolgáltatás és online tanúsítvány-állapot szolgáltatás leállítása

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

- regisztráció,
- tanúsítvány-előállítás,
- tanúsítvány-kibocsátás,
- intelligens kártyák megszemélyesítése,
- tanúsítvány megújítás,
- tanúsítvány módosítás,
- kulcscsere.

A *Hitelesítés-szolgáltató* a tervezett megszűnés előtt legalább 20 nappal intézkedik a végfelhasználói *Tanúsítvány*ok visszavonásáról. Ezzel egyidejűleg leállítja a következő szolgáltatásait:

- tanúsítvány visszavonás/felfüggesztés kezelés,

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

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

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

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

A *Hitelesítés-szolgáltató* a tárgyalások végeredményéről tájékoztatja a végfelhasználókat és a Nemzeti Média- és Hírközlési Hatóságot. A *Hitelesítés-szolgáltató* az *Ügyfel*eket elektronikus levélben, az *Érintett felek*et a honlapján történő közzététel útján tájékoztatja. A *Hitelesítés-szolgáltató* a "Microsec e-Szigno Root CA", "Microsec e-Szigno Root CA 2009" és az "e-Szigno OCSP CA" tanúsítványának visszavonását 5 nappal megelőzően a 2.2.1. fejezetnek megfelelően hirdetményt tesz közzé.

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

A *Hitelesítés-szolgáltató* biztosítja, hogy a visszavont, illetőleg felfüggesztett tanúsítványok nyilvántartásában szereplő adatokat szükség esetén az arra jogosult harmadik felek értelmezhessék.

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

6. Műszaki biztonsági óvintézkedések

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

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

6.1. Kulcspár előállítása és telepítése

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

6.1.1. Kulcspár előállítása

Valamennyi kulcspárt az Eat. [3] 18. § szerint kiadott aktuális NMHH határozatban megfogalmazott követelményeknek megfelelő algoritmussal kell létrehozni.

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

- A szolgáltatói magánkulcs előállítását fizikailag védett környezetben (lásd 5.1 pont), két, bizalmi szerepkört (lásd 5.2.1 pont) betöltő, erre feljogosított személy együttes részvételével, más illetéktelen személyek jelenlétét kizárva végzi.
- A szolgáltatói magánkulcs előállítását olyan eszközön belül hajtja végre, amely:
  - megfelel a FIPS 140-2 [4] 3-as, illetve annál magasabb szintű követelményeinek, vagy
  - megfelel a CEN 14167-2 [22] 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 biztosítja, hogy:

- A kulcsok előállítását fizikailag védett környezetben végzi, kizárólag bizalmi szerepkört betöltő személyek részvételével.
- A *Hardver kriptográfiai eszköz* használatát előíró *Hitelesítési rend*ek esetén a *Hitelesítés-szolgáltató* az aláíró magánkulcsot csak a szolgáltatást igénybe vevő *Alany Hardver kriptográfiai eszköz*én (illetve tárolt kulcsos aláírás szolgáltatás esetében a biztonságos hardver eszközön) generálja, ami lehetetlenné teszi az aláíró magánkulcs felfedését.
- Az előállított magánkulcsokat a *Hitelesítés-szolgáltató* a kulcs átadásáig megfelelően biztonságos környezetben tárolja a felfedés megakadályozása érdekében. Az aláíró magánkulcs *Alany*nak történő dokumentált átadása után a *Hitelesítés-szolgáltató* haladéktalanul megsemmisíti az átadott magánkulcs általa tárolt minden példányát olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon. A *Hitelesítés-szolgáltató* meggyőződik 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 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 felel meg:

Amennyiben az *Alany* részére átadásra kerül a magánkulcs:

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

Amennyiben az *Alany* tárolt kulcsos aláírás szolgáltatást vesz igénybe:

- A *Hitelesítés-szolgáltató* az általa az *Alany*ok részére generált magánkulcsokat a szolgáltatás teljes időtartama alatt biztonságos módon tárolja, amely megakadályozza a kulcsok felfedését, lemásolását, módosítását, sérülését, illetéktelenek általi használatát.
- A *Hitelesítés-szolgáltató* olyan azonosítási eljárást alkalmaz, amely biztosítja, hogy a magánkulcsot csak az arra jogosult *Alany* használhassa.
- A *Hitelesítés-szolgáltató* megfelelő bizonyítékot tárol el arról, hogy a magánkulcs feletti rendelkezést az *Alany* számára adott hiteles időpontban átadta.
- A magánkulcs feletti rendelkezés *Alany* számára történő átadását követően biztosítja, hogy kizárólag az *Alany* legyen képes a magánkulcs használatához szükséges azonosítási folyamat lefolytatására.

Hardver kriptográfiai eszköz használatát megkövetelő *Hitelesítési rend*ek esetén az *Alany* aláíró magánkulcsát a magánkulcs védett tárolását és felhasználását biztosító *Hardver kriptográfiai eszköz*zel együtt a regisztrációs ponton személyesen megjelenő *Alany*nak adják át az eszközt aktivizáló kódot tartalmazó zárt borítékkal együtt.

Hardver eszköz használatát nem megkövetelő *Hitelesítési rend*ek esetén minden esetben az *Ügyfél* generálja a magánkulcsot, így azt nem kell eljuttatni az *Ügyfél*hez.

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.

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

6.1.4. A szolgáltatói nyilvános kulcs közzététele

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

- A *Hitelesítés-szolgáltató* honlapján közzéteszi az összes gyökér és köztes szolgáltatói tanúsítványt tartalmazó teljes szolgáltatói tanúsítvány hierarchiát, ahonnan valamennyi aktuális szolgáltatói *Tanúsítvány* letölthető (lásd a "Szolgáltatói tanúsítványok" pontban a `https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/szolgaltatoi-tanusitvanyok.html` címen).
- A gyökér és köztes hitelesítő egységek megnevezését és a gyökér *Tanúsítvány*ok lenyomatát tartalmazza a *Szolgáltatási szabályzat* 1.3.1 fejezete.
- A köztes hitelesítő egységek *Tanúsítvány*ai publikálásra kerülnek a Nemzeti Média- és Hírközlési Hatóság által az európai közös szabályozás [10] keretében karbantartott és publikált magyar megbízható hitelesítés szolgáltatói listán [11]. A lista tartalmazza valamennyi szolgáltatói *Tanúsítvány*t (a lejártakat, visszavontakat is).
- Az online tanúsítvány-állapot válaszokat aláíró válaszadók számára a *Hitelesítés-szolgáltató* – a legjobb nemzetközi gyakorlatnak megfelelően – rendkívül rövid érvényességi idejű *Tanúsítvány*okat bocsát ki, ezzel kiküszöbölve azt, hogy a *Tanúsítvány*ok visszavonási állapotát ellenőrizni kelljen. Az aktuális *Tanúsítvány*ok folyamatosan elérhetők a *Hitelesítés-szolgáltató* honlapján a `https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/szolgaltatoi-tanusitvanyok.html` címen.

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

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

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

6.1.5. Kulcsméretek

A *Hitelesítés-szolgáltató* mindenkor a Nemzeti Média- és Hírközlési Hatóságnak az Eat. 18. § [3] szerinti felhatalmazása alapján kibocsátott határozata által engedélyezett algoritmusokat és minimális kulcsméreteket használ.

A *Hitelesítés-szolgáltató* valamennyi jelenleg aktív gyökér és köztes szolgáltatói *Tanúsítvány*ában, az időbélyegzők és OCSP válaszadók *Tanúsítvány*aiban egyaránt 2048 bites RSA kulcsot használ.

6.1.6. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

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

Hardver/szoftver kulcselőállítás

A *Hitelesítés-szolgáltató Tanúsítvány*ok kibocsátására használt kulcsainak generálása olyan *Hardver kriptográfiai eszköz*zel történik, amely rendelkezik az Eat. 7. § (5)-(6) szerinti igazolással, illetve FIPS 140-1 Level 3 szerinti tanúsítással. Az egyes eszközök megnevezését a 8. fejezet tartalmazza.

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

A *Biztonságos aláírás-létrehozó eszköz* vagy *Hardver kriptográfiai eszköz* használatát megkövetelő *Hitelesítési rend*ek szerint kibocsátott *Tanúsítvány*ok aláíró kulcspárjainak generálása a *Biztonságos aláírás-létrehozó eszköz*ön (kriptográfiai hardver eszközön) on-board hardver kulcsgenerálással történik.

A *Biztonságos aláírás-létrehozó eszköz* vagy *Hardver kriptográfiai eszköz* használatát nem megkövetelő *Hitelesítési rend* szerint kibocsátott *Tanúsítvány*ok esetén a kulcsgenerálást minden esetben az *Alany* végzi.

A paraméterek megfelelőségének ellenőrzése

A kulcsgenerálás paramétereinek megfelelőségét két szempontból ellenőrzi a rendszer:

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

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

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

A *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítvány*okban szerepelteti a "kulcshasználat" (Key Usage) kiterjesztéseket, amelyek meghatározzák a *Tanúsítvány* felhasználási területét és az X.509v3 [27] kompatibilis alkalmazásokban műszakilag is korlátozzák a kulcsok felhasználhatóságát. A mező tartalmára vonatkozó megkötések a 7.1.2 fejezetben szerepelnek. Az aláíró magánkulcsot az *Aláíró* kizárólag elektronikus aláírás létrehozására használhatja fel, a kulcs minden más alkalmazása kifejezetten tiltott.

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

- a gyökér hitelesítő egység saját önaláírt *Tanúsítvány*ának kibocsátására,
- köztes hitelesítő egységek *Tanúsítvány*ainak aláírására,
- OCSP válaszadó *Tanúsítvány*ának aláírására,
- időbélyegző egység *Tanúsítvány*ának aláírására,
- CRL-ek aláírására.

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

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

A "kulcs használati" (Key Usage) mezők lehetséges – egyúttal kötelezően kitöltendő – értékei az alábbiak:

A hitelesítő szervezet kulcsai

- A *Hitelesítés-szolgáltató* hitelesítő egységeinek kulcsai:
  "keyCertSign", "CRLSign" (kritikus)
- Az időbélyegző egység aláíró kulcsai:
  "NonRepudiation" és "digitalSignature" (kritikus),
  az "Extended Key Usage" mezőben: "timeStamping"
- A *Hitelesítés-szolgáltató* OCSP válaszadójának kulcsa:
  "digitalSignature", "nonRepudiation" (kritikus)
  az "Extended Key Usage" mezőben: "OCSPSigning"

Az *Alany*ok kulcsai

- A végfelhasználói aláíró kulcs:
  "nonRepudiation" (kritikus)
  A hozzá tartozó magánkulcs kizárólag aláírás létrehozására használható.

A kulcsokat kizárólag a fent leírt célokra szabad használni, amelyeket a *Hitelesítés-szolgáltató* a kulcsokhoz tartozó *Tanúsítvány*okban feltüntet.

6.2. A magánkulcsok védelme

A *Hitelesítés-szolgáltató* gondoskodik a birtokában lévő saját és a végfelhasználói magánkulcsok biztonságos kezeléséről, megakadályozza a magánkulcsok felfedését, lemásolását, törlését,

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

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

A *Hitelesítés-szolgáltató* a *Biztonságos aláírás-létrehozó eszköz* használatát megkövetelő *Hitelesítési rend*ek szerint kibocsátott *Tanúsítvány*okhoz használt *Biztonságos aláírás-létrehozó eszköz*öket az onboard kulcsgenerálás után az eszköz *Alany*nak történő átadásáig fizikailag biztonságos helyszínen, kiemelt figyelemmel tárolja a magánkulcsok illegális használatának megakadályozása érdekében.

A *Biztonságos aláírás-létrehozó eszköz* használatát nem megkövetelő *Hitelesítési rend*ek szerint kibocsátott *Tanúsítvány*ok esetén a *Hitelesítés-szolgáltató* nem generál előre magánkulcsokat az *Alany*nak, így nem kell gondoskodni a végfelhasználói magánkulcsok megőrzéséről.

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 tárolják, amelyek rendelkeznek az Eat. 7. § (5)-(6) szerinti igazolással [3], vagy FIPS 140-2 Level 3 szerinti tanúsítással [4].

A használt *Hardver kriptográfiai eszköz*ök megnevezése a 8. fejezetben található.

A *Hitelesítés-szolgáltató* a szolgáltatói magánkulcsokat a *Hardver kriptográfiai eszköz*ön kívül csak kódolt formában tárolja. A kódoláshoz az Eat. [3] 18. § szerint kiadott aktuális Nemzeti Média- és Hírközlési Hatóság határozat szerinti algoritmusokat és kulcsparamétereket használ, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

6.2.2. Magánkulcs többszereplős (n-ből m) használata

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

6.2.3. Magánkulcs letétbe helyezése

A *Hitelesítés-szolgáltató* nem helyezi letétbe saját szolgáltatói magánkulcsát.

A *Hitelesítés-szolgáltató* a végfelhasználói aláíró magánkulcsokhoz nem nyújt letéti szolgáltatást, azokat semmilyen körülmények között sem tárolja, kivéve az új *Biztonságos aláírás-*

*létrehozó eszköz*ön előállított magánkulcs *Biztonságos aláírás-létrehozó eszköz*ön történő megőrzését az eszköz *Alany*nak történő átadásáig.

6.2.4. Magánkulcs mentése

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

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

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

A végfelhasználói aláíró magánkulcsokról a *Hitelesítés-szolgáltató* nem készít semmilyen másolatot.

6.2.5. Magánkulcs archiválása

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

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

A *Hitelesítés-szolgáltató* valamennyi szolgáltatói magánkulcsát a követelményeknek megfelelő *Hardver kriptográfiai eszköz*ben állítja elő. A magánkulcsok nem léteznek nyílt formában a *Hardver kriptográfiai eszköz*ön kívül.

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

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

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

6.2.7. Magánkulcs tárolása hardver kriptográfiai eszközben

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

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

6.2.8. A magánkulcs aktiválásának módja

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

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

A *Hitelesítés-szolgáltató* által előállított végfelhasználói magánkulcsok esetén a *Hitelesítés-szolgáltató* gondoskodik 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 a *Hitelesítés-szolgáltató* úgy konfigurálja és adja át az *Alany* részére, hogy

- egyértelműen megállapítható legyen, hogy az eszközt az átadás előtt nem használták elektronikus aláírás létrehozására;
- elektronikus aláírás létrehozása előtt az *Alany*nak azonosítania kelljen magát az *Aláírás-létrehozó eszköz* felé.

Tárolt kulcsos aláírás szolgáltatás nyújtása esetén a *Hitelesítés-szolgáltató* biztosítja, hogy

- az *Alany* számára generált magánkulcsot az *Alany* rendelkezésére bocsátása előtt nem használhatták aláírás létrehozására;
- elektronikus aláírás létrehozása előtt az *Alany*nak azonosítania kelljen magát az *Aláírás-létrehozó 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* által használt hardver kriptográfia eszközök által kezelt magánkulcs akkor deaktiválódik, ha az eszköz (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetben következik be:

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

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

Végfelhasználói magánkulcsok

A *Hardver kriptográfiai 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 eszköz biztosítja, hogy az aláíró kulcsok deaktiválódnak az alábbi esetekben:

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

A deaktivált kulcs illetve *Hardver kriptográfiai eszköz* csak az *Alany* újbóli azonosítása után használható elektronikus aláírás létrehozására.

Tárolt kulcsos aláírás szolgáltatás esetében a *Hitelesítés-szolgáltató* által alkalmazott műszaki megoldás biztosítja, hogy az aláíró kulcsok deaktiválódnak az alábbi esetekben:

- az eszköz áramellátása bármely okból megszűnik;
- az *Alany* alkalmazásával felépített kapcsolat bármilyen okból megszakad;
- az *Alany* deaktiváló (kilépés) utasítást ad.

A deaktivált kulcs csak az *Alany* újbóli azonosítása után használható elektronikus aláírás létrehozására.

A *Hardver kriptográfiai 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 semmisíti meg, ami lehetetlenné teszi a magánkulcs további használatát.

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

Végfelhasználói magánkulcsok

A *Hardver kriptográfiai 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 *Hardver kriptográfiai eszköz*ön (pl. intelligens kártyán vagy tokenen) kiadott, használatból kivont magánkulcsok megsemmisítése az eszköz fizikai megsemmisítésével lehetséges, ami az *Alany* felelőssége.

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

A végfelhasználók használatból kivont aláíró magánkulcsait javasolt megsemmisíteni.

6.2.11. A hardver kriptográfiai eszközök értékelése

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

- rendelkezik FIPS 140-2 Level 3 szerinti tanúsítással [4], vagy

- rendelkezik a CEN 14167-2 [22] munkacsoport egyezmény követelményeinek való megfelelést igazoló Common Criteria alapú tanúsítvánnyal, vagy
- rendelkezik az Eat. 7. § (5) és (6) bekezdései szerint [3], a Nemzeti Média- és Hírközlési Hatóság által vagy az Európai Unió valamely tagállamában nyilvántartásba vett, elektronikus aláírási termékek értékelésére jogosult független tanúsító szervezet által erre a célra kiadott igazolással.

6.3. A kulcspár kezelés egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

A *Hitelesítés-szolgáltató* minden, a hitelesítő szervezete által előállított *Tanúsítvány*t archivál az érvényesség lejártától számított 10 évig, illetve a tanúsítvánnyal (vagy a *Tanúsítvány*ra épülő elektronikus aláírással) kapcsolatban felmerült jogvita jogerős lezárásáig.

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

6.3.2. A tanúsítványok és kulcspárok használatának periódusa

A végfelhasználói tanúsítványok

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. § [3] szerint kibocsátott határozata értelmében biztonságosan felhasználhatók;
- a *Tanúsítvány*t kibocsátó szolgáltatói tanúsítvány hátralevő érvényességi idejét.

Alanyok kulcsai

Az *Alany*ok kulcsainak érvényességi ideje nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Nemzeti Média- és Hírközlési Hatóság Eat. 18. § [3] szerint kibocsátott határozata értelmében biztonságosan felhasználhatók;

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

A hitelesítő szervezet kulcsai

A gyökér hitelesítő egységek kulcsainak és tanúsítványainak érvényességi ideje:

- a "Microsec e-Szigno Root CA" gyökér hitelesítő egység kulcsa 2017. április 6-ig érvényes;
- a "e-Szigno OCSP CA" gyökér hitelesítő egység kulcsa 2017. április 26-ig érvényes;
- a "Microsec e-Szigno Root CA 2009" gyökér hitelesítő egység kulcsa 2029. december 30-ig érvényes.

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

A *Hitelesítés-szolgáltató* SHA-1 alapú időbélyegző egységeinek kulcsai a hozzájuk tartozó *Tanúsítvány*ok érvényességi idejének lejártáig érvényesek.

A *Hitelesítés-szolgáltató* az SHA-256 alapú időbélyegző egységei számára 12 évig érvényes időbélyegző *Tanúsítvány*okat bocsát ki. A *Hitelesítés-szolgáltató* minden egyes időbélyegző kulcsot 1 évig használ, ezt követően a régi kulcsot megsemmisíti. A *Hitelesítés-szolgáltató* évente új kulcsokkal és *Tanúsítvány*okkal látja el SHA-256 alapú időbélyegző egységeit.

A *Hitelesítés-szolgáltató* OCSP válaszadójának kulcsának érvényességi ideje 12 év. A *Hitelesítés-szolgáltató* OCSP válaszadójának kulcsához tartozó *Tanúsítvány* érvényességi ideje 10 perc.

Mind a szolgáltatói, mind a végfelhasználói kulcsok érvényességi idejét befolyásolhatja, ha a Hatóság Eat. 18. § szerinti határozata értelmében a tanúsítvány aláírására használt algoritmus már nem biztonságos, illetve nem alkalmas aláírások készítésére. Amennyiben ez bekövetkezik, a *Hitelesítés-szolgáltató* visszavonja az érintett *Tanúsítvány*okat.

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

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

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

A *Hitelesítés-szolgáltató* által az *Alany* részére kibocsátott *Hardver kriptográfiai eszköz*ök esetén a *Hitelesítés-szolgáltató*

- az aktivizáló adatokat megfelelő minőségű véletlenszám-generátor segítségével, fizikailag biztonságos körülmények között állítja elő és telepíti a *Hardver kriptográfiai eszköz*re ;
- az aktivizáló adatokat biztonságos módszer felhasználásával kell az *Alany* részére átadni.

Az *Aláíró* számára tárolt kulcsos aláírás szolgáltatás nyújtása esetén:

- A *Hitelesítés-szolgáltató* által alkalmazott azonosítási eljárás biztosítja, hogy a magánkulcsot csak az arra jogosult *Alany* aktiválhassa.

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

- a *Hitelesítés-szolgáltató* az aktivizáló adatokat megfelelő minőségű véletlenszám-generátor segítségével, fizikailag biztonságos körülmények között állítja elő és rendeli a magánkulcshoz;

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

6.4.2. Az aktivizáló adatok védelme

A *Hitelesítés-szolgáltató* alkalmazottai a magánkulcsok aktiválásához szükséges eszközöket, aktivizáló adatokat biztonságosan kezelik, műszaki és szervezési intézkedések segítségével védik, a jelszavakat csak kódolt formában tárolják.
A *Hitelesítés-szolgáltató* által az *Alany*ok részére kibocsátott *Hardver kriptográfiai eszköz*ök illetve az *Alany* számára generált szoftveres magánkulcsok esetén:

- a *Hitelesítés-szolgáltató* az aktivizáló adatokat csak abból a célból rögzíti, hogy azt az *Alany* részére átadhassa;
- a *Hitelesítés-szolgáltató* az aktivizáló adatokat biztonságos módszer felhasználásával osztja szét az *Aláírók* részére.

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

6.4.3. Az aktivizáló adatok kezelésének egyéb szempontjai

Nincs megkötés.

6.5. Informatikai biztonsági előírások

6.5.1. Speciális informatikai biztonsági műszaki követelmények

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

- a rendszerhez vagy alkalmazáshoz való hozzáférés engedélyezése előtt a felhasználó azonosságát többfaktoros azonosítással ellenőrzi kártyán tárolt VPN tanúsítvány felhasználásával;

- a felhasználókhoz szerepköröket rendel és biztosítja, hogy minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezzen;
- minden tranzakcióról naplóbejegyzést állít elő és a naplóbejegyzéseket archiválja;
- a biztonságkritikus folyamatok részére biztosítja, hogy a *Hitelesítés-szolgáltató* belső hálózati tartományai kellően védettek legyenek a jogosulatlan hozzáféréstől;
- megfelelő eljárásokat alkalmaz a kulcsvesztés vagy rendszerhiba utáni szolgáltatás visszaállítás biztosítása érdekében.

6.5.2. Az informatikai biztonság értékelése

A Microsec kiemelten fontosnak tartja *Ügyfel*ei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a *Hitelesítés-szolgáltató* ISO 9001 szabványnak megfelelő minőségirányítási rendszert üzemeltet 2002. január 23. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította. A Microsec nagy figyelmet szentel az általa üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a ISO/IEC 27001-nek megfelelő információbiztonság-irányítási rendszert (korábban BS 7799) üzemeltet 2003. május 19. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

6.6. Életciklusra vonatkozó műszaki előírások

6.6.1. Rendszerfejlesztési előírások

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

- kereskedelmi dobozos szoftverek, amelyeket dokumentált tervezési módszertan szerint terveztek és fejlesztettek;
- vagy a *Hitelesítés-szolgáltató* részére megbízható fél által kifejlesztett egyedi hardver és szoftver megoldások, amelyek 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.

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

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

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 ellenőrzi kártékony kódok után kutatva.

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

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

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

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

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

6.6.2. Biztonságkezelési előírások

A *Hitelesítés-szolgáltató* változáskövető rendszert használ a hitelesítés szolgáltatásban használt rendszerek telepítésének, konfigurációjának dokumentálására, üzemeltetésére, ellenőrzésére, monitorozására és karbantartására, beleértve a módosításokat és továbbfejlesztéseket is. A változás követő rendszer alkalmas arra, hogy észleljen 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* minden esetben meggyőződik arról, hogy a telepítendő program a megfelelő verziójú és mentes mindenféle jogosulatlan módosítástól. A *Hitelesítés-szolgáltató* rendszeresen ellenőrzi a hitelesítés szolgáltatásban használt rendszereiben használt programok integritását.

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

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

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

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

6.6.3. Életciklusra vonatkozó biztonsági előírások

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

6.7. Hálózati biztonsági előírások

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

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

- letiltja a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtat.

6.8. Időbélyegzés

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

7. Tanúsítvány, CRL és OCSP profilok

7.1. Tanúsítvány profil

A *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány*ok megfelelnek az RFC 5280 [6], RFC 6818 [7] és az ETSI TS 101 862 [12] X.509 specifikációknak.

7.1.1. Verzió szám(ok)

A *Hitelesítés-szolgáltató* az X.509 specifikáció [27] szerinti "v3" *Tanúsítvány*okat bocsát ki.

A *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*ok alap mezői a következők:

- Verzió (Version)
  A *Tanúsítvány* az X.509 specifikáció szerinti "v3" *Tanúsítvány*oknak felel meg, így a mezőbe a "2" érték kerül. [6]

- Sorozatszám (Serial Number)
  A *Tanúsítvány*t kibocsátó hitelesítő egység által generált egyedi azonosító.

  A végfelhasználói *Tanúsítvány*ok esetében a "Serial Number" mező legalább 8 bájt entrópiájú véletlen számot tartalmaz.

- Algoritmus azonosító (Algorithm Identifier)
  A *Tanúsítvány*t hitelesítő elektronikus aláírás készítéséhez használt algoritmuskészlet ("sha1WithRSAEncryption", illetve "sha256WithRSAEncryption") azonosítója (OID).

- Aláírás (Signature)
  A *Hitelesítés-szolgáltató* által készített, a *Tanúsítvány*t hitelesítő elektronikus aláírás, amelyet a *Hitelesítés-szolgáltató* az "Algoritmus azonosító" -ban megadott algoritmuskészlettel hozott létre.

- Kibocsátó (Issuer)
  A *Tanúsítvány*t kibocsátó hitelesítő egység egyedi azonosítója egyedi X.501 név formátum szerint (lásd: 3.1. fejezet).

- Érvényesség (Valid From & Valid To)
  A *Tanúsítvány* érvényességének kezdete és vége.

  Az időpontok UTC szerint és az RFC 5280-nak megfelelő kódolásban kerülnek rögzítésre.

- Az *Alany* azonosítója (Subject)
  Az *Alany* egyedi azonosítója egyedi X.501 név formátum szerint (lásd: 3.1. fejezet). Mindig kitöltésre kerül.

- Az *Alany* nyilvános kulcsának algoritmus-azonosítója (Subject Public Key Algorithm Identifier)
  A *Hitelesítés-szolgáltató* az RSA algoritmust támogatja a végfelhasználói *Tanúsítvány*okban.

- Az *Alany* nyilvános kulcsa (Subject Public Key Value)
  Az *Alany* nyilvános kulcsa.

- Kibocsátó egyedi azonosító (Issuer Unique Identifier)
  Nem kitöltött.

- Az *Alany* egyedi azonosítója (Subject Unique Identifier)
  Nem kitöltött.

7.1.2. Tanúsítvány kiterjesztések

A *Hitelesítés-szolgáltató* csak az alábbi, X.509 specifikáció [27] szerinti tanúsítvány kiterjesztéseket használja:

- 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 kitölti ezt a mezőt a következő adatok megadásával:

  - a *Hitelesítési rend* azonosítója (OID);
  - a *Szolgáltatási szabályzat* elérhetősége.
  - szöveges [3] figyelmeztetés angol és magyar nyelven, amelyből megállapítható, hogy II. vagy III. hitelesítési osztályú tanúsítványról van szó, azaz regisztrációkor történt- e személyes megjelenés, a tanúsítvány alanya természetes személy-e, illetve a tanúsítványhoz tartozó magánkulcsot kriptográfiai hardver eszköz védi
  - Ezen információk a hitelesítési rend azonosítója alapján is megállapíthatóak.
  - Az ETSI TS 102 042 által meghatározott hitelesítési rend azonosítója (OID); amely rend követelményeinek a tanúsítvány megfelel. II. hitelesítési osztályba tartozó tanúsítványok esetén LCP, III. hitelesítési osztályba tartozó, kriptográfiai hardver eszköz használatát megkövetelő rendek esetén NCP+, kriptográfiai hardver eszköz használatát meg nem követelő rendek esetén NCP.

  A végfelhasználói *Tanúsítvány*oknál minden esetben meg van adva legalább egy olyan *Hitelesítési rend*, amely szerint a *Hitelesítés-szolgáltató Tanúsítvány*t kibocsátotta, és amely *Hitelesítési rend* szerint később a tanúsítvánnyal kapcsolatban eljár. A *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*okban feltünteti 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 *Tanúsítvány*nak kell tekinteni. A teszt *Tanúsítvány* kizárólag tesztelési célra használható, valós tranzakciók esetén el kell utasítani.

  Gyökér hitelesítési egység *Tanúsítvány*ában nem szerepel ez a mező.

[3] A *Tanúsítvány*ban szintén szereplő Qualified Certificate Statements kiterjesztés géppel feldolgozható formában is tartalmazza ugyanezen információkat.

Köztes hitelesítési egység *Tanúsítvány*ban a mező kitöltése kötelező és nem lehet kritikus. A *Hitelesítés-szolgáltató* saját köztes hitelesítési egységei számára kibocsátott *Tanúsítvány*ok esetében szerepelhet "anyPolicy" Identifier ebben a mezőben. A vonatkozó *Szolgáltatási szabályzat* hivatkozása megadható ebben a mezőben.

Más hitelesítés-szolgáltató számára kibocsátott köztes hitelesítési egység *Tanúsítvány*ainak esetében csak olyan azonosító szerepelhet ebben a mezőben, amely olyan *Hitelesítési rend*re vonatkozik, amely megfelel a kibocsátó *Hitelesítés-szolgáltató* által alkalmazott valamely *Hitelesítési rend*nek, és nem lehet benne anyPolicy 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.

  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 alapértelmezett értéke CA = "FALSE", ezért ez a kiterjesztés nem szerepel a végfelhasználók, OCSP válaszadók és időbélyegző egységek számára kibocsátott *Tanúsítvány*okban.

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

  A "pathLenConstraint" mező nem szerepel a végfelhasználói *Tanúsítvány*okban.

Köztes és gyökér hitelesítő egység *Tanúsítvány*ban szerepelhet a "pathLenConstraint" mező.

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

  A végfelhasználói *Tanúsítvány*okban kizárólag az alábbi érték szerepel: "nonRepudiation", "digitalSignature";

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

  Fokozott aláírói végfelhasználói *Tanúsítvány*okban beállított érték:
  "emailProtection (1.3.6.1.5.5.7.3.4)";
  Kódaláírói (Code Signing) *Tanúsítvány*okban beállított értékek:
  "1.3.6.1.5.5.7.3.3", "1.3.6.1.4.1.311.2.1.22";

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

- Szolgáltatói információ elérése (Authority Information Access) – nem kritikus
  OID: 1.3.6.1.5.5.7.1.1
  A *Hitelesítés-szolgáltató* által rendelkezésre bocsátott, a *Tanúsítvány* használatához kapcsolódó egyéb szolgáltatásainak leírása. Végfelhasználói *Tanúsítvány*ok és köztes hitelesítő egységek tanúsítványai esetében a mező tartalmazza a következő adatokat:

  - A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást nyújt. Ez az elérhetőség szerepel itt.
  - A tanúsítványlánc felépítésének megkönnyítésére a *Hitelesítés-szolgáltató* megadja a *Tanúsítvány*t kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.

- 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.

A fenti mezők – az *Alany* alternatív nevei kivételével – mindig kitöltésre kerülnek. Más tanúsítvány kiterjesztés nem kerül kitöltésre.

7.1.3. Az algoritmus objektum azonosítója

Annak az algoritmusnak a megnevezése, amellyel a tanúsítvány hitelesítésre került. A *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítvány*ok aláírására az alábbi algoritmust használja: "sha256WithRSAEncryption".

7.1.4. Névformák

A *Hitelesítés-szolgáltató* a jelen *Hitelesítési rend*ek alapján kibocsátott *Tanúsítvány*okban egy – az RFC 5280 szabványban [6] meghatározott attribútumokból összeállított – megkülönböztetett nevet használ az *Alany* azonosítására.

A *Tanúsítvány* tartalmazza az *Alany* globálisan egyedi azonosítóját is (OID) a 3.1.1 -es fejezetben meghatározottak szerint kitöltve.

A *Tanúsítvány* "Issuer DN" mezőjében szereplő érték megegyezik a kibocsátó *Tanúsítvány*ának "Subject DN" mezőjében szereplő értékkel.

7.1.5. Névhasználati megkötöttségek

A *Hitelesítés-szolgáltató* nem használ névhasználati megkötéseket a "nameConstraints" mező felhasználásával.

7.1.6. A Hitelesítési rend objektum azonosítója

A *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*okba felveszi a nem kritikus (Hitelesítési Rend) kiterjesztést a 7.1.2. fejezet előírásai szerint.

7.1.7. A Hitelesítési rend megkötöttségek kiterjesztés használata

Nincs előírás.

7.1.8. A Hitelesítési rend jellemzők szintaktikája és szemantikája

A *Hitelesítés-szolgáltató* a Hitelesítési rend (Certificate Policy) kiterjesztés Irányelv minősítő (Policy Qualifier) mezejében rövid információt helyezhet el a *Tanúsítvány* felhasználhatóságával kapcsolatban. A mező tartalmazza a *Szolgáltatási szabályzat* 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 [6] specifikáció szerinti "v2" verziójú tanúsítvány visszavonási listákat bocsát 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".
- Algoritmus azonosító (Signature Algorithm Identifier)
  A visszavonási listát hitelesítő elektronikus aláírás készítéséhez használt algoritmuskészlet azonosítója (OID). A *Hitelesítés-szolgáltató* által használt algoritmuskészlet neve és azonosítója:
  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11).
- Aláírás (Signature)
  A *Hitelesítés-szolgáltató* visszavonási listát hitelesítő elektronikus aláírása. A visszavonási listát az adott hitelesítő egység a *Tanúsítvány*ok aláírására használt kulcsával hitelesíti.
- Kibocsátó (Issuer)
  A visszavonási listát kibocsátó hitelesítő egység egyedi azonosítója.
- Hatálybalépés (Effective Date)
  A visszavonási lista hatálybalépésének kezdete. UTC szerinti érték az RFC 5280 [6] szerinti kódolással. A *Hitelesítés-szolgáltató* által kibocsátott visszavonási listák esetében ez megegyezik a kibocsátás idejével.
- Következő kibocsátás (Next Update)
  A következő visszavonási lista kibocsátásának ideje (lásd: 4.10. fejezet). UTC szerinti érték az RFC 5280 [6] 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 használt visszavonási lista kiterjesztések:

- CRL sorozatszám (CRL number) – nem kritikus
  Ebbe a mezőbe a visszavonási listák egyesével növekvő sorozatszámai kerülnek.

- expiredCertsOnCRL – nem kritikus
  A *Hitelesítés-szolgáltató* az X.509 specifikáció szerinti szabványos jelöléssel jelzi, hogy a lejárt *Tanúsítvány*okat nem távolítja el a CRL-ről. (Lásd: 4.10. fejezet.)

A *Hitelesítés-szolgáltató* által használható tanúsítvány visszavonási lista bejegyzési kiterjesztések:

- Visszavonás oka (Reason Code) – nem kritikus
  Ebbe a mezőbe a visszavonás oka kerül.

  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.

  A *Hitelesítés-szolgáltató* nem tölti ki kötelező jelleggel ezt a mezőt.

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

  A *Hitelesítés-szolgáltató* nem tölti ki kötelező jelleggel ezt a mezőt.

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

7.3. Online tanúsítvány-állapot válasz (OCSP) profil

A *Hitelesítés-szolgáltató* az RFC 2560 [13] és RFC 6960 [14] szerinti online tanúsítvány-állapot szolgáltatást üzemeltet.

7.3.1. Verziószám(ok)

A *Hitelesítés-szolgáltató* támogatja az RFC 2560 [13] és RFC 6960 [14] 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* külső auditor igénybevételével átvilágíttatja üzemeltetését és az átvilágításról készült részletes jelentést a Nemzeti Média- és Hírközlési Hatóság számára előzetesen megküldi. 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 megfelel az alábbi normatív dokumentumoknak:

- 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) [15];
- 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 [16];
- ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates V2.4.1 (2013-02) [24];

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

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

A *Hitelesítés-szolgáltató* az alábbi kriptográfiai modulokat használja *Tanúsítvány*ok aláírására, valamint szolgáltatói magánkulcsainak tárolására:

- nCipher nShield F3 PCI nC4032P-150, firmware verzió: 2.22.6-3;
- nChipher nShield F3 SCSI nC4032W-150, firmware verzió: 2.18.15-3;
- nChipher nShield F3 500e PCIe nC4033E-500, firmware verzió: 2.50.16-3 és 2.51.10-3.

A fenti eszközök FIPS 140-2 [4] Level 3 tanúsítással, illetve az Eat. [3] 7 § (5) -(6) szerinti igazolással rendelkeznek.

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

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

A *Hitelesítés-szolgáltató* 2002 óta rendelkezik az ISO 9001 szabványnak megfelelő minőségirányítási, valamint 2003 óta a ISO/IEC 27001-nek (korábban BS 7799-nek) megfelelő információbiztonság-irányítási rendszerrel, amelyeket külső auditáló szervezet auditál és vizsgál felül folyamatosan (lásd: 1.2. fejezet).

8.1. Az ellenőrzések körülményei és gyakorisága

A *Hitelesítés-szolgáltató* évente külső megfelelőségi auditot hajt végre a szolgáltatások nyújtását végző informatikai rendszerén.

Amennyiben a *Hitelesítés-szolgáltató* külső *Regisztráló szervezet*tel működik együtt, akkor annak folyamatait évente auditálja.

Más szervezet által felügyelt hitelesítési egység számára kibocsátott szolgáltatói *Tanúsítvány* esetében a külső hitelesítési egység működését évente auditálja.

8.2. Az auditor és szükséges képesítése

A *Hitelesítés-szolgáltató* a belső auditokat a független rendszervizsgáló szerepkörrel felruházott alkalmazottai segítségével rendszeresen végzi.

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.

A *Hitelesítés-szolgáltató* rendszeres felülvizsgálatát a nyilvános kulcsú infrastruktúra területén többéves tapasztalattal rendelkező, a Nemzeti Média- és Hírközlési Hatóság által nyilvántartásba vett független elektronikus aláírás szakértő végzi.

8.3. Az auditor és az auditált rendszerelem függetlensége

A külső auditot végző auditor

- 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.
- díjazása nem függ az audit során végzett tevékenységének megállapításaitól.

8.4. Az auditálás által lefedett területek

Az átvizsgálás lefedi az alábbi területeket:

- hatályos jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;
- *Hitelesítési rend*(ek)nek és *Szolgáltatási szabályzat*(ok)nak való megfelelés;
- az alkalmazott folyamatok megfelelősége;
- a dokumentálás;
- a fizikai biztonság;
- a személyi állomány megfelelősége;
- az IT biztonság;
- az adatvédelmi szabályok betartása.

Amennyiben a *Hitelesítés-szolgáltató* külső *Regisztráló szervezet*tel együttműködik, illetve ha bocsátott ki más szervezet hitelesítési egysége számára szolgáltatói *Tanúsítvány*t, akkor a vizsgálat az érintett külső szervezetek tevékenységére is kiterjed.

8.5. A hiányosságok kezelése

A független auditor az átvizsgálás eredményét egy részletes átvilágítási jelentésben foglalja össze, amely kitér a vizsgált rendszerelemekre, folyamatokra, tartalmazza az átvilágítás során felhasznált bizonyítékokat és vizsgálói megállapításokat. A jelentésben külön fejezetben rögzíti a vizsgálat során feltárt eltéréseket és az elhárításukra kitűzött határidőket. A független auditor a vizsgálat során feltárt eltérések, hiányosságok súlyossága alapján a jelentésben rögzíthet

- opcionálisan figyelembe 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 hozza nyilvánosságra a rendszervizsgálatról készült részletes vizsgálati jelentést.

9. Egyéb üzleti és jogi kérdések

A *Szolgáltatási szabályzat* hatálya alá eső közösség (lásd: 1.3) kötelezettségeit és felelősségeit a vonatkozó szerződés és annak elválaszthatatlan részét képező *Szolgáltatási szabályzat*(ok) és *Hitelesítési rend*(ek) tartalmazzák. Az *Előfizető* jogait és kötelezettségeit az általános szerződési feltételek [17] is tartalmazzák.

9.1. Díjak

A szolgáltatási díjakat és árakat a *Hitelesítés-szolgáltató* a honlapján közzéteszi és kérésre ügyfélszolgálati irodájában nyomtatott formában is elérhetővé teszi.

A *Hitelesítés-szolgáltató* az árlistát egyoldalúan módosíthatja. Az árlista módosítását a hatályba lépése előtt 15 nappal a *Hitelesítés-szolgáltató* a honlapján közzéteszi. Az előre kifizetett szolgáltatások árát a módosítás nem érinti.

Az díjak kifizetésével és visszatérítésével kapcsolatos rendelkezéseket a szolgáltatási szerződés és mellékletei – különösen az általános szerződési feltételek – tartalmazzák.

9.1.1. Tanúsítvány kibocsátás és megújítás díjai

Lásd: 9.1. fejezet.

9.1.2. Tanúsítvány hozzáférés díja

A *Hitelesítés-szolgáltató* ingyenes hozzáférést biztosít az *Érintett felek* részére az on-line *Tanúsítványtár*hoz.

9.1.3. Visszavonási állapot információ hozzáférés díja

A *Hitelesítés-szolgáltató* ingyenes on-line CRL és OCSP információt szolgáltat az *Érintett felek* részére valamennyi általa kibocsátott végfelhasználói és köztes szolgáltatói *Tanúsítvány* visszavonási állapotáról.

9.1.4. Egyéb szolgáltatások díjai

Lásd: 9.1. fejezet.

9.1.5. Visszatérítési politika

Lásd: 9.1. fejezet.

9.2. Anyagi felelősségvállalás

A *Hitelesítés-szolgáltató* a megbízhatóság biztosítása érdekében megfelel a 3/2005. IHM rendeletben [8] meghatározott pénzügyi feltételeknek és teljesíti a felelősségvállalásra vonatkozó követelményeket.

9.2.1. Pénzügyi követelmények

A *Hitelesítés-szolgáltató* rendelkezik a szolgáltatások nyújtásával kapcsolatos pénzügyi felelőssége, valamint a megszűnésével kapcsolatos költségek biztosításához szükséges anyagi erőforrásokkal.

9.2.2. További követelmények

Nincs megkötés.

9.2.3. Felelősségbiztosítás

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

- A *Hitelesítés-szolgáltató* a megbízhatóság biztosítása érdekében felelősségbiztosítással rendelkezik.
- A felelősségbiztosítási szerződés kiterjed 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. [3] 16. §-ának (4) bekezdésében foglaltak megszegésével a Nemzeti Média- és Hírközlési Hatóságnak okozott károkra.

- A felelősségbiztosítási szerződés egy biztosítási esemény vonatkozásában káreseményenként a *Tanúsítvány*ban, illetve a *Szolgáltatási szabályzat*ban vállalt felelősségvállalási érték legalább háromszorosáig fedezetet biztosít az összes károsultnak okozott károkra. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.

- A felelősségbiztosítás a 3/2005. IHM rendelet [8] 11. § (3) bekezdésben meghatározott összeg erejéig fedezetet nyújt a károsultnak a szolgáltató károkozó magatartásával összefüggésben keletkező teljes kárára, függetlenül attól, hogy a kárt szerződésszegéssel vagy szerződésen kívül okozták.

- Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

9.3. Bizalmasság

A *Hitelesítés-szolgáltató* az *Ügyfel*ek adatait a jogszabályoknak megfelelően kezeli. A *Hitelesítés-szolgáltató* rendelkezik adatkezelési szabályzattal (lásd 9.4 fejezet), amely a személyes adatok kezelésével kiemelten foglalkozik.

Az *Ügyfél* a *Tanúsítvány* igénylésével, illetve a szolgáltatási szerződés aláírásával hozzájárul ahhoz, hogy a személyes adatait a *Hitelesítés-szolgáltató* (az adatkezelési szabályzatnak megfelelő módon) tárolja és kezelje. A hozzájárulás vonatkozik a törvény által meghatározott és nyilvántartásba vett információk harmadik félhez történő továbbítására a *Hitelesítés-szolgáltató* szolgáltatásainak leállítása esetén, valamint – kizárólag a szolgáltatással összefüggő feladatok elvégzése céljából – a *Hitelesítés-szolgáltató* alvállalkozóinak való továbbításra. A szolgáltatási szerződéshez tartozó tanúsítványkérelem űrlapon az *Alany*nak nyilatkoznia kell arról, hogy hozzájárul a *Tanúsítvány* nyilvánosságra hozatalához. A *Hitelesítés-szolgáltató* az *Ügyfel*ek adatait kizárólag a szolgáltatásaival összefüggésben használja fel.

Az *Alany* és a *Képviselt szervezet* *Tanúsítvány*ban szereplő adatait a *Hitelesítés-szolgáltató* a tanúsítvánnyal együtt nyilvánosságra hozza, amennyiben az *Alany* ehhez hozzájárul. A *Tanúsítvány*ba nem kerülő adataikat a *Hitelesítés-szolgáltató* védett módon tárolja az *Alany*

személyazonosságának, a *Képviselt szervezet* szervezeti azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

A *Hitelesítés-szolgáltató* a tudomására jutott adatokat a jogszabályi követelményeknek megfelelően, az előírt időtartamig megőrzi. A *Hitelesítés-szolgáltató* az adatok megőrzése során gondoskodik az információk sértetlenségéről, bizalmasságáról és biztonságos tárolásáról. Az információkhoz való hozzáférést csak azon személyeknek engedélyezi, akik feladata azt indokolja.

A *Hitelesítés-szolgáltató* az *Ügyfel*ek adatainak továbbítása során gondoskodik a nem nyilvános információk bizalmasságáról és sértetlenségéről.

9.3.1. Bizalmas információk köre

A *Hitelesítés-szolgáltató* bizalmas információként kezeli

- az *Ügyfel*ek minden adatát, kivéve azokat, amelyeket a 9.3.2. fejezetben nem bizalmasnak tekintett információnak minősít;
- az *Ügyfel*ek adatain kívül a:
  - magánkulcsokat és aktivizáló kódokat;
  - tanúsítványigényléseket és szolgáltatási szerződéseket;
  - tranzakciós és napló adatokat;
  - nem nyilvános szabályzatokat;
  - minden olyan adatot, amelynek nyilvánosságra kerülése a szolgáltatás biztonságát előnytelenül befolyásolná.

9.3.2. Bizalmas információk körén kívül eső adatok

Amennyiben az *Alany* ehhez hozzájárul, a *Hitelesítés-szolgáltató* nem bizalmas információként kezeli mindazon adatokat, amelyet a *Tanúsítvány*ba belefoglal. Ezek az adatok a szolgáltatási szerződéshez kapcsolódó tanúsítványkérelem űrlapon egyértelmű jelöléssel szerepelnek.

A *Hitelesítés-szolgáltató* az általa kibocsátott valamennyi végfelhasználói és szolgáltatói köztes *Tanúsítvány* visszavonási és felfüggesztési állapotát nyilvános információként kezeli és ezt korlátozás nélkül elérhetővé teszi az *Érintett felek* részére tanúsítvány visszavonási lista (CRL) publikálásával és on-line tanúsítvány-állapot szolgáltatás (OCSP) nyújtásával. A közzétett információ tartalmazza a *Tanúsítvány* sorszámát, a visszavonás időpontját és opcionálisan a visszavonás okát. Bővebb információ a 7.2. és 7.3. alfejezetekben található.

9.3.3. Bizalmas információ védelme

A *Hitelesítés-szolgáltató* felelősséggel tartozik az általa kezelt bizalmas adatok védelméért.

A *Hitelesítés-szolgáltató* szerződésben vagy titoktartási nyilatkozat aláírásával kötelezi alkalmazottait, alvállalkozóit, szerződött partnereit a bizalmas adatok védelmére.

A *Hitelesítés-szolgáltató* a birtokába jutott bizalmas adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseinek megfelelően kezeli, s csak az alábbi esetekben és személyek/szervezetek részére fedi fel őket:

- **Információszolgáltatás a hatóságok részére**

  A *Hitelesítés-szolgáltató* bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az adatigénylésre meghatározott jogszabályi feltételek teljesülése esetén – a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak haladéktalanul és egyéb feltételek nélkül feltárja a jogszabályban meghatározott bizalmas információkat az Eat. [3] 11.§ (2) bekezdése szerinti körben.

  A *Hitelesítés-szolgáltató* rögzíti az adatátadás tényét, de arról nem tájékoztatja az érintett *Ügyfel*eket.

- **Információszolgáltatás polgári eljárás keretében**

  A *Hitelesítés-szolgáltató* a *Tanúsítvány* érvényességét érintő polgári peres, illetve nem peres eljárás során – az érintettség igazolása esetén – az ellenérdekű peres félnek vagy képviselőjének, valamint a megkereső bíróságnak feltárhatja a jogszabályban meghatározott bizalmas felhasználói információkat, illetőleg azokat közölheti a megkereső bírósággal az Eat. [3] 11.§ (3) bekezdése szerinti körben.

  A *Hitelesítés-szolgáltató* rögzíti az adatátadás tényét, és arról tájékoztatja az érintett *Ügyfel*et.

- **A tulajdonos kérésére történő felfedés**

  A *Hitelesítés-szolgáltató* az *Ügyfél* személyes kérése vagy az általa hivatalosan, írásban adott felhatalmazása alapján tárja fel a rá vonatkozó bizalmas felhasználói információkat harmadik fél részére.

- **Egyéb információ-közzétételt eredményező körülmények**

  A *Hitelesítés-szolgáltató* a nyilvántartásait (a jogszabályban meghatározott bizalmas felhasználói adatokkal együtt) a tevékenysége befejezésekor átadja más – azonos besorolású

– szolgáltató vagy ennek hiányában a Nemzeti Média- és Hírközlési Hatóság részére az Eat. [3] 16. § 2. bekezdése szerint.

9.4. Személyes adatok védelme

A *Hitelesítés-szolgáltató* gondoskodik az általa kezelt személyes adatok védelméről, működése és szabályzatai megfelelnek az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [18] rendelkezéseinek.

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

- megőrzi,
- a szolgáltatási szerződés megszűnésekor az *Ügyfél* kérésére az ügyfél adatbázisából törli.

Ügyfél csak abban az esetben és olyan adatok törlését kérheti, amelyek megőrzését nem írja elő vonatkozó jogszabály.

A *Hitelesítés-szolgáltató* nyilvántartásában azonosító adatokat, *Tanúsítvány*ban szereplő adatokat, elérhetőséggel kapcsolatos adatokat és a szolgáltatás nyújtásával kapcsolatos adatokat tárol az *Alany*ról.

A *Hitelesítés-szolgáltató* kizárólag olyan esetben adja át harmadik félnek az *Alany* adatait, ha ezt jogszabály előírja vagy ha az *Alany* ebbe írásban beleegyezett.

Álneves *Tanúsítvány* esetén a *Hitelesítés-szolgáltató* kizárólag olyan esetben adja át harmadik félnek az *Alany* valódi azonosságára vonatkozó adatait, ha ezt jogszabály előírja, vagy ha az *Alany* illetve képviseletre jogosító *Tanúsítvány* esetén a *Képviselt szervezet* ebbe írásban beleegyezett.

A *Hitelesítés-szolgáltató* – a szolgáltatási szerződésnek megfelelően – nyilvánosságra hozza az *Alany*ok *Tanúsítvány*ban szereplő adatait és a *Tanúsítvány*ra vonatkozó visszavonási információt. A *Tanúsítvány*ban a *Hitelesítés-szolgáltató* feltünteti az *Alany* személyéhez rendelt egyedi azonosítót (OID-et).

A *Hitelesítés-szolgáltató* a szolgáltatások *Előfizető*iről kizárólag a szolgáltatás igénybevételéhez, a hitelesítéshez, valamint a szerződéskötéshez és számlázáshoz szükséges információt tárolja.

9.4.1. Adatkezelési szabályzat

A *Hitelesítés-szolgáltató* rendelkezik adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a személyes információk kezelésére. Az adatkezelési szabályzat megtalálható a *Hitelesítés-szolgáltató* honlapján.

9.4.2. Személyes adatok

A *Hitelesítés-szolgáltató* védi az érintettel kapcsolatba hozható, vagy az érintettre vonatkozó következtetést tartalmazó minden olyan személyes adatot, amely nem érhető el nyilvánosan a *Tanúsítvány*ból vagy más nyilvános adatforrásból.

Az Eat. [3] 11. § (1) bekezdésének megfelelően a *Hitelesítés-szolgáltató* csak az *Alany*tól közvetlenül, vagy annak egyértelmű előzetes hozzájárulásával gyűjt 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* biztonságosan tárolja és védi a *Tanúsítvány* kiadással kapcsolatos és a *Tanúsítvány*ban nem szereplő személyes adatokat. Az adatokat megfelelő intézkedésekkel védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, valamint nyilvánosságra hozatal ellen.

9.4.5. Személyes adatok felhasználása

A *Hitelesítés-szolgáltató* csak a *Tanúsítvány*okban szereplő személyes adatokat hozza nyilvánosságra az *Ügyfél* írásbeli engedélyének birtokában.

9.4.6. Adatkezelés

A *Hitelesítés-szolgáltató* az *Ügyfél* értesítése nélkül is kiadhatja az *Ügyfél*ről tárolt személyes adatokat az Eat. [3] 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 *Tanúsítvány*okat a benne szereplő nyilvános kulccsal együtt a kikötéseiben és feltételeiben ismertetett módon közzéteheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti.

A *Hitelesítés-szolgáltató* tulajdonát képezi a tanúsítvány visszavonási állapot információ, amit a *Hitelesítés-szolgáltató* nyilvánosságra hoz a 7.2. és 7.3. alfejezetekben meghatározott módon.

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

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

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

9.6. Tevékenységért viselt felelősség és helytállás

9.6.1. A Hitelesítés-szolgáltató felelőssége és helytállása

A *Hitelesítés-szolgáltató* felelőssége

A *Hitelesítés-szolgáltató* felelősségét jelen *Szolgáltatási szabályzat*, a vonatkozó *Hitelesítési rend*ek, valamint az *Ügyfél*lel kötött szerződés és annak mellékletei tartalmazzák.

- A *Hitelesítés-szolgáltató* felelősséget vállal az általa támogatott *Hitelesítési rend*ekben leírt eljárásoknak való megfelelésért, még abban az esetben is, amikor a *Hitelesítés-szolgáltató* egyes tevékenységeit alvállalkozók végzik.
- A *Hitelesítés-szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfel*ekkel szemben a Polgári Törvénykönyv [19] a szerződésszegésért való felelősség szabályai szerint felelős.
- A *Hitelesítés-szolgáltató* a vele szerződéses jogviszonyban nem álló harmadik személlyel (ilyen az *Érintett fél*) szemben a Polgári Törvénykönyv [19] általános felelősségi szabálya szerint felelős.

- A *Hitelesítés-szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 9.8. fejezet).
- Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

Az e-Szignó Hitelesítés Szolgáltató nem felelős:

- az *Alany*ok magánkulccsal, illetve *Aláírás-létrehozó eszköz*zel kapcsolatos tevékenységeiért,
- az *Érintett felek* tanúsítvány ellenőrzési és felhasználási tevékenységeiért,
- az *Érintett felek* vagy mások által kibocsátott szabályzatokért.

Az *Hitelesítés-szolgáltató* kötelezettsége

A *Hitelesítés-szolgáltató* alapvető kötelezettsége, hogy a szolgáltatásokat a jelen *Szolgáltatási szabályzat*tal és egyéb nyilvános szabályzatokkal, a szerződéses feltételekkel, továbbá a vállalati és biztonsági belső szabályzatokkal összhangban nyújtsa. Ezen alapvető kötelezettségek a következők:

- a szolgáltatásnak megfelelő jogi-, szabályozási-, anyagi-, szerződéses stb. keretek megteremtése,
- magas színvonalú és biztonságos szolgáltatások nyújtása a vonatkozó szabályzatok szerint,
- a szolgáltatásokhoz kapcsolódó szervezetek (hitelesítő szervezet, ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése,
- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése,
- a szolgáltatások biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket,
- a publikus nyilvántartások és saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az interneten keresztül.

A *Hitelesítés-szolgáltató* általános kötelezettségeit a vonatkozó *Hitelesítési rend*ek tartalmazzák.

A hitelesítő szervezet felelőssége

A hitelesítő szervezet feladata a hitelesítő egységek, valamint az online tanúsítvány-állapot szolgáltatáshoz szükséges egységek (lásd: 1.3.1) felállítása és működtetése, a tanúsítványtár és a visszavonási-állapot információ gondozása, az intelligens kártyák menedzselése és rendelkezésre bocsátása, valamint a szabályzatok menedzselése.

A hitelesítő szervezet belső működtetését a *Hitelesítés-szolgáltató* belső, operatív szabályzatai határozzák meg. A hitelesítő egységek által kibocsátott szolgáltatói tanúsítványok kezelése (regisztrációs munkatársak, ügyeletesek stb. számára) az operatív szabályzatok előírásainak megfelelően történik. Jelen szabályzat csak a nyilvános szolgáltatói és végfelhasználói tanúsítványokkal kapcsolatban tartalmaz előírásokat.

A szabályzatok menedzselése keretében ellátandó feladatok:

- az alkalmazott tanúsítványfajták specifikálása, jóváhagyása és karbantartása,
- a szolgáltatások nyilvános szabályzatainak és a belső (nem nyilvános) előírásoknak előkészítése, egyeztetése a jogszabályokkal és a belső (nem nyilvános) szabályzatokkal, továbbá az aktualizálások elvégzése,
- a szolgáltatásokra vonatkozó szabályzatokkal kapcsolatos észrevételek rögzítése és javaslatok elbírálása.

A vonatkozó *Hitelesítési rend* további kötelezettségeket tartalmazhat a hitelesítő szervezettel kapcsolatban.

Az e-Szignó Hitelesítés Szolgáltató felelős:

- az általa kibocsátott *Tanúsítvány*ok hitelességéért, pontosságáért,
- az általa kibocsátott szabályzatokért, azok jogszabályi megfelelőségéért és betartásáért,
- az általa generált kulcspárok megfelelőségéért, a magánkulcs-nyilvános kulcs és a *Tanúsítvány* összetartozásáért,
- az *Aláírás-létrehozó eszköz*t aktivizáló kód és az eszközre töltött kulcsok összetartozásáért,
- általában a kötelezettségei betartásáért.

9.6.2. A regisztráló szervezet felelőssége és helytállása

Az ügyfélszolgálati iroda feladata a *Hitelesítés-szolgáltató* képviselete a szolgáltatások kapcsán a végfelhasználónál. Ennek keretében a következő feladatokat látja el:

- közreműködik a szolgáltatások értékesítésében;

- elvégzi az *Alany* regisztrációját;
- a különböző tanúsítvány műveletekre vonatkozó kérelmeket fogadja (felfüggesztés, visszavonás, visszaállítás, tanúsítvány módosítás, kulcscsere stb.);
- fogadja és kezeli az adatmódosítási bejelentéseket;
- közreműködik a visszavonási állapot közzétételében;
- információs tevékenységet nyújt *Ügyfel*ek és az *Érintett felek* részére a *Hitelesítés-szolgáltató* által nyújtott szolgáltatásokkal kapcsolatos tevékenységeivel kapcsolatban;
- tájékoztató anyagot bocsát az *Ügyfél* rendelkezésére, amely tartalmazza a 3/2005 IHM rendelet 35 §-ban és az Eat. 9 § (1)-ben szereplő információkat. A *Regisztráló szervezet* regisztrációs munkatársa lehetővé teszi, hogy az *Ügyfél* ezen tájékoztató anyagot alaposan áttanulmányozza, majd az *Ügyfél* esetleges kérdéseit megválaszolja.

A *Regisztráló szervezet* felelős:

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

9.6.3. Az Ügyfél felelőssége és helytállása

Az *Előfizető* felelőssége

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

Az *Előfizető* kötelezettségei

Az *Előfizető* kötelessége a *Hitelesítés-szolgáltató* szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatások felhasználása során, beleértve a *Tanúsítvány*ok és

magánkulcsok igénylését és alkalmazását. Az *Előfizető* kötelezettségeit a a jelen *Szolgáltatási szabályzat*, a szolgáltatási szerződés és annak elválaszthatatlan részét képező általános szerződési feltételek és egyéb dokumentumok, valamint a vonatkozó *Hitelesítési rend*ek tartalmazzák.

Az *Előfizető* jogai

- Az *Előfizető* jogosult a szolgáltatások igénybe vételére a jelen *Szolgáltatási szabályzat*ban leírtak szerint.
- Az elektronikus aláírás hitelesítés szolgáltatás esetén az *Előfizető* jogosult írásban meghatározni, hogy mely *Alany* kaphasson tanúsítványt.
- Az *Előfizető* jogosult a tanúsítványok felfüggesztését és visszavonását kérni.
- Az *Előfizető* jogosult szervezeti ügyintézőt kijelölni.

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;
- *Aláírás-létrehozó eszköz*ének, magánkulcsának 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 *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;
- 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 elvégezése után bocsátja ki;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*okban kizárólag a valóságnak megfelelő adatokat szerepeltet. Ennek megfelelően a *Hitelesítés-szolgáltató* a *Tanúsítvány*ba kerülő adatokat a *Szolgáltatási szabályzat* szerint ellenőrzi;

- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*t visszavonja, amennyiben tudomására jut, hogy a *Tanúsítvány*ban foglalt adatok nem felelnek meg a valóságnak, vagy 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 használták.

Az *Alany* jogai

- Az *Alany* jogosult *Tanúsítvány*t igényelni a jelen *Szolgáltatási szabályzat*ban leírtak szerint.
- Amennyiben ezt a vonatkozó *Hitelesítési rend* lehetővé teszi, az *Alany* jogosult *Tanúsítvány*ának felfüggesztését, illetve visszavonását kérni jelen *Szolgáltatási szabályzat* szerint.

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.

A *Hitelesítés-szolgáltató* kizárja felelősségét, amennyiben az *Érintett fél* nem körültekintően jár el a *Tanúsítvány*ok felhasználása vagy ellenőrzése során, azaz nem a vonatkozó *Hitelesítési rend*, nem jelen *Szolgáltatási szabályzat*, illetve nem a hatályos jogszabályok szerint jár el.

9.6.5. Egyéb szereplők tevékenységéért viselt felelősség és helytállás

A Képviselt Szervezet felelőssége

A *Képviselt szervezet* kizárólag az általa kiadott igazolásokért felel. Különösen azon igazolásokért, amelyben igazolja, hogy az *Alany* jogosult a *Szervezet* nevét is tartalmazó *Tanúsítvány* használatára, illetve jogosult a *Képviselt szervezet Tanúsítvány*ában szerepelni. Amennyiben a *Képviselt szervezet* által kiállított valamely igazolásban szereplő információ megváltozik, a *Képviselt szervezet* felelőssége ezt haladéktalanul jelenteni a *Hitelesítés-szolgáltató*nak.

A Képviselt Szervezet jogai

- A *Hitelesítés-szolgáltató* kizárólag a *Képviselt szervezet* hozzájárulásával bocsát ki olyan *Tanúsítvány*t, amelyben a *Képviselt szervezet* neve is feltüntetésre kerül.
- A *Képviselt szervezet* jogosult azon *Tanúsítvány*okat felfüggesztetni és visszavonatni, amelyekben a *Képviselt szervezet* neve is feltüntetésre került.

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 *Szolgáltatási szabályzat*, a *Hitelesítési rend*

  vagy a hatályos jogszabályok szerint jár el;
- az *Alanyok* nem tartják be az *Aláírás-létrehozó eszköz* illetve a magánkulcs kezelésével kapcsolatos előírásokat;
- az *Érintett felek* vagy mások által kibocsátott szabályzatok nem felelnek meg a jelen *Szolgáltatási szabályzat*nak vagy a *Hitelesítési rend* nek;

- 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 kriptográfiai 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.

- A *Hitelesítés-szolgáltató* nem felelős az olyan károkért, amelyek abból adódnak, hogy az *Érintett fél* a *Tanúsítvány*ok ellenőrzése és felhasználása során nem a hatályos jogszabályok és a *Hitelesítés-szolgáltató* szabályzatai szerint járt el, illetve nem úgy járt el, ahogyan az az adott helyzetben elvárható.
- A *Hitelesítés-szolgáltató* a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag kötelezettségei felróható megszegéséből bekövetkező, bizonyítható károkért tartozik helytállni.
- A *Hitelesítés-szolgáltató* nem felelős az abból adódó károkért, amikor valamely külső, elháríthatatlan esemény miatt az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni.
- A *Hitelesítés-szolgáltató* közhiteles adatbázissal végez adategyeztetést, mielőtt az *Alany Tanúsítvány*át kibocsátja. A *Hitelesítés-szolgáltató* nem vállal felelősséget ezen közhiteles adatbázis által szolgáltatott információk pontatlanságából eredő károkért.
- A *Hitelesítés-szolgáltató* kizárólag azért vállal felelősséget, hogy a szolgáltatásokat a jelen *Szolgáltatási szabályzat*ban, illetve az abban meghivatkozott dokumentumokban (*Hitelesítési rend*ek, szabványok, ajánlások) leírtaknak, valamint saját belső szabályzatainak megfelelően nyújtja.

Adminisztratív folyamatok

A *Hitelesítés-szolgáltató* a vagyoni felelősségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelősség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása

és bizonyíthatósága érdekében naplózza tevékenységeit, védi a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megőrzi (archiválja) a naplóadatokat.

Pénzügyi felelősség

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

A *Hitelesítés-szolgáltató* ezen felül, a megbízhatóság biztosítása érdekében a jogszabályi előírásoknak megfelelő felelősségbiztosítással is rendelkezik.

Pénzügyi felelősség korlátozása

A *Hitelesítés-szolgáltató* – annak ellenére, hogy az elektronikus aláírásról szóló törvény [3] erre lehetőséget ad – nem korlátozza az egy alkalommal vállalható legmagasabb kötelezettség mértékét.
A *Hitelesítés-szolgáltató* korlátozza a szolgáltatásokkal kapcsolatos kártérítési kötelezettségét, ezen korlátozás mértéke

- a III. hitelesítési osztályba tartozó tanúsítványokkal kapcsolatban káreseményenként 100.000,-Ft;
- a II. hitelesítési osztályba tartozó tanúsítványokkal kapcsolatban káreseményenként 20.000,-Ft.

Az egyes *Tanúsítvány*ok esetén a felelősségbiztosítás egy biztosítási káresemény vonatkozásában a fent felsorolt korlát háromszorosáig biztosít fedezetet.

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.

9.9. Kártérítési kötelezettség

9.9.1. A szolgáltató kártérítési kötelezettsége

A *Hitelesítés-szolgáltató* kártérítési kötelezettségének részletes szabályait jelen szabályzat (lásd: 9.8. fejezet), a szolgáltatási szerződés és az *Ügyfel*ekkel kötött szerződések tartalmazzák.

9.9.2. Az előfizető kártérítési kötelezettsége

Az *Előfizető*, illetve az *Alany* kártérítési felelősséggel tartoznak a *Hitelesítés-szolgáltató*nak azokért a veszteségekért és károkért, amelyeket kötelezettségeik és a rájuk vonatkozó ajánlások be nem tartásával okoznak számára.

9.9.3. Az érintett felek kártérítési kötelezettsége

Lásd: 9.8. fejezet

9.10. Érvényesség és megszűnés

9.10.1. Érvényesség

A *Szolgáltatási szabályzat* adott verziója hatályba lépésének napja a *Szolgáltatási szabályzat* címlapján kerül meghatározásra.

9.10.2. Megszűnés

A *Szolgáltatási szabályzat* visszavonásig hatályos időbeli korlátozás nélkül.

A *Szolgáltatási szabályzat* 9. fejezete érvényben marad a *Szolgáltatási szabályzat* hatályának megszűnését követően is (a hatályosság megszűnésének módjától függetlenül) mindazon *Tanúsítvány*okkal kapcsolatosan, amelyet a *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzat* hatálya alatt bocsátott ki.

9.10.3. A megszűnés következményei

A *Szolgáltatási szabályzat* visszavonása esetén a *Hitelesítés-szolgáltató* honlapján közzéteszi a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket. A *Hitelesítés-szolgáltató* garantálja, hogy a *Szolgáltatási szabályzat* visszavonása esetén is érvényben maradnak a bizalmas adatok védelmére vonatkozó előírások.

9.11. A felek közötti kommunikáció

A *Hitelesítés-szolgáltató* az *Ügyfel*ekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát működtet.

Az *Ügyfel*ek jognyilatkozataikat a *Hitelesítés-szolgáltató* felé kizárólag írásban, aláírt módon tehetik meg. Szervezet képviseletében való aláírás csak a képviseleti jogosultság igazolásával együtt érvényes.

A kibocsátott *Tanúsítvány*ok telefonon is felfüggeszthetők. Egyéb jellegű értesítés írásban, elektronikus levél vagy fax formájában is megtehető.

Az e-Szignó *Hitelesítés-szolgáltató Ügyfel*eit a honlapján történő közzététel útján vagy elektronikus levélben tájékoztatja.

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 *Szolgáltatási szabályzat*ot.

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

9.12.1. Módosítási eljárás

A *Hitelesítés-szolgáltató* nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyezteti. A *Hitelesítés-szolgáltató* több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen *Szolgáltatási szabályzat* több ilyet is megemlít). A 8.4. fejezetben leírt eljárások ezeket a dokumentumokat is vizsgálják.

A *Hitelesítés-szolgáltató* hitelesítő szervezetén belül működik egy olyan szervezeti egység, amely felelős a szabályzatok és dokumentációk karbantartásáért. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz. A szabályzatot az e-Szignó Hitelesítés Szolgáltató igazgatója hagyja jóvá.

A változtatásokat gyűjtve a csoport belső, nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. A *Hitelesítés-szolgáltató* törekszik arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

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

A *Hitelesítés-szolgáltató* jelen szabályzatban bekövetkező minden változást – a jogszabályi előírásoknak megfelelően – a változás életbe lépése előtt 30 nappal bejelent a Nemzeti Média- és Hírközlési Hatóságnak, és a megváltozott szabályzat tervezetét közzéteszi weboldalán.

A közzétett új szabályzat tervezettel kapcsolatos észrevételeket *Hitelesítés-szolgáltató* a hatályba lépést megelőző 14. napig fogadja az `info@e-szigno.hu` címen. A szabályzat észrevételekkel módosított változatát a *Hitelesítés-szolgáltató* a hatályba lépést megelőző 7. nap zárja le és teszi közzé.

Jelen *Szolgáltatási szabályzat* [26], [25] szabványoknak, valamint az 1.2.1. fejezetben leírt hitelesítési rendeknek való megfelelőségét közzététel előtt a *Hitelesítés-szolgáltató* megvizsgálta.

A Nemzeti Média- és Hírközlési Hatóság vizsgálja, hogy a *Hitelesítés-szolgáltató* szabályzatai, valamint működése a közigazgatási felhasználásra *Tanúsítvány*t kibocsátók számára előírt követelményeket kielégíti-e.

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 *Szolgáltatási szabályzat* legkisebb változtatása esetén is új verziószámot ad ki, ami része a dokumentum azonosítónak (OID), így a dokumentum minden változása az OID változását eredményezi, vagyis két eltérő tartalmú dokumentumnak nem lehet azonos OID azonosítója.

9.13. Vitás kérdések rendezése

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

A *Hitelesítés-szolgáltató* és az *Ügyfél* kölcsönösen megállapodnak abban, hogy bármilyen vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra való terelése előtt megkísérlik a békés úton, tárgyalással történő egyeztetést. A kezdeményező fél kötelessége, hogy minden érintett többi felet haladéktalanul értesítsen és teljes körűen tájékoztasson az ügy minden vonatkozását illetően. A *Hitelesítés-szolgáltató* tevékenységével vagy a kiadott *Tanúsítvány*ok felhasználásával kapcsolatos kérdéseket, kifogásokat és panaszokat az ügyfélszolgálati iroda címére kell eljuttatni írásos formában. A bejelentés kézhezvételétől számított 3 munkanapon belül a *Hitelesítés-szolgáltató* értesíti a bejelentő felet az általa megadott címen a bejelentés fogadásáról és a kivizsgáláshoz szükséges időről. A megjelölt határidőig a *Hitelesítés-szolgáltató* köteles írásban válaszolni a bejelentőnek. A *Hitelesítés-szolgáltató* a válaszadáshoz szükséges információk megadását kérheti a bejelentőtől. A *Hitelesítés-szolgáltató* a panaszt 30 napon belül kivizsgálja, és az eredményekről értesíti a bejelentőt. Amennyiben a választ a bejelentő nem tartja kielégítőnek, vagy az alapján nem sikerül a *Hitelesítés-szolgáltató* bevonása nélkül rendezni a felmerült vitát, akkor a bejelentő egyeztetést kezdeményezhet a *Hitelesítés-szolgáltató*val és az *Érintett felek*kel. Az egyeztetés minden résztvevőjét írásban értesíteni kell az egyeztetés időpontjáról azt megelőzően 10 munkanappal, és írásban meg kell számukra küldeni a bejelentést, a *Hitelesítés-szolgáltató* válaszát és egyéb szükséges információkat tartalmazó dokumentumokat. Amennyiben az egyeztetés

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

9.14. Irányadó jog

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

9.15. Az érvényben lévő jogszabályoknak való megfelelés

A vonatkozó jogszabályok:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 1999/93/EK IRÁNYELVE (1999. december 13.) az elektronikus aláírással kapcsolatos közösségi keretrendszerről (hatályon kívül helyezve 2016. július 1-től) [15];
- 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 [16];
- 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 *Szolgáltatási szabályzat* alapján nyújtott szolgáltatásokba bevont alvállalkozók vagy egyéb együttműködő partnerek csak a Microsec zrt. előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3. Részleges érvénytelenség

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

9.16.4. Igényérvényesítés

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

9.16.5. Vis maior

A *Hitelesítés-szolgáltató* nem felelős a *Hitelesítési rend*ben és a *Szolgáltatási szabályzat*ban megfogalmazott 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] e-Szignó Hitelesítés Szolgáltató - minősített időbélyegzési rend.

[2] e-Szignó Hitelesítés Szolgáltató - nem minősített aláíró tanúsítvány hitelesítési rendek.

[3] 2001. évi XXXV. törvény az elektronikus aláírásról.

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

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

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

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

[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] EU Trusted Lists of Certification Service Providers, (`https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers`.

[11] Megbízható hitelesítés szolgáltatók listája (`http://www.nmhh.hu/tl/pub/HU_TL.pdf`.

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

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

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

[15] 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).

[16] 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.

[17] e-Szignó Hitelesítés Szolgáltató - nem minősített elektronikus aláírás hitelesítés szolgáltatásra és nem minősített időbélyegzés szolgáltatásra vonatkozó - általános szerződési feltételek.

[18] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

[19] 2013. évi V. törvény a Polgári Törvénykönyvről.

[20] 78/2010. (III. 25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól.

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

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

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

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

[25] ETSI TS 102 280: X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons (v1.1.1; 2004-03).

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

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