

e-Szignó Hitelesítés Szolgáltató

eIDAS Rendelet szerinti weboldal-hitelesítő tanúsítvány hitelesítési rendek

ver. 2.16

Hatálybalépés: 2020-08-14



Azonosító	1.3.6.1.4.1.21528.2.1.1.159.2.16, 1.3.6.1.4.1.21528.2.1.1.161.2.16, 1.3.6.1.4.1.21528.2.1.1.162.2.16
Verzió	2.16
Első verzió hatálybalépése	2016-07-01
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2020-08-10
Hatálybalépés dátuma	2020-08-14

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság
1033 Budapest, Ángel Sanz Briz út 13.

Verzió	A változás leírása	Hatálybalépés	Készítette
2.0	Új szabályzat az RFC 3647 és az eIDAS követelmények szerint.	2016-07-01	Szabóné Endrődi Csilla, Dr. Szőke Sándor, Réti Kornél
2.1	Módosítások az NMHH észrevételei alapján.	2016-09-05	Szomolya Melinda, Dr. Szőke Sándor
2.2	Módosítások a tanúsító észrevételei alapján.	2016-10-30	Dr. Szőke Sándor
2.4	Éves felülvizsgálat.	2017-09-30	Dr. Szőke Sándor
2.6	Teljes felülvizsgálat. Domén validálási módszerek változása. Közjegyzői személy azonosítás bevezetése. Kisebb módosítások.	2018-03-24	Dr. Szőke Sándor
2.7	Éves felülvizsgálat.	2018-09-15	Dr. Szőke Sándor
2.8	Változások az auditor javaslatai alapján.	2018-12-14	Dr. Szőke Sándor
2.9	Domén validálási követelmények változása. Kisebb módosítások. Változások a CABF BR követelményekben.	2019-04-24	Dr. Szőke Sándor
2.10	Kisebb módosítások.	2019-06-25	Dr. Szőke Sándor
2.11	Éves felülvizsgálat.	2019-09-25	Dr. Szőke Sándor
2.12	Változások az auditor javaslatai alapján.	2019-12-12	Dr. Szőke Sándor
2.13	Hatály. Személyes azonosítás szabályai. Tanúsítvány módosítás. HSM követelmények. Kisebb pontosítások.	2020-03-05	Dr. Szőke Sándor
2.14	Kiemelt kockázatú bejelentések kezelésének hozzáadása az 1.5.2. fejezethez. 2. fejezet átszervezése. A visszavonás feltételeinek kibővítése a 4.9 fejezetben. 9.4 fejezet kibővítése. Kisebb pontosítások.	2020-05-26	Dr. Szőke Sándor
2.16	OCSF Signing EKU eltávolítása a CA tanúsítványokból. Tanúsítvány érvényesség max. 398 nap. Kisebb pontosítások.	2020-08-14	Dr. Szőke Sándor

© 2020, Microsec zrt. Minden jog fenntartva.

Tartalomjegyzék

1. Bevezetés	13
1.1. Áttekintés	13
1.2. Dokumentum neve és azonosítója	13
1.2.1. Hitelesítési rendek	14
1.2.2. Hatály	16
1.2.3. Biztonsági szintek	16
1.3. PKI szereplők	17
1.3.1. Hitelesítés-szolgáltató	17
1.3.2. Regisztráló szervezetek	17
1.3.3. Ügyfelek	18
1.3.4. Érintett felek	18
1.3.5. Egyéb szereplők	18
1.4. A tanúsítvány felhasználhatósága	18
1.4.1. Megfelelő tanúsítvány használat	18
1.4.2. Tiltott tanúsítvány használat	18
1.5. A dokumentum adminisztrálása	18
1.5.1. A dokumentum adminisztrációs szervezete	18
1.5.2. Kapcsolattartó személy	19
1.5.3. A Szolgáltatási szabályzat <i>Hitelesítési rend</i> nek való megfeleléséért felelős személy/szervezet	19
1.5.4. A Szolgáltatási szabályzat elfogadási eljárása	19
1.6. Fogalmak és rövidítések	20
1.6.1. Fogalmak	20
1.6.2. Rövidítések	26
2. Közzététel és adattár felelőségek	26
2.1. Adattárak	26
2.2. A tanúsítványokra vonatkozó információk közzététele	27
2.3. A közzététel időpontja vagy gyakorisága	28
2.3.1. Kikötések és feltételek közzétételi gyakorisága	28
2.3.2. Tanúsítványok nyilvánosságra hozatalának gyakorisága	28
2.3.3. A megváltozott visszavonási állapot közzétételének gyakorisága	29
2.4. Az adattárak elérésének szabályai	29
3. Azonosítás és hitelesítés	29
3.1. Elnevezések	29
3.1.1. Név típusok	29
3.1.2. A nevek értelmezhetősége	33

3.1.3.	Álnevek használata	33
3.1.4.	A különböző elnevezési formák értelmezési szabályai	33
3.1.5.	A nevek egyedisége	33
3.1.6.	Márkanév elismerése, azonosítása, szerepük	33
3.2.	Kezdeti regisztráció, azonosság hitelesítése	34
3.2.1.	A magánkulcs birtoklásának igazolása	34
3.2.2.	Szervezet és domén azonosságának hitelesítése	34
3.2.3.	Természetes személy azonosságának hitelesítése	42
3.2.4.	Nem ellenőrzött alany információk	44
3.2.5.	Jogok, felhatalmazások ellenőrzése	44
3.2.6.	Együttműködési képességre vonatkozó követelmények	44
3.3.	Azonosítás és hitelesítés kulcscsere kérelem esetén	45
3.3.1.	Azonosítás és hitelesítés érvényes tanúsítvány esetén	45
3.3.2.	Azonosítás és hitelesítés érvénytelen tanúsítvány esetén	45
3.4.	Azonosítás és hitelesítés tanúsítvány megújítás esetén	45
3.4.1.	Azonosítás és hitelesítés érvényes tanúsítvány esetén	45
3.4.2.	Azonosítás és hitelesítés érvénytelen tanúsítvány esetén	45
3.5.	Azonosítás és hitelesítés tanúsítvány módosítás esetén	45
3.5.1.	Azonosítás és hitelesítés érvényes tanúsítvány esetén	46
3.5.2.	Azonosítás és hitelesítés érvénytelen tanúsítvány esetén	46
3.6.	Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási kérelem esetén	46
3.7.	Ellenőrzött kommunikációs csatorna	46
4.	A tanúsítványok életciklusára vonatkozó követelmények	46
4.1.	Tanúsítványkérelem	46
4.1.1.	Ki nyújthat be tanúsítványkérelmet	47
4.1.2.	A bejegyzés folyamata és a résztvevők felelőssége	48
4.2.	A tanúsítványkérelem feldolgozása	49
4.2.1.	Az igénylő azonosítása és hitelesítése	49
4.2.2.	A tanúsítványkérelem elfogadása vagy visszautasítása	49
4.2.3.	A tanúsítványkérelem feldolgozásának időtartama	49
4.3.	A tanúsítvány kibocsátása	49
4.3.1.	A Hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során	49
4.3.2.	Az Ügyfél értesítése a tanúsítvány kibocsátásáról	50
4.4.	A tanúsítvány elfogadása	50
4.4.1.	A tanúsítvány elfogadás módja	50
4.4.2.	A tanúsítvány közzététele	50
4.4.3.	További szereplők értesítése a tanúsítvány kibocsátásról	50
4.5.	A kulcspár és a tanúsítvány használata	50

4.5.1.	A magánkulcs és a tanúsítvány használata	50
4.5.2.	Az Érintett felek nyilvános kulcs és tanúsítvány használata	50
4.6.	Tanúsítvány megújítás	51
4.6.1.	A tanúsítvány megújítás körülményei	51
4.6.2.	Ki kérelmezheti a tanúsítvány megújítást	51
4.6.3.	A tanúsítvány megújítási kérelmek feldolgozása	52
4.6.4.	Az Ügyfél értesítése az új tanúsítvány kibocsátásáról	52
4.6.5.	A megújított tanúsítvány elfogadása	52
4.6.6.	A megújított tanúsítvány közzététele	52
4.6.7.	További szereplők értesítése a tanúsítvány kibocsátásáról	52
4.7.	Kulcscsere	52
4.7.1.	A kulcscsere körülményei	53
4.7.2.	Ki kérelmezheti a kulcscserét	53
4.7.3.	A kulcscsere kérelmek feldolgozása	53
4.7.4.	Az Ügyfél értesítése az új tanúsítvány kibocsátásáról	53
4.7.5.	A kulcscserével megújított tanúsítvány elfogadása	53
4.7.6.	A kulcscserével megújított tanúsítvány közzététele	53
4.7.7.	További szereplők értesítése a tanúsítvány kibocsátásáról	53
4.8.	Tanúsítvány módosítás	54
4.8.1.	A tanúsítvány módosítás körülményei	54
4.8.2.	Ki kérelmezheti a tanúsítvány módosítást	54
4.8.3.	A tanúsítvány módosítási kérelmek feldolgozása	54
4.8.4.	Az Ügyfél értesítése az új tanúsítvány kibocsátásáról	55
4.8.5.	A módosított tanúsítvány elfogadása	55
4.8.6.	A módosított tanúsítvány közzététele	55
4.8.7.	További szereplők értesítése a tanúsítvány kibocsátásáról	55
4.9.	Tanúsítvány visszavonás és felfüggesztés	55
4.9.1.	A tanúsítvány visszavonás körülményei	55
4.9.2.	Ki kérelmezheti a visszavonást	59
4.9.3.	A visszavonási kérelemre vonatkozó eljárás	59
4.9.4.	A visszavonási kérelemre vonatkozó kivárási idő	60
4.9.5.	A visszavonási eljárás maximális hossza	60
4.9.6.	Az Érintett felek számára javasolt eljárás a visszavonási információ ellenőrzésére	61
4.9.7.	A visszavonási lista kibocsátás gyakorisága	61
4.9.8.	A visszavonási lista előállítás és közzététele közötti idő maximális hossza	61
4.9.9.	Valós idejű tanúsítvány állapot ellenőrzés lehetősége	61
4.9.10.	A valós idejű tanúsítvány állapot ellenőrzésre vonatkozó követelmények	61
4.9.11.	A visszavonási hirdetések egyéb elérhető formái	61

4.9.12.	A kulcs kompromittálódásra vonatkozó speciális követelmények	61
4.9.13.	A felfüggesztés körülményei	62
4.9.14.	Ki kérelmezheti a felfüggesztést	62
4.9.15.	A felfüggesztési kérelemre vonatkozó eljárás	62
4.9.16.	A felfüggesztés maximális hossza	62
4.10.	Tanúsítvány állapot szolgáltatások	62
4.10.1.	Működési jellemzők	62
4.10.2.	A szolgáltatás rendelkezésre állása	63
4.10.3.	Opcionális lehetőségek	63
4.11.	Az előfizetés vége	63
4.12.	Magánkulcs letétbe helyezése és visszaállítása	63
4.12.1.	Kulcsletét és visszaállítás rendje és szabályai	63
4.12.2.	Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai	63
5.	Elhelyezési, eljárásbeli és üzemeltetési előírások	63
5.1.	Fizikai követelmények	64
5.1.1.	A telephely elhelyezése és szerkezeti felépítése	64
5.1.2.	Fizikai hozzáférés	64
5.1.3.	Áramellátás és légkondicionálás	65
5.1.4.	Beázás és elárasztódás veszély kezelése	65
5.1.5.	Tűz megelőzés és tűzvédelem	66
5.1.6.	Adathordozók tárolása	66
5.1.7.	Hulladék megsemmisítése	66
5.1.8.	A mentési példányok fizikai elkülönítése	66
5.2.	Eljárásbeli előírások	66
5.2.1.	Bizalmi szerepkörök	67
5.2.2.	Az egyes feladatok ellátásához szükséges személyzeti létszámok	67
5.2.3.	Az egyes szerepkörökben elvárt azonosítás és hitelesítés	68
5.2.4.	Egymást kizáró szerepkörök	68
5.3.	Személyzetre vonatkozó előírások	68
5.3.1.	Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények	68
5.3.2.	Előélet vizsgálatára vonatkozó eljárások	69
5.3.3.	Képzési követelmények	69
5.3.4.	Továbbképzési gyakoriságok és követelmények	70
5.3.5.	Munkabeosztás körforgásának sorrendje és gyakorisága	70
5.3.6.	Felhatalmazás nélküli tevékenységek büntető következményei	70
5.3.7.	Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények	70

5.3.8.	A személyzet számára biztosított dokumentációk	70
5.4.	Naplózási eljárások	71
5.4.1.	A tárolt események típusai	71
5.4.2.	A naplófájl feldolgozásának gyakorisága	74
5.4.3.	A naplófájl megőrzési időtartama	74
5.4.4.	A naplófájl védelme	74
5.4.5.	A naplófájl mentési eljárásai	75
5.4.6.	A naplózás adatgyűjtési rendszere	75
5.4.7.	Az eseményeket kiváltó alanyok értesítése	75
5.4.8.	Sebezhetőség felmérése	75
5.5.	Adatok archiválása	75
5.5.1.	Az archivált adatok típusai	75
5.5.2.	Az archívum megőrzési időtartama	76
5.5.3.	Az archívum védelme	76
5.5.4.	Az archívum mentési folyamatai	77
5.5.5.	Az adatok időbélyegzésére vonatkozó követelmények	77
5.5.6.	Az archívum gyűjtési rendszere	77
5.5.7.	Archív információk hozzáférését és ellenőrzését végző eljárások	77
5.6.	Szolgáltatói kulcs cseréje	78
5.7.	Kompromittálódást és katasztrófát követő helyreállítás	78
5.7.1.	Váratlan esemény és kompromittálódás kezelési eljárások	78
5.7.2.	Meghibásodott IT erőforrások, szoftverek és/vagy adatok	78
5.7.3.	Magánkulcs kompromittálódása esetén követendő eljárások	79
5.7.4.	Működés folyamatosságának biztosítása katasztrófát követően	79
5.8.	A hitelesítés-szolgáltató vagy a regisztráló szervezet leállítása	79
6.	Műszaki biztonsági óvintézkedések	80
6.1.	Kulcspár előállítása és telepítése	80
6.1.1.	Kulcspár előállítása	80
6.1.2.	Magánkulcs eljuttatása az igénylőhöz	82
6.1.3.	A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz	82
6.1.4.	A szolgáltatói nyilvános kulcs közzététele	82
6.1.5.	Kulcsméretek	83
6.1.6.	A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése	83
6.1.7.	A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)	83
6.2.	A magánkulcsok védelme	84
6.2.1.	Kriptográfiai modulra vonatkozó szabványok és előírások	84
6.2.2.	Magánkulcs többszereplős (n-ből m) használata	85

6.2.3.	Magánkulcs letétbe helyezése	85
6.2.4.	Magánkulcs mentése	85
6.2.5.	Magánkulcs archiválása	85
6.2.6.	Magánkulcs bejuttatása hardver kriptográfiai eszközbe, vagy onnan történő exportja	86
6.2.7.	Magánkulcs tárolása hardver kriptográfiai eszközben	86
6.2.8.	A magánkulcs aktiválásának módja	86
6.2.9.	A magánkulcs deaktiválásának módja	86
6.2.10.	A magánkulcs megsemmisítésének módja	86
6.2.11.	A hardver kriptográfiai eszközök értékelése	87
6.3.	A kulcspár kezelés egyéb szempontjai	87
6.3.1.	Nyilvános kulcs archiválása	87
6.3.2.	A tanúsítványok és kulcspárok használatának periódusa	87
6.4.	Aktivizáló adatok	88
6.4.1.	Aktivizáló adatok előállítása és telepítése	88
6.4.2.	Az aktivizáló adatok védelme	89
6.4.3.	Az aktivizáló adatok kezelésének egyéb szempontjai	89
6.5.	Informatikai biztonsági előírások	89
6.5.1.	Speciális informatikai biztonsági műszaki követelmények	89
6.5.2.	Az informatikai biztonság értékelése	89
6.6.	Életciklusra vonatkozó műszaki előírások	89
6.6.1.	Rendszerfejlesztési előírások	89
6.6.2.	Biztonságkezelési előírások	90
6.6.3.	Életciklusra vonatkozó biztonsági előírások	90
6.7.	Hálózati biztonsági előírások	91
6.8.	Időbélyegzés	92
7.	Tanúsítvány, CRL és OCSP profilok	92
7.1.	Tanúsítvány profil	92
7.1.1.	Verzió szám(ok)	92
7.1.2.	Tanúsítvány kiterjesztések	93
7.1.3.	Az algoritmus objektum azonosítója	99
7.1.4.	Névformák	99
7.1.5.	Névhasználati megkötöttségek	99
7.1.6.	A Hitelesítési rend objektum azonosítója	99
7.1.7.	A Hitelesítési rend megkötöttségek kiterjesztés használata	99
7.1.8.	A Hitelesítési rend jellemzők szintaktikája és szemantikája	100
7.1.9.	A kritikus Hitelesítési rend kiterjesztések feldolgozási szemantikája	100
7.2.	Tanúsítvány visszavonási lista (CRL) profil	100

7.2.1.	Verziószám(ok)	100
7.2.2.	Tanúsítvány visszavonási lista kiterjesztések	100
7.3.	Online tanúsítvány-állapot válasz (OCSP) profil	101
7.3.1.	Verziószám(ok)	102
7.3.2.	OCSP kiterjesztések	102
8.	A megfelelőség vizsgálata	102
8.1.	Az ellenőrzések körülményei és gyakorisága	103
8.2.	Az auditor és szükséges képesítése	103
8.3.	Az auditor és az auditált rendszerelem függetlensége	103
8.4.	Az auditálás által lefedett területek	104
8.5.	A hiányosságok kezelése	104
8.6.	Az eredmények közzététele	104
9.	Egyéb üzleti és jogi kérdések	105
9.1.	Díjak	105
9.1.1.	Tanúsítvány kibocsátás és megújítás díjai	105
9.1.2.	Tanúsítvány hozzáférés díja	105
9.1.3.	Visszavonási állapot információ hozzáférés díja	105
9.1.4.	Egyéb szolgáltatások díjai	105
9.1.5.	Visszatérítési politika	105
9.2.	Anyagi felelősségvállalás	105
9.2.1.	Pénzügyi követelmények	105
9.2.2.	További követelmények	105
9.2.3.	Felelősségbiztosítás	106
9.3.	Bizalmasság	106
9.3.1.	Bizalmas információk köre	106
9.3.2.	Bizalmas információk körén kívül eső adatok	106
9.3.3.	Bizalmas információ védelme	107
9.4.	Személyes adatok védelme	107
9.4.1.	Adatkezelési terv	107
9.4.2.	Személyes adatok	107
9.4.3.	Személyes adatnak nem minősülő adatok	107
9.4.4.	Személyes adatok védelme	108
9.4.5.	Személyes adatok felhasználása	108
9.4.6.	Adatkezelés	108
9.4.7.	Egyéb adatvédelmi követelmények	108
9.5.	Szellemi tulajdonjogok	108
9.6.	Tevékenységért viselt felelősség és helytállás	109

9.6.1.	A szolgáltató felelőssége és helytállása	109
9.6.2.	A regisztráló szervezet felelőssége és helytállása	110
9.6.3.	Az Ügyfél felelőssége és helytállása	111
9.6.4.	Az Érintett fél felelőssége	113
9.6.5.	Egyéb szereplők tevékenységéért viselt felelősség és helytállás	113
9.7.	Helytállás érvénytelenségi köre	114
9.8.	A felelősség korlátozása	114
9.9.	Kártérítési kötelezettség	114
9.9.1.	A szolgáltató kártérítési kötelezettsége	114
9.9.2.	Az előfizető kártérítési kötelezettsége	114
9.9.3.	Az érintett felek kártérítési kötelezettsége	114
9.10.	Érvényesség és megszűnés	114
9.10.1.	Érvényesség	114
9.10.2.	Megszűnés	114
9.10.3.	A megszűnés következményei	115
9.11.	A felek közötti kommunikáció	115
9.12.	Módosítások	115
9.12.1.	Módosítási eljárás	115
9.12.2.	Értesítések módja és határideje	115
9.12.3.	Az OID megváltoztatása	115
9.13.	Vitás kérdések rendezése	115
9.14.	Irányadó jog	115
9.15.	Az érvényben lévő jogszabályoknak való megfelelés	116
9.16.	Vegyes rendelkezések	116
9.16.1.	Teljességi záradék	116
9.16.2.	Átruházás	116
9.16.3.	Részleges érvénytelenség	116
9.16.4.	Igényérvényesítés	116
9.16.5.	Vis maior	117
9.17.	Egyéb rendelkezések	117
A.	A rövid hitelesítési rend azonosítók képzési szabályai	118
B.	Hivatkozások	119

1. Bevezetés

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

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

1.1. Áttekintés

A *Hitelesítési rend* egy "szabálygyűjtemény, amely egy *Tanúsítvány* felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára". Jelen dokumentum tartalmilag és formailag megfelel az IETF RFC 3647 [23] keretrendszer követelményeinek. Kilenc fejezetből áll, amelyek tartalmazzák a *Hitelesítés-szolgáltató* által megfogalmazott biztonsági követelményeket, folyamatokat és a szolgáltatás nyújtása során követendő gyakorlatot. Az IETF RFC 3647 által meghatározott felépítés szigorú megtartása érdekében azok a fejezetek is szerepelnek a dokumentumban, amelyeknél a *Hitelesítési rend* nem ír elő követelményt, ilyen esetben a fejezetben a "Nincs megkötés" szöveg szerepel.

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

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

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

A *Hitelesítési rend* egyike a *Hitelesítés-szolgáltató* által kiadott azon dokumentumoknak, amelyek a *Hitelesítés-szolgáltató* által nyújtott szolgáltatások feltételeit együttesen szabályozzák. További dokumentumok például az Általános szerződési feltételek, a *Szolgáltatási szabályzat*, a felhasználókkal és a partnerekkel kötött egyéb szerződések.

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

1.2. Dokumentum neve és azonosítója

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

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	eIDAS Rendelet szerinti weboldal-hitelesítő tanúsítvány hitelesítési rendek
Dokumentum verziószáma	2.16
Hatálybalépés ideje	2020-08-14

A jelen dokumentum által meghatározott *Hitelesítési rendek* felsorolását és azonosító adatait az 1.2.1 fejezet tartalmazza.

1.2.1. Hitelesítési rendek

A *Hitelesítés-szolgáltató* által kibocsátott valamennyi *Tanúsítványnak* hivatkoznia kell arra a *Hitelesítési rendre*, amely alapján a kibocsátás történt.

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

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

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

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

Jelen dokumentum az alábbi *Hitelesítési rend(ek)*et definiálja:

OID	MEGNEVEZÉS	RÖVID NÉV
-----	------------	-----------

1.3.6.1.4.1.21528.2.1.1.159.2.16	III. hitelesítési osztályba tartozó, weboldal-hitelesítő tanúsítványokhoz használt, álnevet kizáró hitelesítési rend.	HWJSN
1.3.6.1.4.1.21528.2.1.1.161.2.16	II. hitelesítési osztályba tartozó, weboldal-hitelesítő tanúsítványokhoz használt, álnevet kizáró hitelesítési rend.	KWJSN, KWTSN
1.3.6.1.4.1.21528.2.1.1.162.2.16	Automatikus kibocsátás során kibocsátott, weboldal-hitelesítő tanúsítványok kibocsátását szabályozó, álnevet kizáró hitelesítési rend.	AWxSN

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

Ezen *Hitelesítési rendek* alapján a *Hitelesítés-szolgáltató* webszerverek azonosítására használható *Tanúsítványokat* bocsáthat ki.

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

A *Weboldal-hitelesítő tanúsítványok* esetében az *Alany* nevének a doménnév vagy IP cím szerepel.

A *Weboldal-hitelesítő tanúsítvány* nem lehet álneves.

Jelen *Hitelesítési rendek* közül:

- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [12] szabványban definiált [LCP] *Hitelesítési rend*nek;
- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [12] szabványban definiált [DVCP] *Hitelesítési rend*nek;
- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [12] szabványban definiált [OVCP] *Hitelesítési rend*nek, amennyiben a *Tanúsítványban* feltüntetésre kerül a szervezet neve;
- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [12] szabványban definiált [IVCP] *Hitelesítési rend*nek, amennyiben a *Tanúsítványban* feltüntetésre kerül a természetes személy neve.

Megfelelés az ETSI hitelesítési rendeknek

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

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

1.2.2. Hatály

Jelen *Hitelesítési rend* gyűjtemény 2020-08-14 -i hatálybalépési dátumtól visszavonásáig hatályos. A hatályosság automatikusan megszűnik a *Hitelesítési rend* újabb verziójának hatályba lépésekor.

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

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

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

1.2.3. Biztonsági szintek

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

A *Tanúsítvány Alany* autentikáció erőssége alapján csökkenő sorrendben:

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

A használt hordozó alapján a biztonság szerint csökkenő sorrendben:

- *HSM* eszközön kibocsátott *Tanúsítványok* [***B*];
- *Hardver kriptográfiai eszközön* kibocsátott *Tanúsítványok* [***H*];
- egyéb módon, pl. szoftveresen kibocsátott *Tanúsítványok* [***S*].

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

- minősített, *HSM* eszközön kibocsátott *Tanúsítványok* [M**B*];
- minősített, *Hardver kriptográfiai eszközön* kibocsátott *Tanúsítványok* [M**H*];
- minősített, egyéb módon, pl. szoftveresen kibocsátott *Tanúsítványok* [M**S*];
- nem minősített, e-Szignó Hitelesítés Szolgáltató által kiadott III. hitelesítési osztályba tartozó *Tanúsítványok* [H**S*];

- nem minősített, e-Szignó Hitelesítés Szolgáltató által kiadott II. hitelesítési osztályba tartozó *Tanúsítványok* [K**S*];
- nem minősített, nem e-Szignó Hitelesítés Szolgáltató által kiadott *Tanúsítványok*.

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

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

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

1.3. PKI szereplők

1.3.1. Hitelesítés-szolgáltató

A hitelesítés-szolgáltató olyan *Bizalmi szolgáltató*, amely *Bizalmi szolgáltatás* keretében *Tanúsítványokat* bocsát ki, és ellátja az ehhez kapcsolódó feladatokat. Például azonosítja az igénylő személyét, nyilvántartásokat vezet, fogadja a *Tanúsítványokkal* kapcsolatos változások adatait, valamint nyilvánosságra hozza a *Tanúsítványhoz* tartozó szabályzatokat, nyilvános kulcsokat és a *Tanúsítvány* aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat. (Ezt a tevékenységet hitelesítés-szolgáltatásnak is nevezzük.)

Jelen dokumentum előírásai vonatkoznak mindazon *Hitelesítés-szolgáltatókra*, akik a *Szolgáltatási szabályzatukban* vállalják a jelen dokumentumban szereplő *Hitelesítési rend(ek)* valamelyikének való megfelelést.

1.3.2. Regisztráló szervezetek

Meghatározását lásd az 1.6 fejezetben.

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

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

A *Hitelesítés-szolgáltató* nem veheti igénybe tőle független *Regisztráló szervezet* szolgáltatásait a 3.2.2 fejezet szerinti teljes doménnév és IP cím validálásra, azt csak saját *Regisztráló szervezete* végezheti el.

1.3.3. Ügyfelek

Az *Előfizető* határozza meg a szolgáltatást igénybe vevő *Igénylők* körét és megfizeti az ezen szolgáltatások igénybevételével kapcsolatos szolgáltatási díjakat.

Az *Igénylő* az a természetes személy, aki az adott *Weboldal-hitelesítő tanúsítvány* igénylése során eljár.

1.3.4. Érintett felek

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

1.3.5. Egyéb szereplők

A megfelelőség értékelést végző független auditor.

A szolgáltatás felügyeletét ellátó hatóság.

A *Képviselet szervezet*, amelynek neve feltüntetésre kerül egy webszerver számára kibocsátott *Tanúsítványban*.

1.4. A tanúsítvány felhasználhatósága

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

1.4.1. Megfelelő tanúsítvány használat

A *Hitelesítés-szolgáltató* által jelen *Hitelesítési rendek* valamelyike alapján kibocsátott végfelhasználói *Tanúsítványokhoz* tartozó magánkulcsok kizárólag webszerverek azonosítására használhatók fel.

1.4.2. Tiltott tanúsítvány használat

A jelen *Hitelesítési rend* alapján kibocsátott *Tanúsítványokat*, illetve a hozzájuk tartozó magánkulcsokat weboldalak azonosításától eltérő célra felhasználni tilos.

1.5. A dokumentum adminisztrálása

1.5.1. A dokumentum adminisztrációs szervezete

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

Szervezet neve	Microsec e-Szignó Hitelesítés Szolgáltató
Szervezet címe	Magyarország, H-1033 Budapest, Angel Sanz Briz út 13.
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445

Email cím	info@e-szigno.hu
-----------	------------------

1.5.2. Kapcsolattartó személy

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

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

Tanúsítvánnyal kapcsolatos problémák sürgősségi bejelentése

A *Hitelesítés-szolgáltató* tartson fenn egy folyamatosan elérhető 24/7 belső ügyeletet a tanúsítvánnyal kapcsolatos biztonsági problémák sürgősségi bejelentésére. A *Szolgáltatási szabályzatban* adja meg a bejelentés módját.

1.5.3. A Szolgáltatási szabályzat *Hitelesítési rendnek* való megfeleléséért felelős személy/szervezet

A *Szolgáltatási szabályzatnak* a benne meghivatkozott *Hitelesítési rendnek* való megfeleléséért és az abban foglaltak szerinti szolgáltatás nyújtásáért az adott *Szolgáltatási szabályzatot* kibocsátó szolgáltató a felelős.

A *Szolgáltatási szabályzatok* 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 rendekről* valamint az ezeket alkalmazó *Hitelesítés-szolgáltatókról*.

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

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

1.5.4. A Szolgáltatási szabályzat elfogadási eljárása

A jelen *Hitelesítési rendnek* való megfelelést kinyilatkoztató *Szolgáltatási szabályzat* elfogadási eljárását a *Hitelesítés-szolgáltató*nak ismertetnie kell az adott *Szolgáltatási szabályzatban*.

1.6. Fogalmak és rövidítések

1.6.1. Fogalmak

II. hitelesítési osztály	Olyan nem minősített <i>Hitelesítési rendek</i> csoportja, amelyek az <i>Igénylő</i> távoli regisztrációja alapján is lehetővé teszik a <i>Tanúsítvány</i> kibocsátását.
III. hitelesítési osztály	Olyan nem minősített <i>Hitelesítési rendek</i> csoportja, amelyek a <i>Tanúsítvány</i> kibocsátását az <i>Igénylő</i> személyes regisztrációjához kötik.
Adatközpont	Számítógépes rendszerek és a hozzájuk kapcsolódó komponensek elhelyezésére és üzemeltetésére kialakított létesítmény. Ezek a komponensek rendszerint magukba foglalják a távközlési rendszereket és kommunikációs kapcsolatokat, redundáns áramforrást, adattárolókat, légkondicionáló, tűzvédelmi és biztonsági rendszereket.
Alany (Subject)	<i>Weboldal-hitelesítő tanúsítvány</i> esetében az <i>Alany</i> a webszerver, amelyet a doménnév vagy IP cím azonosít.
Bizalmi felügyelet	"A <i>Bizalmi szolgáltatások</i> felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [7] 91.§ 1. bekezdés)
Bizalmi szolgáltatás (Trust Service)	"Rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások: <ul style="list-style-type: none"> • elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy • <i>Weboldal-hitelesítő tanúsítványok</i> létrehozása, ellenőrzése és érvényesítése; vagy • elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése; <p>" (eIDAS [1] 3. cikk 16. pont)</p>

Bizalmi szolgáltatási rend (Trust Service Policy)	"Olyan szabálygyűjtemény, amelyben egy <i>Bizalmi szolgáltató</i> , igénybe vevő vagy más személy valamely <i>Bizalmi szolgáltatás</i> használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára. " (2015. évi CCXXII. törvény [7] 1. § 8. pont)
Bizalmi szolgáltató (Trust Service Provider)	"Egy vagy több <i>Bizalmi szolgáltatást</i> nyújtó természetes vagy jogi személy; a <i>Bizalmi szolgáltató</i> lehet minősített vagy nem minősített <i>Bizalmi szolgáltató</i> ." (eIDAS [1] 3. cikk 19. pont)
Certificate Transparency (CT) naplószolgáltató	A Certificate Transparency [31] által definiált naplószolgáltató, amely a kibocsátott <i>Tanúsítványokat</i> vagy az ahhoz tartozó <i>Előtanúsítványokat</i> tárolja.
Elektronikus dokumentum	"Elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom." (eIDAS [1] 3. cikk 35. pont)
Elektronikus időbélyegző (Electronic Time Stamp)	"Olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnék, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban. " (eIDAS [1] 3. cikk 33. pont)
Előfizető (Subscriber)	A Szolgáltatóval valamely szolgáltatás igénybevétele érdekében Szolgáltatási szerződést kötő személy vagy szervezet.
Előtanúsítvány	A Certificate Transparency [31] által definiált aláírt adatstruktúra (PreCert), amely a kibocsátandó <i>Tanúsítványban</i> megjelenítendő, <i>Alanyra</i> vonatkozó adatokat tartalmazza.
Érintett fél (Relying Party)	Az a kommunikáló fél, aki egy weboldal elérésekor azonosítja a webszervert a <i>Weboldal-hitelesítő tanúsítványa</i> alapján, továbbá azok a szoftvergyártók, akik olyan internet böngészőket vagy alkalmazásokat készítenek, amelyek működésük során <i>Weboldal-hitelesítő tanúsítványokat</i> használnak.
Felfüggesztés	A <i>Tanúsítvány</i> érvényességének ideiglenes megszüntetése a <i>Tanúsítványban</i> is feltüntetett érvényességi idő lejártá előtt. A <i>Tanúsítvány</i> felfüggesztése nem végleges, a felfüggesztett <i>Tanúsítvány</i> érvényessége visszaállítható.

Gyökér tanúsítvány (Root Certificate)	Más néven legfelső szintű tanúsítvány. Őnhitelesített <i>Tanúsítvány</i> , amelyet adott <i>Hitelesítő egység</i> saját maga számára bocsátott ki, azaz saját magánkulcsával van aláírva, így a saját – a tanúsítványban szereplő – nyilvános kulcsával ellenőrizhető.
Hardver kriptográfiai eszköz (HSM: Hardware Security Module)	Egy olyan hardver alapú biztonságos eszköz, mely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására.
Hitelesítés-szolgáltató	Olyan <i>Bizalmi szolgáltató</i> , aki/amely a hitelesítés-szolgáltatás keretében azonosítja az igénylő személyt, <i>Tanúsítványt</i> bocsát ki, nyilvántartásokat vezet, fogadja a <i>Tanúsítványokkal</i> kapcsolatos változások adatait, valamint nyilvánosságra hozza a <i>Tanúsítványhoz</i> tartozó szabályzatokat, és a <i>Tanúsítvány</i> aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.
Hitelesítő egység	A <i>Hitelesítés-szolgáltató</i> rendszerének egy egysége, amely <i>Tanúsítványok</i> digitális aláírását végzi. Egy <i>Hitelesítő egység</i> hez mindig egy elektronikus aláírás vagy bélyegző létrehozásához használt adat (magánkulcs) tartozik. Előfordulhat, hogy egy <i>Hitelesítés-szolgáltató</i> egyszerre több <i>Hitelesítő egységet</i> is működtet.
Hitelesítési rend (Certificate Policy)	"Olyan <i>Bizalmi szolgáltatási rend</i> , amely <i>Bizalmi szolgáltatás</i> keretében kibocsátott <i>Tanúsítványra</i> vonatkozik." (2015. évi CCXXII. törvény [7] 1. § 24. pont)
Igénylő	Az a természetes személy, aki az adott <i>Tanúsítvány</i> igénylése során eljár.
Képviselet szervezet	Az a <i>Szervezet</i> , amelynek a nevében a <i>Szervezeti ügyintéző</i> eljár a <i>Szervezethez</i> tartozó <i>Tanúsítványokkal</i> kapcsolatos ügyekben.
Kompromittálódás	Egy kriptográfiai kulcs abban az esetben tekintendő kompromittálódottnak, ha vélelmezhető, hogy illetéktelen személynek is hozzáférése van hozzá.
Köztes hitelesítő egység	Olyan <i>Hitelesítő egység</i> amelynek <i>Tanúsítványát</i> egy másik <i>Hitelesítő egység</i> bocsátotta ki.

Kriptográfiai kulcs (Cryptographic Key)	Olyan – kriptográfiai transzformációt vezérlő – egyedi digitális jelsorozat, amelynek ismerete szükséges titkosításhoz és dekódoláshoz, illetve digitális aláírás előállításához és ellenőrzéséhez.
Kulcsgondozás (Key Management)	A kriptográfiai kulcsok előállítása, a felhasználókhöz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, amely szoros kapcsolatban áll az alkalmazott biztonsági eljárásmóddal.
Magánkulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az <i>Igénylő</i> nek szigorúan titokban kell tartania. Webszerver azonosságának igazolása esetében a webszervernek a magánkulcsát kell használnia az azonosságát ellenőrző eljárás során. A <i>Hitelesítés-szolgáltató</i> a <i>Tanúsítványok</i> kibocsátása során a <i>Hitelesítő egység</i> magánkulcsát használja arra, hogy a <i>Tanúsítványt</i> védő elektronikus aláírást vagy bélyegzőt elhelyezze rajta.
Nemzetközi tartománynév (Internationalized Domain Name)	Olyan internetes tartománynév, aminek legalább egy címkéjét (a pontokkal elválasztott részek) az alkalmazások ASCII kódtáblán kívül eső karakterekkel mutatják – pl. "ékezet.example.com". Ezeket a tartományneveket az internetes névfeloldást végző DNS-ben a Punycode átírás segítségével ASCII karakterláncokként tárolják.
Nyilvános kulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. A nyilvánosságra hozatal jellemzően egy <i>Tanúsítvány</i> formájában történik, amely összekapcsolja a szereplő nevét az ő nyilvános kulcsával. Webszerver azonosságának igazolása esetében a webszervernek a nyilvános kulcsa szükséges ahhoz, hogy az azonosságát ellenőrizni lehessen. A <i>Tanúsítványok</i> hitelességét az őket kibocsátó <i>Hitelesítő egység</i> nyilvános kulcsa segítségével lehet ellenőrizni.
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	Aszimmetrikus kulcsú kriptográfiára épülő infrastruktúra, beleértve a kriptográfiai algoritmusokat, kulcsokat, tanúsítványokat, a rájuk vonatkozó szabványokat és jogszabályokat, a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.

Regisztrációs igény	A <i>Tanúsítványkérelem</i> és a szolgáltatói szerződés előkészítése céljából az <i>Ügyfél</i> által a Szolgáltatónak előzetesen megadott adatok és nyilatkozatok, amelyben többek között felhatalmazza a Szolgáltatót az adatok kezelésére.
Regisztráló szervezet (Registration Authority)	Szervezet, amely ellenőrzi a <i>Tanúsítvány</i> ba kerülő adatok valódiságát, az <i>Igénylő</i> személy azonosságát, ellenőrzi, hogy a <i>Tanúsítványkérelem</i> hiteles-e, és azt egy arra jogosult személy nyújtotta-e be.
Rendkívüli üzemeltetési helyzet	Olyan, a <i>Hitelesítés-szolgáltató</i> üzemmenetében zavart okozó rendkívüli helyzet, amikor a <i>Hitelesítés-szolgáltató</i> rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
SCT - Signed Certificate Timestamp	A CT naplószolgáltató által az <i>Előtanúsítvány</i> illetve a <i>Tanúsítvány</i> nyilvánosságra hozatalakor küldött aláírt válasz (az aláírt <i>Tanúsítvány</i> időbélyegzője), mely az <i>Előtanúsítvány</i> illetve a <i>Tanúsítvány</i> adott naplóba történő felvételét igazolja.
Szerver autentikációs tanúsítvány	Olyan <i>Tanúsítvány</i> amely egy adott szerver, vagy annak egy szolgáltatásának azonosítására szolgál. Az ilyen <i>Tanúsítvány</i> okban a CN mezőben egy adott doménnév vagy IP cím szerepel. Ilyenek például a CISCO VPN szerver, domén kontroller, SCEP szerver, VPN szerver számára kiadott <i>Tanúsítvány</i> ok.
Szervezet	Jogi személy.
Szervezeti tanúsítvány	Olyan <i>Tanúsítvány</i> , amelyben szerepel a <i>Szervezet</i> megnevezése. Ilyen esetben a <i>Tanúsítvány</i> "O" mezőjében a <i>Szervezet</i> neve feltüntetésre kerül.
Szervezeti ügyintéző	Az <i>Előfizető</i> képviselőjében eljáró természetes személy, aki jogosult az <i>Előfizető</i> nevében a <i>Tanúsítványkérelem</i> benyújtására, a <i>Tanúsítvány</i> kibocsátás jóváhagyására, az <i>Előfizető</i> höz kapcsolódó <i>Tanúsítvány</i> ok igénylése, cseréje és visszavonása során eljárni.
Szolgáltatási szabályzat (Trust Service Practice Statement)	"A <i>Bizalmi szolgáltató</i> nyilatkozata az egyes <i>Bizalmi szolgáltatások</i> nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről." (2015. évi CCXXII. törvény [7] 1. § 41. pont)

Szolgáltatási szerződés	"A <i>Bizalmi szolgáltató</i> és a <i>Bizalmi szolgáltatási ügyfél</i> között létrejött szerződés, amely a <i>Bizalmi szolgáltatás</i> nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza. " (2015. évi CCXXII. törvény [7] 1. § 42. pont)
Tanúsítvány (Certificate)	"Az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a <i>Weboldal-hitelesítő tanúsítvány</i> , valamint mindazon, a <i>Bizalmi szolgáltatás</i> keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a tanúsítványra vonatkozó érvényesítési adatot és a tanúsítvány használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen. " (2015. évi CCXXII. törvény [7] 1. § 44.)
Tanúsítványkérelem	Az <i>Igénylő</i> által, a Szolgáltató számára a <i>Tanúsítvány</i> kibocsátás érdekében benyújtott adatok és nyilatkozatok, amelyekben többek között az <i>Igénylő</i> megerősíti a <i>Tanúsítvány</i> ba kerülő adatok valódiságát.
Tanúsítványtár	Különböző <i>Tanúsítvány</i> okat tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott <i>Tanúsítvány</i> okat publikálja, de Tanúsítványtárnak nevezzük az <i>Érintett fél</i> számítógépén a használt alkalmazás számára elérhető <i>Tanúsítvány</i> okat tartalmazó rendszert is.
Ügyfél	Az <i>Előfizető</i> és a hozzá tartozó összes <i>Igénylő</i> együttes elnevezése.
Visszavonás	A <i>Tanúsítvány</i> érvényességének megszüntetése a <i>Tanúsítvány</i> ban is feltüntetett érvényességi idő lejárta előtt. A <i>Tanúsítvány</i> visszavonása végleges, visszavont <i>Tanúsítvány</i> többet nem tehető érvényessé.
Visszavonási állapot nyilvántartás	A <i>Hitelesítés-szolgáltató</i> által vezetett belső nyilvántartás a felfüggesztett, illetőleg a visszavont <i>Tanúsítvány</i> okról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját másodperc pontossággal.
Weboldal hitelesítő tanúsítvány (Certificate for Website Authentication)	"Olyan igazolás, amely lehetővé teszi a weboldal hitelesítését és a weboldalt ahhoz a természetes vagy jogi személyhez kapcsolja, akinek vagy amelynek részére a tanúsítványt kiállították. " (eIDAS [1] 3. cikk 38. pont) Egy <i>Weboldal-hitelesítő tanúsítvány</i> ban a név mezőben a webszerver doménneve vagy IP címe szerepel.

Wildcard doménnév	Olyan doménnév, amely egy csillag karakterből ("*"), az azt követő pont karakterből ("."), majd az azt követő teljes doménnévből (FQDN) áll.
Wildcard tanúsítvány	Olyan <i>Weboldal-hitelesítő tanúsítvány</i> , amely <i>Weboldal-hitelesítő tanúsítvány</i> ban feltüntetett bármely doménnév legelső pozícióján egy csillag ("*") karaktert tartalmaz.

1.6.2. Rövidítések

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

2. Közzététel és adattár felelőségek

2.1. Adattárak

A *Hitelesítés-szolgáltató* hozza nyilvánosságra szerződéses feltételeit és szabályzatait a honlapján elektronikus formában.

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

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

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

A *Hitelesítés-szolgáltató* a szerződéskötést követően tartós adathordozón bocsássa az *Ügyfél* rendelkezésére a *Hitelesítési rendet*, a *Szolgáltatási szabályzatot* és a *Szolgáltatási szerződést*.

A *Hitelesítés-szolgáltató* értesítse *Ügyfeleit* az Általános Szerződési Feltételek változásáról.

2.2. A tanúsítványokra vonatkozó információk közzététele

A *Hitelesítés-szolgáltató* tegye közzé a honlapján a

- szolgáltatói *Tanúsítványait*;
- a végfelhasználói *Tanúsítványokat*, amennyiben a *Tanúsítványhoz* tartozó *Igénylő* ehhez hozzájárul;
- a kereszt hitelesített szolgáltatói *Tanúsítványokat*, amelyek *Alanya* a *Hitelesítés-szolgáltató*, amennyiben a *Hitelesítés-szolgáltató* kérte vagy elfogadta a bizalmi kapcsolat létesítését.

Szolgáltatói tanúsítványok

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

- A gyökér hitelesítő egységek megnevezését, illetve *Gyökér tanúsítványaik* lenyomatát a *Szolgáltatási szabályzatban* (lásd: 1.3.1. fejezet). Az állapotváltozásukkal kapcsolatos információk legyenek elérhetőek a *Hitelesítés-szolgáltató* honlapján.
- A köztes (nem gyökér) hitelesítő egységek *Tanúsítványainak* állapotváltozását hozza nyilvánosságra a *Tanúsítvány 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 *Tanúsítványt* bocsásson ki, ezzel kiküszöbölve azt, hogy a *Tanúsítvány* visszavonási állapotát ellenőrizni kelljen.

Minden OSCP válaszadói *Tanúsítvány* tartalmazzon egy jelzést ("nocheck"), miszerint a visszavonási állapotát nem kell ellenőrizni.

Végfelhasználói tanúsítványok

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

- a *Tanúsítvány visszavonási listákon*,

- az online tanúsítvány-állapot válasz szolgáltatás keretében.

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

A *Hitelesítés-szolgáltató* biztosítsa, hogy szolgáltatói *Tanúsítványait*, a *Tanúsítványtárat* és a visszavonási információkat közlétező rendszer rendelkezésre állása éves szinten legalább 99% -os legyen és egy kiesés hossza legfeljebb 24 óra legyen.

A *Hitelesítés-szolgáltató* az ismert Certificate Transparency naplószolgáltatókon keresztül tegye közzé azon *Előtanúsítványait*, amelyek közzétételéhez az *Igénylő* hozzájárult.

2.3. A közzététel időpontja vagy gyakorisága

2.3.1. Kikötések és feltételek közzétételi gyakorisága

A szolgáltatás szempontjából leglényegesebb kikötéseket és feltételeket tartalmazza az *Ügyfél* által a szerződéskötés során aláírandó szolgáltatási szerződés, vagy az abban meghivatkozott Általános Szerződési Feltételek [36] dokumentum.

A *Hitelesítés-szolgáltató* évi rendszerességgel illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja az Általános Szerződési Feltételek dokumentumot és elvégzi a szükségesnek tartott változtatásokat. A dokumentum a legkisebb változtatás után is új verziószámot kap és az elfogadási procedura időigényét figyelembe véve meghatározásra kerül a tervezett hatálybalépés időpontja is.

A *Hitelesítés-szolgáltató* a jóváhagyott dokumentumot legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre megküldi a Nemzeti Média- és Hírközlési Hatóság részére és publikálja honlapján.

A *Hitelesítés-szolgáltató* a közzétett új Általános Szerződési Feltételek tervezettel kapcsolatos észrevételeket a hatálybalépést megelőző 14. napig fogadja az alábbi címen:

info@e-szigno.hu

Érdemi változtatást igénylő észrevétel esetén a dokumentumot megváltoztatja.

Az Általános Szerződési Feltételek észrevételekkel módosított változatát a *Hitelesítés-szolgáltató* a hatálybalépést megelőző 7. napon lezárja és közzé teszi.

2.3.2. Tanúsítványok nyilvánosságra hozatalának gyakorisága

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

- az általa működtetett gyökér hitelesítő egységek *Tanúsítványait* a szolgáltatás megkezdését megelőzően tegye közzé;
- az általa működtetett köztes hitelesítő egységek *Tanúsítványait* a kibocsátást követően 5 munkanapon belül hozza nyilvánosságra;
- a *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítványra* vonatkozó *Előtanúsítványt* a *Tanúsítvány* kibocsátását megelőzően nyilvánosságra hozza a Certificate Transparency naplószolgáltatókon keresztül;

- a *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítványok*at a kibocsátást követően haladéktalanul jelenítse meg a *Tanúsítványtárban* az *Igénylő* hozzájárulása esetén.

2.3.3. A megváltozott visszavonási állapot közzétételének gyakorisága

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

A *Tanúsítványok* állapotára vonatkozó információk a *Tanúsítványtárban* és a *Tanúsítvány visszavonási listák*on is jelenjenek meg. A *Tanúsítvány visszavonási listák* kibocsátási gyakoriságával kapcsolatos előírásokat a 4.10. fejezet tárgyalja.

2.4. Az adattárak elérésének szabályai

A *Hitelesítés-szolgáltató* által közzétett információk nyilvánosak, olvasás céljából bárki számára biztosítani kell a hozzáférési lehetőséget a közzététel sajátosságainak megfelelően.

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

3. Azonosítás és hitelesítés

3.1. Elnevezések

A fejezet a jelen *Hitelesítési rend*eknek megfelelően kibocsátott *Tanúsítványok*ba kerülő adatokkal kapcsolatban tartalmaz követelményeket.

A *Tanúsítvány* alapmezői között található Kibocsátó azonosító (Issuer), illetve *Alany* azonosító (Subject) mezők feleljenek meg az IETF RFC 5280 [26] illetve IETF RFC 6818 [28] ajánlások szerinti egyedi név formátum előírásainak, ezen kívül a *Hitelesítés-szolgáltató* támogassa a kiterjesztések között található Alternatív név mezők (Subject Alternative Names), (Issuer Alternative Names) kitöltését is.

3.1.1. Név típusok

Az *Alany* megnevezése

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

- commonName (CN) – OID: 2.5.4.3 – Az *Alany* neve
Ha kitöltésre kerül, a mezőben egy teljes doménnévnek vagy IP címnek kell szerepelnie, amely meg kell egyezzen a "Subject Alternative Names" mezőben feltüntetett értékek valamelyikével.
Használata opcionális.

Csak létező és az *Igénylő* által jogosan használt doménnév vagy IP cím tüntethető fel .
Weboldal-hitelesítő tanúsítvány nem lehet álneves.

- Surname – OID: 2.5.4.4 – Természetes személy vezetékneve
IVCP típusú *Weboldal-hitelesítő tanúsítvány* esetében a *Tanúsítványban* feltüntetett természetes személy vezetékneve kerüljön ebbe a mezőbe.
DVCP és OVCP *Tanúsítvány* esetében nem szabad kitölteni.
- Given Name – OID: 2.5.4.42 – Természetes személy keresztnéve
IVCP típusú *Weboldal-hitelesítő tanúsítvány* esetében a *Tanúsítványban* feltüntetett természetes személy keresztnéve kerüljön ebbe a mezőbe.
DVCP és OVCP *Tanúsítvány* esetében nem szabad kitölteni.
- Pseudonym (PSEUDO) – OID: 2.5.4.65 – Alany álneve
Kizárólag álneves tanúsítvány esetén kerülhet kitöltésre.
- Serial Number – OID: 2.5.4.5 – Az *Alany* egyedi azonosítója
A *Tanúsítványban* legalább egy kitöltött "Serial Number" mezőnek kötelezően szerepelnie kell, amely teljesíti az alábbi követelményeket, és ezáltal alkalmas arra, hogy az IETF RFC 4043 [25] ajánlás szerinti "Permanent Identifier" kiterjesztés használata esetén az *Alany* állandó azonosítójának részét képezze:
 - az azonosító értéke a *Tanúsítványban* megnevezett, a *Hitelesítés-szolgáltató* által azonosított *Alanyhoz* tartozik, és a *Hitelesítés-szolgáltató* rendszerén belül egyedi;
 - a *Hitelesítés-szolgáltató* garantálja, hogy két általa kibocsátott *Tanúsítványban* kizárólag akkor szerepel megegyező azonosító érték, ha a két *Tanúsítvány* ugyanahhoz az *Alanyhoz* tartozik.E mező az *Alany* megnevezésének része, és nem azonos a *Tanúsítvány* IETF RFC 5280 által definiált sorozatszámával.
- Organization (O) – OID: 2.5.4.10 – A *Szervezet* megnevezése
OVCP *Tanúsítvány* esetében az "O" mezőben kell, hogy szerepeljen a *Szervezet* teljes vagy rövid neve, amelyet a *Hitelesítés-szolgáltató* a 3.2.2 fejezetben leírtak szerint ellenőrzött.
DVCP és IVCP *Tanúsítvány* esetében nem szabad kitölteni.
Bizalmi szolgáltató számára kibocsátott szolgáltatói *Tanúsítvány* esetében az "O" mező kitöltése kötelező, és a szolgáltatást nyújtó szervezet valódi nevének kell szerepelnie benne.
- Organization Identifier (OrgId) – OID: 2.5.4.97 – Szervezet azonosítója
OVCP *Tanúsítvány* esetében az "O" mezőben feltüntetett *Szervezet* azonosítója kerülhet ebbe a mezőbe.
Csak olyan adat kerülhet bele, amelyet a *Hitelesítés-szolgáltató* ellenőrzött.
OVCP *Tanúsítvány* esetében a mező kitöltése opcionális.
DVCP és IVCP *Tanúsítvány* esetében a mező nem tölthető ki.

- Organizational Unit (OU) – OID: 2.5.4.11 – Szervezeti egység elnevezése
OVCP *Tanúsítvány* esetében az "O" mezőben feltüntetett szervezethez kapcsolódó szervezeti egység elnevezése, vagy védjegy vagy egyéb információ kerülhet ebbe a mezőbe.
Csak olyan adat kerülhet bele, amelyet a *Hitelesítés-szolgáltató* ellenőrzött, és amire az adott *Szervezet*nek használati joga van.
Az "OU" mező csak akkor kerülhet kitöltésre, ha az "O", "L" és "C" mezők is ki vannak töltve.
Kitöltése opcionális.
DVCP és IVCP *Tanúsítvány* – esetében nem kerülhet kitöltésre.
- CountryName (C) – OID: 2.5.4.6 – Ország azonosítója
DVCP *Tanúsítvány* esetében a doménhez vagy IP címhez kapcsolódó ország, vagy ha ez nem egyértelműen eldönthető, akkor az *Igénylő* országának ISO 3166-1 [19] szerinti kétbetűs kódja.
OVCP *Tanúsítvány* esetében az "O" mezőben szereplő *Szervezet* székhelye szerinti ország ISO 3166-1 [19] szerinti kétbetűs kódja.
IVCP *Tanúsítvány* esetében az "SN" és "GN" mezőkben megnevezett természetes személy lakcíme szerinti ország ISO 3166-1 [19] szerinti kétbetűs kódja.
Kitöltése kötelező.
Magyarország esetében a "C" mező értéke: "HU".
- Street Address (SA) – OID: 2.5.4.9 – Cím adatok
DVCP *Tanúsítvány* esetében nem tölthető ki.
OVCP *Tanúsítvány* esetében az "O" mezőben szereplő *Szervezet* székhelye szerinti cím.
IVCP *Tanúsítvány* esetében az "SN" és "GN" mezőkben megnevezett természetes személy lakcíme szerinti cím.
Amennyiben kitöltésre kerül, a *Hitelesítés-szolgáltató* által ellenőrzött adatokat kell tartalmaznia.
- Locality Name (L) – OID: 2.5.4.7 – Településnév
DVCP *Tanúsítvány* esetében nem tölthető ki.
OVCP *Tanúsítvány* esetében az "O" mezőben szereplő *Szervezet* székhelye szerinti település megnevezése.
IVCP *Tanúsítvány* esetében az "SN" és "GN" mezőkben megnevezett természetes személy lakcíme szerinti település megnevezése.
- State or Province Name – OID: 2.5.4.8 – Tagállam, tartomány elnevezése
DVCP *Tanúsítvány* esetében nem tölthető ki.
OVCP *Tanúsítvány* esetében az "O" mezőben szereplő *Szervezet* székhelye szerinti tagállam vagy tartomány neve, vagy a "C" mezőben megadott ország teljes neve.

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

Kitöltése opcionális.

- Postal Code – OID: 2.5.4.17 – Irányítószám

DVCP *Tanúsítvány* esetében nem tölthető ki.

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

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

Kitöltése opcionális.

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

Nem lehet kitöltve.

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

Nem lehet kitöltve.

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

Kiterjesztések

- Az Alany alternatív nevei - "Subject Alternative Names"

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

A "Subject Alternative Names" mezőben mindig szerepelnie kell legalább egy bejegyzésnek.

Kitöltése kötelező.

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

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

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

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

Wildcard doménnév használata engedélyezett.

3.1.2. A nevek értelmezhetősége

A "SubjectDN" mezőre a következő szabályokat kell alkalmazni:

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

3.1.3. Álnevek használata

Weboldal-hitelesítő tanúsítvány nem lehet álneves.

3.1.4. A különböző elnevezési formák értelmezési szabályai

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

3.1.5. A nevek egyedisége

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

Eljárások a nevekre vonatkozó vitás kérdések megoldására

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

3.1.6. Márkanevek elismerése, azonosítása, szerepük

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

3.2. Kezdeti regisztráció, azonosság hitelesítése

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

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

3.2.1. A magánkulcs birtoklásának igazolása

A *Tanúsítvány* kiállítása előtt a *Hitelesítés-szolgáltatónak* biztosítania kell illetve meg kell győződnie arról, hogy az *Igénylő* valóban birtokolja illetve ellenőrzése alatt tartja a *Tanúsítványba* kerülő nyilvános kulcshoz tartozó magánkulcsot.

A követelmény teljesítésének módját rögzíteni kell a *Szolgáltatási szabályzatban*.

3.2.2. Szervezet és domén azonosságának hitelesítése

3.2.2.1 Szervezet azonosságának hitelesítése

Szervezeti tanúsítványok kibocsátása előtt a *Hitelesítés-szolgáltatónak* megbízható harmadik fél vagy közhiteles nyilvántartás alapján meg kell győződnie a *Tanúsítványba* kerülő szervezeti adatok valóságáról.

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

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

A *Tanúsítványban* feltüntetendő védjegyekkel kapcsolatosan ld. a 3.1.6 fejezetet.

A *Szolgáltatási szabályzatnak* meg kell határoznia a részletes eljárásrendet.

A *Hitelesítés-szolgáltatónak* biztosítania kell, hogy a szervezeti adatok rögzítését és az adatok hitelességének ellenőrzését nem végezheti el ugyanaz a személy.

3.2.2.2 Domén birtoklásának és kontrolljának hitelesítése

A *Weboldal-hitelesítő tanúsítványok*ban szerepelnie kell legalább egy IP címnek vagy doménnévnek.

Weboldal-hitelesítő tanúsítványok kibocsátása előtt a *Hitelesítés-szolgáltatónak* meg kell győződnie a *Tanúsítványba* kerülő doménnév vagy IP cím valóságáról, valamint az *Igénylőnek* a gyakorlatban bizonyítania kell, hogy rendelkezik az adott doménnév vagy IP cím feletti irányítással. Amennyiben a *Tanúsítványban* egynél több doménnév vagy IP cím kerül feltüntetésre, a fenti ellenőrzéseket mindegyik esetében el kell végezni.

Amennyiben a *Tanúsítványban* "*" dzsóker karaktert tartalmazó doménnév kerül feltüntetésre (wildcard tanúsítvány), a *Hitelesítés-szolgáltatónak* meg kell győződnie róla, hogy az *Igénylő* a wildcard doménnév által lefedett teljes doménnévtér jogosult használója.

A *Hitelesítés-szolgáltató* nem bocsáthat ki olyan *Tanúsítványt*, amelyben a wildcard doménnév által lefedni kívánt doménnévtér egy regisztrált gTLD vagy ccTLD (pl. "*.com", "*.co.uk"), vagy ezen TLD-k alá tartozó olyan aldomén, amely alá közvetlenül lehetséges a nyilvános doménnév regisztráció.

A *Hitelesítés-szolgáltató* kizárólag az interneten használható nyilvános doménnevekre és IP címekre bocsáthat ki *Tanúsítványt*, belső használatú nevekre és lefoglalt IP címekre nem.

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

A *Hitelesítés-szolgáltató* támogassa a Nemzetközi tartománynevek használatát az IDNA2003 [22] követelményeknek megfelelően.

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

3.2.2.2.1 Az Igénylő azonosítása a domén kapcsolattartójaként (BR 3.2.2.4.1)

Ez a validálási módszer nem használatos.

3.2.2.2.2 Email küldése a domén kapcsolattartónak (BR 3.2.2.4.2)

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

A véletlenszámot a domén kapcsolattartó regisztrált email címére kell küldeni.

Minden email felhasználható több doménnév azonosítására is.

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

Minden email egyedi véletlenszámot kell tartalmazzon.

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

A véletlenszám a létrehozásától számított legfeljebb 30 napig maradhat érvényes.

3.2.2.2.3 A domén kapcsolattartó felhívása telefonon (BR 3.2.2.4.3)

Ez a validálási módszer nem használatos.

3.2.2.2.4 A domén kapcsolattartónak küldött szerkesztett email (BR 3.2.2.4.4)

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

- email küldése az alábbiak szerint létrehozott legalább egy email címre:
 - "admin",

- "administrator",
- "webmaster",
- "hostmaster" vagy
- "postmaster"

helyi cím, amit a kukac ("@") karakter után egy ellenőrzendő doménnév követ,

- amely email tartalmaz egy egyedi véletlenszámot, és
- a küldött véletlenszámot tartalmazó megerősítő válasz fogadása.

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

A véletlenszámnak minden emailben egyedinek kell lennie.

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

A véletlenszám a létrehozásától számított legfeljebb 30 napig maradhat érvényes.

3.2.2.2.5 Domén felhatalmazó dokumentum (BR 3.2.2.4.5)

Ez a validálási módszer nem használatos.

3.2.2.2.6 A weboldal egyeztetett megváltoztatása (BR 3.2.2.4.6)

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

"/.well-known/pki-validation"

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

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

A *Hitelesítés-szolgáltató* minden *Tanúsítványkérelem* esetében egyedi ellenőrző adatot kell használjon ami legfeljebb 30 napig lehet érvényes.

A validálási módszer nem használható 2020. június 1. után.

3.2.2.2.7 DNS megváltoztatása (BR 3.2.2.4.7)

Az *Igénylő* domén feletti kontrolljának ellenőrzése egy ellenőrző adat (véletlenszám vagy token) meglétének ellenőrzésével a DNS CNAME, TXT vagy CAA rekordok bármelyikén az

- azonosítandó doménnév vagy
- egy aláhúzás (underscore) karakterrel kezdődő előtag címkével kiegészített azonosítandó doménnév

valamelyikén.

Véletlenszám használata esetén a *Hitelesítés-szolgáltató* minden *Tanúsítványkérelem* esetében egyedi véletlenszámot kell használnjon.

A véletlenszám felhasználható

- 30 naptári napon belül illetve
- amennyiben az *Igénylő* nyújtotta be a *Tanúsítványkérelem* et, a *Tanúsítvány* kibocsátása szempontjából lényeges ellenőrzött adatok újra felhasználására engedélyezett időtartamon belül.

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

A módszer Wildcard doménnevek validálására is használható.

3.2.2.2.8 IP cím (BR 3.2.2.4.8)

Ez a validálási módszer nem használatos.

3.2.2.2.9 Teszt tanúsítvány (BR 3.2.2.4.9)

Ez a validálási módszer nem használatos.

3.2.2.2.10 TLS véletlenszám felhasználásával (BR 3.2.2.4.10)

Ez a validálási módszer nem használatos.

3.2.2.2.11 Egyéb módszerek (BR 3.2.2.4.11)

Ez a validálási módszer nem használatos.

3.2.2.2.12 Az igénylő azonosítása domén kapcsolattartóként (BR 3.2.2.4.12)

Ez a validálási módszer nem használatos.

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

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

A véletlenszámot a DNS CAA rekord email kontakt címére kell küldeni. A megfelelő CAA forrás adatot az IETF RFC 6844 [29] szabvány Errata 5065 (Appendix A) által módosított 4 fejezete által meghatározott kereső algoritmus szerint kell megtalálni.

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

tartozó DNS CAA kapcsolattartó. Az email teljes egészében újraküldhető beleértve a véletlenszám ismételt használatát, amennyiben az email teljes tartalma és a címzettek köre változatlan marad. A véletlenszámnak minden emailben egyedinek kell lennie. A véletlenszám a létrehozásától számított legfeljebb 30 napig maradhat érvényes.

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

A módszer Wildcard doménnevek validálására is használható.

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

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

A véletlenszámot a validálandó doménnévhez tartozó DNS TXT rekord kapcsolattartói email címére kell küldeni.

A DNS TXT rekordnak a validálandó domén "_validation-contactemail" aldoménjében kell lennie. Ezen TXT rekord teljes RDATA értékének az érvényes email címet kell tartalmaznia az RFC 6532 [27] 3.2 fejezete szerinti formátumban további kiegészítés vagy formázás nélkül, ellenkező esetben az email cím nem használható.

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

A véletlenszámnak minden emailben egyedinek kell lennie. A véletlenszám a létrehozásától számított legfeljebb 30 napig maradhat érvényes.

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

A módszer Wildcard doménnevek validálására is használható.

3.2.2.2.15 A domén kapcsolattartó felhívása telefonon (BR 3.2.2.4.15)

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

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

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

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

A módszer Wildcard doménnevek validálására is használható.

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

Az *Igénylő* domén feletti kontrolljának ellenőrzése a DNS TXT rekord kapcsolattartói telefonszám felhívásával és egy megerősítő válasz kapásával. A DNS TXT rekordnak a validálandó domén "_validation-contactphone" aldoménjében kell lennie. Ezen TXT rekord teljes RDATA értékének az érvényes globális telefonszámot tartalmaznia az RFC 3966 [24] 5.1.4 fejezete szerinti formátumban, ellenkező esetben a telefonszám nem használható.

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

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

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

A módszer Wildcard doménnevek validálására is használható.

3.2.2.2.17 A DNS CAA kapcsolattartó felhívása telefonon (BR 3.2.2.4.17)

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

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

A megfelelő CAA forrás adatot az IETF RFC 6844 [29] szabvány Errata 5065 (Appendix A) által módosított 4. fejezete által meghatározott kereső algoritmus szerint kell megtalálni.

A CAA kapcsolattartói telefonszámot a CAA contactphone tulajdonság kell tartalmazza paraméterként. A teljes paraméter értéknek az érvényes globális telefonszámot kell tartalmaznia az RFC 3966 [24] 5.1.4 fejezete szerinti formátumban, egyéb esetben nem használható. A Globális telefonszám "+" karakterrel és az országgóddal kezdődik és tartalmazhat vizuális tagoló karaktereket.

Példa:

```
$ORIGIN example.com
```

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

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

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

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

A módszer Wildcard doménnevek validálására is használható.

3.2.2.2.18 A Weboldal egyeztetett megváltoztatása v2 (BR 3.2.2.4.18)

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

- Az elvárt teljes egyedi ellenőrző adat nem jelenhet meg az információ elérésére használt kérésben.
- a *Hitelesítés-szolgáltató*nak egy sikeres HTTP választ kell kapnia a kérésre (vagyis egy 2xx HTTP válaszkódot kell kapnia).

Az egyedi ellenőrző adatot tartalmazó fájl:

- az ellenőrzött doménnév (ADN) alatt legyen elérhető,
- a `"/.well-known/pki-validation"` könyvtárban legyen található,
- `"http"` vagy `"https"` protokoll használatával legyen elérhető és
- egy engedélyezett porton keresztül legyen elérhető.

A *Hitelesítés-szolgáltató* nem fogadhat el átirányítást (3xx HTTP válaszkód).

Az azonosító adatban található véletlenszám:

- legyen egyedi minden *Tanúsítványkérelem*hez;
- a létrehozásától számított legfeljebb 30 napig fogadható el validálásra a megerősítő válaszban.

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

A módszer Wildcard doménnevek validálására is használható.

3.2.2.2.19 A weboldal egyeztetett megváltoztatása - ACME (BR 3.2.2.4.19)

Ez a validálási módszer nem használatos.

3.2.2.3 IP cím azonosítása

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

A *Hitelesítés-szolgáltató* igazolja, hogy a *Tanúsítvány* kibocsátása előtt minden, a *Tanúsítvány*ban feltüntetésre kerülő IP címet ellenőriz legalább egy, a fejezetben felsorolt módszer felhasználásával. Az *Igénylő* jogosultságát igazoló vizsgálati eredmények több *Tanúsítvány* kibocsátása során is felhasználhatók, amennyiben a vizsgálat megkezdésének időpontja a *Tanúsítvány* kibocsátását megelőzően a 4.2.1. fejezetben meghatározott időtartamnál nem korábban volt.

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

3.2.2.3.1 Weboldal egyeztetett módosítása (BR 3.2.2.5.1)

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

A véletlenszám nem szerepelhet a kiolvasásra szolgáló kérdésben.

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

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

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

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

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

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

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

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

3.2.2.3.3 Reverz IP cím keresés alapján (BR 3.2.2.5.3)

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

3.2.2.3.4 Egyéb módszer (BR 3.2.2.5.4)

Ez a validálási módszer nem használatos.

3.2.2.3.5 Az IP cím kapcsolattartó felhívása telefonon (BR 3.2.2.5.5)

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

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

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

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

Ez a validálási módszer nem használatos.

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

Ez a validálási módszer nem használatos.

3.2.3. Természetes személy azonosságának hitelesítése

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

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

1. Személyesen történő azonosítás során.

A III. hitelesítési osztályba tartozó *Tanúsítványok* esetében:

- A természetes személynek személyesen meg kell jelennie a személyes azonosítást végző személy előtt, aki az alábbiak valamelyike lehet:
 - *Regisztráló szervezet* tisztviselője,
 - közjegyző,
 - harmadik fél a magyar szabályozás szerint.
- A személyes azonosítás során a természetes személy azonosságát ellenőrizni kell egy személyazonosság igazolására alkalmas hatósági igazolványa alapján. Az azonosítás az alábbi hatósági igazolványok alapján történhet:

- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény (a továbbiakban: Nytv. [3]) hatálya alá tartozó természetes személyek esetében a Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolvány az Eüt. 82.§ (3) [7] szerint;
 - a Nytv. [3] hatálya alá nem tartozó természetes személy esetén a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról, illetve a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló törvény [4] szerinti úti okmány alapján az Eüt. 82.§ (4) [7] szerint;
 - a fenti okmányok egyikével sem rendelkező természetes személyek azonosítása során a *Hitelesítés-szolgáltató* csak európai állampolgárok azonosságának ellenőrzése esetében alkalmazza az Eüt. 82.§ (5) [7] bekezdése szerinti személyazonosság ellenőrzést. Ebben az esetben a természetes személy állampolgársága szerinti európai ország által kibocsátott fényképes személyi igazolványt fogadja el, mint személyazonosság igazolására szolgáló megbízható okmányt.
- A személyazonosság ellenőrzésére szolgáló adatok helyességét a természetes személynek papír alapú írásos nyilatkozatban, saját kezű - az azonosítást végző személy jelenlétében létrehozott - aláírásával igazolnia kell.
 - A természetes személy lakcímét ellenőrizni kell egy lakcím azonosítására alkalmas igazolvány alapján.
 - A személyes azonosítást végző személynek ellenőriznie kell, hogy a bemutatott igazolványokon történt-e módosítás vagy hamisítás.

A II. hitelesítési osztályba tartozó *Tanúsítványok* esetében:

- a természetes személy azonosításához személyes találkozásra nincs szükség, ilyen esetben a *Hitelesítés-szolgáltató* távolról is azonosíthatja az *Igénylőt*;
- az *Igénylő* eljuttatja a *Hitelesítés-szolgáltató*nak valamely személyazonosság igazolására alkalmas hatósági igazolványának másolatát.
- az *Igénylő* eljuttatja a *Hitelesítés-szolgáltató*nak a lakcímének igazolására alkalmas hatósági igazolványának másolatát.
- A személyazonosság ellenőrzésére szolgáló adatok helyességét a természetes személynek nyilatkozatban, saját kezű aláírással ellátva igazolnia kell.
- A személyazonosító adatok helyességét a *Regisztráló szervezet*nek megbízható harmadik fél vagy közhiteles nyilvántartás segítségével ellenőriznie kell.
- A *Regisztráló szervezet*nek ellenőriznie kell a bemutatott igazolványok hitelességét. A *Hitelesítés-szolgáltató*nak megbízható kommunikációs csatornán keresztül ellenőriznie kell, hogy a *Tanúsítványkérelmet* valóban az azonosított *Igénylő* küldte.

2. Elektronikus aláírás tanúsítványára visszavezetett azonosítással.

Ebben az esetben:

- Az *Igénylő* a *Tanúsítványkérelmet* elektronikus formában nyújtja be egy nem álneves – az igényelt *Tanúsítvány*énál nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) – *Tanúsítvány*án alapuló elektronikus aláírással ellátva.

- Az elektronikus aláírással ellátott *Tanúsítványkérelem*nek tartalmaznia kell a természetes személy egyértelmű azonosításához szükséges azonosító adatokat.
- A *Tanúsítványkérelem* hitelességét és sértetlenségét ellenőrizni kell a teljes tanúsítási lánc vizsgálatával.
- A *Hitelesítés-szolgáltató* csak olyan *Tanúsítványon* alapuló elektronikus aláírást fogad be, amelyet egy az Európai Unió fő bizalmi listán publikált nemzeti bizalmi listán szereplő bizalmi szolgáltatás keretében bocsátottak ki, és az aláírás létrehozás időpontjában érvényes volt.

A Szolgáltatási szerződés érvényességének időtartama alatt a *Hitelesítés-szolgáltató* lehetőséget biztosíthat az *Igénylő* számára újabb *Tanúsítványkérelem* esetén a személyes azonosításkor egyeztetett adatok alapján az új *Tanúsítvány* kibocsátására. A kérelem hitelességét, a *Tanúsítvány*ba kerülő adatok pontosságát és a kérelmet benyújtó személy azonosságát is ellenőrizni kell. A *Szolgáltatási szabályzat*ban pontosan meg kell határozni az ellenőrzés folyamatát.

A *Hitelesítés-szolgáltató*nak biztosítania kell, hogy a személyes adatok rögzítését és az adatok hitelességének ellenőrzését nem végezheti el ugyanaz a személy.

3.2.4. Nem ellenőrzött alany információk

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

3.2.5. Jogok, felhatalmazások ellenőrzése

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

Ellenőrizni kell a természetes személy képviseleti jogosultságát.

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

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.

3.2.6. Együttműködési képességre vonatkozó követelmények

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

A *Hitelesítés-szolgáltató*nak meg kell győződnie arról, hogy a másik *Hitelesítés-szolgáltató* az együttműködés szerinti, nyilvános körben nyújtott szolgáltatás végzésére – jogszabályi kijelölés, vagy hatósági nyilvántartás alapján – jogosult.

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

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

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

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 *Tanúsítványt*, hogy a nyilvános kulcs lecserélésre kerül. Kulcscsere csak a Szolgáltatási szerződés időtartama alatt kérhető.

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

Kulcscsere kérelmeket a *Hitelesítés-szolgáltató* érvényes és nem érvényes (visszavont vagy lejárt) *Tanúsítványokhoz* is elfogadhat.

A kulcscserével kapcsolatos eljárás részletei a 4.7. fejezetben olvashatóak.

3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

Az *Igénylő* azonosítása a 3.2.3. fejezetben leírtak szerint kell történjen.

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

3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

A *Hitelesítés-szolgáltató* kizárólag a szolgáltatás nyújtásának időtartama alatt elfogadhat kulcscsere kérelmeket. Az *Igénylő* azonosítása a 3.2.3. fejezetben leírtak szerint kell történjen.

3.4. Azonosítás és hitelesítés tanúsítvány megújítás esetén

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

3.4.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

Az *Igénylő* azonosítása a 3.2.3. fejezetben leírtak szerint kell történjen.

3.4.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen *Tanúsítvány* nem újítható meg.

3.5. Azonosítás és hitelesítés tanúsítvány módosítás esetén

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

3.5.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

Az *Igénylő* azonosítása a 3.2.3. fejezetben leírtak szerint kell történjen.

Amennyiben a módosított *Tanúsítvány* érvényesség vége ideje egegyezik az eredeti *Tanúsítvány* érvényesség vége idejével, az eljárás során a *Hitelesítés-szolgáltató* felhasználhatja az eredeti *Tanúsítvány* kiadása előtt elvégzett ellenőrzések eredményeit.

3.5.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen *Tanúsítvány* nem módosítható.

3.6. Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási kérelem esetén

A *Hitelesítés-szolgáltató*nak fogadnia kell és fel kell dolgoznia a *Tanúsítványok* visszavonására vonatkozó kérelmeket, valamint a *Tanúsítványok* visszavonását érintő (pl. a magánkulcs kompromittálódásával vagy a *Tanúsítvány* nem megfelelő használatával kapcsolatos) bejelentéseket.

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

Az erre vonatkozó kérelmek benyújtásának és feldolgozásának körülményeit a *Szolgáltatási szabályzatban* rögzíteni kell.

Weboldal-hitelesítő tanúsítványok esetében felfüggesztésre nincs lehetőség.

3.7. Ellenőrzött kommunikációs csatorna

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

4. A tanúsítványok életciklusára vonatkozó követelmények

4.1. Tanúsítványkérelem

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

A *Hitelesítés-szolgáltató* mindaddig nem tekintheti a *Regisztrációs igényben* szereplő adatokat hitelesnek, amíg az *Igénylő* a *Tanúsítványkérelemben* meg nem erősíti azokat. Amennyiben új *Szolgáltatási szerződés* megkötésére van szükség, a *Hitelesítés-szolgáltató*

a *Regisztrációs igényben* megadott adatok alapján előkészítheti az *Előfizetővel* kötendő Szolgáltatási szerződést.

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

Amennyiben az *Igénylő* nem azonos az *Előfizetővel*, akkor az *Igénylő* számára is meg kell adni a fenti tájékoztatást.

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

A *Tanúsítványkérelem*nek tartalmaznia kell legalább a következő adatokat:

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

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

- az *Igénylő* azonosításához szükséges okmányokat a 3.2.3 fejezetnek megfelelően;
- *Szervezeti tanúsítvány* igénylése esetén a *Szervezet* azonosításához szükséges okmányokat a 3.2.2 fejezetnek megfelelően;
- *Szervezeti tanúsítvány* igénylése esetén a *Szervezet* által kiadott igazolást vagy meghatalmazást arról, hogy az igénylő személy jogosult a *Szervezet* képviselőre ;
- amennyiben a kért *Tanúsítvány*ban szerepel márkanév vagy védjegy, akkor annak igazolását, hogy az *Igénylő* jogosult annak használatára.

4.1.1. Ki nyújthat be tanúsítványkérelmet

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

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

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

- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában vagy a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál, előzetesen egyeztetett időpontban (ekkor a III. hitelesítési osztályba tartozó *Tanúsítványok* esetén a személyes azonosítás megtörténik a találkozás során);

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

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

4.1.2. A bejegyzés folyamata és a résztvevők felelőssége

A kérelem feldolgozása során a *Hitelesítés-szolgáltató* regisztrációs munkatársának meg kell győződnie a *Tanúsítványkérelmet* benyújtó személyazonosságáról (lásd: 3.2.3 fejezet).

A *Hitelesítés-szolgáltató*nak ellenőriznie kell egy másik – megbízható – csatornán, hogy a *Tanúsítványkérelem* valóban attól a személytől származik, akinek az adatai (igazolványai) a *Tanúsítványkérelemben* szerepelnek.

Szervezeti tanúsítvány igénylése esetén a *Szervezetet* is azonosítani kell, illetve meg kell győződni arról, hogy a megjelent személy jogosult a *Szervezet* képviselőjére illetve a *Szervezethez* kapcsolódó *Tanúsítvány* igénylésére (lásd: 3.2.2. fejezet).

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

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

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

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

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

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

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

Amennyiben az *Igénylő* személyazonossága vagy a *Képviselet szervezet*hez való tartozása nem állapítható meg minden kétséget kizáróan, vagy valamely, a tanúsítványkérelem űrlapon feltüntetett adat nem helyes, akkor az igénylési eljárás félbeszakad. Ekkor az *Ügyfél*nek lehetősége van a hiányos vagy hibás adatokat korigálni, illetve a hiányzó igazolásokat átadni.

4.2. A tanúsítványkérelem feldolgozása

4.2.1. Az igénylő azonosítása és hitelesítése

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

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

A *Hitelesítés-szolgáltató* fejlesszen ki, tartson karban és üzemeltessen dokumentált eljárásokat a magas kockázatú *Tanúsítványkérelmek* észlelésére és kiemelt kezelésére további ellenőrzések végrehajtásával a *Tanúsítványkérelem* engedélyezése előtt, hogy biztosítsa az ilyen kérelmek megfelelő feldolgozását.

4.2.2. A tanúsítványkérelem elfogadása vagy visszautasítása

A *Hitelesítés-szolgáltató* az összeférhetetlenség elkerülése érdekében biztosítania kell személyi és szervezeti függetlenségét az *Előfizető*kkal szemben. Nem minősül az összeférhetetlenség megsértésének, amikor a *Hitelesítés-szolgáltató* munkatársai számára bocsát ki *Tanúsítványt*.

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

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

A *Hitelesítés-szolgáltató* alakítson ki olyan folyamatokat, amelyek során azonosítja a megtévesztésre alkalmas névhasználat miatt magas kockázatot jelentő *Weboldal-hitelesítő tanúsítvány* kérelmeket, amelyeket szigorúbban kell ellenőrizni. A gyanús kérelmek azonosításának folyamatát és a szigorúbb ellenőrzés folyamatát dokumentálni kell a *Szolgáltatási szabályzat*ában.

4.2.3. A tanúsítványkérelem feldolgozásának időtartama

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

4.3. A tanúsítvány kibocsátása

A *Hitelesítés-szolgáltató* csak a *Tanúsítványkérelem* elfogadása után állíthatja ki a *Tanúsítványt* az *Alany* részére.

4.3.1. A Hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során

A *Tanúsítványok* kibocsátásának megfelelően biztonságos módon kell történnie.

A *Hitelesítés-szolgáltató*nak biztosítania kell, hogy a *Tanúsítvány* kibocsátás teljes folyamatát nem végezheti el egyetlen személy.

4.3.2. Az Ügyfél értesítése a tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* a *Tanúsítvány* kibocsátásáról értesítse az *Igénylőt* és az *Előfizetőt*, valamint tegye lehetővé az *Igénylő* számára a *Tanúsítvány* átvételét.

4.4. A tanúsítvány elfogadása

4.4.1. A tanúsítvány elfogadás módja

A III. hitelesítési osztályba tartozó *Tanúsítványok* esetén az *Igénylőnek* a *Tanúsítvány* átvétele előtt ellenőriznie kell a *Tanúsítványban* szereplő adatok helyességét és erről írásbeli nyilatkozatot kell tennie. A nyilatkozat aláírásával az *Igénylő* igazolja a *Tanúsítvány* átvételét.

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

4.4.2. A tanúsítvány közzététele

A *Tanúsítvány* átadása után a *Hitelesítés-szolgáltató* köteles nyilvánosságra hozni a kiadott *Tanúsítványt*.

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

4.4.3. További szereplők értesítése a tanúsítvány kibocsátásáról

Szervezeti tanúsítvány esetén a *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell a *Képviselet* szervezet *Szervezeti ügyintézőjét* is.

4.5. A kulcspár és a tanúsítvány használata

4.5.1. A magánkulcs és a tanúsítvány használata

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

Lejárt érvényességű vagy visszavont *Tanúsítványhoz* tartozó magánkulcs nem használható.

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

A használat során be kell tartani az 1.4. fejezetben leírt korlátozásokat.

4.5.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata

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

- ellenőrizze a *Tanúsítvány* érvényességét és visszavonási állapotát;
- a *Weboldal-hitelesítő tanúsítványokhoz* kapcsolódó nyilvános kulcsokat csak webservertől való azonosságának igazolására használja;
- vegyen figyelembe minden korlátozást, amely a *Tanúsítványban* vagy a *Tanúsítványban* meghivatkozott szabályzatokban szerepel.

A *Hitelesítés-szolgáltató* tegyen elérhetővé olyan szolgáltatást az *Ügyfelei* és az *Érintett felek* számára, amely segítségével ellenőrizhetik az általa kibocsátott *Tanúsítványok*at.

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 *Tanúsítványt* állít ki új érvényességi időszakra.

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

4.6.1. A tanúsítvány megújítás körülményei

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

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

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

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

4.6.2. Ki kérelmezheti a tanúsítvány megújítást

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

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

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

4.6.3. A tanúsítvány megújítási kérelmek feldolgozása

A tanúsítvány megújítási kérelem elbírálása során a *Hitelesítés-szolgáltató*nak ellenőriznie kell, hogy:

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

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

4.6.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

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

4.6.5. A megújított tanúsítvány elfogadása

A *Hitelesítés-szolgáltató* a megújított *Tanúsítványt* személyes találkozás nélkül is átadhatja, letölthetővé teheti.

4.6.6. A megújított tanúsítvány közzététele

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

4.6.7. További szereplők értesítése a tanúsítvány kibocsátásáról

Szervezeti tanúsítvány esetén a *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell a *Képviselet szervezet Szervezeti ügyintézőjét* is.

4.7. Kulcscsere

A kulcscsere alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* egy adott *Alany* részére úgy bocsát ki új *Tanúsítványt*, 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.

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 fogadhat el.

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

4.7.2. Ki kérelmezheti a kulcscserét

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

4.7.3. A kulcscsere kérelmek feldolgozása

A benyújtott kulcscsere kérelem elbírálása során a *Hitelesítés-szolgáltatónak* ellenőriznie kell, 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* értesítse az *Igénylőt* és az *Előfizetőt* az új *Tanúsítvány* kibocsátásáról.

4.7.5. A kulcscserével megújított tanúsítvány elfogadása

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

4.7.6. A kulcscserével megújított tanúsítvány közzététele

A *Hitelesítés-szolgáltatónak* az eredeti *Tanúsítvány* kibocsátásával megegyező módon kell publikálnia a megújított *Tanúsítványt*.

4.7.7. További szereplők értesítése a tanúsítvány kibocsátásáról

Szervezeti tanúsítvány esetén a *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell a *Képviselet szervezet Szervezeti ügyintézőjét* is.

4.8. Tanúsítvány módosítás

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

4.8.1. A tanúsítvány módosítás körülményei

A tanúsítvány módosítás szükségessé válik az alábbi esetekben:

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

A tanúsítvány módosítás feltételei:

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

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

Az új *Tanúsítvány* kibocsátása során tájékoztatni kell az *Igénylőt* arról, ha a korábbi *Tanúsítvány* kibocsátása óta változtak a *Tanúsítvány* használatával kapcsolatos kikötések illetve feltételek.

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

4.8.2. Ki kérelmezheti a tanúsítvány módosítást

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

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

4.8.3. A tanúsítvány módosítási kérelmek feldolgozása

A benyújtott *Tanúsítvány* módosítási kérelem elbírálása során a *Hitelesítés-szolgáltató*nak ellenőriznie kell, hogy:

- a benyújtott kérelem hiteles;

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

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

4.8.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

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

4.8.5. A módosított tanúsítvány elfogadása

A *Hitelesítés-szolgáltató* a módosított *Tanúsítványt* személyes találkozás nélkül is átadhatja, letölthetővé teheti.

4.8.6. A módosított tanúsítvány közzététele

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

4.8.7. További szereplők értesítése a tanúsítvány kibocsátásáról

Szervezeti tanúsítvány esetén a *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell a *Képviselet szervezet Szervezeti ügyintézőjét* is.

4.9. Tanúsítvány visszavonás és felfüggesztés

A tanúsítvány visszavonás alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* a *Tanúsítvány* érvényességét megszünteti az eredetileg tervezett érvényességi idő lejárta előtt. A tanúsítvány visszavonás visszafordíthatatlan és végleges állapotváltozást jelent, a visszavont *Tanúsítvány* már soha többé nem lehet újra érvényes.

Weboldal-hitelesítő tanúsítvány nem függeszthető fel.

4.9.1. A tanúsítvány visszavonás körülményei

Végfelhasználói tanúsítvány visszavonásának okai

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

- az *Igénylő* vagy az *Előfizető* írásban kéri a *Tanúsítvány* visszavonását;

- az *Igénylő* vagy az *Előfizető* értesíti a *Hitelesítés-szolgáltatót* arról, hogy az eredeti *Tanúsítványkérelmet* nem hagyta jóvá, és utólag sem ad erre jóváhagyást;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódott;
- a *Hitelesítés-szolgáltató* bizonyítékot szerez arról, hogy a *Tanúsítványban* szereplő valamely teljes minőségű domain név vagy IP cím feletti kontrol vagy engedély ellenőrzésére nem támaszkodhat;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* 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 *Tanúsítványt* jogellenesen használták;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy az *Előfizető* megszegte a *Szolgáltatási szerződés* vagy az *Általános Szerződési Feltételek* szerinti egy vagy több kötelezettségét;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* szereplő doménnév (FQDN) vagy IP cím használati jogosultsága megszűnt (pl.: a bíróság megtiltotta a domén használatát vagy a tulajdonos nem hosszabbította meg a domén regisztrációját);
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a wildcard tanúsítványt megtévesztő doménnév hitelesítésére használták;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* szereplő adatokban lényeges változás történt;
- a *Tanúsítvány* módosítása az *Alanya*ra vonatkozó adatok változása miatt;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* nem a CABF Baseline Requirements, a vonatkozó *Hitelesítési rend* illetve *Szolgáltatási szabályzat* szerint bocsátották ki;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* foglalt bármely adat pontatlan;
- a *Hitelesítés-szolgáltató* már nem jogosult *Tanúsítványokat* kibocsátani és a meglévő *Tanúsítványokra* vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodik;
- a visszavonást előírja a *Hitelesítés-szolgáltató Hitelesítési rendje* vagy *Szolgáltatási szabályzata*;
- a *Hitelesítés-szolgáltató* értesül egy bemutatott vagy bizonyított eljárásról, amellyel az *Előfizető* magánkulcsa meghatározható, olyan módszereket fejlesztettek ki, amelyekkel az könnyen kiszámítható a nyilvános kulcs alapján (pl. a Debian gyenge kulcsok, lásd <http://wiki.debian.org/SSLkeys>), vagy ha egyértelmű bizonyíték van arra, hogy a magánkulcs létrehozásához használt eljárás hibás volt.
- a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);

- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* kibocsátó hitelesítő egység magánkulcsa kompromittálódhatott;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy az *Előfizető* nem teljesítette valamely anyagi kötelezettségét a vonatkozó Szolgáltatási szerződésnek megfelelően;
- a *Hitelesítés-szolgáltató* tevékenységét befejezte;
- a bizalmi felügyelet ezt jogerős és végrehajtható határozatában elrendeli;
- a visszavonást jogszabály kötelezővé teszi.

A *Szolgáltatási szabályzat* előírhat a fentiekén kívül egyéb feltételeket is, amelyek esetén a *Hitelesítés-szolgáltató* a *Tanúsítványt* visszavonja.

Szolgáltatói Tanúsítvány visszavonásának okai

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

- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató írásban kéri a *Tanúsítvány* visszavonását;
- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató értesíti a kibocsátó *Hitelesítés-szolgáltatót* arról, hogy az eredeti *Tanúsítvány* kérelmet nem hagyta jóvá, és utólag sem ad erre jóváhagyást;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem a kizárólagos birtokában van;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* 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 *Tanúsítványt* jogellenesen használták;
- amennyiben a *Tanúsítványt* nem a vonatkozó *Hitelesítési rend* illetve *Szolgáltatási szabályzat* szerint bocsátották ki vagy a köztes hitelesítő egység működése nem felel meg a rá vonatkozó *Hitelesítési rendnek* vagy *Szolgáltatási szabályzatnak*;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* szereplő valamely információ téves vagy félrevezető;
- a kibocsátó CA vagy a köztes CA bármilyen okból megszünteti a tevékenységét, és nem állapodott meg más *Hitelesítés-szolgáltató-val* a *Tanúsítvány* visszavonási szolgáltatás nyújtásáról ;
- amennyiben a *Hitelesítés-szolgáltató* már nem lenne jogosult *Tanúsítványok*at kibocsátani és a meglevő *Tanúsítványokra* vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;
- a visszavonást előírja a kibocsátó CA *Hitelesítési rendje* vagy *Szolgáltatási szabályzata*;

- a *Tanúsítvány* módosítása a hitelesítési egységre, vagy a *Hitelesítés-szolgáltatóra* vonatkozó adatok változása miatt;
- amennyiben a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);
- a *Hitelesítés-szolgáltató* a tevékenységét befejezte;
- a visszavonást jogszabály kötelezővé teszi.

A Szolgáltatási szabályzat előírhat a fentiekén kívül egyéb feltételeket is, amelyek esetén a *Hitelesítés-szolgáltató* a *Tanúsítványt* visszavonja.

Más Szolgáltató által üzemeltetett köztes CA Tanúsítvány visszavonásának okai

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

- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató írásban kéri a *Tanúsítvány* visszavonását;
- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató értesíti a kibocsátó *Hitelesítés-szolgáltatót* arról, hogy az eredeti *Tanúsítvány* kérelmet nem hagyta jóvá, és utólag sem ad erre jóváhagyást;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató kizárólagos birtokában van;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* szereplő nyilvános kulcs már nem felel meg a 6.1.5 és 6.1.6 fejezetekben meghatározott követelményeknek;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* jogellenesen használták;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* 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 szabályzatnak*;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* szereplő valamely adat téves vagy félrevezető;
- a kibocsátó CA vagy a köztes CA bármilyen okból megszünteti a tevékenységét, és nem állapodott meg más *Hitelesítés-szolgáltató-val* a *Tanúsítvány* visszavonási szolgáltatás nyújtásáról ;
- amennyiben a *Hitelesítés-szolgáltató* már nem lenne jogosult *Tanúsítványokat* kibocsátani és a meglévő *Tanúsítványokra* vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;

- a visszavonást előírja a kibocsátó CA *Hitelesítési rendje* vagy *Szolgáltatási szabályzata*;
- a *Tanúsítvány* módosítása a hitelesítési egységre, vagy az azt üzemeltető hitelesítés-szolgáltatóra vonatkozó adatok változása miatt;
- amennyiben a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);
- a hitelesítési egységet működtető hitelesítés-szolgáltató, vagy a *Tanúsítványát* kibocsátó *Hitelesítés-szolgáltató* a tevékenységét befejezte;
- a visszavonást jogszabály kötelezővé teszi.

A *Szolgáltatási szabályzat* előírhat a fentiekén kívül egyéb feltételeket is, amelyek esetén a *Hitelesítés-szolgáltató* a *Tanúsítványt* visszavonja.

4.9.2. Ki kérelmezheti a visszavonást

A *Tanúsítvány* visszavonását kezdeményezhetik az *Ügyfelek*, részletezve:

- az *Előfizető*;
- az *Igénylő*
- *Szervezeti tanúsítvány* esetén a *Szervezet* nevében eljárásra jogosult természetes személy;
- az *Előfizető* által bejelentett *Szervezeti ügyintéző*;

illetve

- a *Hitelesítés-szolgáltató*.

Ezenkívül az *Előfizetők*, az *Érintett felek*, az alkalmazásszoftverek szállítói és más harmadik felek magas kockázatú tanúsítvány problémákról szóló jelentéseket nyújthatnak be, amelyekben a *Hitelesítés-szolgáltatót* értesítik a *Tanúsítvány* visszavonását igénylő okokról, mint például csalás, visszaélés vagy kulcskompromittálódás.

A *Hitelesítés-szolgáltató* nyilvánosan elérhető módon tegyen elérhetővé egyértelmű utasításokat a feltételezett magánkulcs kompromittálódás, a helytelen *Tanúsítvány* használat vagy más lehetséges típusú csalás, kompromittálódás, visszaélés, nem megfelelő használat vagy a *Tanúsítvánnyal* kapcsolatos egyéb kérdések bejelentésére.

4.9.3. A visszavonási kérelemre vonatkozó eljárás

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

- A *Hitelesítés-szolgáltató* honlapján keresztül a nap 24 órájában.
A *Hitelesítés-szolgáltató* honlapján benyújtott kérelmeket a *Hitelesítés-szolgáltató* informatikai rendszerének azonnal el kell bírálnia, az elbírálás eredményéről az oldalon tájékoztatnia kell a kérelem benyújtóját;

- elektronikus formában, a kérelmező nem álneves, a visszavonni kívánt *Tanúsítványnál* nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) *Tanúsítványán* alapuló elektronikus aláírásával ellátva;
- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában ügyfélszolgálati időben, vagy postai úton.

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

Amennyiben a benyújtott visszavonási kérelem hiányos vagy érvénytelen, a *Hitelesítés-szolgáltató* elutasítja a kérelmet. Az elutasítás tényéről és okáról emailben tájékoztatja az *Alanyt* és az *Előfizetőt*.

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

Sikeres visszavonás esetén a *Hitelesítés-szolgáltató* értesítse az *Alanyt* és az *Előfizetőt* a visszavonás tényéről.

Tanúsítvánnyal kapcsolatos problémák sürgősségi bejelentése

A *Hitelesítés-szolgáltató*nak egy folyamatosan elérhető 24/7 felületet kell biztosítania a tanúsítvánnyal kapcsolatos problémák sürgősségi bejelentésére. Szükség esetén a bejelentett problémáról értesíteni kell a felügyelő hatóságot, és/vagy vissza kell vonni az érintett *Tanúsítványt*.

4.9.4. A visszavonási kérelemre vonatkozó kivárási idő

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

4.9.5. A visszavonási eljárás maximális hossza

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

A *Hitelesítés-szolgáltató* a *Weboldal-hitelesítő tanúsítványokkal* kapcsolatos problémabejelentéseket 24 órán belül vizsgálja ki és döntsön a további szükséges lépésekről.

A *Hitelesítés-szolgáltató* küldje meg a vizsgálat eredményét tartalmazó előzetes jelentést az érintett *Előfizetőnek* és a bejelentést tévő személynek.

A *Hitelesítés-szolgáltató* a *Weboldal-hitelesítő tanúsítványokat* a 4.9.1-ben meghatározott feltételek bekövetkezését követően legkésőbb 24 órán belül vonja vissza.

A *Hitelesítés-szolgáltató* a *Weboldal-hitelesítő tanúsítványokat* kibocsátó köztes hitelesítési egységek *Tanúsítványait* a 4.9.1-ben meghatározott feltételek bekövetkezését követően legkésőbb 7 napon belül vonja vissza.

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

A *Tanúsítvány*ban foglalt információ elfogadását és felhasználását megelőzően a *Hitelesítés-szolgáltató* által garantált biztonsági szint megtartásához szükséges, hogy az *Érintett felek* megfelelően gondosan járjanak el, így különösen javasolt ellenőrizniük a tanúsítási láncban található valamennyi *Tanúsítvány* érvényességét a vonatkozó műszaki szabványoknak megfelelően. Az ellenőrzésnek ki kell terjednie a *Tanúsítványok* érvényességének ellenőrzésére, a szabályzatok és a kulcshasználat megkötéseire, az egyes *Tanúsítványok*ban meghivatkozott CRL vagy OCSP alapú visszavonási státusz információk ellenőrzésére.

4.9.7. A visszavonási lista kibocsátás gyakorisága

A *Hitelesítés-szolgáltató* legalább naponta egyszer bocsásson ki új *Tanúsítvány visszavonási listát* a végfelhasználói *Tanúsítványok*at kibocsátó hitelesítési egységeire.

A *Tanúsítvány visszavonási listák* érvényességi ideje legfeljebb 26 óra lehet.

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

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

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

4.9.9. Valós idejű tanúsítvány állapot ellenőrzés lehetősége

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

4.9.10. A valós idejű tanúsítvány állapot ellenőrzésre vonatkozó követelmények

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

4.9.11. A visszavonási hirdetések egyéb elérhető formái

Nincs megkötés.

4.9.12. A kulcs kompromittálódásra vonatkozó speciális követelmények

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

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

4.9.13. A felfüggesztés körülményei

A *Weboldal-hitelesítő tanúsítványok* érvényességét nem lehet felfüggeszteni.

4.9.14. Ki kérelmezheti a felfüggesztést

Nem értelmezhető.

4.9.15. A felfüggesztési kérelemre vonatkozó eljárás

Nem értelmezhető.

4.9.16. A felfüggesztés maximális hossza

Nem értelmezhető.

4.10. Tanúsítvány állapot szolgáltatások

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

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

A *Tanúsítvány visszavonási listában* kerüljenek feltüntetésre a visszavont *Tanúsítványok*.

A visszavonási információ nem távolítható el a *Tanúsítvány visszavonási listáról* a visszavont *Tanúsítvány* lejáratú időpontja előtt.

A visszavont *Tanúsítványok* a *Tanúsítvány* érvényességének lejáratú után se törölődjenek a *Tanúsítvány visszavonási listából*.

Visszavonás esetén a folyamat sikeres lezárását követően a *Tanúsítvány* új állapota azonnal jelenjen meg a *Hitelesítés-szolgáltató Visszavonási állapot nyilvántartásában*.

Ettől a pillanattól kezdve a *Hitelesítés-szolgáltató* által nyújtott OCSP válaszok már a *Tanúsítvány* új visszavonási állapotát tartalmazzák.

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

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

4.10.1. Működési jellemzők

Nincs megkötés.

4.10.2. A szolgáltatás rendelkezésre állása

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

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

A *Visszavonási állapot nyilvántartások* válaszideje normál terhelés esetén legyen 10 másodpercnél kevesebb.

4.10.3. Opcionális lehetőségek

Nincs megkötés.

4.11. Az előfizetés vége

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

4.12. Magánkulcs letétbe helyezése és visszaállítása

A *Hitelesítés-szolgáltató* a *Weboldal-hitelesítő tanúsítványhoz* tartozó magánkulcshoz nem nyújthat kulcsletét szolgáltatást.

4.12.1. Kulcsletét és visszaállítás rendje és szabályai

A *Weboldal-hitelesítő tanúsítványhoz* tartozó magánkulcs nem helyezhető letétbe.

4.12.2. Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

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

5. Elhelyezési, eljárásbeli és üzemeltetési előírások

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

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

A *Hitelesítés-szolgáltató*nak figyelemmel kell kísérnie a kapacitás igényeket és biztosítania kell, hogy megfelelő feldolgozási teljesítmény és tárolási kapacitás álljon rendelkezésre a szolgáltatás nyújtásához.

5.1. Fizikai követelmények

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

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

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken kell megvalósítani.

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

5.1.1. A telephely elhelyezése és szerkezeti felépítése

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

5.1.2. Fizikai hozzáférés

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

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

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

Jogosulatlan személyek jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva kell tartani;

- a bejelentkezett terminálokat nem szabad felügyelet nélkül hagyni;
- nem szabad olyan munkafolyamatot végezni, amely során bizalmas adat felfedésre kerülhet.

A gépterem elhagyásakor az adminisztrátornak ellenőriznie kell, hogy:

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

A fizikai biztonsági vizsgálatok rendszeres elvégzésére felelősöket kell kijelölni. A vizsgálatok eredményét megfelelő naplóbejegyzésekben kell rögzíteni.

5.1.3. Áramellátás és légkondicionálás

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

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

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

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

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

5.1.4. Beázás és elárasztódás veszély kezelése

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

5.1.5. Tűz megelőzés és tűzvédelem

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

5.1.6. Adathordozók tárolása

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

5.1.7. Hulladék megsemmisítése

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

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

5.1.8. A mentési példányok fizikai elkülönítése

A *Hitelesítés-szolgáltatónak* legalább heti rendszerességgel elő kell állítania olyan mentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható. A mentéseket - legalább az utolsó teljes mentést is beleértve - egy olyan külső helyszínen kell tárolni, amelynek a fizikai és működési védelme azonos az elsődleges helyszínevel. Az elsődleges és a tartalék helyszínek között meg kell oldani az adatok biztonságos továbbítását.

A mentett állományokból legalább évente szűrőpróbaszerű kiválasztással jegyzőkönyvezett helyreállítási tesztet kell végezni.

5.2. Eljárásbeli előírások

A *Hitelesítés-szolgáltatónak* gondoskodnia kell arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltesse.

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

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

5.2.1. Bizalmi szerepkörök

A *Hitelesítés-szolgáltató*nak feladatai ellátásához 24/2016. BM rendelet [8] előírásainak megfelelő bizalmi szerepköröket (a rendelet szövegezésében bizalmi munkaköröket) kell létrehozni. A jogosultságokat és funkciókat oly módon kell megosztani az egyes bizalmi szerepkörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére.

A megvalósítandó bizalmi szerepkörök:

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

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

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

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

5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

A *Hitelesítés-szolgáltató* biztonsági és üzemeltetési szabályzataiban elő kell írni, hogy csak védett környezetben, kettő, bizalmi szerepkört betöltő munkatárs egyidejű fizikai jelenlétében végezhető el az alábbi műveletek:

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

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

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

5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés

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

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

Az azonosító és hitelesítő adatokat a felhasználói jogosultságok megszűnésekor haladéktalanul vissza kell vonni.

5.2.4. Egymást kizáró szerepkörök

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

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

5.3. Személyzetre vonatkozó előírások

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

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

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

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

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

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

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

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

5.3.2. Előélet vizsgálatára vonatkozó eljárások

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

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

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

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

5.3.3. Képzési követelmények

A *Hitelesítés-szolgáltató* az újonnan felvett alkalmazottakat ki kell képezze, amely során elsajátítják az adott munkakör ellátásához szükséges mértékben:

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

A *Hitelesítés-szolgáltató* a regisztrációban közreműködő munkatársakat ki kell képezze a *Tanúsítvány*ba kerülő adatok ellenőrzésével kapcsolatos veszélyekről és kockázatokról.

A regisztrációban közreműködő munkatársaknak kinevezésük előtt sikeres vizsgát kell tenniük a vonatkozó adatellenőrzési követelmények és eljárások ismeretéből, és ennek megtörténtét dokumentálni kell.

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

5.3.4. Továbbképzési gyakoriságok és követelmények

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

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

A képzési anyagot legalább 12 havonta felül kell vizsgálni, és tartalmaznia kell az új fenyegetéseket és biztonsági megoldásokat.

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

5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

Nincs előírás.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

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

5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

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

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

5.3.8. A személyzet számára biztosított dokumentációk

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

5.4. Naplózási eljárások

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

5.4.1. A tárolt események típusai

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

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

Az elmentett naplóbejegyzések nem kerülhetnek módosításra vagy törlésre.

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

Naplózni kell minimálisan az alábbi eseményeket:

- BELSŐ ÓRA
 - a belső óra szinkronizációja az UTC időhöz, beleértve az üzemszerű újrakalibrálásokat is;
 - a szinkronizáció elvesztése;
- NAPLÓZÁS
 - a naplózó rendszer vagy egyes komponenseinek leállítása, újraindítása;
 - a naplózás bármilyen beállításának módosítása, mint pl. gyakoriság, riasztási küszöb érték, vizsgált esemény;
 - a tárolt naplózási adatok módosítása vagy törlése;
 - a naplózó rendszer hibája miatt végzett tevékenységek;
- RENDSZER BEJELENTKEZÉSEK
 - sikeres bejelentkezések, sikertelen bejelentkezési próbálkozások bizalmi szerepkörökbe;
 - jelszó alapú azonosítás esetén:
 - * az engedélyezett sikertelen bejelentkezési próbálkozások számának megváltoztatása;
 - * az engedélyezett sikertelen bejelentkezési próbálkozások számának elérése felhasználói bejelentkezéskor;

- * sikertelen bejelentkezések miatt zárolt felhasználó újbóli engedélyezése;
- az azonosítási technika változtatása (például jelszó alapúról PKI alapúra);
- KULCSKEZELÉS
 - a szolgáltatói kulcsok teljes életciklusára vonatkozó valamennyi esemény (kulcsgenerálás, elmentés, betöltés, megsemmisítés stb.);
 - a felhasználói kulcsok generálásával, kezelésével kapcsolatos események;
 - a *Hitelesítés-szolgáltató* által bármilyen célból tárolt felhasználói magánkulcsok kezelésével kapcsolatos minden esemény;
- TANÚSÍTVÁNY KEZELÉS
 - szolgáltatói *Tanúsítványok* kibocsátásával, állapotváltásával kapcsolatos minden esemény;
 - minden kérés, beleértve a *Tanúsítvány* kibocsátást, kulcscserét, megújítást, visszavonást;
 - a kérések feldolgozásával kapcsolatos események;
 - a *Tanúsítvány* kibocsátásával kapcsolatban végrehajtott minden ellenőrzési tevékenység, ide értve az ellenőrzéssel kapcsolatban történt telefonbeszélgetések időpontját, telefonszámot, a hívott személy nevét és a megtudott információkat;
 - tanúsítványkérelmek elutasítása;
 - *Tanúsítvány* kibocsátása, állapotváltása;
- ADATMOZGÁSOK
 - bármilyen, a biztonság szempontjából kritikus adat manuális bevitele a rendszerbe;
 - a rendszer által fogadott, biztonsági szempontból fontos adatok, üzenetek;
- CA KONFIGURÁCIÓ
 - a CA tetszőleges komponensének átparaméterezése, a beállításon történt bármilyen változtatás;
 - felhasználók felvétele, törlése;
 - felhasználói szerepkörök, jogosultságok megváltoztatása;
 - a tanúsítvány profil megváltoztatása;
 - CRL profil megváltoztatása;
 - új CRL lista előállítása;
 - OCSP válasz generálása;
 - *Időbélyegző* generálása;
 - az előírt időpontossági küszöb túllépése;
- *HSM* eszköz

- *HSM* eszköz installálása;
 - *HSM* eszköz eltávolítása;
 - *HSM* eszköz selejtezése, megsemmisítése;
 - *HSM* eszköz szállítása;
 - *HSM* eszköz tartalmának törlése (nullázás);
 - *HSM* eszköz feltöltése kulcsokkal, tanúsítványokkal;
- KONFIGURÁCIÓ VÁLTOZÁSA
 - hardver;
 - szoftver;
 - operációs rendszer;
 - javító csomag;
- FIZIKAI HOZZÁFÉRÉS, TELEPHELY BIZTONSÁG
 - személy belépése a bizalmi szolgáltatást nyújtó rendszer komponenseket tartalmazó biztonsági területre és onnan kilépése;
 - hozzáférés egy bizalmi szolgáltatást nyújtó rendszer komponenshez;
 - a fizikai biztonság ismert vagy gyanított megsértése;
 - tűzfal és router forgalmak;
- MŰKÖDÉSI RENDELLENESÉGEK
 - 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 *Szolgáltatási szabályzat* megsértése;
 - operációs rendszer órájának törlése;
- EGYÉB ESEMÉNYEK
 - személy kinevezése biztonsági szerepkörbe;
 - operációs rendszer telepítése;
 - PKI alkalmazás telepítése;
 - rendszer elindítása;
 - belépési kísérlet a PKI alkalmazásba;

- jelszó módosítási, beállítási kísérlet;
- a belső adatbázis elmentése, visszaállítása mentésből;
- fájl műveletek (pl. létrehozás, átnevezés, áthelyezés);
- adatbázis hozzáférés.

5.4.2. A naplófájl feldolgozásának gyakorisága

A *Hitelesítés-szolgáltató*nak biztosítania kell a keletkezett naplóállományok rendszeres kiértékelését.

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

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

A *Hitelesítés-szolgáltató* használhat automatizált eszközöket az elektronikus naplóállományok kiértékelésének segítésére. Az automata figyelő rendszerből kapott értesítéseket 24 órán belül fel kell dolgozni és ki kell értékelni.

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

A kiértékelés során elemezni kell a rendszerek által generált hibaüzeneteket.

Statisztikai módszerekkel elemezni kell a forgalmi adatokban bekövetkezett jelentős változásokat.

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

5.4.3. A naplófájl megőrzési időtartama

Az online rendszerből való kitörlés előtt a naplóállományokat archiválni kell és gondoskodni kell azok biztonságos megőrzéséről az 5.5.2 fejezetben meghatározott ideig, de legalább a keletkezésüktől számított 10 évig.

5.4.4. A naplófájl védelme

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

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

5.4.5. A naplófájl mentési eljárásai

Az üzemeltetés során az egyes rendszerekben folyamatosan keletkező naplóbejegyzésekből napi naplóállományokat kell előállítani.

A napi naplóállományokat a kiértékelés után 2 példányban archiválni kell és a példányokat egymástól fizikailag elkülönülő helyszíneken az előírt ideig meg kell őrizni.

A mentések pontos menetét a *Szolgáltatási szabályzat*ban elő kell írni.

5.4.6. A naplózás adatgyűjtési rendszere

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

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

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

5.4.7. Az eseményeket kiváltó alanyok értesítése

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

5.4.8. Sebezhetőség felmérése

A *Hitelesítés-szolgáltató*nak évente sebezhetőség vizsgálatot kell végeznie, amely segítségével feltérképezi a potenciális belső és külső fenyegetettségeket, amelyek jogosulatlan hozzáférések eredményezhetnek, hatással lehetnek a *Tanúsítvány* kiadási folyamatra, vagy lehetővé teszik a *Tanúsítvány*ban tárolt adatok módosítását.

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

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

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

5.5. Adatok archiválása

5.5.1. Az archivált adatok típusai

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

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

- a *Hitelesítés-szolgáltató* akkreditációjával kapcsolatos valamennyi irat;

- a *Hitelesítési rend(ek)* valamennyi kibocsátott verziója;
- a *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 *Tanúsítványkérelemmel* 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 *Tanúsítványokkal* kapcsolatos valamennyi információ a teljes életciklusra vonatkozóan;
- valamennyi elektronikus és papíralapú naplóbejegyzés.

5.5.2. Az archívum megőrzési időtartama

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

- a *Hitelesítési rendet* a hatályon kívül helyezéstől számított legalább 10 évig;
- a *Szolgáltatási szabályzatot* a hatályon kívül helyezéstől számított legalább 10 évig;
- *Általános Szerződési Feltételeket* a hatályon kívül helyezéstől számított legalább 10 évig;
- a *Tanúsítványokkal* kapcsolatos valamennyi elektronikus és/vagy papír alapú információt legalább
 - a *Tanúsítvány* érvényességének lejáratától számított 10 évig;
- minden egyéb archiválandó dokumentomot a keletkezésétől számított legalább 10 évig.

5.5.3. Az archívum védelme

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

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

Az archivált adatok megőrzése során gondoskodni kell az archivált adatok

- sértetlenségének megőrzéséről;

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

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

5.5.4. Az archívum mentési folyamatai

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

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

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

A *Hitelesítés-szolgáltató*nak biztosítania kell, hogy a szolgáltatást nyújtó rendszerein a gépidő maximum 1 másodpercre térjen el a referenciaidőtől. Az időjel előállításához használt gépidőt naponta legalább egy alkalommal szinkronizálni kell az UTC időhöz.

A napi naplóállományokat minősített *Időbélyegző*vel kell ellátni.

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

5.5.6. Az archívum gyűjtési rendszere

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

5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

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

Az archivált adatállományokat védeni kell a jogosulatlan hozzáféréstől.

Az arra jogosultaknak biztosítani kell az archivált adatokhoz való ellenőrzött hozzáférést:

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

5.6. Szolgáltatói kulcs cseréje

A *Hitelesítés-szolgáltató* gondoskodjon arról, hogy az általa üzemeltetett *Hitelesítő* egységek folyamatosan rendelkezzenek a működéshez szükséges érvényes kulccsal és Tanúsítvánnyal. Ennek érdekében a *Tanúsítványuk* lejártá illetve a hozzájuk kapcsolódó kulcsok használati idejének lejártá előtt elegendő idővel generáljon új kulcspárt a *Hitelesítő egység* számára, és arról időben értesítse *Ügyfeleit*. Az új szolgáltatói kulcsot a jelen szabályzatnak megfelelően kell generálni és kezelni.

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

- publikálnia kell az érintett *Tanúsítványait* és nyilvános kulcsait a 2.2 fejezetben meghatározott előírásoknak megfelelően;
- a szolgáltatói kulcscsere után a kibocsátandó végfelhasználói *Tanúsítványokat* már csak az új szolgáltatói kulcsok felhasználásával írhatja alá;
- meg kell őriznie a régi szolgáltatói *Tanúsítványokat* és nyilvános kulcsokat.

5.7. Kompromittálódást és katasztrófát követő helyreállítás

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

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

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

5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások

A *Hitelesítés-szolgáltató* rendelkeznie kell üzletmenet folytonossági tervvel. A *Hitelesítés-szolgáltató* ki kell alakítania és fenn kell tartania egy teljes értékű tartalékrendszert, amely az elsődleges helyszíntől biztonságos távolságra, földrajzilag különböző helyszínen található és önállóan is alkalmas a szolgáltatások teljes körű ellátására.

A *Hitelesítés-szolgáltató* rendszeresen tesztelnie kell a tartalékrendszer működését és évente felül kell vizsgálnia az üzletmenet folytonossági terveit.

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

5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

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

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

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

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

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

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

5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások

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

- vissza kell vonni a *Hitelesítés-szolgáltató* összes érintett *Tanúsítványát*;
- új szolgáltatói magánkulcsokat kell generálni a szolgáltatások helyreállításához;
- nyilvánosságra kell hozni a visszavont szolgáltatói *Tanúsítványok* adatait a 2.2 fejezetben szabályozott módon;
- vissza kell vonni az összes *Weboldal-hitelesítő tanúsítványt*, amelyet az érintett magánkulcsokkal írtak alá;
- a visszavont *Weboldal-hitelesítő tanúsítványok* helyett új *Tanúsítványok*at kell kibocsátani az új szolgáltatói kulcsok felhasználásával;
- a kompromittálódással kapcsolatos információt elérhetővé kell tenni valamennyi *Előfizető* és *Érintett fél* részére;

5.7.4. Működés folyamatosságának biztosítása katasztrófát követően

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

A katasztrófa bekövetkezése esetén haladéktalanul életbe kell léptetni a rendelkezéseket és meg kell kezdeni a károk elhárítását, a szolgáltatások helyreállítását.

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

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

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

5.8. A hitelesítés-szolgáltató vagy a regisztráló szervezet leállítása

A *Hitelesítés-szolgáltató*nak a szolgáltatás megszüntetésekor teljesítenie kell a jogszabályokban megfogalmazott követelményeket.

A leállítás során kiemelten kezelendő feladatok:

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

6. Műszaki biztonsági óvintézkedések

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

Folyamatosan nyomon kell követni a kapacitás igényeket és becsülni kell a jövőbeni várható kapacitást, hogy biztosítani lehessen a szükséges feldolgozási és tárolási igények rendelkezésre állását.

6.1. Kulcspár előállítása és telepítése

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

6.1.1. Kulcspár előállítása

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

- ETSI TS 119 312 [17];
- CABF Baseline Requirements ajánlás [33];
- az Eüt. [7] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

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

- A szolgáltatói magánkulcs előállítását fizikailag védett környezetben (lásd 5.1 pont), legalább két, bizalmi szerepkört (lásd 5.2.1 pont) betöltő, erre feljogosított személy együttes részvételével, más illetéktelen személyek jelenlétét kizárva végzi.

- A szolgáltatói magánkulcs előállítását olyan eszközön belül hajtja végre, amely:
 - megfelel az ISO/IEC 19790 [21] követelményeinek,
 - vagy megfelel a FIPS 140-2 [34] 3-as, illetve annál magasabb szintű követelményeinek,
 - vagy megfelel a CEN 419 221-5 [18] követelményeinek,
 - vagy olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [20] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint EAL 4-es vagy magasabb értékelési garancia szinten van értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előírányzaton kell alapulnia.
- A szolgáltatói magánkulcs előállítását egy kulcsgenerálási forgatókönyv alapján végzi.
- Szolgáltatói gyökér hitelesítő egység magánkulcsának előállítása esetén jelen van egy külső auditor. A külső auditor igazolja, hogy a kulcs generálása a forgatókönyv szerint történt.

A *Hitelesítés-szolgáltató* a saját IT rendszereiben használt infrastruktúrális kulcsok előállítása esetén biztosítsa, hogy:

- a szolgáltatói infrastruktúrális kulcs előállítását fizikailag védett környezetben (lásd 5.1 pont), bizalmi szerepkört (lásd 5.2.1 pont) betöltő, erre feljogosított személy végzi, más illetéktelen személyek jelenlétét kizárva;
- a kulcs előállítása során maradéktalanul betartja az eszköz felhasználói dokumentációjában szereplő előírásokat.

A *Hitelesítés-szolgáltató* által az *Alanyok* számára előállított kulcspár előállítása esetén biztosítsa, hogy:

- A kulcsok előállítását fizikailag védett környezetben végzi, kizárólag bizalmi szerepkört betöltő személyek részvételével.
- A magánkulcs *Igénylő* részére 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 *Igénylő* által előállított kulcspár esetén:

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

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

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

6.1.2. Magánkulcs eljuttatása az igénylőhöz

Amennyiben a *Hitelesítés-szolgáltató* állította elő a weboldal-hitelesítés során használni kívánt magánkulcsot, akkor az alábbi követelményeknek kell megfelelni:

- A *Hitelesítés-szolgáltató* az általa az *Alanyok* 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 *Igénylő* vehesse át.
- A *Hitelesítés-szolgáltató* megfelelő bizonyítékot szerez a magánkulcs *Igénylő* részére történő átadásáról, az átadás pontos időpontjáról.
- A magánkulcs *Igénylő* részére történő átadása után a *Hitelesítés-szolgáltató* nem őriz meg másolatot a magánkulcsból.

6.1.3. A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

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

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

6.1.4. A szolgáltatói nyilvános kulcs közzététele

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

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

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

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

6.1.5. Kulcsméretek

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

- ETSI TS 119 312 [17];
- CABF Baseline Requirements ajánlás [33];
- az Eüt. [7] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

6.1.6. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A kulcsparaméterek előállítására vonatkozó követelményeket a 6.1.1. fejezet tartalmazza.

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

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

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

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

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

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

A *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítvány*okban szerepeltesse a "kulcshasználat" (Key Usage) kiterjesztéseket, amelyek meghatározzák a *Tanúsítvány* felhasználási területét és az X.509v3 [32] kompatibilis alkalmazásokban műszakilag is korlátozzák a kulcsok felhasználhatóságát. A mező tartalmára vonatkozó megkötések a 7.1.2 fejezetben szerepelnek.

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

6.2. A magánkulcsok védelme

A *Hitelesítés-szolgáltató*nak gondoskodnia kell a birtokában lévő magánkulcsok biztonságos kezeléséről, meg kell akadályoznia a magánkulcsok felfedését, lemásolását, törlését, módosítását, jogosulatlan használatát. A *Hitelesítés-szolgáltató* csak addig őrizheti a magánkulcsokat, ameddig azt a szolgáltatás nyújtása feltétlenül megköveteli.

A *HSM* eszközök kezelése során a használatból kivont *HSM* eszközökben tárolt aláíró magánkulcsokat olyan módon kell törölni, hogy ne legyen lehetséges a kulcsok visszaállítása.

6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

A *Hitelesítés-szolgáltató* *Tanúsítvány*okat, OCSP válaszokat, CRL listákat kibocsátó rendszerei a magánkulcsokat olyan biztonságos hardver eszközökben kell tárolják, amelyek

- megfelelnek az ISO/IEC 19790 [21] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [34] 3-as, illetve annál magasabb szintű követelményeknek,
- vagy megfelelnek a CEN 14167-2 [35] munkacsoport egyezmény követelményeinek,
- vagy megfelelnek a CEN 419 221-5 [18] követelményeinek,

- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [20] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten vannak értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előírányzaton kell alapulnia.

A szolgáltatói magánkulcsok a *HSM* eszközön kívül csak kódolt formában tárolhatók. A kódoláshoz csak az Eüt. [7] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozatban foglalt algoritmusok és kulcsparaméterek használhatók, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

A szolgáltatói magánkulcsokat kódolt formában is fizikailag biztonságos helyszínen kell tárolni, ahol azokhoz csak az arra jogosultak férhetnek hozzá.

A kriptográfiai algoritmusok vagy kulcsparaméterek gyengülése esetén a kódolt kulcsokat meg kell semmisíteni vagy erősebb védelmet biztosító algoritmus és kulcsparaméterek felhasználásával tovább kell kódolni.

6.2.2. Magánkulcs többszereplős (n-ből m) használata

A *Hitelesítés-szolgáltató*nak biztosítania kell, 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* csak titkosított formában helyezheti letétbe a szolgáltatói magánkulcsait.

6.2.4. Magánkulcs mentése

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

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

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

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

6.2.5. Magánkulcs archiválása

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

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

A *Hitelesítés-szolgáltató* valamennyi szolgáltatói magánkulcsát a követelményeknek megfelelő *HSM* eszközben kell előállítani.

A magánkulcsok nem létezhetnek nyílt formában a *HSM* eszközön kívül.

A *Hitelesítés-szolgáltató* a magánkulcsot csak biztonsági másolat készítése céljából exportálhatja a *HSM* eszközből.

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

6.2.7. Magánkulcs tárolása hardver kriptográfiai eszközben

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

A *HSM* eszközön belüli tárolási formára vonatkozóan nincs előírás.

6.2.8. A magánkulcs aktiválásának módja

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

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

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

6.2.9. A magánkulcs deaktiválásának módja

Szolgáltatói magánkulcsok

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

Végfelhasználói magánkulcsok

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

6.2.10. A magánkulcs megsemmisítésének módja

Szolgáltatói magánkulcsok

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

A szolgáltatói magánkulcsok megsemmisítését a felhasznált *HSM* eszköz felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell elvégezni.

A magánkulcsról készült minden mentett példányt dokumentált módon meg kell semmisíteni olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon.

Végfelhasználói magánkulcsok

A használatból kivont weboldal hitelesítő magánkulcsokat javasolt megsemmisíteni.

6.2.11. A hardver kriptográfiai eszközök értékelése

A 6.2.1 fejezet előírásaival összhangban a *Hitelesítés-szolgáltató* valamennyi szolgáltatói magánkulcsát olyan *HSM* eszközben kell tárolni, amely rendelkezik:

- ISO/IEC 19790 [21] szerinti tanúsítvánnyal,
- vagy FIPS 140-2 Level 3 [34] szerinti tanúsítvánnyal,
- vagy a CEN 14167-2 [35] munkacsoport egyezmény követelményeinek való megfelelést igazoló legalább EAL-4 szintű Common Criteria alapú tanúsítvánnyal,
- vagy a CEN 419 221-5 [18] követelményeinek való megfelelést igazoló legalább EAL-4 szintű Common Criteria alapú tanúsítvánnyal,
- vagy a Nemzeti Média- és Hírközlési Hatóság által vagy az Európai Unió valamely tagállamában nyilvántartásba vett, elektronikus aláírási termékek értékelésére jogosult független tanúsító szervezet által erre a célra kiadott igazolással.

6.3. A kulcspár kezelés egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

A *Hitelesítés-szolgáltató*nak archiválnia kell valamennyi általa kibocsátott *Tanúsítványt*.

6.3.2. A tanúsítványok és kulcspárok használatának periódusa

A gyökér hitelesítő egységek tanúsítványai és kulcsai

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

A köztes hitelesítő egységek tanúsítványai és kulcsai

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

- nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozata szerint biztonságosan felhasználhatók;
- nem haladhatja meg az adott köztes szolgáltatói *Tanúsítványt* kibocsátó gyökér vagy köztes szolgáltatói *Tanúsítvány* érvényességi idejét.

A végfelhasználói tanúsítványok

A *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítványok* érvényességi ideje:

- 2020-08-31-ig kibocsátott *Tanúsítvány* esetén legfeljebb a kibocsátástól számított 825 nap (≈27 hónap);
2020-09-01-től kibocsátott *Tanúsítvány* esetén legfeljebb a kibocsátástól számított 398 nap (≈13 hónap);
- nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozata szerint biztonságosan felhasználhatók;
- nem haladhatja meg a *Tanúsítványt* kibocsátó szolgáltatói *Tanúsítvány* érvényességi idejét.

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

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

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

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

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

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

A *Hitelesítés-szolgáltató* által az *Igénylő* részére előállított, szoftveresen átadott magánkulcsok esetén a *Hitelesítés-szolgáltatónak* az aktivizáló adatokat megfelelő minőségű véletlenszám-generátor segítségével, fizikailag biztonságos körülmények között kell előállítania és a magánkulcshoz rendelnie;

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

6.4.2. Az aktivizáló adatok védelme

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

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

6.4.3. Az aktivizáló adatok kezelésének egyéb szempontjai

Nincs megkötés.

6.5. Informatikai biztonsági előírások

6.5.1. Speciális informatikai biztonsági műszaki követelmények

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

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

6.5.2. Az informatikai biztonság értékelése

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

6.6. Életciklusra vonatkozó műszaki előírások

6.6.1. Rendszerfejlesztési előírások

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

- kereskedelmi dobozos szoftverek, amelyeket dokumentált tervezési módszertan szerint terveztek és fejlesztettek;

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

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

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

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

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

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

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

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

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

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

6.6.2. Biztonságkezelési előírások

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

6.6.3. Életciklusra vonatkozó biztonsági előírások

A *Hitelesítés-szolgáltató*nak gondoskodnia kell a felhasznált *HSM* eszközök védelméről azok teljes életciklusa alatt.

- Megfelelő tanúsítással rendelkező *HSM* eszközöket kell használni.

- A *HSM* eszközök átvételekor meg kell róla győződni, hogy a szállítás során biztosították a *HSM* eszközök feltörés elleni védelmét.
- A tárolás során biztosítani kell a *HSM* eszközök feltörés elleni védelmét.
- Az _____ üzemeltetés _____ során _____ folyamatosan be kell tartani a *HSM* eszközök biztonsági előírányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket.
- A használatból kivont *HSM* eszközökben tárolt magánkulcsokat olyan módon kell törölni, hogy lehetetlenné váljon a kulcsok visszaállítása.
- A használatból kivont *HSM* eszközöket a biztonsági előírányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeknek megfelelően kell kezelni és megsemmisíteni.

6.7. Hálózati biztonsági előírások

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

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

- IT rendszereit jól elválasztott biztonsági zónákra kell osztania;
- el kell különítenie az IT rendszer üzemeltetését támogató rendszereit az éles szolgáltatást nyújtó rendszereitől;
- el kell különítenie az éles szolgáltatást nyújtó rendszereit a fejlesztésre és tesztelésre szolgáló rendszerektől;
- az elkülönített megbízható rendszerek között csak olyan megbízható kommunikációs csatornákon keresztül létesíthet kapcsolatot, amelyek logikailag el vannak választva más kommunikációs csatornáktól, megbízható végponti azonosítást használnak és védik a csatornákon küldött adatokat a módosítástól és a felfedéstől;
- az éles szolgáltatást nyújtó IT rendszereit biztonságos hálózati zónában kell üzemeltesse;
- a zónákhoz való hozzáférést és a zónák közötti kommunikációt csak a szolgáltatás nyújtásához szükségesre kell korlátoznia;
- le kell tiltani a nem használt protokollokat és felhasználókat;
- tiltsa le a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtasson;

- a használt szabályrendszert rendszeresen felül kell vizsgálnia.

A *Hitelesítés-szolgáltató*nak sérülékenységvizsgálatot kell végeznie vagy végeztetnie a *Hitelesítés-szolgáltató* nyilvános és privát IP címein:

- a CA/Browser Forum kérésétől számított egy héten belül;
- a *Hitelesítés-szolgáltató* által jelentősnek minősített rendszer vagy hálózati változtatás után;
- legalább minden három (3) hónapban.

6.8. Időbélyegzés

A *Hitelesítés-szolgáltató*nak valamely Európai Unió tagállam bizalmi listáján szereplő minősített időbélyegzés-szolgáltató által biztosított *Időbélyegzőket* kell használnia a naplóbejegyzések és egyéb archiválandó elektronikus állományok hitelesítésére.

7. Tanúsítvány, CRL és OCSP profilok

7.1. Tanúsítvány profil

A *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítványok* illetve az azokat kibocsátó tanúsítvány láncban található gyökér és köztes hitelesítő egységek *Tanúsítványai* feleljenek meg az alábbi ajánlásoknak, specifikációknak:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [32];
- IETF RFC 5280 [26];
- IETF RFC 6818 [28];
- IETF RFC 6962 [31];
- ETSI EN 319 412-1 [13];
- ETSI EN 319 412-4 [16];

7.1.1. Verzió szám(ok)

A *Hitelesítés-szolgáltató* által használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítványai* és a *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítványok* legyenek az X.509 specifikáció [32] szerinti "v3" *Tanúsítványok*.

A *Tanúsítványok* alapmezői a következők:

- Verzió (Version)
A *Tanúsítvány* az X.509 specifikáció [32] szerinti "v3" *Tanúsítványok*nak felel meg, így a mezőbe a "2" érték kerül.

- Sorozatszám (Serial Number)
A *Tanúsítványt* kibocsátó hitelesítő egység által generált egyedi azonosító.
A végfelhasználói *Tanúsítványok* esetében a "Serial Number" mezőnek legalább 8 bájt entrópiájú véletlen számot kell tartalmaznia.
- Algoritmus azonosító (Algorithm Identifier)
A *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző készítéséhez használt kriptográfiai algoritmuskészlet azonosítója (OID).
- Aláírás (Signature)
A *Hitelesítés-szolgáltató* által készített, a *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző, amelyet a *Hitelesítés-szolgáltató* az "Algoritmus azonosító" -ban megadott algoritmuskészlettel hozott létre.
- Kibocsátó (Issuer)
A *Tanúsítványt* kibocsátó *Hitelesítő egység* megkülönböztetett neve egyedi X.501 név formátum szerint (lásd: 3.1. fejezet).
- Érvényesség (Valid From & Valid To)
A *Tanúsítvány* érvényességének kezdete és vége.
Az időpontok UTC szerint és az IETF RFC 5280-nak megfelelő kódolásban kerülnek rögzítésre.
- Az *Alany* azonosítója (Subject)
Az *Alany* megkülönböztetett neve egyedi X.501 név formátum szerint (lásd: 3.1. fejezet).
Mindig kitöltésre kerül.
- Az *Alany* nyilvános kulcsának algoritmus-azonosítója (Subject Public Key Algorithm Identifier)
Az *Alany* nyilvános kulcsának algoritmus azonosítója.
- 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* az X.509 specifikáció [32] szerinti tanúsítvány kiterjesztéseket használhat, saját maga által definiált kritikus kiterjesztések használata nem megengedett.

A tanúsítvány kiterjesztéssel kapcsolatos konkrét előírások:

Gyökér hitelesítési egység tanúsítványa

- Hitelesítési rendek (Certificate Policies) – nem kritikus
OID: 2.5.29.32
Nem szerepelhet ez a mező.
- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
OID: 2.5.29.35
A *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.
Használata kötelező.
A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata.
- *Alany* kulcsazonosító (Subject Key Identifier) – nem kritikus
OID: 2.5.29.14
Az *Alany* nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.
A mező értéke: a nyilvános kulcs SHA-1 lenyomata.
Használata kötelező.
- *Alany* alternatív nevei (Subject Alternative Names) – nem kritikus
OID: 2.5.29.17
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 kitöltése kötelező és az értéke: CA = "TRUE".
A *Tanúsítványban* szerepelhet a "pathLenConstraint" mező.
- Kulcshasználat (Key Usage) – kritikus
OID: 2.5.29.15
A kulcs engedélyezett használati körének meghatározása.
Kötelezően beállítandó, értéke:
 - "keyCertSign",
 - "cRLSign".
- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus
OID: 2.5.29.37
A kulcs további engedélyezett használati körének meghatározása.
Nem szerepelhet.

Más tanúsítvány kiterjesztés nem kerülhet kitöltésre.

Köztes hitelesítési egység tanúsítványa

- Hitelesítési rendek (Certificate Policies) – nem kritikus
OID: 2.5.29.32

Ez a mező korlátozhatja a köztes *Tanúsítványt* tartalmazó tanúsítványláncban használható *Hitelesítési rendeket*. A köztes hitelesítési egység alá tartozó alrendszerben csak olyan végfelhasználói *Tanúsítvány* adható ki, amely megfelel az itt felsorolt *Hitelesítési rendek* közül legalább egynek.

A mező kitöltése kötelező és nem lehet kritikus. A *Hitelesítés-szolgáltató* saját köztes hitelesítési egységei számára kibocsátott *Tanúsítványok* esetében szerepelhet "anyPolicy" Identifier ebben a mezőben.

A vonatkozó *Szolgáltatási szabályzat* hivatkozása megadható ebben a mezőben.

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

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
OID: 2.5.29.35

A *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.

Használata kötelező.

A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata.

- *Alany* kulcsazonosító (Subject Key Identifier) – nem kritikus
OID: 2.5.29.14

Az *Alany* nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.

A mező értéke: a nyilvános kulcs SHA-1 lenyomata.

Használata kötelező.

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

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 kitöltése kötelező, és az értéke: CA = "TRUE".

A *Tanúsítványban* szerepelhet a "pathLenConstraint" mező.

- Kulcshasználat (Key Usage) – kritikus
OID: 2.5.29.15

A kulcs engedélyezett használati körének meghatározása.

Kötelezően beállítandó érték:

- "keyCertSign",

- "cRLSign".
- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus
OID: 2.5.29.37
A kulcs további engedélyezett használati körének meghatározása.
A 2019-01-01 után kiadandó *Weboldal-hitelesítő tanúsítvány*okat kiadó köztes szolgáltatói *Tanúsítvány*okban kötelezően szereplő értékek:
 - Server Authentication (1.3.6.1.5.5.7.3.1)
 - Client Authentication (1.3.6.1.5.5.7.3.2)
- CRL szétosztási pont (CRL Distribution Points) – nem kritikus
OID: 2.5.29.31
A mező tartalmazza a CRL elérhetőségét http és/vagy LDAP protokollon keresztül.
Kitöltése kötelező.
- Szolgáltatói információ elérése (Authority Information Access) – nem kritikus
OID: 1.3.6.1.5.5.7.1.1
A *Hitelesítés-szolgáltató* által rendelkezésre bocsátott, a *Tanúsítvány* használatához kapcsolódó egyéb szolgáltatásainak leírása.
Kötelező a kitöltése, és a mező tartalmazza a következő adatokat:
 - A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást kell nyújtson. Ennek elérhetőségét kell itt szerepeltetni.
 - A tanúsítványlánc felépítésének megkönnyítésére a *Hitelesítés-szolgáltató* adja meg a *Tanúsítvány*t kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.

Más tanúsítvány kiterjesztés nem kerülhet kitöltésre.

Végfelhasználói tanúsítvány

- Hitelesítési rendek (Certificate Policies) – nem kritikus
OID: 2.5.29.32
E mező tartalmazza a *Tanúsítvány* kiadása és használata során érvényes *Hitelesítési rend* (lásd 1.2.1.fejezet) azonosítóját, valamint a *Tanúsítvány* alkalmazhatóságára vonatkozó egyéb információkat.
Végfelhasználói *Tanúsítvány* esetében a *Hitelesítés-szolgáltató* minden esetben töltse ki ezt a mezőt a következő adatok megadásával:
 - a *Hitelesítési rend* azonosítója (1.2.1 fejezet szerinti OID) ;
 - a *Szolgáltatási szabályzat* elérhetősége;
 - szöveges figyelmeztetés angol és magyar nyelven, amelyből megállapítható, hogy II. vagy III. hitelesítési osztályú *Tanúsítvány*ról van-e szó, azaz regisztrációkor történt-e személyes azonosítás, illetve hogy a *Tanúsítvány* alanya természetes személy-e;

- az ETSI EN 319 411-1 [12] által meghatározott hitelesítési rend azonosítója (OID), amelynek a *Tanúsítvány* megfelel az alábbiak szerint:
 - * DVCP *Tanúsítvány* esetében OID 0.4.0.2042.1.6,
 - * OVCP *Tanúsítvány* esetében OID 0.4.0.2042.1.7,
 - * IVCP *Tanúsítvány* esetében OID 0.4.0.2042.1.8.
- A CA/Browser Forum által meghatározott hitelesítési rend azonosítója az alábbiak szerint:
 - * DVCP *Tanúsítvány* esetében OID 2.23.140.1.2.1,
 - * OVCP *Tanúsítvány* esetében OID 2.23.140.1.2.2,
 - * IVCP *Tanúsítvány* esetében OID 2.23.140.1.2.3.

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

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

A vonatkozó *Szolgáltatási szabályzat* hivatkozása megadható ebben a mezőben.

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
OID: 2.5.29.35
A *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.
Használata kötelező.
A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata.
- *Alany* kulcsazonosító (Subject Key Identifier) – nem kritikus
OID: 2.5.29.14
Az *Alany* nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.
A mező értéke: a nyilvános kulcs SHA-1 lenyomata.
Használata kötelező.
- *Alany* alternatív nevei (Subject Alternative Names) – nem kritikus
OID: 2.5.29.17
Lásd: 3.1.1. fejezet.
- 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 szerepelhet a végfelhasználói *Tanúsítvány*okban.
A "pathLenConstraint" mező nem szerepelhet a végfelhasználói *Tanúsítvány*okban.

- Kulcshasználat (Key Usage) – kritikus
OID: 2.5.29.15
A kulcs engedélyezett használati körének meghatározása.
A *Weboldal-hitelesítő tanúsítvány*okban kötelezően beállítandó és kizárólagosan megadandó érték:
 - "digitalSignature" és
 - RSA esetében "keyEncipherment",
 - ECC esetében "keyAgreement".Ugynevezek az értékek szerepelnek a Szerver autentikációs *Tanúsítvány*okban is, mint pl. a CISCO VPN szerver, domén kontroller, SCEP szerver, VPN szerver autentikációs *Tanúsítvány*.
- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus
OID: 2.5.29.37
A kulcs engedélyezett használati körének további meghatározása.
A *Weboldal-hitelesítő tanúsítvány*okban kötelezően beállítandó érték:
 - "serverAuth (1.3.6.1.5.5.7.3.1)"A *Weboldal-hitelesítő tanúsítvány*okban feltüntethető további érték:
 - "clientAuth (1.3.6.1.5.5.7.3.2)"
- CRL szétosztási pont (CRL Distribution Points) – nem kritikus
OID: 2.5.29.31
A mező tartalmazza a Tanúsítvánnyal kapcsolatban releváns CRL elérhetőségét http és/vagy LDAP protokollon keresztül.
Kitöltése opcionális.
- Szolgáltatói információ elérése (Authority Information Access) – nem kritikus
OID: 1.3.6.1.5.5.7.1.1
A *Hitelesítés-szolgáltató* által rendelkezésre bocsátott, a *Tanúsítvány* használatához kapcsolódó egyéb szolgáltatásainak leírása.
Végfelhasználói *Tanúsítvány*ok esetében kötelező a kitöltése, és a mező tartalmazza a következő adatokat:
 - A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást kell nyújtson. Ennek elérhetőségét kell itt szerepeltetni.
 - A tanúsítványlánc felépítésének megkönnyítésére a *Hitelesítés-szolgáltató* adja meg a *Tanúsítvány* kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.A mezőben a *Hitelesítés-szolgáltató* több szolgáltatás illetve hitelesítési egység *Tanúsítvány* elérhetőségi adatait is megadhatja.

- Minősített tanúsítvánnyal kapcsolatos állítások (Qualified Certificate Statements) – nem kritikus
OID: 1.3.6.1.5.5.7.1.3
A mező a minősített *Tanúsítvány*okkal kapcsolatos állítások jelzésére szolgál, azonban van olyan mezője is, amely a nem minősített *Tanúsítvány* esetében is használható.
Kizárólag a QCType mező használata engedélyezett.
- Beágyazott aláírt tanúsítványok időbélyegzőinek listája - nem kritikus
OID: 1.3.6.1.4.1.11129.2.4.2
A mező a Certificate Transparency naplószolgáltatók által aláírt SCT-eket tartalmazza.
Kitöltése opcionális és az *Igénylő* engedélyéhez kötött.

Más tanúsítvány kiterjesztés nem kerülhet kitöltésre.

7.1.3. Az algoritmus objektum azonosítója

Annak a kriptográfiai algoritmusnak a megnevezése, amellyel a *Tanúsítvány* hitelesítésre került. Csak olyan aláíró algoritmus használható, amely megfelel a 6.1.5 fejezetben meghatározott követelményeknek.

A *Hitelesítés-szolgáltató* által használható kriptográfiai algoritmusokat a *Szolgáltatási szabályzatban* fel kell sorolni.

7.1.4. Névformák

A *Hitelesítés-szolgáltató* a jelen *Hitelesítési rendek* alapján kibocsátott *Tanúsítvány*okban egy – az IETF RFC 5280 szabványban [26] illetve az ETSI EN 319 412-2, -3, -4 szabványokban [14], [15], [16] meghatározott attribútumokból összeállított – megkülönböztetett nevet kell használnon az *Alany* azonosítására.

A *Tanúsítvány*nak tartalmaznia kell az *Alany* szolgáltatói egyedi azonosítóját is a 3.1.1. fejezetben meghatározottak szerint kitöltve.

A *Tanúsítvány* "Issuer DN" mezőjében szereplő értéknek meg kell egyeznie a kibocsátó *Tanúsítvány*ának "Subject DN" mezőjében szereplő értékkel.

7.1.5. Névhasználati megkötöttségek

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

7.1.6. A Hitelesítési rend objektum azonosítója

A *Hitelesítés-szolgáltató*nak a jelen *Hitelesítési rendek* alapján kibocsátott *Tanúsítvány*okba fel kell vennie a nem kritikus (Hitelesítési Rend) kiterjesztést a 7.1.2. fejezet előírásai szerint.

7.1.7. A Hitelesítési rend megkötöttségek kiterjesztés használata

Nincs előírás.

7.1.8. A Hitelesítési rend jellemzők szintaktikája és szemantikája

A *Hitelesítés-szolgáltató* a Hitelesítési rend (Certificate Policy) kiterjesztés Irányelv minősítő (Policy Qualifier) mezőjében rövid információt helyezhet el a *Tanúsítvány* felhasználhatóságával kapcsolatban. A mezőnek tartalmaznia kell a *Szolgáltatási szabályzat* online elérhetőségét (URI).

7.1.9. A kritikus Hitelesítési rend kiterjesztések feldolgozási szemantikája

Nincs megkötés.

7.2. Tanúsítvány visszavonási lista (CRL) profil

7.2.1. Verziószám(ok)

A *Hitelesítés-szolgáltató* az IETF RFC 5280 [26] specifikáció szerinti "v2" verziójú *Tanúsítvány visszavonási listákat* bocsásson ki.

7.2.2. Tanúsítvány visszavonási lista kiterjesztések

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

- Verzió (Version)
A mező értéke kötelezően "1".
- Algoritmus azonosító (Signature Algorithm Identifier)
A *Tanúsítvány visszavonási listát* hitelesítő elektronikus aláírás vagy bélyegző készítéséhez használt kriptográfiai algoritmuskészlet azonosítója (OID). A minimálisan támogatandó algoritmuskészletek:
 - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
 - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
- Aláírás (Signature)
A *Hitelesítés-szolgáltató* visszavonási listát hitelesítő elektronikus aláírása vagy bélyegzője. A *Tanúsítvány visszavonási listát* az adott hitelesítő egység a *Tanúsítványok* aláírására vagy bélyegzésére használt kulcsával kell hitelesítse.
- Kibocsátó (Issuer)
A *Tanúsítvány visszavonási listát* kibocsátó hitelesítő egység egyedi azonosítója.
- Hatálybalépés (thisUpdate)
A *Tanúsítvány visszavonási lista* hatálybalépésének kezdete. UTC szerinti érték az IETF RFC 5280 [26] szerinti kódolással.
- Következő kibocsátás (nextUpdate)
A következő *Tanúsítvány visszavonási lista* kibocsátásának ideje (lásd: 4.10. fejezet). UTC szerinti érték az IETF RFC 5280 [26] szerinti kódolással.

- *Visszavont Tanúsítványok (Revoked Certificates)*

A visszavont *Tanúsítványok* listája a *Tanúsítvány* sorozatszámával és a visszavonás idejével.

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

- CRL sorozatszám (CRL number) – nem kritikus
OID: 2.5.29.20
Ebbe a mezőbe a *Tanúsítvány visszavonási listák* egyesével növekvő sorozatszámai kerüljenek.

A *Hitelesítés-szolgáltató* által feltételesen használható *Tanúsítvány visszavonási lista* kiterjesztés:

- expiredCertsOnCRL – nem kritikus
OID: 2.5.29.60
A *Hitelesítés-szolgáltató* az X.509 specifikáció szerinti szabványos jelöléssel jelezze, ha a lejárt *Tanúsítványok*at nem távolítja el a CRL-ről. (Lásd: 4.10. fejezet.)

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

- Visszavonás oka (Reason Code) – nem kritikus
OID: 2.5.29.21
Ebbe a mezőbe a visszavonás oka kerülhet.
- Érvénytelenség ideje (Invalidity Date) – nem kritikus
Ebbe a mezőbe a magánkulcs megbízhatatlanná válásának ideje kerülhet.
- Útmutató a felfüggesztett *Tanúsítványok*hoz (Hold Instruction) – nem kritikus
Ebbe a mezőbe a felfüggesztett *Tanúsítvány* kezelése kerülhet.

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

7.3. Online tanúsítvány-állapot válasz (OCSP) profil

A *Hitelesítés-szolgáltató*nak az IETF RFC 6960 [30] szerinti online tanúsítvány-állapot szolgáltatást kell üzemeltetnie.

A *Hitelesítés-szolgáltató* által kibocsátott OCSP válaszok az alábbi mezőket tartalmazzák:

- Algoritmus azonosító (signatureAlgorithm)
Az OCSP választ hitelesítő digitális aláírás készítéséhez használt algoritmuskészlet azonosítója (OID). A minimálisan támogatandó algoritmuskészletek:
 - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
 - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
- Aláírás (Signature)
A *Hitelesítés-szolgáltató* OCSP választ hitelesítő digitális aláírása.

- Válaszadó azonosítója (responderID)
Az OCSP választ kibocsátó hitelesítő egység egyedi azonosítója.
- Hatálybalépés (thisUpdate)
Az OCSP válasz hatálybalépésének ideje. UTC szerinti érték az IETF RFC 5280 [26] szerinti kódolással.
- Következő kibocsátás (nextUpdate)
A következő OCSP válasz kibocsátásának legkésőbbi ideje. UTC szerinti érték az IETF RFC 5280 [26] szerinti kódolással.
Kötelezően kitöltendő.
- *Tanúsítvány* állapot válasz (SingleResponse)
A válasz tartalmazza a *Tanúsítvány* azonosítóját (CertID) és a *Tanúsítvány* visszavonási állapotát (CertStatus).
A *Hitelesítés-szolgáltató* a CABF BR követelményeinek megfelelő pozitív OCSP választ nyújt, vagyis a válasz csak akkor tartalmazza a "good" értéket, ha az adott *Tanúsítvány* megtalálható a *Hitelesítés-szolgáltató Tanúsítványtárában* és nincs visszavont állapotban.

7.3.1. Verziószám(ok)

A *Hitelesítés-szolgáltató*nak támogatnia kell az IETF RFC 6960 [30] szerinti "v1" verziójú online tanúsítvány-állapot kéréseket és válaszokat.

7.3.2. OCSP kiterjesztések

A *Hitelesítés-szolgáltató* által feltételeesen használható OCSP kiterjesztés:

- ArchiveCutoff – nem kritikus
A *Hitelesítés-szolgáltató* az IETF RFC 6960 [30] specifikáció szerinti szabványos jelöléssel jelezheti, ha a lejárt *Tanúsítványokra* is szolgálat visszavonási állapot információt. (Lásd: 4.10. fejezet.)

A *Hitelesítés-szolgáltató* által használható OCSP bejegyzési kiterjesztések:

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

8. A megfelelés vizsgálat

A *Hitelesítés-szolgáltató* működését rendszeres időközönként vizsgálta meg külső független auditorral. Az átvizsgálás során meg kell vizsgálni, hogy a *Hitelesítés-szolgáltató* működése megfelel-e az alábbi normatív dokumentumoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [11]
- ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [12]

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

A megfelelőségértékelési jelentés alapján kiállított megfelelőségi tanúsítványt közzé kell tenni a *Hitelesítés-szolgáltató* honlapján.

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

8.1. Az ellenőrzések körülményei és gyakorisága

A *Hitelesítés-szolgáltató* évente köteles elvégeztetni a megfelelőségértékelő vizsgálatot.

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

Negyedévente szűrőpróbaszerűen ellenőrizni kell az előző ellenőrzés óta kibocsátott *Weboldal-hitelesítő tanúsítványok* legalább 3% -át, hogy megfelelnek-e a vonatkozó *Hitelesítési rend(ek)*nek és *Szolgáltatási szabályzat*nak.

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

Más szervezet hitelesítési egysége számára kibocsátott szolgáltatói *Tanúsítvány* esetében a külső hitelesítési egység működését évente auditálni kell.

8.2. Az auditor és szükséges képesítése

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

Az eIDAS és ETSI követelményeknek való megfelelőséget igazoló vizsgálatot olyan szervezet végzi el, amely rendelkezik egy EU tagállam nemzeti akkreditációs szervezete által kiadott erre feljogosító felhatalmazással.

8.3. Az auditor és az auditált rendszer elem függetlensége

A külső auditot csak olyan személy végezheti:

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

8.4. Az auditálás által lefedett területek

Az átvizsgálásnak le kell fednie minimálisan az alábbi területeket:

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

Amennyiben a *Hitelesítés-szolgáltató* külső *Regisztráló szervezettel* együttműködik, illetve ha bocsátott ki más szervezet hitelesítési egysége számára szolgáltatói *Tanúsítványt*, akkor a felsorolt területeket ezeknél a külső szervezeteknél is meg kell vizsgálni.

8.5. A hiányosságok kezelése

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

- opcionálisan figyelembe vehető módosítási javaslatokat;
- kötelezően elhárítandó eltéréseket.

8.6. Az eredmények közzététele

A *Hitelesítés-szolgáltató* a vizsgálat eredményét összefoglaló jelentést köteles nyilvánosságra hozni. Nem köteles a független rendszervizsgálat során feltárt hiányosságok publikálására, azokat bizalmas információként kezelheti.

9. Egyéb üzleti és jogi kérdések

9.1. Díjak

A *Hitelesítés-szolgáltató* által alkalmazható díjakat a vonatkozó szabályozásnak megfelelően nyilvánosan közzé kell tenni.

9.1.1. Tanúsítvány kibocsátás és megújítás díjai

A *Hitelesítés-szolgáltató* díjat állapíthat meg a *Tanúsítványok* kibocsátásával, megújításával, módosításával és a kulcsцерével kapcsolatos tevékenységéért.

9.1.2. Tanúsítvány hozzáférés díja

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

9.1.3. Visszavonási állapot információ hozzáférés díja

A *Hitelesítés-szolgáltató* ingyenesen köteles az *Érintett felek* részére online CRL és OCSP információt szolgáltatni a kibocsátott *Tanúsítványok* visszavonási állapotáról.

9.1.4. Egyéb szolgáltatások díjai

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

9.1.5. Visszatérítési politika

Nincs megkötés.

9.2. Anyagi felelősségvállalás

A *Hitelesítés-szolgáltató* megbízhatósága érdekében anyagi felelősséget vállal a jelen *Hitelesítési rendben*, a vonatkozó *Szolgáltatási szabályzatban* valamint az *Ügyféllel* kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért.

9.2.1. Pénzügyi követelmények

Nincs megkötés.

9.2.2. További követelmények

Nincs megkötés.

9.2.3. Felelősségbiztosítás

- A *Hitelesítés-szolgáltató*nak a megbízhatóság biztosítása érdekében felelősségbiztosítással kell rendelkeznie.
- A felelősségbiztosítási szerződésnek ki kell terjednie az alábbi, a *Hitelesítés-szolgáltató* által a szolgáltatások nyújtásával összefüggésben okozott károkra:
 - a bizalmi szolgáltatási *Ügyfél*nek a Szolgáltatási szerződés megszegésével összefüggésben okozott károkra;
 - a bizalmi szolgáltatási *Ügyfél*nek és harmadik személynek szerződésen kívüli okozott károkra;
 - a Nemzeti Média- és Hírközlési Hatóságnak a bizalmi szolgáltatási tevékenységet befejező *Hitelesítés-szolgáltató* által okozott költségekre;
 - az eIDAS Rendelet [1] 17. cikk (4) bekezdés e) pontja alapján a Nemzeti Média- és Hírközlési Hatóság által felkért megfelelőségértékelő szervek eljárásának költségeire, ha azt a Nemzeti Média- és Hírközlési Hatóság eljárási költségként érvényesíti.
- A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként legalább 3.000.000 forint. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.
- A felelősségbiztosításnak a meghatározott összeg erejéig fedezetet kell nyújtania a károsultnak a szolgáltató károkozó magatartásával összefüggésben keletkező teljes kárára, függetlenül attól, hogy a kárt szerződésszegéssel vagy szerződésen kívül okozták.
- Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

9.3. Bizalmasság

A *Hitelesítés-szolgáltató*nak az *Ügyfelek* adatait a jogszabályoknak megfelelően kell kezelnie.

9.3.1. Bizalmas információk köre

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

9.3.2. Bizalmas információk körén kívül eső adatok

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

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

9.3.3. Bizalmas információ védelme

A *Hitelesítés-szolgáltató* felelősséggel tartozik az általa kezelt bizalmas adatok védelméért.

A *Hitelesítés-szolgáltató* szerződésben vagy titoktartási nyilatkozat aláírásával kell kötelezze alkalmazottait, alvállalkozóit, szerződött partnereit a bizalmas adatok védelmére.

A *Hitelesítés-szolgáltató Szolgáltatási szabályzatában* tételesen meg kell határozni azon eseteket, amikor a *Hitelesítés-szolgáltató* felfedheti a bizalmas adatokat.

Ilyen esetek például:

- kötelező információszolgáltatás a hatóságok részére,
- információszolgáltatás polgári eljárás keretében,
- az érintett kérésére történő adatszolgáltatás.

9.4. Személyes adatok védelme

A *Hitelesítés-szolgáltatónak* gondoskodnia kell az általa kezelt személyes adatok védelméről. Működésének és szabályzatainak meg kell felelniük az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [5] és a 2016/679 EU általános adatvédelmi rendelet [2] rendelkezéseinek.

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

- megőrizni,
- azokat a megőrzési kötelezettség lejártával – amennyiben az *Ügyfél* erről másképpen nem rendelkezik – az ügyfél adatbázisból törölni.

9.4.1. Adatkezelési terv

A *Hitelesítés-szolgáltatónak* rendelkeznie kell Adatkezelési Szabályzattal, amely részletes előírásokat tartalmaz a személyes adatok kezelésére. Az Adatkezelési Szabályzatot nyilvánosságra kell hozni a *Hitelesítés-szolgáltató* honlapján.

9.4.2. Személyes adatok

A *Hitelesítés-szolgáltatónak* védenie kell az érintettel kapcsolatba hozható, vagy az érintettre vonatkozó következtetést tartalmazó minden olyan személyes adatot, amely nem érhető el nyilvánosan a *Tanúsítványból* vagy más nyilvános adatforrásból.

9.4.3. Személyes adatnak nem minősülő adatok

A *Hitelesítés-szolgáltató* az *Igénylő* írásbeli hozzájárulása alapján nyilvánosságra hozhatja az *Alanyok Tanúsítványban* szereplő adatait.

A *Tanúsítványban* a *Hitelesítés-szolgáltató* feltünteti az *Alanyhoz* rendelt szolgáltatói egyedi azonosítót.

9.4.4. Személyes adatok védelme

A *Hitelesítés-szolgáltató* köteles biztonságosan tárolni és védeni a *Tanúsítvány* kiadással kapcsolatos és a *Tanúsítványban* nem szereplő személyes adatokat. Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, valamint nyilvánosságra hozatal ellen.

9.4.5. Személyes adatok felhasználása

A *Hitelesítés-szolgáltató* csak a *Tanúsítványokban* szereplő személyes adatokat hozhatja nyilvánosságra az *Ügyfél* írásbeli engedélyének birtokában.

9.4.6. Adatkezelés

A *Hitelesítés-szolgáltató* az *Ügyfél* értesítése nélkül is kiadhatja az *Ügyfélről* tárolt személyes adatokat a vonatkozó jogszabályok által meghatározott esetekben.

9.4.7. Egyéb adatvédelmi követelmények

Nincs előírás.

9.5. Szellemi tulajdonjogok

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

A *Hitelesítés-szolgáltató* által ügyfelei részére kibocsátott magán- és nyilvános kulcs tulajdonosa az *Előfizető*, teljes jogú felhasználója pedig az *Igénylő*, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

A *Hitelesítés-szolgáltató* által ügyfelei részére kibocsátott *Tanúsítvány* tulajdonosa a *Hitelesítés-szolgáltató*, a *Tanúsítványok* teljes jogú felhasználója pedig az *Előfizető*.

A *Hitelesítés-szolgáltató* az általa kibocsátott végfelhasználói *Tanúsítványokat* a benne szereplő nyilvános kulccsal együtt a kikötéseiben és feltételeiben ismertetett módon közzéteheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti.

A *Hitelesítés-szolgáltató* tulajdonát képezi a tanúsítvány visszavonási állapot információ, amit a *Hitelesítés-szolgáltató* nyilvánosságra hozhat a 7.2. és 7.3. alfejezetekben meghatározott módon.

A *Hitelesítés-szolgáltató* által az *Ügyfelek* részére kibocsátott szolgáltatói egyedi azonosító a *Hitelesítés-szolgáltató* tulajdonát képezi, amit a *Hitelesítés-szolgáltató* nyilvánosságra hozhat a *Tanúsítvány* részeként.

A *Tanúsítványban* szereplő azonosító (amely a *Tanúsítvány* alanyát azonosítja) használatára az *Ügyfél* jogosult.

A jelen *Hitelesítési rend* a *Hitelesítés-szolgáltató* kizárólagos tulajdonát képezi. Az *Ügyfelek* és egyéb *Érintett felek* a dokumentumot csak a jelen *Hitelesítési rend* előírásainak megfelelően jogosultak felhasználni, minden egyéb kereskedelmi vagy egyéb célú felhasználás szigorúan tilos.

A jelen *Hitelesítési rend* szabadon terjeszthető, de csak változatlan formában, teljes terjedelemben és az eredet feltüntetésével.

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

9.6. Tevékenységért viselt felelősség és helytállás

9.6.1. A szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

A *Hitelesítés-szolgáltató* felel a jelen *Hitelesítési rendben*, a vonatkozó *Szolgáltatási szabályzatban* valamint az *Ügyféllel* kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért, különösen a következő esetekben:

- a *Hitelesítés-szolgáltató* felelősséget vállal azért, hogy megfelelő eljárásokkal ellenőrizte, hogy az *Igénylő* jogosult a *Tanúsítványban* feltüntetett domén nevek és IP címek használatára, vagy azok felett a gyakorlatban ellenőrzéssel bír;
- a *Hitelesítés-szolgáltató* felelősséget vállal az általa támogatott *Hitelesítési rend(ek)*ben leírt eljárásoknak való megfelelésért;
- a *Hitelesítés-szolgáltató* sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- a *Hitelesítés-szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfelekkel* szemben a Polgári Törvénykönyv [6] 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 [6] általános felelősségi szabálya szerint felelős;
- a *Hitelesítés-szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyféllel* megkötött Szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 9.8. fejezet);

A Szolgáltató kötelezettsége

A *Hitelesítés-szolgáltató* alapvető kötelezettsége, hogy a szolgáltatásokat a *Hitelesítési renddel*, a *Szolgáltatási szabályzattal* és egyéb nyilvános szabályzatokkal, a szerződéses feltételekkel, továbbá a vállalati és biztonsági belső szabályzatokkal összhangban nyújtsa. Ezen alapvető kötelezettségek a következők:

- a szolgáltatásnak megfelelő jogi-, szabályozási-, anyagi-, szerződéses stb. keretek megteremtése;
- magas színvonalú és biztonságos szolgáltatások nyújtása a vonatkozó szabályzatok szerint;
- a szolgáltatásokhoz kapcsolódó szervezetek (hitelesítő szervezet, ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése;

- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése;
- a szolgáltatások biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket;
- a publikus nyilvántartások és saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az interneten keresztül.

A hitelesítő szervezet felelőssége

A hitelesítő szervezet feladata a hitelesítő egységek, valamint az online tanúsítvány-állapot szolgáltatáshoz szükséges egységek (lásd: 1.3.1) felállítása és működtetése, a tanúsítványtár és a visszavonási-állapot információ gondozása, valamint a szabályzatok menedzselése.

A hitelesítő szervezet belső működtetését a *Hitelesítés-szolgáltató* belső, operatív szabályzatai határozzák meg. A hitelesítő egységek által kibocsátott szolgáltatói tanúsítványok kezelése (például regisztrációs munkatársak, ügyeletesek számára) az operatív szabályzatok előírásainak megfelelően történik. Jelen szabályzat csak a nyilvános szolgáltatói és végfelhasználói tanúsítványokkal kapcsolatban tartalmaz előírásokat.

A szabályzatok menedzselése keretében ellátandó feladatok:

- az alkalmazott tanúsítványfajták specifikálása, jóváhagyása és karbantartása;
- a szolgáltatások nyilvános szabályzatainak és a belső (nem nyilvános) előírásoknak előkészítése, egyeztetése a jogszabályokkal és a belső (nem nyilvános) szabályzatokkal, továbbá az aktualizálások elvégzése;
- a szolgáltatásokra vonatkozó szabályzatokkal kapcsolatos észrevételek rögzítése és javaslatok elbírálása.

Az e-Szignó Hitelesítés Szolgáltató felelős:

- az általa kibocsátott *Tanúsítványok* hitelességéért, pontosságáért;
- az általa kibocsátott szabályzatokért, azok jogszabályi megfeleléséért és betartásáért;
- az általa generált kulcspárok megfeleléséért, a magánkulcs-nyilvános kulcs és a *Tanúsítvány* összetartozásáért;
- általában a kötelezettségei betartásáért.

9.6.2. A regisztráló szervezet felelőssége és helytállása

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

A *Regisztráló* szervezet felelőssége:

- az *Igénylő* személyazonosságának megállapítása;

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

9.6.3. Az Ügyfél felelőssége és helyállása

Az *Előfizető* felelőssége

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

Az *Előfizető* kötelezettségei

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

Az *Előfizető* kötelezettségeit a jelen *Hitelesítési rend*, a Szolgáltatási szerződés és annak mellékletei – különösen az Általános Szerződési Feltételek – és a *Szolgáltatási szabályzat* írja le.

Az *Igénylő* felelőssége

Az *Igénylő* felelős:

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

Az Igénylő kötelezettségei

Az *Igénylő* köteles:

- a szolgáltatás igénybevétele előtt megismerni a jelen *Hitelesítési rendet* és a *Szolgáltatási szabályzatot*;
- a *Hitelesítés-szolgáltató* által kért, a szolgáltatás igénybevételéhez szükséges adatokat hiánytalanul megadni, a valóságnak megfelelő adatokat szolgáltatni;
- amennyiben az *Igénylő* tudomására jut, hogy az általa megadott, a szolgáltatás igénybevételéhez szükséges adat – különösen valamely *Tanúsítványban* is szereplő adat – megváltozott, haladéktalanul köteles:
 - erről írásban értesíteni a *Hitelesítés-szolgáltatót*,
 - kérni a *Tanúsítvány* visszavonását és
 - megszüntetni a *Tanúsítvány* használatát;
- amennyiben az *Igénylő* tudomására jut, hogy az általa igényelt *Tanúsítványt* visszavonták, vagy a kibocsátó CA magánkulcsa kompromittálódott, haladéktalanul köteles megszüntetni a *Tanúsítvány* használatát;
- a szolgáltatást kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a hivatkozott szabályzatokban és dokumentumokban foglaltaknak megfelelően használni;
- a *Weboldal-hitelesítő tanúsítványt* kizárólag olyan szerverre telepíteni, amely a *Tanúsítványban* szereplő doménnéven vagy IP címen elérhető;
- biztosítani, hogy a szolgáltatás igénybevételéhez szükséges adatokhoz és eszközökhöz (jelszavakhoz, titkos kódokhoz, aláírás-létrehozó eszközökhöz) illetéktelen személyek ne férhessenek hozzá;
- a *Hitelesítés-szolgáltatót* haladéktalanul írásban értesíteni, amennyiben valamely *Tanúsítvánnyal* kapcsolatban jogvita indul;
- a *Tanúsítvány* kiadásához szükséges adatok ellenőrzése érdekében a *Hitelesítés-szolgáltatóval* együttműködni és mindent megtenni azért, hogy az ellenőrzés a lehető leghamarabb befejeződhessen;
- kulcs kompromittálódás vagy nem jogszerű használat gyanújának felmerülése esetében a *Hitelesítés-szolgáltató* megkereséseire az *Igénylő* köteles a *Hitelesítés-szolgáltató* által megadott időn belül reagálni;
- tudomásul venni, hogy az *Előfizető* jogosult a *Tanúsítvány* visszavonását kérni;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a *Tanúsítványt* a *Szolgáltatási szabályzatban* leírt meghatározott módon, az ott leírt ellenőrzési lépések elvégzése után bocsátja ki;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítványokban* kizárólag a valóságnak megfelelő adatokat szerepeltet. Ennek megfelelően a *Hitelesítés-szolgáltató* a *Tanúsítványba* kerülő adatokat a *Szolgáltatási szabályzat* szerint ellenőrzi;

- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítványt* visszavonja, amennyiben tudomására jut, hogy a *Tanúsítványban* foglalt adatok nem felelnek meg a valóságnak, vagy a magánkulcs nem az *Igénylő* kizárólagos birtokában vagy használatában van, és ebben az esetben az *Igénylő* köteles a *Tanúsítvány* használatát beszüntetni;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* jogosult a *Tanúsítványt* visszavonni, amennyiben az *Előfizető* nem fizeti meg határidőre a szolgáltatások díját;
- *Szervezeti tanúsítvány* igénylése esetén köteles tudomásul venni, hogy a *Hitelesítés-szolgáltató* a *Tanúsítványt* 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 *Tanúsítványt* visszavonni, amennyiben az *Előfizető* megszegi a Szolgáltatási szerződést vagy a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* illegális tevékenységhez használták.

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

9.6.4. Az Érintett fél felelőssége

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

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

9.6.5. Egyéb szereplők tevékenységéért viselt felelősség és helyállás

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

9.7. Helytállás érvénytelenségi köre

A *Hitelesítés-szolgáltató* kizárja felelősségét, amennyiben:

- az *Igénylők* nem tartják be a magánkulcs kezelésével kapcsolatos előírásokat;
- az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozat által elfogadott kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8. A felelősség korlátozása

A *Hitelesítés-szolgáltató* korlátozhatja a kártérítési felelősségét.

9.9. Kártérítési kötelezettség

9.9.1. A szolgáltató kártérítési kötelezettsége

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

9.9.2. Az előfizető kártérítési kötelezettsége

A *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzatban* és a Szolgáltatási szerződésben szabályozza az *Előfizetőkkel* szemben támasztott kártérítési igényeit.

9.9.3. Az érintett felek kártérítési kötelezettsége

A *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzatban* szabályozza az *Érintett felekkel* szemben támasztott kártérítési igényeit.

9.10. Érvényesség és megszűnés

9.10.1. Érvényesség

A *Hitelesítési rend* adott verziója hatálybalépésének napja a dokumentum címlapján kerül meghatározásra.

9.10.2. Megszűnés

A *Hitelesítési rend* visszavonásig illetve a *Hitelesítési rend* újabb verziójának hatályba lépéséig hatályos időbeli korlátozás nélkül.

9.10.3. A megszűnés következményei

A *Hitelesítési rend* visszavonása esetén a *Hitelesítés-szolgáltató* honlapján közzéteszi a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket.

9.11. A felek közötti kommunikáció

A *Hitelesítés-szolgáltató* az *Ügyfelekkel* történő kapcsolattartás érdekében működtessen ügyfélszolgálati irodát.

9.12. Módosítások

A *Hitelesítés-szolgáltató* fenntartja magának a jogot, hogy a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén szabályozott módon megváltoztassa a *Hitelesítési rendet*.

9.12.1. Módosítási eljárás

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

Hitelesítés-szolgáltató a jóváhagyott dokumentumot a tervezett hatálybalépés előtt publikálja honlapján.

9.12.2. Értesítések módja és határideje

A *Hitelesítés-szolgáltató* a 9.12.1. pontban leírtak szerint értesíti az *Érintett feleket* az új dokumentum verziók kibocsátásáról.

9.12.3. Az OID megváltoztatása

A *Hitelesítés-szolgáltató* a *Hitelesítési rend* legkisebb változtatása esetén is új verziószámot ad ki, ami része a dokumentum azonosítónak (OID), így a dokumentum minden változása az OID változását eredményezi, vagyis két eltérő tartalmú – hatályba léptetett – dokumentumnak nem lehet azonos OID azonosítója.

9.13. Vitás kérdések rendezése

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

9.14. Irányadó jog

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

9.15. Az érvényben lévő jogszabályoknak való megfelelés

A jelen *Hitelesítési rend* megfelel az alábbi jogszabályoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [5];
- 2013. évi V. törvény a Polgári Törvénykönyvről [6].
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól [7];
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről [8];
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről [9];
- 470/2017. (XII. 28.) Kormányrendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről [10];

9.16. Vegyes rendelkezések

9.16.1. Teljességi záradék

Nincs megkötés.

9.16.2. Átruházás

A jelen *Hitelesítési rend*nek megfelelően működő szolgáltatók csak a *Hitelesítés-szolgáltató* előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3. Részleges érvénytelenség

A jelen *Hitelesítési rend* egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4. Igényérvényesítés

A *Hitelesítés-szolgáltató* kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben a *Hitelesítés-szolgáltató* egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben vagy a jelen *Hitelesítési rend* más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5. Vis maior

A *Hitelesítés-szolgáltató* nem felelős a *Hitelesítési rendben* és a *Szolgáltatási szabályzatban* megfogalmazott kötelezettség hibás vagy késedelmes teljesítéséért, illetve nem teljesítéséért, amennyiben a hiba vagy késedelem oka a *Hitelesítés-szolgáltató* ellenőrzési körén kívül eső, előre nem látható elháríthatatlan külső ok.

9.17. Egyéb rendelkezések

Nincs megkötés.

A. A rövid hitelesítési rend azonosítók képzési szabályai

A *Hitelesítés-szolgáltató* az egyszerűbb kezelhetőség érdekében minden *Hitelesítési rend*hez rendel egy öt karakteres rövid nevet (azonosítót), amelyben az egyes karakterek meghatározzák az adott rend egyes paramétereit az alábbi szabályok szerint:

- Az első karakter [?....]
 - M: minősített *Tanúsítvány Hitelesítési rend*
 - H: nem minősített, III. hitelesítési osztályú *Tanúsítvány Hitelesítési rend*
 - K: nem minősített, II. hitelesítési osztályú *Tanúsítvány Hitelesítési rend*
 - A: nem minősített, automatikus kibocsátású *Tanúsítvány Hitelesítési rend*
- A második karakter [.?...]
 - A: Aláírás célú *Tanúsítvány Hitelesítési rend*
 - B: Bélyegző létrehozása célú *Tanúsítvány Hitelesítési rend*
 - W: *Weboldal-hitelesítő tanúsítvány Hitelesítési rend*
 - K: *Kódalíró tanúsítvány Hitelesítési rend*
 - E: Egyéb célú *Tanúsítvány Hitelesítési rend*
- A harmadik karakter [..?..]
 - T: természetes személynek kibocsátott *Tanúsítvány Hitelesítési rend*
 - J: jogi személynek kibocsátott *Tanúsítvány Hitelesítési rend*
 - x: nincs megkötés, tetszőleges *Alany* részére kiadható
- A negyedik karakter [...?..]
 - B: *HSM* eszközön kibocsátott *Tanúsítvány Hitelesítési rend*
 - H: *Hardver kriptográfiai* eszközön kibocsátott *Tanúsítvány Hitelesítési rend*
 - S: Szoftveresen kibocsátott *Tanúsítvány Hitelesítési rend*
 - x: nincs megkötés, tetszőleges hordozón kiadható
- Az ötödik karakter [....?]
 - A: álneves *Tanúsítvány Hitelesítési rend*
 - N: álnevet kizáró *Tanúsítvány Hitelesítési rend*

B. Hivatkozások

- [1] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről .
- [2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) .
- [3] 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról .
- [4] 2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról .
- [5] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról .
- [6] 2013. évi V. törvény a Polgári Törvénykönyvről .
- [7] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól .
- [8] 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről .
- [9] 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről .
- [10] 470/2017. (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről .
- [11] ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- [12] ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- [13] ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- [14] ETSI EN 319 412-2 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
- [15] ETSI EN 319 412-3 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- [16] ETSI EN 319 412-4 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.

-
- [17] ETSI TS 119 312 V1.3.1 (2019-02); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- [18] CEN 419 221-5; Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.
- [19] ISO 3166-1:2013, Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.
- [20] MSZ/ISO/IEC 15408-2002, Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai, 2002 december .
- [21] ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules.
- [22] IETF RFC 3490: Internationalizing Domain Names in Applications (IDNA), March 2003.
- [23] IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.
- [24] IETF RFC 3966: The tel URI for Telephone Numbers, December 2004.
- [25] IETF RFC 4043: Internet X.509 Public Key Infrastructure - Permanent Identifier, May 2005.
- [26] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.
- [27] IETF RFC 6532: Internationalized Email Headers, February 2012.
- [28] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.
- [29] IETF RFC 6844: DNS Certification Authority Authorization (CAA) Resource Record, January 2013.
- [30] IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.
- [31] IETF RFC 6962: Certificate Transparency, June 2013.
- [32] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
- [33] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.7.0. CA/Browser Forum, <https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.7.0.pdf>, 2020.
- [34] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.
- [35] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.
- [36] e-Szignó Hitelesítés Szolgáltató - Általános Szerződési Feltételek .