

e-Szignó Hitelesítés Szolgáltató

**eIDAS rendelet szerinti
weboldal-hitelesítő tanúsítvány
hitelesítési rendek**

ver. 2.0

Hatályba lépés: 2016-07-01



Azonosító	1.3.6.1.4.1.21528.2.1.1.59.2.0 , 1.3.6.1.4.1.21528.2.1.1.61.2.0 , 1.3.6.1.4.1.21528.2.1.1.62.2.0
Verzió	2.0
Első verzió hatálybalépése	2016-07-01
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2016-05-31
Hatálybalépés dátuma	2016-07-01

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

Verzió	A változás leírása	Hatálybalépés	Készítette
2.0	Új szabályzat az RFC 3647 és az eIDAS követelmények szerint.	2016-07-01	Szabóné Endrődi Csilla, Dr. Szőke Sándor, Réti Kornél

Tartalomjegyzék

1. Bevezetés	12
1.1. Áttekintés	12
1.2. Dokumentum neve és azonosítója	12
1.2.1. Hitelesítési rendek	13
1.2.2. Hatály	15
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	17
1.3.4. Érintett felek	17
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	19
1.6.1. Fogalmak	19
1.6.2. Rövidítések	25
2. Közzététel és tanúsítványtár	25
2.1. Adatbázisok - tanúsítványtárak	25
2.2. A tanúsítványokra vonatkozó információk közzététele	26
2.3. A közzététel időpontja vagy gyakorisága	27
2.3.1. Kikötések és feltételek közzétételi gyakorisága	27
2.3.2. Tanúsítványok nyilvánosságra hozatalának gyakorisága	27
2.3.3. A megváltozott visszavonási állapot közzétételének gyakorisága	27
2.4. A tanúsítványtár elérésének szabályai	28
3. Azonosítás és hitelesítés	28
3.1. Elnevezések	28
3.1.1. Név típusok	28
3.1.2. A nevek értelmezhetősége	31

3.1.3.	Álnevek használata	31
3.1.4.	A különböző elnevezési formák értelmezési szabályai	31
3.1.5.	A nevek egyedisége	32
3.1.6.	Márkanevek elismerése, azonosítása, szerepük	32
3.2.	Kezdeti regisztráció, azonosság hitelesítése	32
3.2.1.	A magánkulcs birtoklásának igazolása	32
3.2.2.	Szervezet és domain azonosságának hitelesítése	32
3.2.3.	Természetes személy azonosságának hitelesítése	33
3.2.4.	Nem ellenőrzött alany információk	35
3.2.5.	Jogok, felhatalmazások ellenőrzése	35
3.2.6.	Együttműködési képességre vonatkozó követelmények	35
3.3.	Azonosítás és hitelesítés kulcscsere kérelem esetén	35
3.3.1.	Azonosítás és hitelesítés érvényes tanúsítvány esetén	36
3.3.2.	Azonosítás és hitelesítés érvénytelen tanúsítvány esetén	36
3.4.	Azonosítás és hitelesítés tanúsítvány megújítás esetén	36
3.4.1.	Azonosítás és hitelesítés érvényes tanúsítvány esetén	36
3.4.2.	Azonosítás és hitelesítés érvénytelen tanúsítvány esetén	37
3.5.	Azonosítás és hitelesítés tanúsítvány módosítás esetén	37
3.5.1.	Azonosítás és hitelesítés érvényes tanúsítvány esetén	37
3.5.2.	Azonosítás és hitelesítés érvénytelen tanúsítvány esetén	38
3.6.	Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási kérelem esetén	38
4.	A tanúsítványok életciklusára vonatkozó követelmények	38
4.1.	Tanúsítvány kérelem	38
4.1.1.	Ki nyújthat be tanúsítvány kérelmet	39
4.1.2.	A bejegyzés folyamata és a résztvevők felelőssége	40
4.2.	A tanúsítvány kérelem feldolgozása	40
4.2.1.	Az igénylő azonosítása és hitelesítése	40
4.2.2.	A tanúsítvány kérelem elfogadása vagy visszautasítása	40
4.2.3.	A tanúsítvány kérelem feldolgozásának időtartama	41
4.3.	A tanúsítvány kibocsátása	41
4.3.1.	A Hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során	41
4.3.2.	Az Ügyfél értesítése a tanúsítvány kibocsátásáról	41
4.4.	A tanúsítvány elfogadása	41
4.4.1.	A tanúsítvány elfogadás módja	41
4.4.2.	A tanúsítvány közzététele	41
4.4.3.	További szereplők értesítése a tanúsítvány kibocsátásról	42
4.5.	A kulcspár és a tanúsítvány használata	42
4.5.1.	A magánkulcs és a tanúsítvány használata	42

4.5.2.	Az Érintett felek nyilvános kulcs és tanúsítvány használata	42
4.6.	Tanúsítvány megújítás	42
4.6.1.	A tanúsítvány megújítás körülményei	43
4.6.2.	Ki kérelmezheti a tanúsítvány megújítást	43
4.6.3.	A tanúsítvány megújítási kérelmek feldolgozása	43
4.6.4.	Az Ügyfél értesítése az új tanúsítvány kibocsátásáról	44
4.6.5.	A megújított tanúsítvány elfogadása	44
4.6.6.	A megújított tanúsítvány közzététele	44
4.6.7.	További szereplők értesítése a tanúsítvány kibocsátásáról	44
4.7.	Kulcscsere	44
4.7.1.	A kulcscsere körülményei	44
4.7.2.	Ki kérelmezheti a kulcscserét	44
4.7.3.	A kulcscsere kérelmek feldolgozása	45
4.7.4.	Az Ügyfél értesítése az új tanúsítvány kibocsátásáról	45
4.7.5.	A kulcscserével megújított tanúsítvány elfogadása	45
4.7.6.	A kulcscserével megújított tanúsítvány közzététele	45
4.7.7.	További szereplők értesítése a tanúsítvány kibocsátásáról	45
4.8.	Tanúsítvány módosítás	45
4.8.1.	A tanúsítvány módosítás körülményei	45
4.8.2.	Ki kérelmezheti a tanúsítvány módosítást	46
4.8.3.	A tanúsítvány módosítási kérelmek feldolgozása	46
4.8.4.	Az Ügyfél értesítése az új tanúsítvány kibocsátásáról	47
4.8.5.	A módosított tanúsítvány elfogadása	47
4.8.6.	A módosított tanúsítvány közzététele	47
4.8.7.	További szereplők értesítése a tanúsítvány kibocsátásáról	47
4.9.	Tanúsítvány visszavonás és felfüggesztés	47
4.9.1.	A tanúsítvány visszavonás körülményei	47
4.9.2.	Ki kérelmezheti a visszavonást	50
4.9.3.	A visszavonási kérelemre vonatkozó eljárás	50
4.9.4.	A visszavonási kérelemre vonatkozó kivárási idő	50
4.9.5.	A visszavonási eljárás maximális hossza	51
4.9.6.	Az Érintett felek számára javasolt eljárás a visszavonási információ ellenőrzésére	51
4.9.7.	A visszavonási lista kibocsátás gyakorisága	51
4.9.8.	A visszavonási lista előállítás és közzététele közötti idő maximális hossza	51
4.9.9.	Valós idejű tanúsítvány állapot ellenőrzés lehetősége	51
4.9.10.	A valós idejű tanúsítvány állapot ellenőrzésre vonatkozó követelmények	51
4.9.11.	A visszavonási hirdetmények egyéb elérhető formái	51
4.9.12.	A kulcs kompromittálódásra vonatkozó speciális követelmények	52

4.9.13.	A felfüggesztés körülményei	52
4.9.14.	Ki kérelmezheti a felfüggesztést	52
4.9.15.	A felfüggesztési kérelemre vonatkozó eljárás	52
4.9.16.	A felfüggesztés maximális hossza	52
4.10.	Tanúsítvány állapot szolgáltatások	52
4.10.1.	Működési jellemzők	53
4.10.2.	A szolgáltatás rendelkezésre állása	53
4.10.3.	Opcionális lehetőségek	53
4.11.	Az előfizetés vége	53
4.12.	Magánkulcs letétbe helyezése és visszaállítása	53
4.12.1.	Kulcsletét és visszaállítás rendje és szabályai	53
4.12.2.	Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai	53
5.	Elhelyezési, eljárásbeli és üzemeltetési előírások	54
5.1.	Fizikai követelmények	54
5.1.1.	A telephely elhelyezése és szerkezeti felépítése	54
5.1.2.	Fizikai hozzáférés	54
5.1.3.	Áramellátás és légkondicionálás	55
5.1.4.	Beázás és elárasztódás veszély kezelése	56
5.1.5.	Tűz megelőzés és tűzvédelem	56
5.1.6.	Adathordozók tárolása	56
5.1.7.	Hulladék megsemmisítése	56
5.1.8.	A mentési példányok fizikai elkülönítése	56
5.2.	Eljárásbeli előírások	56
5.2.1.	Bizalmi szerepkörök	57
5.2.2.	Az egyes feladatok ellátásához szükséges személyzeti létszámok	57
5.2.3.	Az egyes szerepkörökben elvárt azonosítás és hitelesítés	58
5.2.4.	Egymást kizáró szerepkörök	58
5.3.	Személyzetre vonatkozó előírások	58
5.3.1.	Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények	59
5.3.2.	Előélet vizsgálatára vonatkozó eljárások	59
5.3.3.	Képzési követelmények	59
5.3.4.	Továbbképzési gyakoriságok és követelmények	60
5.3.5.	Munkabeosztás körforgásának sorrendje és gyakorisága	60
5.3.6.	Felhatalmazás nélküli tevékenységek büntető következményei	60
5.3.7.	Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények	60
5.3.8.	A személyzet számára biztosított dokumentációk	60

5.4.	Naplózási eljárások	61
5.4.1.	A tárolt események típusai	61
5.4.2.	A naplófájl feldolgozásának gyakorisága	64
5.4.3.	A naplófájl megőrzési időtartama	64
5.4.4.	A naplófájl védelme	64
5.4.5.	A naplófájl mentési eljárásai	64
5.4.6.	A naplózás adatgyűjtési rendszere	65
5.4.7.	Az eseményeket kiváltó alanyok értesítése	65
5.4.8.	Sebezhetőség felmérése	65
5.5.	Adatok archiválása	65
5.5.1.	Az archivált adatok típusai	65
5.5.2.	Az archívum megőrzési időtartama	66
5.5.3.	Az archívum védelme	66
5.5.4.	Az archívum mentési folyamatai	66
5.5.5.	Az adatok időbélyegzésére vonatkozó követelmények	67
5.5.6.	Az archívum gyűjtési rendszere	67
5.5.7.	Archív információk hozzáférését és ellenőrzését végző eljárások	67
5.6.	Szolgáltatói kulcs cseréje	67
5.7.	Kompromittálódást és katasztrófát követő helyreállítás	68
5.7.1.	Váratlan esemény és kompromittálódás kezelési eljárások	68
5.7.2.	Meghibásodott IT erőforrások, szoftverek és/vagy adatok	68
5.7.3.	Magánkulcs kompromittálódása esetén követendő eljárások	68
5.7.4.	Működés folyamatosságának biztosítása katasztrófát követően	69
5.8.	A hitelesítés-szolgáltató vagy a regisztráló szervezet leállítása	69
6.	Műszaki biztonsági óvintézkedések	70
6.1.	Kulcspár előállítás és telepítése	70
6.1.1.	Kulcspár előállítás	70
6.1.2.	Magánkulcs eljuttatása az igénylőhöz	71
6.1.3.	A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz	72
6.1.4.	A szolgáltatói nyilvános kulcs közzététele	72
6.1.5.	Kulcsméret	73
6.1.6.	A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése	73
6.1.7.	A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)	73
6.2.	A magánkulcsok védelme	74
6.2.1.	Kriptográfiai modulra vonatkozó szabványok és előírások	74
6.2.2.	Magánkulcs többszereplős (n-ből m) használata	74
6.2.3.	Magánkulcs letétbe helyezése	74

6.2.4.	Magánkulcs mentése	75
6.2.5.	Magánkulcs archiválása	75
6.2.6.	Magánkulcs bejuttatása hardver kriptográfiai eszközbe, vagy onnan történő exportja	75
6.2.7.	Magánkulcs tárolása hardver kriptográfiai eszközben	75
6.2.8.	A magánkulcs aktiválásának módja	75
6.2.9.	A magánkulcs deaktiválásának módja	76
6.2.10.	A magánkulcs megsemmisítésének módja	76
6.2.11.	A hardver kriptográfiai eszközök értékelése	76
6.3.	A kulcspár kezelés egyéb szempontjai	77
6.3.1.	Nyilvános kulcs archiválása	77
6.3.2.	A tanúsítványok és kulcspárok használatának periódusa	77
6.4.	Aktivizáló adatok	78
6.4.1.	Aktivizáló adatok előállítás és telepítése	78
6.4.2.	Az aktivizáló adatok védelme	78
6.4.3.	Az aktivizáló adatok kezelésének egyéb szempontjai	78
6.5.	Informatikai biztonsági előírások	78
6.5.1.	Speciális informatikai biztonsági műszaki követelmények	78
6.5.2.	Az informatikai biztonság értékelése	79
6.6.	Életciklusra vonatkozó műszaki előírások	79
6.6.1.	Rendszerfejlesztési előírások	79
6.6.2.	Biztonságkezelési előírások	80
6.6.3.	Életciklusra vonatkozó biztonsági előírások	80
6.7.	Hálózati biztonsági előírások	80
6.8.	Időbélyegzés	81
7.	Tanúsítvány, CRL és OCSP profilok	81
7.1.	Tanúsítvány profil	81
7.1.1.	Verzió szám(ok)	81
7.1.2.	Tanúsítvány kiterjesztések	82
7.1.3.	Az algoritmus objektum azonosítója	87
7.1.4.	Névformák	87
7.1.5.	Névhasználati megkötöttségek	87
7.1.6.	A Hitelesítési rend objektum azonosítója	87
7.1.7.	A Hitelesítési rend megkötöttségek kiterjesztés használata	87
7.1.8.	A Hitelesítési rend jellemzők szintaktikája és szemantikája	87
7.1.9.	A kritikus Hitelesítési rend kiterjesztések feldolgozási szemantikája	88
7.2.	Tanúsítvány visszavonási lista (CRL) profil	88
7.2.1.	Verziószám(ok)	88

7.2.2.	Tanúsítvány visszavonási lista kiterjesztések	88
7.3.	Online tanúsítvány-állapot válasz (OCSP) profil	89
7.3.1.	Verziószám(ok)	89
7.3.2.	OCSP kiterjesztések	89
8.	A megfelelés vizsgálat	89
8.1.	Az ellenőrzések körülményei és gyakorisága	90
8.2.	Az auditor és szükséges képesítése	90
8.3.	Az auditor és az auditált rendszerelem függetlensége	90
8.4.	Az auditálás által lefedett területek	91
8.5.	A hiányosságok kezelése	91
8.6.	Az eredmények közzététele	91
9.	Egyéb üzleti és jogi kérdések	91
9.1.	Díjak	91
9.1.1.	Tanúsítvány kibocsátás és megújítás díjai	92
9.1.2.	Tanúsítvány hozzáférés díja	92
9.1.3.	Visszavonási állapot információ hozzáférés díja	92
9.1.4.	Egyéb szolgáltatások díjai	92
9.1.5.	Visszatérítési politika	92
9.2.	Anyagi felelősségvállalás	92
9.2.1.	Pénzügyi követelmények	92
9.2.2.	További követelmények	92
9.2.3.	Felelősségbiztosítás	92
9.3.	Bizalmasság	92
9.3.1.	Bizalmas információk köre	93
9.3.2.	Bizalmas információk körén kívül eső adatok	93
9.3.3.	Bizalmas információ védelme	93
9.4.	Személyes adatok védelme	93
9.4.1.	Adatkezelési szabályzat	93
9.4.2.	Személyes adatok	94
9.4.3.	Személyes adatnak nem minősülő adatok	94
9.4.4.	Személyes adatok védelme	94
9.4.5.	Személyes adatok felhasználása	94
9.4.6.	Adatkezelés	94
9.4.7.	Egyéb adatvédelmi követelmények	94
9.5.	Személyes tulajdonjogok	94
9.6.	Tevékenységért viselt felelősség és helytállás	95
9.6.1.	A szolgáltató felelőssége és helytállása	95

9.6.2.	A regisztráló szervezet felelőssége és helytállása	97
9.6.3.	Az Ügyfél felelőssége és helytállása	97
9.6.4.	Az Érintett fél felelőssége	99
9.6.5.	Egyéb szereplők tevékenységéért viselt felelősség és helytállás	99
9.7.	Helytállás érvénytelenségi köre	100
9.8.	A felelősség korlátozása	100
9.9.	Kártérítési kötelezettség	100
9.9.1.	A szolgáltató kártérítési kötelezettsége	100
9.9.2.	Az előfizető kártérítési kötelezettsége	100
9.9.3.	Az érintett felek kártérítési kötelezettsége	100
9.10.	Érvényesség és megszűnés	100
9.10.1.	Érvényesség	100
9.10.2.	Megszűnés	101
9.10.3.	A megszűnés következményei	101
9.11.	A felek közötti kommunikáció	101
9.12.	Módosítások	101
9.12.1.	Módosítási eljárás	101
9.12.2.	Értesítések módja és határideje	101
9.12.3.	Az OID megváltoztatása	102
9.13.	Vitás kérdések rendezése	102
9.14.	Irányadó jog	102
9.15.	Az érvényben lévő jogszabályoknak való megfelelés	102
9.16.	Vegyes rendelkezések	102
9.16.1.	Teljességi záradék	102
9.16.2.	Átruházás	102
9.16.3.	Részleges érvénytelenség	103
9.16.4.	Igényérvényesítés	103
9.16.5.	Vis maior	103
9.17.	Egyéb rendelkezések	103
A.	Hivatkozások	104

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zrt. (továbbiakban: Microsec vagy *Hitelesítés-szolgáltató*) által üzemeltetett e-Szignó Hitelesítés Szolgáltató által meghatározott weboldal-hitelesítő 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 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 RFC 3647 [15] keretrendszer követelményeinek. Kilenc fejezetből áll, amelyek tartalmazzák a *Hitelesítés-szolgáltató* által megfogalmazott biztonsági követelményeket, folyamatokat és a szolgáltatás nyújtása során követendő gyakorlatot. Az RFC 3647 által meghatározott felépítés szigorú megtartása érdekében azok a fejezetek is szerepelnek a dokumentumban, amelyeknél a *Hitelesítési rend* nem ír elő követelményt, ilyen esetben a fejezetben a "Nincs megkötés" szöveg szerepel.

Jelen dokumentum több *Hitelesítési rend* követelményeit tartalmazza. A dokumentumban megfogalmazott követelmények túlnyomó többsége a *Hitelesítési 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* 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	2.0
Hatályba lépés ideje	2016-07-01

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
1.3.6.1.4.1.21528.2.1.1.59.2.0	III. hitelesítési osztályba tartozó, weboldal-hitelesítő tanúsítványokhoz használt, álnevet kizáró hitelesítési rend.	HWxxN
1.3.6.1.4.1.21528.2.1.1.61.2.0	II. hitelesítési osztályba tartozó, weboldal-hitelesítő tanúsítványokhoz használt, álnevet kizáró hitelesítési rend.	KWxxN

1.3.6.1.4.1.21528.2.1.1.62.2.0	Automatikus kibocsátás során kibocsátott, weboldal-hitelesítő tanúsítványok kibocsátását szabályozó, álnevet kizáró hitelesítési rend.	AWxxN
--------------------------------	--	-------

A *Hitelesítési rendek* rövid nevének képzése illetve értelmezése az alábbi szabályok szerint történik:

- Az első karakter [Xxxxx]
 - M: minősített *Tanúsítvány Hitelesítési rend*
 - N: nem 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*
 - x: nincs megkötés
- A második karakter [xXxxx]
 - A: Aláírás célú *Tanúsítvány Hitelesítési rend*
 - B: Bélyegző létrehozása célú *Tanúsítvány Hitelesítési rend*
 - W: *Weboldal-hitelesítő tanúsítvány Hitelesítési rend*
 - K: Kódaláíró *Tanúsítvány Hitelesítési rend*
 - E: Egyéb célú *Tanúsítvány Hitelesítési rend*
 - x: nincs megkötés
- A harmadik karakter [xxXxx]
 - T: természetes személynek kibocsátott *Tanúsítvány Hitelesítési rend*
 - J: jogi személynek kibocsátott *Tanúsítvány Hitelesítési rend*
 - x: nincs megkötés
- A negyedik karakter [xxxXx]
 - B: *Hardver kriptográfiai eszközön kibocsátott Tanúsítvány Hitelesítési rend*
 - H: *Hardver kriptográfiai eszközön kibocsátott Tanúsítvány Hitelesítési rend*
 - S: *Szoftveresen kibocsátott Tanúsítvány Hitelesítési rend*
 - x: nincs megkötés
- Az ötödik karakter [xxxxX]
 - A: álneves *Tanúsítvány Hitelesítési rend*
 - N: álnevet kizáró *Tanúsítvány Hitelesítési rend*
 - x: nincs megkötés

Ezen *Hitelesítési rendek* alapján a *Hitelesítés-szolgáltató* webszerverek azonosítására használható *Tanúsítványok*at 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 nem természetes személyek számára kibocsátott *Tanúsítványokra* vonatkozó *Hitelesítési rendek* esetén az *Alany* jogi személy.

A *Weboldal-hitelesítő tanúsítványok* esetében az *Alany* nevének a domain név vagy IP cím szerepel. A *Weboldal-hitelesítő tanúsítvány* nem lehet álneves.

A jelen *Hitelesítési rendek* mindegyike kizárja az álnév használatát, a *Tanúsítványban* minden esetben az *Alany* valódi neve szerepel.

Jelen *Hitelesítési rendek* közül:

- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [6] szabványban definiált [DVCP] *Hitelesítési rend*nek.
- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [6] szabványban definiált [OVCP] *Hitelesítési rend*nek, amennyiben a *Tanúsítványban* feltüntetésre kerül a szervezet neve.

Megfelelés az ETSI hitelesítési rendeknek

	[DVCP]	[OVCP]
HW _{xx} N	X	X*
KW _{xx} N	X	X*
AW _{xx} N	X	X*

* amennyiben a tanúsítványban feltüntetésre kerül a *Szervezet* neve

1.2.2. Hatály

Jelen *Hitelesítési rend* gyűjtemény 2016-07-01-i hatálybalépési dátumtól visszavonásáig hatályos. Jelen *Hitelesítési rend* gyűjteményt és az ezen alapuló *Szolgáltatási szabályzatok*at legalább évente felül kell vizsgálni, és gondoskodni kell az esetlegesen megváltozott követelményekhez illetve igényekhez igazodó módosításokról.

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

A jelen *Hitelesítési rendek* 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* [Mxxxx];
- nem minősített, e-Szignó Hitelesítés Szolgáltató által kiadott III. hitelesítési osztályba tartozó *Tanúsítványok* [Hxxxx];
- nem minősített, e-Szignó Hitelesítés Szolgáltató által kiadott II. hitelesítési osztályba tartozó *Tanúsítványok* [Kxxxx];
- nem minősített, nem e-Szignó Hitelesítés Szolgáltató által kiadott *Tanúsítványok* [xxxxx];.

A használt hordozó alapján a biztonság szerint csökkenő sorrendben:

- *Hardver kriptográfiai eszközön* kibocsátott *Tanúsítványok* [xxxBx];
- *Hardver kriptográfiai eszközön* kibocsátott *Tanúsítványok* [xxxHx];
- egyéb módon, pl. szoftveresen kibocsátott *Tanúsítványok* [xxxSx], [xxxxx];

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

- minősített, *Hardver kriptográfiai eszközön* kibocsátott *Tanúsítványok* [MxxBx];
- minősített, *Hardver kriptográfiai eszközön* kibocsátott *Tanúsítványok* [MxxHx];
- minősített, egyéb módon, pl. szoftveresen kibocsátott *Tanúsítványok* [MxxSx],[Mxxxx];
- nem minősített, *Hardver kriptográfiai eszközön* kibocsátott, e-Szignó Hitelesítés Szolgáltató által kiadott III. hitelesítési osztályba tartozó *Tanúsítványok* [HxxHx];
- nem minősített, egyéb módon, pl. szoftveresen kibocsátott, e-Szignó Hitelesítés Szolgáltató által kiadott III. hitelesítési osztályba tartozó *Tanúsítványok* [HxxSx][Hxxxx];
- nem minősített, *Hardver kriptográfiai eszközön* kibocsátott, e-Szignó Hitelesítés Szolgáltató által kiadott II. hitelesítési osztályba tartozó *Tanúsítványok* [KxxHx];
- nem minősített, egyéb módon, pl. szoftveresen kibocsátott, e-Szignó Hitelesítés Szolgáltató által kiadott II. hitelesítési osztályba tartozó *Tanúsítványok* [KxxSx][Kxxxx];
- nem minősített, nem e-Szignó Hitelesítés Szolgáltató által kiadott *Tanúsítványok* [xxxxx];.

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 *Tanúsítványok*hoz 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 *Tanúsítványok*at bocsát ki, és ellátja az ehhez kapcsolódó feladatokat. Például azonosítja az igénylő személyét, nyilvántartásokat vezet, fogadja a *Tanúsítványok*kal kapcsolatos változások adatait, valamint nyilvánosságra hozza a *Tanúsítvány*hoz 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-szolgáltató*kra, akik a *Szolgáltatási szabályzat*ukban 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 szervezet*et a vonatkozó követelmények betartására.

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-szolgáltató*val. A tevékenységére vonatkozó ajánlásokat a *Szolgáltatási szabályzat* és az abban megnevezett egyéb szabályzatok tartalmazzák.

1.3.5. Egyéb szereplők

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

A *Hitelesítés-szolgáltató* a *Képviselt szervezettel* nem feltétlenül áll szerződéses viszonyban, de a *Hitelesítés-szolgáltató Szervezeti tanúsítványt* ezen *Szervezet* hozzájárulása nélkül nem bocsáthat ki. A *Hitelesítés-szolgáltató* a *Képviselt szervezet* kérésére a *Tanúsítványt* visszavonhatja.

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

Szolgáltatói tanúsítványok

A szolgáltatói gyökér és köztes *Tanúsítványok* illetve a hozzájuk tartozó magánkulcsok nem használhatók *Tanúsítványok* kibocsátására a szolgáltatói *Tanúsítványok* nyilvánosságra hozatalát megelőzően.

Végfelhasználói tanúsítványok

A jelen *Hitelesítési rendek* alapján kibocsátott *Tanúsítványokat*, illetve a hozzájuk tartozó magánkulcsokat webszerverek 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-1037 Budapest, Záhony utca 7. D épület
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
E-mail cím	info@e-szigno.hu

1.5.2. Kapcsolattartó személy

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

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

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

Egy *Szolgáltatási szabályzatnak* a benne meghivatkozott *Hitelesítési rendnek* való megfelelőségéért 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 a megfelelőség vizsgálatokor független megfelelőségértékelő szervezet megállapításaira támaszkodik.

1.5.4. A Szolgáltatási szabályzat elfogadási eljárása

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

1.6. Fogalmak és rövidítések

1.6.1. Fogalmak

II. hitelesítési osztály	Olyan <i>Hitelesítési rendek</i> csoportja, amelyek az <i>Igénylő</i> távoli regisztrációja alapján is lehetővé teszi a <i>Tanúsítvány</i> kibocsátását.
III. hitelesítési osztály	Olyan <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 domain név vagy IP cím azonosít.
Bizalmi felügyelet	"A <i>Bizalmi szolgáltatások</i> felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [4] 91.§ 1. bekezdés)
Bizalmi szolgáltatás (Trust Service)	<p>"Rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások:</p> <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;
Bizalmi szolgáltatási rend (Trust Service Policy)	" (eIDAS [1] 3. cikk 16. pont)
Bizalmi szolgáltató (Trust Service Provider)	"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 [4] 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)

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.
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 lejárta előtt. A <i>Tanúsítvány</i> felfüggesztése nem végleges, a felfüggesztett <i>Tanúsítvány</i> érvényessége visszaállítható.
Gyökér tanúsítvány (Root Certificate)	Más néven legfelső szintű tanúsítvány. Önhitelesített <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 személyét, <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 [4] 1. § 24. pont)
Igénylő	Az a természetes személy, aki az adott <i>Tanúsítvány</i> igénylése során eljár.
Képviselt szervezet	Amennyiben a <i>Tanúsítvány</i> egy <i>Szervezet</i> tevékenységének érdekében történő felhasználás céljából kerül kibocsátásra az <i>Igénylő</i> részére, akkor a <i>Képviselt szervezet</i> a szóban forgó <i>Szervezet</i> , amely szintén megjelölésre kerül a <i>Tanúsítványban</i> .
Kompromittálódás	Egy kriptográfiai kulcs akkor kompromittálódott, ha illetéktelen személyek is hozzáférhettek.
Köztes hitelesítő egység	Olyan <i>Hitelesítő egység</i> amelynek <i>Tanúsítványát</i> egy másik <i>Hitelesítő egység</i> bocsátotta ki.
Kriptográfiai kulcs (Key)	Olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete titkosításhoz és dekódoláshoz, illetve digitális aláírás előállításához és ellenőrzéséhez szükséges.
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	<p>A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az <i>Igénylőnek</i> szigorúan titokban kell tartania.</p> <p>Webszerver azonosságának igazolása esetében a webszervernek a magánkulcsát kell használnia az azonosságát ellenőrző eljárás során.</p> <p>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.</p>
Nyilvános kulcs	<p>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.</p> <p>Webszerver azonosságának igazolása esetében a webszervernek a nyilvános kulcsa szükséges ahhoz, hogy az azonosságát ellenőrizni lehessen.</p> <p>A <i>Tanúsítványok</i> hitelességét az őket kibocsátó <i>Hitelesítő egység</i> nyilvános kulcsa segítségével lehet ellenőrizni.</p>
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	<p>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.</p>
Regisztrációs igény	<p>A <i>Tanúsítvány kérelem</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.</p>
Regisztráló szervezet (Registration Authority)	<p>Szervezet, amely ellenőrzi a <i>Tanúsítványba</i> kerülő adatok valóságát, az <i>Igénylő</i> személy azonosságát, ellenőrzi, hogy a <i>Tanúsítvány kérelem</i> hiteles-e, és azt egy arra jogosult személy nyújtotta-e be.</p>
Rendkívüli üzemeltetési helyzet	<p>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.</p>
Szervezet	<p>Jogi személy.</p>

Szervezeti tanúsítvány	Olyan <i>Tanúsítvány</i> , amely <i>Szervezet</i> számára kerül kibocsátásra, azaz amelynek <i>Alanya</i> a <i>Szervezet</i> irányítása alatt álló webszerver. Ilyen esetben a <i>Tanúsítvány</i> "O" mezijében a <i>Szervezet</i> neve feltüntetésre kerül.
Szervezeti ügyintéző	Az a természetes személy, aki jogosult az adott <i>Szervezet</i> számára igényelt weboldal-hitelesítő <i>Tanúsítványok</i> igénylése és visszavonása során eljárni, valamint az adott <i>Szervezethez</i> kapcsolódó <i>Tanúsítványok</i> kibocsáthatóságát jóváhagyni illetve ezen <i>Tanúsítványok</i> at visszavonadni. A Szervezeti ügyintézőt az adott szervezet képviselőjére jogosult személy jelölheti ki. Szervezeti ügyintéző kijelölése nem kötelező, ha nincs kijelölve, akkor az adott szervezet képviselőjére jogosult személy láthatja el ezt a feladatot.
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 [4] 1. § 41. pont)
Szolgáltatási szerződés	"A <i>Bizalmi szolgáltató</i> és a <i>Bizalmi szolgáltatási</i> ügyfél között létrejött szerződés, amely a <i>Bizalmi szolgáltatás</i> nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza. " (2015. évi CCXXII. törvény [4] 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 [4] 1. § 44.)
Tanúsítvány kérelem	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>Tanúsítványba</i> kerülő adatok valódiságát.
Tanúsítványtár	Különböző <i>Tanúsítványok</i> at tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott <i>Tanúsítványok</i> at publikálja, de Tanúsítványtárnak nevezzük az <i>Érintett fél</i> számítógépén a használt alkalmazás számára elérhető <i>Tanúsítványok</i> at 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>Tanúsítványban</i> is feltüntetett érvényességi idő lejártá 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 nyilvántartás a felfüggesztett, illetőleg a visszavont <i>Tanúsítványokról</i> , amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját.
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 tanúsítványban</i> a név mezőben a webszerver domain neve vagy IP címe szerepel.

1.6.2. Rövidítések

CA	(Certification Authority)	Hitelesítés-szolgáltató
CP	(Certificate Policy)	Hitelesítési rend
CPS	(Certification Practice Statement)	Hitelesítés-szolgáltatási szabályzat
CRL	(Certificate Revocation List)	Tanúsítvány visszavonási lista
eIDAS	(electronic Identification, Authentication and Signature)	A 910/2014/EU rendelet általánosan használt hivatkozása
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
PKI	(Public Key Infrastructure)	Nyilvános kulcsú infrastruktúra
QCP	(Qualified Certificate Policy)	Minősített hitelesítési rend
RA	(Registration Authority)	Regisztráló szervezet
TSP	(Trust Service Provider)	Bizalmi szolgáltató

2. Közzététel és tanúsítványtár

2.1. Adatbázisok - tanúsítványtárak

A *Hitelesítés-szolgáltató* a honlapján és LDAP protokollon keresztül is tegye közzé szolgáltatói *Tanúsítványait*, valamint az általa kibocsátott azon végfelhasználói *Tanúsítványokat*, amelyek

közzétételéhez az *Igénylő* hozzájárult.

A *Hitelesítés-szolgáltató* publikálja a működése alapjául szolgáló *Hitelesítési rendet*, *Szolgáltatási szabályzatot* valamint a szerződési feltételeket tartalmazó egyéb dokumentumokat.

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

2.2. A tanúsítványokra vonatkozó információk közzététele

A *Hitelesítés-szolgáltató* tegye közzé a honlapján a szolgáltatói *Tanúsítványait*, valamint a végfelhasználói *Tanúsítványokat* az *Érintett felek* részére, amennyiben a *Tanúsítványhoz* tartozó *Igénylő* ehhez hozzájárul.

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 gyökértanúsítványaik 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 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. Az OCSP válaszadói *Tanúsítványok* visszavonási állapotát a *Hitelesítés-szolgáltató* kizárólag olyan módon tegye közzé, hogy kulcs kompromittálódás vagy bármilyen egyéb probléma esetén az OCSP válaszokat aláíró régi magánkulcshoz ne kerüljön kibocsátásra újabb *Tanúsítvány*. A *Hitelesítés-szolgáltató* az OCSP válaszadói *Tanúsítványokat* ezt követően új, biztonságos magánkulcshoz bocsássa ki.

Végfelhasználói tanúsítványok

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

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

A végfelhasználói *Tanúsítvány* visszavonását 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* hozza nyilvánosságra szerződéses feltételeit és szabályzatait a honlapján elektronikus formában.

A honlapon legalább 30 nappal a hatálybalépés előtt kerüljenek publikálásra a bevezetésre váró új dokumentumok.

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

A 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.

2.3. A közzététel időpontja vagy gyakorisága

2.3.1. Kikötések és feltételek közzétételi gyakorisága

A *Hitelesítési renddel* kapcsolatos új verziók közzététele a 9.12. fejezetben ismertetett eljárásoknak megfelelően történik.

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

A *Hitelesítés-szolgáltató* a rendkívüli információkat a jogszabályi előírásoknak megfelelően tegye közzé, külön rendelkezés hiányában pedig késedelem nélkül.

2.3.2. Tanúsítványok nyilvánosságra hozatalának gyakorisága

A *Hitelesítés-szolgáltatónak* 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 *Tanúsítványokat* 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 listákon is jelenjenek meg. A tanúsítvány visszavonási listák kibocsátási gyakoriságával kapcsolatos előírásokat a 4.10. fejezet tárgyalja.

2.4. A tanúsítványtár elérésének szabályai

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

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

3. Azonosítás és hitelesítés

3.1. Elnevezések

A fejezet 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 RFC 5280 [17] illetve RFC 6818 [18] ajánlások szerinti egyedi név formátum előírásainak, ezen kívül a *Hitelesítés-szolgáltató* támogassa a kiterjesztések között található Alternatív név mezők (Subject Alternative Names), (Issuer Alternative Names) kitöltését is.

3.1.1. Név típusok

Az *Alany* megnevezése

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

- Common Name (CN) – OID: 2.5.4.3 – Az *Alany* neve
Weboldal-hitelesítő tanúsítványok esetében a kért domain név vagy IP cím.
Használata opcionális. Csak létező és a Igénylő által jogosan használt domain név vagy IP cím tüntethető fel. *Weboldal-hitelesítő tanúsítványok* esetében csak ebben a mezőben, illetve a Subject Alternative Names mezőben szerepelhet domain név vagy IP cím. *Weboldal-hitelesítő tanúsítvány* nem lehet álneves.
Kitöltése kötelező.
- Surname – OID: 2.5.4.4 – Természetes személy vezetékneve
Amennyiben az igényelt domain vagy IP cím mögött álló személy természetes személy, akkor e mezőbe az ő vezetékneve kerüljön, ahol a vezetéknevet a *Hitelesítés-szolgáltató* a CN mezőben szereplő teljes névből képi. Álneves tanúsítvány esetén a *Hitelesítés-szolgáltató* nem tölti ki ezt a mezőt.
Kitöltése kötelező.
- Given Name – OID: 2.5.4.42 – Természetes személy keresztnéve
Amennyiben az igényelt domain vagy IP cím mögött álló személy természetes személy, akkor e mezőbe az ő keresztnéve kerüljön, ahol a vezetéknevet a *Hitelesítés-szolgáltató* a CN

mezőben szereplő teljes névből képzí. Álneves tanúsítvány esetén a *Hitelesítés-szolgáltató* nem tölti ki ezt a mezőt.

Kitöltése kötelező.

- Pseudonym (PSEUDO) – OID: 2.5.4.65 – Alany álneve
Kizárólag álneves tanúsítvány esetén kerülhet kitöltésre.
Weboldal-hitelesítő tanúsítvány nem lehet álneves.
- Serial Number – OID: 2.5.4.5 – Az *Alany* egyedi azonosítója
A *Tanúsítvány*ban legalább egy kitöltött "Serial Number" mezőnek kötelezően szerepelnie kell, amely teljesíti az alábbi követelményeket, és ezáltal alkalmas arra, hogy az RFC 4043 [16] ajánlás szerinti "Permanent Identifier" kiterjesztés használata esetén az *Alany* állandó azonosítójának részét képezze:
 - az azonosító értéke a *Tanúsítvány*ban megnevezett, a *Hitelesítés-szolgáltató* által azonosított *Alany*hoz tartozik, és a *Hitelesítés-szolgáltató* rendszerén belül egyedi;
 - a *Hitelesítés-szolgáltató* garantálja, hogy két általa kibocsátott *Tanúsítvány*ban kizárólag akkor szerepel megegyező azonosító érték, ha a két *Tanúsítvány* ugyanahhoz az *Alany*hoz tartozik.A fenti követelményeknek megfelelő "Serial Number" értéket nevezünk az *Alany* szolgáltatói egyedi azonosítójának.
- Organization (O) – OID: 2.5.4.10 – A *Szervezet* elnevezése
Szervezeti tanúsítvány esetében az "O" mezőben kell, hogy szerepeljen a *Szervezet* teljes vagy rövid neve, az alapító okirat vagy valamely közhiteles nyilvántartás szerint.
Weboldal-hitelesítő tanúsítványok esetében az Igénylő kérésére ebben a mezőben feltüntethető az Igénylő által jogosan használt védjegy, márkanév vagy DBA is.
Szervezeti tanúsítvány esetében a mező kitöltése kötelező.
Személyes – szervezethez nem kapcsolódó – tanúsítványok esetében a mező kitöltése tilos.
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
Szervezeti tanúsítvány esetében az "O" mezőben feltüntetett *Szervezet* azonosítója kerülhet ebbe a mezőbe.
Csak olyan adat kerülhet bele, amelyet a *Hitelesítés-szolgáltató* ellenőrzött.
Szervezeti tanúsítvány esetében a mező kitöltése opcionális.
Személyes – szervezethez nem kapcsolódó – tanúsítványok esetében a mező kitöltése tilos.
- Organizational Unit (OU) – OID: 2.5.4.11 – Szervezeti egység elnevezése
Szervezeti 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. Személyes – szervezethez nem kapcsolódó – *Tanúsítvány* – esetében nem kerülhet kitöltésre.

- Country (C) – OID: 2.5.4.6 – Ország azonosítója
Szervezeti tanúsítvány esetén az "O" mezőben szereplő *Szervezet* székhelye szerinti ország kétbetűs kódja.

Szervezet megnevezését nem tartalmazó *Weboldal-hitelesítő tanúsítvány* esetén a domainhez vagy IP címhez kapcsolódó ország, vagy ha ez nem egyértelműen eldönthető, akkor az *Igénylő* országának kétbetűs kódja.

Kitöltése kötelező.

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

- Street Address (SA) – OID: 2.5.4.9 – Cím adatok
Szervezeti tanúsítvány esetében a szervezet székhelye szerinti cím. Kitöltése opcionális, amennyiben kitöltésre kerül, akkor csak ellenőrzött információ tüntethető fel. *Szervezethez* nem kapcsolódó *Tanúsítványok* esetében a használata tilos.

- Locality Name (L) – OID: 2.5.4.7 – Településnév
Szervezeti tanúsítvány esetében a *Szervezet* székhelye szerinti helység neve.

Weboldal-hitelesítő tanúsítvány esetében:

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

- State or Province Name – OID: 2.5.4.8 – Tagállam, tartomány elnevezése
Szervezeti tanúsítvány esetében a *Szervezet* székhelye szerinti tagállam, megye vagy tartomány neve.

Weboldal-hitelesítő tanúsítvány esetében:

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

- Postal Code – OID: 2.5.4.17 – Irányítószám
Szervezeti tanúsítvány esetében a *Szervezet* székhelye szerinti postai irányítószám. Amennyiben kitöltésre kerül, akkor csak ellenőrzött információ tüntethető fel.

Weboldal-hitelesítő tanúsítvány esetében:

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

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

Nem lehet kitöltve.

- E-mail address (EMAIL) – OID: 1.2.840.113549.1.9.1 – Az *Alany* e-mail 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 " ").

Az Alany alternatív nevei

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

- A "Subject Alternative Names" mezőben szerepelnie kell legalább egy domain névnek vagy IP címnek . Kitöltése kötelező. Ebben a mezőben minden domain / IP címet fel kell sorolni, azt is, ami a "CN"-ben szerepel a "domain" mezőben. Csak teljesen minősített domain név (FQDN: Fully Qualified Domain Name) szerepelhet itt, illetve nem szerepelhet lefoglalt tartománybeli IP cím.

A *Tanúsítványban* csak itt és a "Subject" mező "CN"-jében szerepelhet domain név.

3.1.2. A nevek értelmezhetősége

A "SubjectDN" mezőre a következő szabályokat kell alkalmazni:

- az azonosítónak értelmezhetőnek kell lennie;
- a *Tanúsítványban* szereplő személynevet a közhiteles nyilvántartásban szereplő írásmóddal kell feltüntetni;
- a *Tanúsítványban* szereplő *Szervezet* nevét a közhiteles nyilvántartásban – annak hiányában az alapító okiratban – szereplő írásmóddal 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 feleknek* a jelen dokumentumban leírtak alapján kell eljárniuk. Amennyiben az azonosító, illetve a *Tanúsítványban* foglalt bármely más adat értelmezésével kapcsolatban az *Érintett félnek* segítségre lenne szüksége, akkor a *Hitelesítés-szolgáltatóval* 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 *Tanúsítványban* feltüntetett adatok értelmezését segítő információt szolgáltathatja.

3.1.5. A nevek egyedisége

Az *Alany*nak a *Hitelesítés-szolgáltató Tanúsítványtár*ában egyedi névvel kell rendelkeznie. Az egyediség biztosítása érdekében a *Hitelesítés-szolgáltató* adjon minden *Alany*nak egy – a *Hitelesítés-szolgáltató* nyilvántartásában egyedi – azonosítót, 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* 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-szolgáltató*nak biztosítani kell illetve meg kell győződnie arról, hogy a *Tanúsítványt* kérelmező valóban birtokolja illetve ellenőrzése alatt tartja a *Tanúsítvány*ba kerülő nyilvános kulcshoz tartozó magánkulcsot.

A követelmény teljesítésének módját rögzíteni kell a *Szolgáltatási szabályzat*ban.

3.2.2. Szervezet és domain azonosságának hitelesítése

Szervezet azonosságának hitelesítése

Szervezeti tanúsítványok kibocsátása előtt a *Hitelesítés-szolgáltató*nak megbízható harmadik fél vagy közhiteles nyilvántartás alapján meg kell győződnie a *Tanúsítvány*ba kerülő szervezeti adatok 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 *Tanúsítvány*ban feltüntetendő védjegyekkel kapcsolatosan ld. a 3.1.6 fejezetet.

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

Domain azonosságának hitelesítése

A *Weboldal-hitelesítő tanúsítvány*okban szerepelnie kell legalább egy domain névnek vagy IP címnek.

*Weboldal-hitelesítő tanúsítvány*ok kibocsátása előtt a *Hitelesítés-szolgáltató*nak meg kell győződnie a *Tanúsítvány*ba kerülő domain név vagy IP cím valódiságáról, valamint az *Alany* jogosultságáról a domain név vagy IP cím használatára vonatkozóan. Az ellenőrzés során közhiteles nyilvántartásból vagy megbízható harmadik féltől igazolást kell szerezni arról, hogy az *Alany* jogosult a domain név vagy IP cím használatára, vagy az *Alany*nak a gyakorlatban bizonyítania kell, hogy rendelkezik az adott domain név vagy IP cím feletti irányítással.

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

Amennyiben a *Tanúsítvány*ban "*" dzsóker karaktert tartalmazó domain név kerül feltüntetésre (wildcard tanúsítvány), a *Hitelesítés-szolgáltató*nak meg kell győződnie róla, hogy az *Igénylő* a wildcard domain név által lefedett teljes domain névtér jogosult használója. A *Hitelesítés-szolgáltató* nem bocsáthat ki olyan *Tanúsítványt*, amelyben a "*" dzsóker karakter a legmagasabb szintű regisztrálható domain név helyén, azaz közvetlenül egy nyilvános domain végződés bal oldalán található (pl. "*.com", "*.co.uk").

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

3.2.3. Természetes személy azonosságának hitelesítése

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

A *Hitelesítés-szolgáltató* a III. hitelesítési osztályba tartozó *Tanúsítvány*ok esetében a természetes személy azonosságát az alábbi lehetőségek valamelyikének alkalmazásával ellenőrizheti:

1. Személyesen történő azonosítás során. Ebben az esetben:

- A természetes személynek a személyes azonosítás elvégzéséhez személyesen meg kell jelennie a *Regisztráló szervezet* előtt.
- A személyes azonosítás során a természetes személy azonosságát ellenőrizni kell a személyazonosság igazolására alkalmas hatósági igazolványa alapján.
- A személyazonosság ellenőrzésére szolgáló adatok helyességét a természetes személynek nyilatkozatban, saját kezű aláírással ellátva igazolnia kell.
- A személyazonosításra használt igazolvány adatainak helyességét és az igazolvány érvényességét a *Regisztráló szervezet*nek megbízható harmadik fél vagy közhiteles nyilvántartás segítségével ellenőriznie kell.
- A természetes személy lakcímét ellenőrizni kell egy lakcím azonosítására alkalmas igazolvány alapján.

- A *Hitelesítés-szolgáltató* ellenőrzi, hogy a bemutatott igazolványokon történt-e módosítás vagy hamisítás.
2. Távolról, olyan elektronikus azonosító eszköz használatával, amely tekintetében a minősített tanúsítvány kibocsátása előtt biztosították a természetes személynek vagy a jogi személy képviselőre jogosult képviselőjének személyes jelenlétét, és amely megfelel az eIDAS rendelet [1] 8. cikkben a "jelentős", illetve a "magas" biztonsági szintre vonatkozóan meghatározott követelményeknek. Ebben az esetben:
- Az azonosítás során az alany nevén kívül meg kell adni egy olyan nemzeti szinten elfogadott azonosítószámot vagy egyéb adatot, amelynek segítségével a természetes személy az azonos nevű más személyektől megkülönböztethető.
 - A személyazonosság megállapításához használt azonosító adatokat a *Regisztráló szervezet*nek megbízható harmadik fél vagy közhiteles nyilvántartás segítségével ellenőriznie kell.
 - A természetes személy azonosságát ellenőrizni kell a személyazonosság igazolására alkalmas hatósági igazolványának másolata alapján.
 - A természetes személy lakcímét ellenőrizni kell egy lakcím azonosítására alkalmas igazolvány másolata alapján.
 - A *Hitelesítés-szolgáltató* ellenőrzi, hogy a bemutatott igazolványokon történt-e módosítás vagy hamisítás.
3. Elektronikus aláírás tanúsítványára visszavezetett azonosítással. Ebben az esetben:
- az *Igénylő* a *Tanúsítvány kérelmet* 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.
 - A személyazonosság megállapításához használt azonosító adatokat a *Regisztráló szervezet*nek megbízható harmadik fél vagy közhiteles nyilvántartás segítségével ellenőriznie kell.
 - A természetes személy azonosságát ellenőrizni kell a személyazonosság igazolására alkalmas hatósági igazolványának másolata alapján.
 - A természetes személy lakcímét ellenőrizni kell egy lakcím azonosítására alkalmas igazolvány másolata alapján.
 - A *Hitelesítés-szolgáltató* ellenőrzi, hogy a bemutatott igazolványokon történt-e módosítás vagy hamisítás.

A II. hitelesítési osztályba tartozó *Tanúsítvány*ok esetén a természetes személy azonosításához személyes találkozásra nincs szükség, ilyen esetben a *Hitelesítés-szolgáltató* távolról is azonosíthatja az *Igénylőt* az alábbi módon:

- az *Igénylő* eljuttatja a *Hitelesítés-szolgáltató*nak valamely személyazonosság igazolására alkalmas hatósági igazolványának másolatát;
- az *Igénylő* elektronikus aláírással ellátott *Tanúsítvány kérelmet* is benyújthat, amennyiben az aláírás létrehozásához használt nem álneves *Tanúsítvány*ának biztonsági besorolása (lásd 1.2.3. fejezet) nem alacsonyabb az igényelt *Tanúsítvány*énál.

A személyazonosító adatok helyességét a *Regisztráló szervezet*nek megbízható harmadik fél vagy közhiteles nyilvántartás segítségével ellenőriznie kell. A *Regisztráló szervezet* ellenőrzi a bemutatott igazolványok hitelességét. A *Hitelesítés-szolgáltató*nak megbízható kommunikációs csatornán keresztül ellenőriznie kell, hogy a *Tanúsítvány kérelmet* valóban az azonosított *Igénylő* küldte.

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

3.2.4. Nem ellenőrzött alany információk

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

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 *Szervezet* kijelölhet egy vagy több Szervezeti ügyintézőt, aki jogosult az adott *Szervezet* számára igényelt *Tanúsítványok* igénylése, visszavonása során eljárni.

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-szolgáltatókkal*, akik magukra kötelező érvényűnek ismerik el jelen *Hitelesítési rendek* követelményeinek betartását.

Az együttműködő *Hitelesítés-szolgáltatóknak* a *Szolgáltatási szabályzatok*ban 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 kulcsere kérelem esetén

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

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

A kulcscserével kapcsolatos eljárás részletei a 4.7. fejezetben olvashatóak.

3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

Kulcscsere kérelmek benyújtására a következő lehetőségeket kell biztosítani:

- papíralapon az *Igénylő* kézi aláírásával ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában;
- elektronikus formában, az *Igénylő* nem álneves, a megújítani kívánt *Tanúsítványnál* nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) *Tanúsítványán* alapuló elektronikus aláírással ellátva;
- kézi aláírással ellátva postai úton az Ügyfélszolgáltatónak eljuttatva.

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

A fentiek szerinti elektronikus aláírással hitelesített elektronikus formában benyújtott kérelem esetében nincs szükség a kérelmező azonosságának és a kérelem hitelességének további vizsgálatára.

3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

A *Hitelesítés-szolgáltató* kizárólag a szolgáltatás nyújtásának időtartama alatt elfogadhat kulcscsere kérelmeket kulcs kompromittálódás miatt visszavont *Tanúsítványok* esetén is. A kérelmet benyújtó személy azonosságát a 3.2.3 fejezetben ismertetett folyamat szerint kell ellenőrizni.

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

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

- papíralapon az *Igénylő* kézi aláírásával ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely külső *Regisztráló szervezet* regisztrációs munkatársa előtt, előzetesen egyeztetett időpontban;

- elektronikus formában, az *Igénylő* nem álneves, a megújítani kívánt *Tanúsítványnál* nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) *Tanúsítványán* alapuló elektronikus aláírással ellátva;
- kézi aláírással ellátva postai úton az Ügyfélszolgálatnak eljuttatva.

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

A fentiek szerinti elektronikus aláírással hitelesített elektronikus formában benyújtott kérelem esetében nincs szükség a kérelmező azonosságának és a kérelem hitelességének további vizsgálatára.

A III. hitelesítési osztályba tartozó *Tanúsítványok* megújítása esetén a megújítási kérelem papíralapon, postai úton történő benyújtása esetében a kérelmező azonosítása és a kérelem megerősítése a kérelem benyújtását követően, személyes találkozás során történik.

3.4.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen *Tanúsítvány* nem újítható meg.

3.5. Azonosítás és hitelesítés tanúsítvány módosítás esetén

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

Ilyen esetben az *Alany* megváltozott adatait a *Hitelesítés-szolgáltató*nak a 3.2. fejezetben leírtaknak megfelelően ellenőriznie kell a *Tanúsítvány* kibocsátása előtt.

3.5.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

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

- papíralapon az *Igénylő* kézi aláírásával ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely külső *Regisztráló szervezet* regisztrációs munkatársa előtt, előzetesen egyeztetett időpontban;
- elektronikus formában, az *Igénylő* nem álneves, a módosítani kívánt *Tanúsítványnál* nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) *Tanúsítványán* alapuló elektronikus aláírással ellátva;
- kézi aláírással ellátva postai úton az Ügyfélszolgálatnak eljuttatva.

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

A fentiek szerinti elektronikus aláírással hitelesített elektronikus formában benyújtott kérelem esetében nincs szükség a kérelmező azonosságának és a kérelem hitelességének további vizsgálatára.

A III. hitelesítési osztályba tartozó *Tanúsítványok* módosítása esetén a tanúsítvány módosítási kérelem papíralapon, postai úton történő benyújtása esetében a kérelmező azonosítása és a kérelem megerősítése a kérelem benyújtását követően, személyes találkozás során történik.

3.5.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen *Tanúsítvány* nem módosítható.

3.6. Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási kérelem esetén

A *Hitelesítés-szolgáltató*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 szabályzat*ban rögzíteni kell.

Weboldal-hitelesítő tanúsítványok esetében felfüggesztésre nincs lehetőség.

4. A tanúsítványok életciklusára vonatkozó követelmények

4.1. Tanúsítvány kérelem

Új *Tanúsítvány* kiadásához *Tanúsítvány kérelem* benyújtására van szükség. Az első *Tanúsítvány kérelem* 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 *Tanúsítvány kérelemben* 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 *Tanúsítvány kérelemnek* tartalmaznia kell legalább a következő adatokat: *Tanúsítvány kérelemben* az *Alany*nak a következő adatokat kell megadnia:

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

A *Tanúsítvány* kérelemmel 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* képviselőjére ;
- amennyiben a kért *Tanúsítvány*ban szerepel márkanév vagy védjegy, akkor annak igazolását, hogy az *Igénylő* jogosult annak használatára.

4.1.1. Ki nyújthat be tanúsítvány kérelmet

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

A *Tanúsítvány* kérelmet az *Igénylő* a következő módokon nyújthatja be:

- papíralapon kézi aláírásával ellátva a személyes azonosítás alkalmával a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, a *Hitelesítés-szolgáltató* mobil regisztrációs munkatársainál vagy valamely külső *Regisztráló szervezet* regisztrációs munkatársa előtt;
- papíralapon postai úton a *Hitelesítés-szolgáltató* postacímére megküldve (ekkor a III. hitelesítési osztályba tartozó *Tanúsítványok* esetén a személyes azonosításra később 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, a *Hitelesítés-szolgáltató* e-mail címére megküldve.

A *Hitelesítés-szolgáltató*nak ellenőriznie kell egy másik -- megbízható -- csatornán, hogy a kérelem valóban attól a személytől származik, akinek az adatai (igazolmányai) az igénylésben szerepelnek. 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* (vagy a *Regisztráló szervezet*) regisztrációs munkatársának meg kell győződnie a *Tanúsítvány kérelmet* benyújtó személyazonosságáról (lásd: 3.2.3 fejezet). *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 *Előfizetővel* 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 *Tanúsítvány kérelmet*, amelynek tartalmaznia kell a következőket:

- annak megerősítését, hogy a *Tanúsítvány kérelemben* megadott adatok pontosak;
- azt, hogy hozzájárul ahhoz, hogy a *Hitelesítés-szolgáltató* a kérelemben megadott adatait nyilvántartsa és kezelje;
- azt, hogy hozzájárul-e a *Tanúsítvány* közzétételéhez;
- nyilatkozatot arról, hogy az igényelt *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 tanúsítvány kérelem feldolgozása

4.2.1. Az igénylő azonosítása és hitelesítése

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

4.2.2. A tanúsítvány kérelem elfogadása vagy visszautasítása

A *Hitelesítés-szolgáltató*nak 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 *Tanúsítvány* kérelemben megadott, a *Tanúsítvány*ba kerülő valamennyi információ hitelességét.

A *Hitelesítés-szolgáltató* a *Tanúsítvány* kérelem feldolgozása után elfogadja, vagy visszautasítja a *Tanúsítvány* kérelem 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 tanúsítvány kérelem feldolgozásának időtartama

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

4.3. A tanúsítvány kibocsátása

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

4.3.1. A Hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során

A *Tanúsítványok* kibocsátásának megfelelően biztonságos módon kell történnie.

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 *Tanúsítvány*ban szereplő adatok helyességét és erről írásbeli nyilatkozatot kell tennie. A nyilatkozat aláírásával az *Igénylő* igazolja a *Tanúsítvány* átvételét.

A II. hitelesítési osztályba tartozó *Tanúsítványok* esetén az *Igénylő* (vagy képviselője) nem tesz külön nyilatkozatot a kiállított *Tanúsítvány* átvételéről. A *Szolgáltatási szerződés* aláírásával az *Előfizető*, a *Tanúsítvány* kérelem aláírásával az *Igénylő* 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 kibocsátásról

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

4.5. A kulcspár és a tanúsítvány használata

4.5.1. A magánkulcs és a tanúsítvány használata

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

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

Az *Alany* köteles gondoskodni magánkulcsának és aktivizáló adatának (PIN kód vagy jelszó) megfelelő védelméről.

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

4.5.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata

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

- ellenőrizze a *Tanúsítvány* érvényességét, visszavonási állapotát;
- a *Weboldal-hitelesítő tanúsítványok*hoz kapcsolódó nyilvános kulcsokat csak webszerver azonosságának igazolására használja;
- vegyen figyelembe minden korlátozást, amely a *Tanúsítvány*ban vagy a *Tanúsítvány*ban meghivatkozott szabályzatokban szerepel.

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

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

4.6. Tanúsítvány megújítás

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

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

4.6.1. A tanúsítvány megújítás körülményei

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

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

Tanúsítvány megújítási kérelmet a *Hitelesítés-szolgáltató* csak a Szolgáltatási szerződés hatálya alatt 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 *Előfizető*vel, akkor az *Előfizető* számára is meg kell adni a fenti tájékoztatást.

4.6.2. Ki kérelmezheti a tanúsítvány megújítást

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

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

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

4.6.3. A tanúsítvány megújítási kérelmek feldolgozása

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

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

4.7.3. A kulcscsere kérelmek feldolgozása

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

- a benyújtott kérelem hiteles;
- a kérelem benyújtója rendelkezik a szükséges jogosultságokkal, felhatalmazásokkal;
- a 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-szolgáltató*nak 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* kapcsolattartóját is.

4.8. Tanúsítvány módosítás

A tanúsítvány módosítás alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* egy adott *Alany* részére bocsát ki új *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 Tanúsítvány*ban 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 *Tanúsítvány kérelem* 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*nak az új *Alany* azonosító adatok valódiságának ellenőrzése során ugyanúgy kell eljárnia, mint az új *Tanúsítvány* kibocsátása előtti kezdeti ellenőrzésnél.

4.8.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* értesítse az *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-szolgáltatónak* 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* kapcsolattartóját is.

4.9. Tanúsítvány visszavonás és felfüggesztés

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

Weboldal-hitelesítő tanúsítvány nem függeszthető fel.

4.9.1. A tanúsítvány visszavonás körülményei

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

- a *Tanúsítvány* módosítása az *Alanya*ra vonatkozó adatok változása miatt;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban foglalt adatok nem felelnek meg a valóságnak;
- az *Igénylő* vagy az *Előfizető* értesíti a *Hitelesítés-szolgáltatót* arról, hogy az eredeti *Tanúsítvány kérelmet* nem hagyta jóvá, és utólag sem ad erre jóváhagyást;
- az *Igénylő* vagy az *Előfizető* írásban kéri a *Tanúsítvány* visszavonását;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem az *Igénylő* kizárólagos birtokában van;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* jogellenesen használták;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy az *Előfizető* nem teljesítette valamely anyagi kötelezettségét a vonatkozó Szolgáltatási szerződésnek megfelelően;

- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő domain név vagy IP cím használati jogosultsága megszűnt (pl.: a bíróság megtiltotta a domain használatát vagy a tulajdonos nem hosszabbította meg a domain regisztrációját);
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a wildcard tanúsítványt megtevesztő domain név hitelesítésére használták;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő nyilvános kulcs már nem felel meg a 6.1.5. és 6.1.6. fejezetekben meghatározott követelményeknek;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* nem a vonatkozó *Hitelesítési rend* illetve szolgáltatási szabályzat szerint bocsátották ki;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* kibocsátó hitelesítő egység magánkulcsa kompromittálódhatott;
- a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);
- a *Hitelesítés-szolgáltató* már nem lenne jogosult *Tanúsítványok*at kibocsátani és a meglévő *Tanúsítványokra* vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;
- a *Hitelesítés-szolgáltató* 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.

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

- a *Tanúsítvány* módosítása a hitelesítési egységre, vagy a *Hitelesítés-szolgáltatóra* vonatkozó adatok változása miatt;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem a kizárólagos birtokában van;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* jogellenesen használták;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő nyilvános kulcs már nem felel meg a 6.1.5 és 6.1.6 fejezetekben meghatározott követelményeknek;
- amennyiben a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);
- amennyiben a *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;

- amennyiben a *Hitelesítés-szolgáltató* már nem lenne jogosult *Tanúsítványok*at kibocsátani és a meglévő *Tanúsítványok*ra vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;
- 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.

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

- a *Tanúsítvány* módosítása a hitelesítési egységre, vagy az azt üzemeltető hitelesítés-szolgáltatóra vonatkozó adatok változása miatt;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban foglalt adatok nem felelnek meg a valóságnak;
- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató értesíti a kibocsátó *Hitelesítés-szolgáltatót* arról, hogy az eredeti *Tanúsítvány* kérelmet nem hagyta jóvá, és utólag sem ad erre jóváhagyást;
- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató írásban kéri a *Tanúsítvány* visszavonását;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató kizárólagos birtokában van;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* jogellenesen használták;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő nyilvános kulcs már nem felel meg a 6.1.5 és 6.1.6. fejezetekben meghatározott követelményeknek;
- amennyiben a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *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;
- amennyiben a *Hitelesítés-szolgáltató* már nem lenne jogosult *Tanúsítványok*at kibocsátani és a meglévő *Tanúsítványok*ra vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;
- a hitelesítési egységet működtető hitelesítés-szolgáltató, vagy a *Tanúsítvány*át kibocsátó *Hitelesítés-szolgáltató* a tevékenységét befejezte;

- a visszavonást jogszabály kötelezővé teszi.

A *Szolgáltatási szabályzat* előírhat a 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 *Előfizető*;
- az *Igénylő*
- *Szervezeti tanúsítvány* esetén a *Szervezet* nevében eljárásra jogosult természetes személy;
- a Szolgáltatási szerződésben megjelölt kapcsolattartó;
- a *Hitelesítés-szolgáltató*.

4.9.3. A visszavonási kérelemre vonatkozó eljárás

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

- Papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában, ügyfélszolgálati időben.
- Elektronikus formában, a kérelmező nem álneves, a visszavonni kívánt *Tanúsítványnál* nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) *Tanúsítványán* alapuló elektronikus aláírásával ellátva.
- Kézi aláírással ellátva postai úton az Ügyfélszolgálatnak eljuttatva.
- 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.
- A *Hitelesítés-szolgáltató* telefonos ügyeletén keresztül a nap 24 órájában. A *Hitelesítés-szolgáltató* ügyeleti telefonján fogadott kérelmeket a *Hitelesítés-szolgáltató* ügyintézőjének a hívás időtartama alatt el kell bírálnia, döntéséről szóban értesíteni kell a kérelmezőt.

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

4.9.4. A visszavonási kérelemre vonatkozó kivárási idő

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

4.9.5. A visszavonási eljárás maximális hossza

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

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 *Tanúsítványban* 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 *Tanúsítványokban* 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 *Tanúsítványokat* kibocsátó hitelesítési egységeire.

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

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

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

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

4.9.9. Valós idejű tanúsítvány állapot ellenőrzés lehetősége

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

4.9.10. A valós idejű tanúsítvány állapot ellenőrzésre vonatkozó követelmények

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

4.9.11. A visszavonási 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 *Tanúsítványokhoz* 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* állapotának lekérdezésére a *Hitelesítés-szolgáltató* biztosítsa a következő lehetőségeket:

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

A visszavonási listában kerüljenek feltüntetésre a visszavont *Tanúsítványok*.

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

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

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

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

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

4.10.1. Működési jellemzők

Nincs megkötés.

4.10.2. A szolgáltatás rendelkezésre állása

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

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

A visszavonási nyilvántartások válaszüzeje 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 tanúsítvány*hoz tartozó magánkulcshoz nem nyújthat kulcsletét szolgáltatást.

4.12.1. Kulcsletét és visszaállítás rendje és szabályai

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

4.12.2. Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

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

5. Elhelyezési, eljárásbeli és üzemeltetési előírások

A *Hitelesítés-szolgáltató*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, video 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 géptermen belül sem tárolhatók nyílt formában.

Jogosulatlan személyek jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva kell tartani;
- a bejelentkezett terminálokat nem szabad felügyelet nélkül hagyni;
- nem szabad olyan munkafolyamatot végezni, amely során bizalmas 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 Adatközpontját* megfelelően védeni kell a vízbetöréstől és az elárasztódástól.

5.1.5. Tűz megelőzés és tűzvédelem

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

5.1.6. Adathordozók tárolása

A *Hitelesítés-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 helyszínével. Az elsődleges és a tartalék helyszínek között meg kell oldani az adatok biztonságos továbbítását.

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 bizalmi szerepköröket kell létrehoznia. 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, 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.

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 hónapnál 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.

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

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

Naplózni kell minimálisan az alábbi eseményeket:

- NAPLÓZÁS
 - a naplózó rendszer vagy egyes komponenseinek leállítása, újraindítása;
 - a naplózás bármilyen beállításának módosítása, mint pl. gyakoriság, riasztási küszöb érték, vizsgált esemény;
 - a tárolt naplózási adatok módosítása vagy törlése;
 - a naplózó rendszer hibája miatt végzett tevékenységek;
- RENDSZER BEJELENTKEZÉSEK
 - sikeres bejelentkezések, sikertelen bejelentkezési próbálkozások bizalmi szerepkörökbe;
 - jelszó alapú azonosítás esetén:
 - * az engedélyezett sikertelen bejelentkezési próbálkozások számának megváltoztatása;
 - * az engedélyezett sikertelen bejelentkezési próbálkozások számának elérése felhasználói bejelentkezéskor;
 - * sikertelen bejelentkezések miatt zárolt felhasználó újbóli engedélyezése;
 - az azonosítási technika változtatása (például jelszó alapúról PKI alapúra);
- KULCSKEZELÉS
 - a szolgáltatói
kulcsok teljes életciklusára vonatkozó valamennyi esemény (kulcsgenerálás, betöltés, elmentés stb.);

- a felhasználói kulcsok generálásával, kezelésével kapcsolatos események;
 - a *Hitelesítés-szolgáltató* által bármilyen célból tárolt felhasználói magánkulcsok kezelésével kapcsolatos minden esemény;
- TANÚSÍTVÁNY KEZELÉS
 - 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;
 - tanúsítvány kérelmek 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 előállítás;
 - OCSP válasz generálása;
 - *Időbélyegző* generálása;
 - az előírt időpontossági küszöb túllépése;
- HSM
 - HSM installálása;
 - HSM eltávolítása;
 - HSM selejtezése, megsemmisítése;
 - HSM szállítása;
 - HSM tartalmának törlése (nullázás);

- HSM feltöltése kulcsokkal, tanúsítványokkal;
- KONFIGURÁCIÓ VÁLTOZÁSA
 - hardver;
 - szoftver;
 - operációs rendszer;
 - javító csomag;
- FIZIKAI HOZZÁFÉRÉS, TELEPHELY BIZTONSÁG
 - személy belépése a CA komponenseket tartalmazó biztonsági területre és onnan kilépése;
 - hozzáférés egy CA rendszer komponenshez;
 - a fizikai biztonság ismert vagy gyanított megsértése;
 - tűzfal és router forgalmak;
- MŰKÖDÉSI 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 *Hitelesítési rend* vagy a *Szolgáltatási szabályzat* megsértése;
 - operációs rendszer órájának törlése;
- EGYÉB ESEMÉNYEK
 - személy kinevezése biztonsági szerepkörbe;
 - operációs rendszer telepítése;
 - PKI alkalmazás telepítése;
 - rendszer elindítása;
 - belépési kísérlet a PKI alkalmazásba;
 - jelszó módosítási, beállítási kísérlet;
 - a belső adatbázis elmentése, visszaállítása mentésből;
 - fájl műveletek (pl. létrehozás, átnevezés, áthelyezés);
 - adatbázis hozzáférés.

5.4.2. A naplófájl feldolgozásának gyakorisága

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

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

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

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

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

A kiértékelés során elemezni kell a rendszerek által generált hibaüzeneteket.

Statisztikai módszerekkel elemezni kell a forgalmi adatokban bekövetkezett jelentős változásokat.

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

5.4.3. A naplófájl megőrzési időtartama

Az online rendszerből való kitörítés előtt a naplóállományokat archiválni kell és gondoskodni kell azok biztonságos megőrzéséről az 5.5.2 fejezetben meghatározott ideig.

5.4.4. A naplófájl védelme

A *Hitelesítés-szolgáltató*nak meg kell védenie a keletkezett naplóállományokat az előírt megőrzési ideig. A megőrzési idő teljes időtartama alatt biztosítania kell a 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 szabályzatban* 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-szolgáltatónak* 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-szolgáltatónak* fel kell készülnie elektronikus és papíralapú dokumentumok megfelelően biztonságos, hosszú idejű archiválására.

A *Hitelesítés-szolgáltatónak* az alábbi jellegű információt kell archiválnia:

- a *Hitelesítés-szolgáltató* akkreditációjával kapcsolatos valamennyi irat;
- a *Hitelesítési rend(ek)* és *Szolgáltatási szabályzat(ok)* valamennyi kibocsátott verziója;
- az Általános szerződési feltételek valamennyi kibocsátott verziója;
- a *Hitelesítés-szolgáltató* működésével kapcsolatos szerződések;
- a regisztrációval kapcsolatos valamennyi információ, beleértve
 - a *Tanúsítvány kérelemmel* 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 *Szolgáltatási szabályzatot* a hatályon kívül helyezéstől számított 10 évig;
- a *Tanúsítványokkal* kapcsolatos valamennyi elektronikus és/vagy papír alapú információt legalább
 - a *Tanúsítvány* érvényességének lejáratától számított 10 évig;

5.5.3. Az archívum védelme

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

A *Hitelesítés-szolgáltató*nak 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*nak 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-szolgáltatónak* 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 *Tanúsítványok*at 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 [11];
- az Eüt. [4] 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), 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 [13] követelményeinek, vagy
 - megfelel a FIPS 140-2 [22] 3-as, illetve annál magasabb szintű követelményeinek, vagy
 - megfelel a CEN 14167-2 [23] munkacsoport egyezmény követelményeinek, vagy
 - olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [12] 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, vagy videofelvétel készül az eseményről. A külső auditor igazolja, hogy a kulcs generálása a forgatókönyv szerint történt.

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

- A kulcsok előállítását fizikailag védett környezetben végzi, kizárólag bizalmi szerepkört betöltő személyek részvételével.
- A *Hardver kriptográfiai eszköz* használatát előíró *Hitelesítési rendek* esetén a *Hitelesítés-szolgáltató* a magánkulcsot csak a szolgáltatást igénybe vevő *Hardver kriptográfiai eszköz*én generálja, ami lehetlenné teszi a magánkulcs felfedését.
- 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 lehetlenné 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-szolgáltatónak* meg kell győződnie arról, hogy az előállított kulcspár megfelel a 6.1.5 és 6.1.6 fejezetekben meghatározott követelményeknek és a nyilvános kulcs nem egy ismert gyenge kulcspár tagja.

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

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

6.1.2. Magánkulcs eljuttatása az igénylőhöz

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 *Tanúsítvány kérelem* folyamatának bizonyítania kell, hogy az *Igénylő* valóban rendelkezik a nyilvános kulcshoz tartozó magánkulccsal.

6.1.4. A szolgáltatói nyilvános kulcs közzététele

A *Hitelesítés-szolgáltató*nak olyan módszerrel kell elérhetővé tennie legfelsőbb szintű szolgáltatói tanúsítványainak nyilvános kulcsait az *Érintett felek* részére, amely lehetetlenné teszi a kulcsok megváltoztatására irányuló támadásokat. Ennek keretében a *Hitelesítés-szolgáltató* legalább a honlapján tegye közzé a szolgáltatói *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 gyökértanúsítványaik lenyomatát tartalmazza a *Szolgáltatási szabályzat*. Az állapotváltozásukkal kapcsolatos információk legyenek elérhetőek a *Hitelesítés-szolgáltató* honlapján.
- A köztes (nem gyökér) hitelesítő egységek tanúsítványainak állapotváltozását hozza nyilvánosságra a visszavonási listákon, saját honlapján, valamint az online tanúsítvány-állapot válasz szolgáltatás keretében.
- Az online tanúsítvány-állapot válaszokat aláíró válaszadók számára a *Hitelesítés-szolgáltató* – a legjobb nemzetközi gyakorlatnak megfelelően – rendkívül rövid érvényességi idejű *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 *Tanúsítványokat* 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 algoritmusokat és minimális kulcsméreteket használhat, amelyek megfelelnek az alábbi normatívákban megfogalmazott követelményeknek:

- ETSI TS 119 312 [11];
- CABF Baseline Requirements ajánlás [21];
- az Eüt. [4] 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,
- *Időbélyegző egység* *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 "kulcsasználat" (Key Usage) kiterjesztéseket, amelyek meghatározzák a *Tanúsítvány* felhasználási területét és az X.509v3 [20] 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* 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 *Hardver kriptográfiai eszközök* kezelése során a használatból kivont *Hardver kriptográfiai 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 Tanúsítványokat*, OCSP válaszokat, CRL listákat kibocsátó rendszerei az elektronikus aláírás vagy bélyegző létrehozásához használt magánkulcsokat olyan biztonságos hardver eszközökben kell tárolják, amelyek:

- megfelelnek az ISO/IEC 19790 [13] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [22] 3-as, illetve annál magasabb szintű követelményeknek,
- vagy megfelelnek a CEN 14167-2 [23] munkacsoport egyezmény követelményeinek,
- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [12] 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 előírányaton kell alapulnia.

A szolgáltatói magánkulcsok a *Hardver kriptográfiai eszközön* kívül csak kódolt formában tárolhatók. A kódoláshoz csak az Eüt. [4] 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* 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* nem helyezheti letétbe a szolgáltatói aláíró magánkulcsait. A weboldal-hitelesítéshez használt magánkulcsok nem helyezhetők letétbe.

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 *Hardver kriptográfiai eszközben* kell előállítani. A magánkulcsok nem létezhetnek nyílt formában a *Hardver kriptográfiai eszközön* kívül.

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

A magánkulcs *Hardver kriptográfiai 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 *Hardver kriptográfiai eszközön* belüli tárolási formára vonatkozóan nincs előírás.

6.2.8. A magánkulcs aktiválásának módja

A *Hitelesítés-szolgáltató* szolgáltatói magánkulcsait a felhasznált *Hardver kriptográfiai 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.

A *Hitelesítés-szolgáltató* által előállított végfelhasználói magánkulcsok esetén a *Hitelesítés-szolgáltató*nak gondoskodnia kell róla, hogy a magánkulcsokat és a magánkulcsok aktiváló adatait megfelelően biztonságos módon állítsa elő és kezelje, amely kizárja a magánkulcsok illetéktelen használatának lehetőségét.

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 *Hardver kriptográfiai eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell deaktiválni.

Végfelhasználói magánkulcsok

A *Hardver kriptográfiai eszköz* használatát nem megkövetelő *Hitelesítési rendek* esetén a 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 *Hardver kriptográfiai eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell elvégezni.

Végfelhasználói magánkulcsok

A *Hardver kriptográfiai eszköz* használatát nem megkövetelő *Hitelesítési rendek* esetén a magánkulcsok megfelelően biztonságos megsemmisítése szintén az *Igénylő* felelőssége.

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 *Hardver kriptográfiai eszközben* kell tárolni, amely:

- rendelkezik ISO/IEC 19790 [13] szerinti tanúsítással,
- vagy rendelkezik FIPS 140-2 Level 3 [22] szerinti tanúsítással,
- vagy rendelkezik a CEN 14167-2 [23] munkacsoport egyezmény követelményeinek való megfelelést igazoló Common Criteria alapú tanúsítvánnyal,
- vagy rendelkezik a Nemzeti Média- és Hírközlési Hatóság által vagy az Európai Unió valamely tagállamában nyilvántartásba vett, elektronikus aláírási termékek értékelésére jogosult független tanúsító szervezet által erre a célra kiadott igazolással.

6.3. A kulcspár kezelés egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

A *Hitelesítés-szolgáltató*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:

- legfeljebb a kibocsátástól számított 3 év;
- nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozata szerint biztonságosan felhasználhatók;
- nem haladhatja meg a *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 *Hardver kriptográfiai eszköz* felhasználói útmutatójában és az eszköz tanúsítványban megfogalmazott eljárásoknak, követelményeknek megfelelő aktivizáló 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.

A *Hitelesítés-szolgáltató* által az *Igénylő* számára generált szoftveres magánkulcsok esetén:

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

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* 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-szolgáltatónak* 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 *Hardver kriptográfiai eszközök* védelméről azok teljes életciklusa alatt.

- Megfelelő tanúsítással rendelkező *Hardver kriptográfiai eszköz* kell használnia.
- A *Hardver kriptográfiai eszköz* átvételekor meg kell róla győződni, hogy a szállítás során biztosították a *Hardver kriptográfiai eszközök* feltörés elleni védelmét.
- A tárolás során biztosítani kell a *Hardver kriptográfiai eszközök* feltörés elleni védelmét.
- Az üzemeltetés során folyamatosan be kell tartani a *Hardver kriptográfiai eszközök* biztonsági előírányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket.
- A használatból kivont *Hardver kriptográfiai eszközök*ben tárolt magánkulcsokat olyan módon kell törölni, hogy lehetetlenné váljon a kulcsok visszaállítása.

6.7. Hálózati biztonsági előírások

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

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

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

6.8. Időbélyegzés

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

7. Tanúsítvány, CRL és OCSP profilok

7.1. Tanúsítvány profil

A *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*ok illetve a szolgáltatás során használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítvány*ai feleljenek meg az alábbi ajánlásoknak, specifikációknak:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [20];
- RFC 5280 [17];
- RFC 6818 [18];
- ETSI EN 319 412-1 [7];
- ETSI EN 319 412-2 [8] természetes személyek számára kibocsátott *Tanúsítvány*ok esetén;
- ETSI EN 319 412-3 [9] nem természetes személyek számára kibocsátott *Tanúsítvány*ok esetén;
- ETSI EN 319 412-4 [10].

7.1.1. Verzió szám(ok)

A *Hitelesítés-szolgáltató* által használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítvány*ai és a *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*ok legyenek az X.509 specifikáció [20] szerinti "v3" *Tanúsítvány*ok.

A *Hitelesítés-szolgáltató* által használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítvány*ai és a *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*ok alapmezői a következők:

- Verzió (Version)
A *Tanúsítvány* az X.509 specifikáció [20] szerinti "v3" *Tanúsítvány*oknak felel meg, így a mezőbe a "2" érték kerül.
- Sorozatszám (Serial Number)
A *Tanúsítvány* kibocsátó hitelesítő egység által generált egyedi azonosító.
A végfelhasználói *Tanúsítvány*ok 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 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 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 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 [20] 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
Lásd: 3.1.1. fejezet.
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 *Tanúsítvány*ban 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
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 alrendszerekben 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
Lásd: 3.1.1. fejezet. 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
A kulcs további engedélyezett használati körének meghatározása.
Nem szerepelhet.
- 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 *Tanúsítványok* 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 *Tanúsítványt* kibocsátó hitelesítési egység *Tanúsítványának* 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 (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, a *Tanúsítvány* alanya természetes személy-e;
 - az ETSI EN 319 411-1 által meghatározott hitelesítési rend azonosítója (OID), amelynek a *Tanúsítvány* megfelel.

A végfelhasználói *Tanúsítványok*nál 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 *Tanúsítványok*ban 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 webszerver *Tanúsítvány*okban kötelezően beállítandó és kizárólagosan megadandó érték: "digitalSignature", "keyEncipherment", "keyAgreement".
- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus
A kulcs engedélyezett használati körének további meghatározása.
A *Weboldal-hitelesítő tanúsítvány*okban kötelezően beállítandó és kizárólagosan megadandó érték: "serverAuth (1.3.6.1.5.5.7.3.1)"
- 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 *Tanúsítványt* kibocsátó hitelesítési egység *Tanúsítványának* http protokollon keresztüli elérési helyét.

- 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.

Más tanúsítvány kiterjesztés nem kerülhet kitöltésre.

7.1.3. Az algoritmus objektum azonosítója

Annak az algoritmusnak a megnevezése, amellyel a *Tanúsítvány* hitelesítésre került. Csak olyan aláíró algoritmus használható, amely megfelel a 6.1.5 fejezetben meghatározott követelményeknek. A *Hitelesítés-szolgáltató* által használható algoritmusokat a *Szolgáltatási szabályzatban* fel kell sorolni.

7.1.4. Névformák

A *Hitelesítés-szolgáltató* a jelen *Hitelesítési rendek* alapján kibocsátott *Tanúsítvány*okban egy – az RFC 5280 szabványban [17] illetve az ETSI EN 319 412-2, -3, -4 szabványokban [8], [9], [10] meghatározott attribútumokból összeállított – megkülönböztetett nevet kell használjon az *Alany* azonosítására.

A *Tanúsítványnak* 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) mezejében 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 RFC 5280 [17] 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 visszavonási listát hitelesítő elektronikus aláírás vagy bélyegző készítéséhez használt algoritmuskészlet azonosítója (OID). A minimálisan támogatandó algoritmuskészletek:
 - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11).
- Aláírás (Signature)
A *Hitelesítés-szolgáltató* visszavonási listát hitelesítő elektronikus aláírása vagy bélyegzője. A visszavonási listát az adott hitelesítő egység a *Tanúsítványok* aláírására vagy bélyegzésére használt kulcsával kell hitelesítse.
- Kibocsátó (Issuer)
A visszavonási listát kibocsátó hitelesítő egység egyedi azonosítója.
- Hatálybalépés (This Update)
A visszavonási lista hatálybalépésének kezdete. UTC szerinti érték az RFC 5280 [17] szerinti kódolással.
- Következő kibocsátás (Next Update)
A következő visszavonási lista kibocsátásának ideje (lásd: 4.10. fejezet). UTC szerinti érték az RFC 5280 [17] szerinti kódolással.
- Visszavont *Tanúsítványok* (Revoked Certificates)
A visszavont *Tanúsítványok* listája a *Tanúsítvány* sorozatszámával és a visszavonás idejével.

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

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

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

- expiredCertsOnCRL – nem kritikus
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
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 RFC 2560 [14] és RFC 6960 [19] szerinti online tanúsítvány-állapot szolgáltatást kell üzemeltetnie.

7.3.1. Verziószám(ok)

A *Hitelesítés-szolgáltató*nak támogatnia kell az RFC 2560 [14] és RFC 6960 [19] szerinti "v1" verziójú online tanúsítvány-állapot kéréseket és válaszokat.

7.3.2. OCSP kiterjesztések

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

- expiredCertsOnCRL – nem kritikus
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 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 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [5]
- ETSI EN 319 411-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [6]

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 szabályzatban* 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 végezheti el, amely rendelkezik egy EU tagállam nemzeti akkreditációs szervezete által kiadott erre feljogosító felhatalmazással.

8.3. Az auditor és az auditált rendszerem 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 megfelelősége;
- a dokumentálás;
- a fizikai biztonság;
- a személyi állomány megfelelősége;
- 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 elérhetővé kell tenni az *Előfizetők* részére.

9.1.1. Tanúsítvány kibocsátás és megújítás díjai

A *Hitelesítés-szolgáltató* díjat állapíthat meg a *Tanúsítványok* kibocsátásával, megújításával, módosításával és a kulcscserével 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* nem rendelkezik felelősségbiztosítással. A *Hitelesítés-szolgáltató* helytállását a 9.6.1. fejezet szabályozza.

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 információknak.

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 szabályzat*ában 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-szolgáltató*nak gondoskodnia kell az általa kezelt személyes adatok védelméről. Működésének és szabályzatainak meg kell felelniük az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [2] rendelkezéseinek.

A *Hitelesítés-szolgáltató* köteles az *Ügyfél*ről 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 szabályzat

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

9.4.3. Személyes adatnak nem minősülő adatok

A *Hitelesítés-szolgáltató* az *Igénylő* írásbeli hozzájárulása alapján nyilvánosságra hozhatja az *Alanyok Tanúsítvány*ban szereplő adatait. A *Tanúsítvány*ban a *Hitelesítés-szolgáltató* feltünteti az *Alany* személyéhez rendelt szolgáltatói egyedi azonosítót. A *Tanúsítvány*ban a *Hitelesítés-szolgáltató* feltünteti az *Alany*hoz rendelt szolgáltatói egyedi azonosítót.

9.4.4. Személyes adatok védelme

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

9.4.5. Személyes adatok felhasználása

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

9.4.6. Adatkezelés

A *Hitelesítés-szolgáltató* az *Ügyfél* értesítése nélkül is kiadhatja az *Ügyfél*ről tárolt személyes adatokat 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*, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

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

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

A *Hitelesítés-szolgáltató* tulajdonát képezi a tanúsítvány visszavonási állapot információ, amit a *Hitelesítés-szolgáltató* nyilvánosságra 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 *Tanúsítvány*ban szereplő azonosító (amely a *Tanúsítvány* alanyát azonosítja) használatára az *Ügyfél* jogosult.

A jelen *Hitelesítési rend* a *Hitelesítés-szolgáltató* kizárólagos tulajdonát képezi. Az *Ügyfelek*, *Igénylők* 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 szabályzat*ban 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 rend*ben, a vonatkozó *Szolgáltatási szabályzat*ban valamint az *Ügyfél*lel kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért, különösen a következő esetekben:

- 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 *Ügyfelek*kel szemben a Polgári Törvénykönyv [3] 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 [3] általános felelősségi szabálya szerint felelős;
- a *Hitelesítés-szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött Szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 9.8. fejezet);

A Szolgáltató kötelezettsége

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

9.6.3. Az Ügyfél felelőssége és helytállása

Az *Előfizető* felelőssége

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

Az *Előfizető* kötelezettségei

Az *Előfizető* 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* felfüggesztését vagy visszavonását és
 - 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 domain néven vagy IP címen elérhető;
- biztosítani, hogy a szolgáltatás igénybevételéhez szükséges adatokhoz és eszközökhöz (jelszavakhoz, titkos kódokhoz, aláírás-létrehozó eszközökhöz) illetéktelen személyek ne férhessenek hozzá;
- a *Hitelesítés-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 vagy felfüggesztését 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* felfüggeszteni, illetve visszavonni, amennyiben az *Előfizető* nem fizeti meg határidőre a szolgáltatások díját;
- *Szervezeti tanúsítvány* igénylése esetén köteles tudomásul venni, hogy a *Hitelesítés-szolgáltató* a *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
- *Weboldal-hitelesítő tanúsítvány* kibocsátásához az *Igénylő* köteles az adott domain tulajdonosának hozzájáruló nyilatkozatát a *Hitelesítés-szolgáltató* részére átadni;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* jogosult a *Tanúsítványt* felfüggeszteni illetve 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 jelen *Hitelesítési rendben* és a *Szolgáltatási szabályzatban* szerepel.

9.6.5. Egyéb szereplők tevékenységéért viselt felelősség és helytállás

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

9.7. Helytállás érvénytelenségi köre

A *Hitelesítés-szolgáltató* kizárja felelősségét, amennyiben:

- az *Érintett fél* nem körültekintően jár el a *Tanúsítványok* felhasználása vagy ellenőrzése során, azaz nem a jelen *Hitelesítési rend*, a *Szolgáltatási szabályzat* vagy a hatályos jogszabályok szerint jár el;
- az *Igénylők* nem tartják be a magánkulcs kezelésével kapcsolatos előírásokat;
- az *Érintett felek* vagy mások által kibocsátott szabályzatok nem felelnek meg a jelen *Hitelesítési rend*nek vagy a *Szolgáltatási szabályzat*nak;
- az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a Nemzeti Média- és Hírközlési Hatóság 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 szabályzat*ban és a Szolgáltatási szerződésben szabályozza az *Előfizetőkkel* szemben támasztott kártérítési igényeit.

9.9.3. Az érintett felek kártérítési kötelezettsége

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

9.10. Érvényesség és megszűnés

9.10.1. Érvényesség

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

9.10.2. Megszűnés

A *Hitelesítési rend* visszavonásig 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*.

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

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.

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

A *Hitelesítés-szolgáltató* a közzétett új szabályzat tervezettel kapcsolatos észrevételeket a hatályba lépést megelőző 14. napig fogadja az alábbi címen:

info@e-szigno.hu

Érdemi változtatást igénylő észrevétel esetén a dokumentumot megváltoztatja.

A szabályzat észrevételekkel módosított változatát a *Hitelesítés-szolgáltató* a hatályba lépést megelőző 7. napon zárja le és teszi közzé.

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];
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól [4];
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [5];
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [2];
- 2013. évi V. törvény a Polgári Törvénykönyvről [3].

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. 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] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
- [3] 2013. évi V. törvény a Polgári Törvénykönyvről.
- [4] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól.
- [5] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- [6] ETSI EN 319 411-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements .
- [7] ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- [8] 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; (Replaces ETSI TS 102 280).
- [9] 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 (Replaces ETSI TS 101 861).
- [10] 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.
- [11] ETSI TS 119 312 V1.1.1 (2014-11); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- [12] MSZ/ISO/IEC 15408 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai, 2002 december .
- [13] ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules".
- [14] IETF RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 1999.
- [15] IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.
- [16] IETF RFC 4043: Internet X.509 Public Key Infrastructure - Permanent Identifier, May 2005.

- [17] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.
- [18] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.
- [19] IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.
- [20] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
- [21] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.0. CA/Browser Forum, <https://cabforum.org/wp-content/uploads/CAB-Forum-BR-1.3.0.pdf>, 2015.
- [22] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.
- [23] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.