

## **e-Szignó Hitelesítés Szolgáltató**

### **Nem eIDAS Rendelet szerinti tanúsítvány hitelesítési rendek**

**ver. 2.13**

**Hatálybalépés: 2020-03-05**



Azonosító	1.3.6.1.4.1.21528.2.1.1.155.2.13, 1.3.6.1.4.1.21528.2.1.1.156.2.13, 1.3.6.1.4.1.21528.2.1.1.157.2.13, 1.3.6.1.4.1.21528.2.1.1.158.2.13, 1.3.6.1.4.1.21528.2.1.1.160.2.13, 1.3.6.1.4.1.21528.2.1.1.163.2.13, 1.3.6.1.4.1.21528.2.1.1.190.2.13, 1.3.6.1.4.1.21528.2.1.1.191.2.13
Verzió	2.13
Első verzió hatálybalépése	2016-07-01
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2020-03-03
Hatálybalépés dátuma	2020-03-05

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

Verzió	A változás leírása	Hatálybalépés	Készítette
2.0	Új szabályzat az RFC 3647 szerint.	2016-07-01	Szabóné Endrődi Csilla, Dr. Szőke Sándor
2.1	Módosítások az NMHH észrevételei alapján.	2016-09-05	Szomolya Melinda, Dr. Szőke Sándor
2.2	Módosítások a tanúsító észrevételei alapján.	2016-10-30	Dr. Szőke Sándor
2.4	Éves felülvizsgálat.	2017-09-30	Dr. Szőke Sándor
2.6	Teljes felülvizsgálat. Közjegyzői személy azonosítás bevezetése. Kisebb módosítások.	2018-03-24	Dr. Szőke Sándor
2.7	Éves felülvizsgálat.	2018-09-15	Dr. Szőke Sándor
2.8	Változások az auditor javaslatai alapján.	2018-12-14	Dr. Szőke Sándor
2.11	Éves felülvizsgálat.	2019-09-25	Dr. Szőke Sándor
2.12	Változások az auditor javaslatai alapján.	2019-12-12	Dr. Szőke Sándor
2.13	Hatály. Személyes azonosítás szabályai. Tanúsítvány módosítás. HSM követelmények. Kisebb pontosítások.	2020-03-05	Dr. Szőke Sándor

## Tartalomjegyzék

<b>1. Bevezetés</b>	<b>12</b>
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 . . . . .	17
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 . . . . .	18
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
<b>2. Közzététel és tanúsítványtár</b>	<b>26</b>
2.1. Adatbázisok - tanúsítványtárak . . . . .	26
2.2. A tanúsítványokra vonatkozó információk közzététele . . . . .	26
2.2.1. Szolgáltatói információ közzététele . . . . .	27
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 . . . . .	28
2.4. A tanúsítványtár elérésének szabályai . . . . .	28
<b>3. Azonosítás és hitelesítés</b>	<b>28</b>
3.1. Elnevezések . . . . .	28
3.1.1. Név típusok . . . . .	28

3.1.2.	A nevek értelmezhetősége . . . . .	32
3.1.3.	Álnevek használata . . . . .	33
3.1.4.	A különböző elnevezési formák értelmezési szabályai . . . . .	33
3.1.5.	A nevek egyedisége . . . . .	33
3.1.6.	Márkanév elismerése, azonosítása, szerepük . . . . .	33
3.2.	Kezdeti regisztráció, azonosság hitelesítése . . . . .	33
3.2.1.	A magánkulcs birtoklásának igazolása . . . . .	33
3.2.2.	Szervezet azonosságának hitelesítése . . . . .	34
3.2.3.	Természetes személy azonosságának hitelesítése . . . . .	34
3.2.4.	Nem ellenőrzött alany információk . . . . .	36
3.2.5.	Jogok, felhatalmazások ellenőrzése . . . . .	36
3.2.6.	Együttműködési képességre vonatkozó követelmények . . . . .	36
3.3.	Azonosítás és hitelesítés kulcscsere kérelem esetén . . . . .	37
3.3.1.	Azonosítás és hitelesítés érvényes tanúsítvány esetén . . . . .	37
3.3.2.	Azonosítás és hitelesítés érvénytelen tanúsítvány esetén . . . . .	37
3.4.	Azonosítás és hitelesítés tanúsítvány megújítás esetén . . . . .	37
3.4.1.	Azonosítás és hitelesítés érvényes tanúsítvány esetén . . . . .	37
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 . . . . .	38
3.5.2.	Azonosítás és hitelesítés érvénytelen tanúsítvány esetén . . . . .	38
3.6.	Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási kérelem esetén . . . . .	38
3.7.	Ellenőrzött kommunikációs csatorna . . . . .	38
<b>4.</b>	<b>A tanúsítványok életciklusára vonatkozó követelmények</b>	<b>38</b>
4.1.	Tanúsítványkérelem . . . . .	38
4.1.1.	Ki nyújthat be tanúsítványkérelmet . . . . .	39
4.1.2.	A bejegyzés folyamata és a résztvevők felelőssége . . . . .	40
4.2.	A tanúsítványkérelem feldolgozása . . . . .	41
4.2.1.	Az igénylő azonosítása és hitelesítése . . . . .	41
4.2.2.	A tanúsítványkérelem elfogadása vagy visszautasítása . . . . .	41
4.2.3.	A tanúsítványkérelem 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 . . . . .	42
4.4.	A tanúsítvány elfogadása . . . . .	42
4.4.1.	A tanúsítvány elfogadás módja . . . . .	42
4.4.2.	A tanúsítvány közzététele . . . . .	42
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 . . . . .	43
4.6.	Tanúsítvány megújítás . . . . .	43
4.6.1.	A tanúsítvány megújítás körülményei . . . . .	43
4.6.2.	Ki kérelmezheti a tanúsítvány megújítást . . . . .	44
4.6.3.	A tanúsítvány megújítási kérelmek feldolgozása . . . . .	44
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 . . . . .	45
4.7.1.	A kulcscsere körülményei . . . . .	45
4.7.2.	Ki kérelmezheti a kulcscserét . . . . .	45
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 . . . . .	46
4.7.7.	További szereplők értesítése a tanúsítvány kibocsátásáról . . . . .	46
4.8.	Tanúsítvány módosítás . . . . .	46
4.8.1.	A tanúsítvány módosítás körülményei . . . . .	46
4.8.2.	Ki kérelmezheti a tanúsítvány módosítást . . . . .	46
4.8.3.	A tanúsítvány módosítási kérelmek feldolgozása . . . . .	47
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 . . . . .	48
4.9.2.	Ki kérelmezheti a visszavonást . . . . .	51
4.9.3.	A visszavonási kérelemre vonatkozó eljárás . . . . .	51
4.9.4.	A visszavonási kérelemre vonatkozó kivárási idő . . . . .	52
4.9.5.	A visszavonási eljárás maximális hossza . . . . .	52
4.9.6.	Az Érintett felek számára javasolt eljárás a visszavonási információ ellenőrzésére . . . . .	52
4.9.7.	A visszavonási lista kibocsátás gyakorisága . . . . .	52
4.9.8.	A visszavonási lista előállítás és közzététele közötti idő maximális hossza . . . . .	52
4.9.9.	Valós idejű tanúsítvány állapot ellenőrzés lehetősége . . . . .	52
4.9.10.	A valós idejű tanúsítvány állapot ellenőrzésre vonatkozó követelmények . . . . .	52

4.9.11.	A visszavonási hirdetések egyéb elérhető formái . . . . .	52
4.9.12.	A kulcs kompromittálódásra vonatkozó speciális követelmények . . . . .	53
4.9.13.	A felfüggesztés körülményei . . . . .	53
4.9.14.	Ki kérelmezheti a felfüggesztést . . . . .	53
4.9.15.	A felfüggesztési kérelemre vonatkozó eljárás . . . . .	53
4.9.16.	A felfüggesztés maximális hossza . . . . .	53
4.10.	Tanúsítvány állapot szolgáltatások . . . . .	53
4.10.1.	Működési jellemzők . . . . .	54
4.10.2.	A szolgáltatás rendelkezésre állása . . . . .	54
4.10.3.	Opcionális lehetőségek . . . . .	54
4.11.	Az előfizetés vége . . . . .	54
4.12.	Magánkulcs letétbe helyezése és visszaállítása . . . . .	55
4.12.1.	Kulcsletét és visszaállítás rendje és szabályai . . . . .	55
4.12.2.	Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai . . . . .	55
<b>5.</b>	<b>Elhelyezési, eljárásbeli és üzemeltetési előírások</b>	<b>55</b>
5.1.	Fizikai követelmények . . . . .	55
5.1.1.	A telephely elhelyezése és szerkezeti felépítése . . . . .	56
5.1.2.	Fizikai hozzáférés . . . . .	56
5.1.3.	Áramellátás és légkondicionálás . . . . .	57
5.1.4.	Beázás és elárasztódás veszély kezelése . . . . .	57
5.1.5.	Tűz megelőzés és tűzvédelem . . . . .	57
5.1.6.	Adathordozók tárolása . . . . .	57
5.1.7.	Hulladék megsemmisítése . . . . .	57
5.1.8.	A mentési példányok fizikai elkülönítése . . . . .	58
5.2.	Eljárásbeli előírások . . . . .	58
5.2.1.	Bizalmi szerepkörök . . . . .	58
5.2.2.	Az egyes feladatok ellátásához szükséges személyzeti létszámok . . . . .	59
5.2.3.	Az egyes szerepkörökben elvárt azonosítás és hitelesítés . . . . .	59
5.2.4.	Egymást kizáró szerepkörök . . . . .	59
5.3.	Személyzetre vonatkozó előírások . . . . .	60
5.3.1.	Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények . . . . .	60
5.3.2.	Előélet vizsgálatára vonatkozó eljárások . . . . .	60
5.3.3.	Képzési követelmények . . . . .	61
5.3.4.	Továbbképzési gyakoriságok és követelmények . . . . .	61
5.3.5.	Munkabeosztás körforgásának sorrendje és gyakorisága . . . . .	62
5.3.6.	Felhatalmazás nélküli tevékenységek büntető következményei . . . . .	62

5.3.7.	Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények . . .	62
5.3.8.	A személyzet számára biztosított dokumentációk . . . . .	62
5.4.	Naplózási eljárások . . . . .	62
5.4.1.	A tárolt események típusai . . . . .	62
5.4.2.	A naplófájl feldolgozásának gyakorisága . . . . .	65
5.4.3.	A naplófájl megőrzési időtartama . . . . .	66
5.4.4.	A naplófájl védelme . . . . .	66
5.4.5.	A naplófájl mentési eljárásai . . . . .	66
5.4.6.	A naplózás adatgyűjtési rendszere . . . . .	66
5.4.7.	Az eseményeket kiváltó alanyok értesítése . . . . .	66
5.4.8.	Sebezhetőség felmérése . . . . .	66
5.5.	Adatok archiválása . . . . .	67
5.5.1.	Az archivált adatok típusai . . . . .	67
5.5.2.	Az archívum megőrzési időtartama . . . . .	67
5.5.3.	Az archívum védelme . . . . .	68
5.5.4.	Az archívum mentési folyamatai . . . . .	68
5.5.5.	Az adatok időbélyegzésére vonatkozó követelmények . . . . .	68
5.5.6.	Az archívum gyűjtési rendszere . . . . .	68
5.5.7.	Archív információk hozzáférését és ellenőrzését végző eljárások . . . . .	69
5.6.	Szolgáltatói kulcs cseréje . . . . .	69
5.7.	Kompromittálódást és katasztrófát követő helyreállítás . . . . .	69
5.7.1.	Váratlan esemény és kompromittálódás kezelési eljárások . . . . .	69
5.7.2.	Meghibásodott IT erőforrások, szoftverek és/vagy adatok . . . . .	70
5.7.3.	Magánkulcs kompromittálódása esetén követendő eljárások . . . . .	70
5.7.4.	Működés folyamatosságának biztosítása katasztrófát követően . . . . .	70
5.8.	A hitelesítés-szolgáltató vagy a regisztráló szervezet leállítása . . . . .	71
<b>6.</b>	<b>Műszaki biztonsági óvintézkedések</b>	<b>71</b>
6.1.	Kulcspár előállítás és telepítése . . . . .	71
6.1.1.	Kulcspár előállítás . . . . .	71
6.1.2.	Magánkulcs eljuttatása az igénylőhöz . . . . .	73
6.1.3.	A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz . . . . .	73
6.1.4.	A szolgáltatói nyilvános kulcs közzététele . . . . .	73
6.1.5.	Kulcsméret . . . . .	74
6.1.6.	A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése . . . . .	74
6.1.7.	A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően) . . . . .	74
6.2.	A magánkulcsok védelme . . . . .	75
6.2.1.	Kriptográfiai modulra vonatkozó szabványok és előírások . . . . .	75



6.2.2.	Magánkulcs többszereplős (n-ből m) használata . . . . .	76
6.2.3.	Magánkulcs letétbe helyezése . . . . .	76
6.2.4.	Magánkulcs mentése . . . . .	76
6.2.5.	Magánkulcs archiválása . . . . .	76
6.2.6.	Magánkulcs bejuttatása hardver kriptográfiai eszközbe, vagy onnan történő exportja . . . . .	76
6.2.7.	Magánkulcs tárolása hardver kriptográfiai eszközben . . . . .	77
6.2.8.	A magánkulcs aktiválásának módja . . . . .	77
6.2.9.	A magánkulcs deaktiválásának módja . . . . .	77
6.2.10.	A magánkulcs megsemmisítésének módja . . . . .	78
6.2.11.	A hardver kriptográfiai eszközök értékelése . . . . .	78
6.3.	A kulcspár kezelés egyéb szempontjai . . . . .	79
6.3.1.	Nyilvános kulcs archiválása . . . . .	79
6.3.2.	A tanúsítványok és kulcspárok használatának periódusa . . . . .	79
6.4.	Aktivizáló adatok . . . . .	80
6.4.1.	Aktivizáló adatok előállítása és telepítése . . . . .	80
6.4.2.	Az aktivizáló adatok védelme . . . . .	80
6.4.3.	Az aktivizáló adatok kezelésének egyéb szempontjai . . . . .	81
6.5.	Informatikai biztonsági előírások . . . . .	81
6.5.1.	Speciális informatikai biztonsági műszaki követelmények . . . . .	81
6.5.2.	Az informatikai biztonság értékelése . . . . .	81
6.6.	Életciklusra vonatkozó műszaki előírások . . . . .	81
6.6.1.	Rendszerfejlesztési előírások . . . . .	81
6.6.2.	Biztonságkezelési előírások . . . . .	82
6.6.3.	Életciklusra vonatkozó biztonsági előírások . . . . .	82
6.7.	Hálózati biztonsági előírások . . . . .	83
6.8.	Időbélyegzés . . . . .	84
<b>7.</b>	<b>Tanúsítvány, CRL és OCSP profilok</b>	<b>84</b>
7.1.	Tanúsítvány profil . . . . .	84
7.1.1.	Verzió szám(ok) . . . . .	84
7.1.2.	Tanúsítvány kiterjesztések . . . . .	85
7.1.3.	Az algoritmus objektum azonosítója . . . . .	91
7.1.4.	Névformák . . . . .	91
7.1.5.	Névhasználati megkötöttségek . . . . .	92
7.1.6.	A Hitelesítési rend objektum azonosítója . . . . .	92
7.1.7.	A Hitelesítési rend megkötöttségek kiterjesztés használata . . . . .	92
7.1.8.	A Hitelesítési rend jellemzők szintaktikája és szemantikája . . . . .	92
7.1.9.	A kritikus Hitelesítési rend kiterjesztések feldolgozási szemantikája . . . . .	92

7.2.	Tanúsítvány visszavonási lista (CRL) profil . . . . .	92
7.2.1.	Verziószám(ok) . . . . .	92
7.2.2.	Tanúsítvány visszavonási lista kiterjesztések . . . . .	92
7.3.	Online tanúsítvány-állapot válasz (OCSP) profil . . . . .	94
7.3.1.	Verziószám(ok) . . . . .	94
7.3.2.	OCSP kiterjesztések . . . . .	94
<b>8.</b>	<b>A megfelelés vizsgálat</b>	<b>95</b>
8.1.	Az ellenőrzések körülményei és gyakorisága . . . . .	95
8.2.	Az auditor és szükséges képesítése . . . . .	96
8.3.	Az auditor és az auditált rendszerelem függetlensége . . . . .	96
8.4.	Az auditálás által lefedett területek . . . . .	96
8.5.	A hiányosságok kezelése . . . . .	96
8.6.	Az eredmények közzététele . . . . .	97
<b>9.</b>	<b>Egyéb üzleti és jogi kérdések</b>	<b>97</b>
9.1.	Díjak . . . . .	97
9.1.1.	Tanúsítvány kibocsátás és megújítás díjai . . . . .	97
9.1.2.	Tanúsítvány hozzáférés díja . . . . .	97
9.1.3.	Visszavonási állapot információ hozzáférés díja . . . . .	97
9.1.4.	Egyéb szolgáltatások díjai . . . . .	97
9.1.5.	Visszatérítési politika . . . . .	97
9.2.	Anyagi felelősségvállalás . . . . .	97
9.2.1.	Pénzügyi követelmények . . . . .	98
9.2.2.	További követelmények . . . . .	98
9.2.3.	Felelősségbiztosítás . . . . .	98
9.3.	Bizalmasság . . . . .	98
9.3.1.	Bizalmas információk köre . . . . .	98
9.3.2.	Bizalmas információk körén kívül eső adatok . . . . .	98
9.3.3.	Bizalmas információ védelme . . . . .	98
9.4.	Személyes adatok védelme . . . . .	98
9.4.1.	Adatkezelési szabályzat . . . . .	99
9.4.2.	Személyes adatok . . . . .	99
9.4.3.	Személyes adatnak nem minősülő adatok . . . . .	99
9.4.4.	Személyes adatok védelme . . . . .	99
9.4.5.	Személyes adatok felhasználása . . . . .	99
9.4.6.	Adatkezelés . . . . .	99
9.4.7.	Egyéb adatvédelmi követelmények . . . . .	99
9.5.	Szellemi tulajdonjogok . . . . .	100

9.6.	Tevékenységért viselt felelősség és helytállás . . . . .	100
9.6.1.	A szolgáltató felelőssége és helytállása . . . . .	100
9.6.2.	A regisztráló szervezet felelőssége és helytállása . . . . .	102
9.6.3.	Az Ügyfél felelőssége és helytállása . . . . .	102
9.6.4.	Az Érintett fél felelőssége . . . . .	104
9.6.5.	Egyéb szereplők tevékenységéért viselt felelősség és helytállás . . . . .	105
9.7.	Helytállás érvénytelenségi köre . . . . .	105
9.8.	A felelősség korlátozása . . . . .	105
9.9.	Kártérítési kötelezettség . . . . .	105
9.9.1.	A szolgáltató kártérítési kötelezettsége . . . . .	105
9.9.2.	Az előfizető kártérítési kötelezettsége . . . . .	105
9.9.3.	Az érintett felek kártérítési kötelezettsége . . . . .	105
9.10.	Érvényesség és megszűnés . . . . .	105
9.10.1.	Érvényesség . . . . .	105
9.10.2.	Megszűnés . . . . .	106
9.10.3.	A megszűnés következményei . . . . .	106
9.11.	A felek közötti kommunikáció . . . . .	106
9.12.	Módosítások . . . . .	106
9.12.1.	Módosítási eljárás . . . . .	106
9.12.2.	Értesítések módja és határideje . . . . .	106
9.12.3.	Az OID megváltoztatása . . . . .	106
9.13.	Vitás kérdések rendezése . . . . .	106
9.14.	Irányadó jog . . . . .	107
9.15.	Az érvényben lévő jogszabályoknak való megfelelés . . . . .	107
9.16.	Vegyes rendelkezések . . . . .	107
9.16.1.	Teljességi záradék . . . . .	107
9.16.2.	Átruházás . . . . .	107
9.16.3.	Részleges érvénytelenség . . . . .	107
9.16.4.	Igényérvényesítés . . . . .	107
9.16.5.	Vis maior . . . . .	108
9.17.	Egyéb rendelkezések . . . . .	108
<b>A.</b>	<b>A rövid hitelesítési rend azonosítók képzési szabályai</b>	<b>109</b>
<b>B.</b>	<b>Hivatkozások</b>	<b>110</b>

## 1. Bevezetés

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

### 1.1. Áttekintés

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

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

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

A *Hitelesítési rendek* alapvető követelményeket fogalmaznak meg a *Tanúsítvány*okkal kapcsolatban, elsősorban a *Tanúsítványt* 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	Nem eIDAS Rendelet szerinti tanúsítvány hitelesítési rendek

Dokumentum verziószáma	2.13
Hatálybalépés ideje	2020-03-05

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
1.3.6.1.4.1.21528.2.1.1.155.2.13	Nem eIDAS Rendelet szerinti, III. hitelesítési osztályba tartozó, természetes személyek számára <i>Hardver kriptográfiai eszközön kibocsátott Tanúsítványokat szabályozó, álnevet kizáró hitelesítési rend.</i>	HETHN

1.3.6.1.4.1.21528.2.1.1.156.2.1	3Nem eIDAS Rendelet szerinti, III. hitelesítési osztályba tartozó, természetes személyek számára szoftveresen kibocsátott <i>Tanúsítványok</i> at szabályozó, álnevet kizáró hitelesítési rend.	HETSN
1.3.6.1.4.1.21528.2.1.1.158.2.1	3Nem eIDAS Rendelet szerinti, III. hitelesítési osztályba tartozó, nem természetes személyek számára szoftveresen kibocsátott <i>Tanúsítványok</i> at szabályozó, álnevet kizáró hitelesítési rend.	HEJSN
1.3.6.1.4.1.21528.2.1.1.160.2.1	3Nem eIDAS Rendelet szerinti, II. hitelesítési osztályba tartozó, álnevet kizáró hitelesítési rend.	KExxN
1.3.6.1.4.1.21528.2.1.1.190.2.1	3Nem eIDAS Rendelet szerinti kódalíró, III. hitelesítési osztályba tartozó <i>Tanúsítványok</i> kibocsátását szabályozó, álnevet kizáró hitelesítési rend.	HKxxN
1.3.6.1.4.1.21528.2.1.1.191.2.1	3Nem eIDAS Rendelet szerinti kódalíró, II. hitelesítési osztályba tartozó <i>Tanúsítványok</i> kibocsátását szabályozó, álnevet kizáró hitelesítési rend.	KKxxN

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

A *Hitelesítés-szolgáltató* nem ad ki álneves *Tanúsítványt*.

Ezen *Hitelesítési rendek* alapján a *Hitelesítés-szolgáltató* többféle felhasználási célra (titkosítás, autentikáció stb.) bocsáthat ki *Tanúsítványt*. (A megadható felhasználási célok listáját a 7.1.2. *Tanúsítvány* kiterjesztések fejezet tartalmazza.)

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 természetes személyek számára kibocsátott *Tanúsítványokra* vonatkozó *Hitelesítési rendek* esetén az *Alany* minden esetben természetes személy.

A nem természetes személyek számára kibocsátott *Tanúsítványokra* vonatkozó *Hitelesítési rendek* esetén az *Alany* jogi személy.

A *Tanúsítványok*ban szerepeltethető az informatikai rendszer, alkalmazás vagy automatizmus megnevezése is, amely segítségével a *Tanúsítványt* használják (*Automata tanúsítvány*).

A *Hardver kriptográfiai eszköz* használatát megkövetelő *Hitelesítési rendek* ([xxxHx]) esetén a *Hitelesítés-szolgáltató* meggyőződik róla, hogy a *Tanúsítványhoz* tartozó magánkulcs az alábbi *Tanúsítványok* legalább egyikével rendelkező *Hardver kriptográfiai eszközön* helyezkedik el:

- az Európai Unió valamely tagállamában nyilvántartásba vett tanúsító szervezet által kiadott igazolás szerint *HSM* eszközre vonatkozó tanúsítás;
- legalább EAL-4 szintű Common Criteria [28] *Tanúsítvány* a CEN SSCD PP [30] szerint;

- legalább EAL-4 szintű Common Criteria [28] tanúsítvány a CEN 419 221-5 [17] szerint;
- FIPS 140-2, Level 2 (vagy magasabb szintű) tanúsítvány [27].

Jelen *Hitelesítési rendek* közül:

- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [10] szabványban definiált [LCP] *Hitelesítési rend*nek;
- a [KE<sub>xx</sub>N] és [KK<sub>xx</sub>N] *Hitelesítési rend* kivételével az összes *Hitelesítési rend* megfelel az [NCP] *Hitelesítési rend*nek;
- a [HETHN] *Hitelesítési rend* megfelel az [NCP+] *Hitelesítési rend*nek.

### Megfelelés az ETSI hitelesítési rendeknek

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

	[LCP]	[NCP]	[NCP+]
HETHN	(x)	(x)	X
HETSN	(x)	X	
HEJSN	(x)	X	
KE <sub>xx</sub> N	X		
HK <sub>xx</sub> N	(x)	X	
KK <sub>xx</sub> N	X		

#### 1.2.2. Hatály

Jelen *Hitelesítési rend* gyűjtemény 2020-03-05 -i hatálybalépési dátumtól visszavonásáig hatályos. A hatályosság automatikusan megszűnik a *Hitelesítési rend* újabb verziójának hatályba lépésekor.

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

A *Hitelesítési rend* hatálya kiterjed az 1.3. alfejezetben azonosított közösség minden egyes tagjára. A jelen *Hitelesítési 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* [M\*\*\*\*];
- nem minősített, e-Szignó Hitelesítés Szolgáltató által kiadott III. hitelesítési osztályba tartozó *Tanúsítványok* [H\*\*\*\*];
- nem minősített, e-Szignó Hitelesítés Szolgáltató által kiadott II. hitelesítési osztályba tartozó *Tanúsítványok* [K\*\*\*\*];
- nem minősített, nem e-Szignó Hitelesítés Szolgáltató által kiadott *Tanúsítványok*.

A használt hordozó alapján a biztonság szerint csökkenő sorrendben:

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

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

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

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

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

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



### 1.3. PKI szereplők

#### 1.3.1. Hitelesítés-szolgáltató

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

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

#### 1.3.2. Regisztráló szervezetek

Meghatározását lásd az 1.6 fejezetben.

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

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

#### 1.3.3. Ügyfelek

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

Az *Alany* az a természetes személy vagy jogi személy, aki vagy amely adatai a *Tanúsítványban* szerepelnek.

#### 1.3.4. Érintett felek

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

#### 1.3.5. Egyéb szereplők

A megfelelésértékelést végző független auditor.

A szolgáltatás felügyeletét ellátó hatóság.

A *Képviselt szervezet*, amelynek neve feltüntetésre kerül egy természetes személy 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* felfüggesztheti illetve 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 a *Tanúsítványban* a *Hitelesítés-szolgáltató* által beállított attribútum értékek, a *Hitelesítési rend* és a *Szolgáltatási szabályzat* által meghatározott célra használhatóak fel. A felhasználási cél jellemzően lehet titkosítás vagy autentikáció, de a konkrét felhasználási céltől függően ezeken belül is lehetnek eltérések a beállított attribútum értékekben (lásd: 6.1.7. fejezet).

##### 1.4.2. Tiltott tanúsítvány használat

A jelen *Hitelesítési rend* alapján kibocsátott *Tanúsítványokat*, illetve a hozzájuk tartozó magánkulcsokat a *Tanúsítványban* a *Hitelesítés-szolgáltató* által beállított attribútum értékek, a *Hitelesítési rend* és a *Szolgáltatási szabályzat* által meghatározottól 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 találhatóak:

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

##### 1.5.2. Kapcsolattartó személy

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

Kapcsolattartó	Folyamatszervezés részleg vezetője
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1033 Budapest, Angel Sanz Briz út 13. C épület
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445

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

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

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

### 1.5.4. A Szolgáltatási szabályzat elfogadási eljárása

A jelen *Hitelesítési rend*nek való megfelelést kinyilatkoztató *Szolgáltatási szabályzat* elfogadási eljárását a *Hitelesítés-szolgáltatónak* ismertetnie kell az adott *Szolgáltatási szabályzat*ban.

## 1.6. Fogalmak és rövidítések

### 1.6.1. Fogalmak

II. hitelesítési osztály	Olyan nem minősített <i>Hitelesítési rend</i> ek csoportja, amelyek az <i>Igénylő</i> távoli regisztrációja alapján is lehetővé teszik a <i>Tanúsítvány</i> kibocsátását.
III. hitelesítési osztály	Olyan nem minősített <i>Hitelesítési rend</i> ek 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)	A <i>Tanúsítvány</i> által azonosított természetes személy, <i>Szervezet</i> , vagy informatikai eszköz, rendszer, egység. Az <i>Alany</i> lehet maga az <i>Igénylő</i> vagy az <i>Igénylő</i> kontrollja alatt álló eszköz.
Autentikáció	Nyilvános kulcsú tanúsítvány alapú autentikáció alatt azt a folyamatot értjük, amikor egy <i>Érintett fél</i> ellenőrzi a <i>Tanúsítvány Alanyának</i> (természetes személy, szervezet vagy alkalmazás, weboldal, szolgáltatás, szerver) azonosságát egy erre szolgáló eljárás segítségével, amelyben az azonosítandó <i>Alany</i> nak a magánkulcsát kell használnia, és azonossága a <i>Tanúsítványa</i> alapján ellenőrizhető.

<i>Automata tanúsítvány</i>	Olyan <i>Tanúsítvány</i> , amelyben az <i>Alany</i> adatai között feltüntetésre kerül az informatikai eszköz (alkalmazás, rendszer) elnevezése is, amely segítségével az <i>Alany</i> a <i>Tanúsítványt</i> használja.
Bizalmi felügyelet	"A <i>Bizalmi szolgáltatások</i> felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [8] 91.§ 1. bekezdés)
Bizalmi szolgáltatás (Trust Service)	<p>"Rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások:</p> <ul style="list-style-type: none"> <li>• elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy</li> <li>• <i>Weboldal-hitelesítő tanúsítványok</i> létrehozása, ellenőrzése és érvényesítése; vagy</li> <li>• elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése;</li> </ul>
	" (eIDAS [1] 3. cikk 16. pont)
Bizalmi szolgáltatási rend (Trust Service Policy)	"Olyan szabálygyűjtemény, amelyben egy <i>Bizalmi szolgáltató</i> , igénybe vevő vagy más személy valamely <i>Bizalmi szolgáltatás</i> használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára. " (2015. évi CCXXII. törvény [8] 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)	Titkosítás esetében az a fél, aki a címzett számára az elektronikus dokumentumot titkosítja. Autentikáció esetében az a fél, aki egy erre szolgáló eljárás során ellenőrzi a magát azonosítani kívánó fél azonosságát.
Érvényességi lánc	"Az elektronikus dokumentum vagy annak lenyomata és azon egymáshoz rendelhető információk (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás vagy bélyegző létrehozásához használt adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató érvényességi adatára és annak visszavonására vonatkozó információk) sorozata, amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, bélyegző vagy időbélyegző, az aláírás, bélyegző vagy időbélyegző elhelyezésének időpontjában érvényes volt. " (2015. évi CCXXII. törvény [8] 1. § 21. pont)
Felfüggesztés	A <i>Tanúsítvány</i> érvényességének ideiglenes megszüntetése a <i>Tanúsítványban</i> is feltüntetett érvényességi idő lejártá előtt. A <i>Tanúsítvány</i> felfüggesztése nem végleges, a felfüggesztett <i>Tanúsítvány</i> érvényessége visszaállítható.
Gyökér tanúsítvány (Root Certificate)	Más néven legfelső szintű tanúsítvány. 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, nyilvános kulcsokat 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 [8] 1. § 24. pont)
Igénylő	Az a természetes személy, aki az adott <i>Tanúsítvány</i> igénylése során eljár.
Képviselet szervezet	Az a <i>Szervezet</i> , amelynek a nevében a <i>Szervezeti ügyintéző</i> eljár a <i>Szervezethez</i> tartozó <i>Tanúsítványokkal</i> kapcsolatos ügyekben.
Kompromittálódás	Egy kriptográfiai kulcs abban az esetben tekintendő kompromittálódottnak, ha vélelmezhető, hogy illetéktelen személynek is hozzáférése van hozzá.
Köztes hitelesítő egység	Olyan <i>Hitelesítő egység</i> amelynek <i>Tanúsítványát</i> egy másik <i>Hitelesítő egység</i> bocsátotta ki.
Kriptográfiai kulcs (Cryptographic Key)	Olyan – kriptográfiai transzformációt vezérlő – egyedi digitális jelsorozat, amelynek ismerete szükséges titkosításhoz és dekódoláshoz, illetve digitális aláírás előállításához és ellenőrzéséhez.
Kulcsgondozás (Key Management)	A kriptográfiai kulcsok előállítása, a felhasználókhöz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, amely szoros kapcsolatban áll az alkalmazott biztonsági eljárásmóddal.

Magánkulcs	<p>A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az <i>Alan</i>nak szigorúan titokban kell tartania. Titkosítás esetében a címzettnek a magánkulcsára van szüksége ahhoz, hogy a számára titkosított dokumentumot vissza tudja fejteni. Autentikáció esetében az azonosítandó félnek a magánkulcsát kell használnia az azonosságát ellenőrző eljárás során.</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. Titkosítás esetében a címzett fél nyilvános kulcsa szükséges ahhoz, hogy számára titkosított dokumentumot készítsünk. Autentikáció esetében az azonosítandó fél nyilvános kulcsa szükséges ahhoz, hogy az azonosságát ellenőrizni lehessen.</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>Tanúsítványkérelem</i> és a szolgáltatói szerződés előkészítése céljából az <i>Ügyfél</i> által a Szolgáltatónak előzetesen megadott adatok és nyilatkozatok, amelyben többek között felhatalmazza a Szolgáltatót az adatok kezelésére.</p>
Regisztráló szervezet (Registration Authority)	<p>Szervezet, amely ellenőrzi a <i>Tanúsítványba</i> kerülő adatok valódiságát, az <i>Igénylő</i> személy azonosságát, ellenőrzi, hogy a <i>Tanúsítványkérelem</i> hiteles-e, és azt egy arra jogosult személy nyújtotta-e be.</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>

Szerver autentikációs tanúsítvány	Olyan <i>Tanúsítvány</i> amely egy adott szerver, vagy annak egy szolgáltatásának azonosítására szolgál. Az ilyen <i>Tanúsítvány</i> okban a CN mezőben egy adott doménnév vagy IP cím szerepel. Ilyenek például a CISCO VPN szerver, domén kontroller, SCEP szerver, VPN szerver számára kiadott <i>Tanúsítvány</i> ok.
Szervezet	Jogi személy.
Szervezeti tanúsítvány	Olyan <i>Tanúsítvány</i> , amelynek <i>Alanya Szervezet</i> , vagy amely egy természetes személy <i>Alany</i> valamely <i>Szervezethez</i> való tartozását mutatja. Ilyen esetben a <i>Tanúsítvány</i> "O" mezejében a <i>Szervezet</i> neve feltüntetésre kerül.
Szervezeti ügyintéző	Az <i>Előfizető</i> képviselőjében eljáró természetes személy, aki jogosult az <i>Előfizető</i> nevében a <i>Tanúsítványkérelem</i> benyújtására, a <i>Tanúsítvány</i> kibocsátás jóváhagyására, az <i>Előfizető</i> höz kapcsolódó <i>Tanúsítvány</i> ok igénylése, cseréje, felfüggesztése, visszaállítása és visszavonása során eljárni.
Szolgáltatási szabályzat (Trust Service Practice Statement)	"A <i>Bizalmi szolgáltató</i> nyilatkozata az egyes <i>Bizalmi szolgáltatások</i> nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről. " (2015. évi CCXXII. törvény [8] 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 [8] 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 [8] 1. § 44.)
Tanúsítványkérelem	Az <i>Igénylő</i> által, a Szolgáltató számára a <i>Tanúsítvány</i> kibocsátás érdekében benyújtott adatok és nyilatkozatok, amelyekben többek között az <i>Igénylő</i> megerősíti a <i>Tanúsítvány</i> ba kerülő adatok valóságát.



Tanúsítványtár	Különböző <i>Tanúsítvány</i> okat tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott <i>Tanúsítvány</i> okat publikálja, de Tanúsítványtárnak nevezzük az <i>Alany</i> illetve az <i>Érintett fél</i> számítógépén a használt alkalmazás számára elérhető <i>Tanúsítvány</i> okat tartalmazó rendszert is.
Titkosítás	Nyilvános kulcsú titkosítás alatt azt a folyamatot értjük, amikor a feladó a címzett nyilvános kulcsának segítségével kódolja a dokumentumot, amely ezután csak a címzett fél magánkulcsával fejthető vissza.
Ügyfél	Az <i>Előfizető</i> és a hozzá tartozó összes <i>Igénylő</i> együttes elnevezése.
Visszavonás	A <i>Tanúsítvány</i> érvényességének megszüntetése a <i>Tanúsítvány</i> ban is feltüntetett érvényességi idő lejárta előtt. A <i>Tanúsítvány</i> visszavonása végleges, visszavont <i>Tanúsítvány</i> többet nem tehető érvényessé.
Visszavonási állapot nyilvántartás	A <i>Hitelesítés-szolgáltató</i> által vezetett belső nyilvántartás a felfüggesztett, illetőleg a visszavont <i>Tanúsítvány</i> okról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját másodperc pontossággal.

### 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 közlétező 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* hozza nyilvánosságra a bizalmi szolgáltatásainak tanúsítványait.

A *Hitelesítés-szolgáltató* tegye közzé a honlapján a

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

#### Szolgáltatói tanúsítványok

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

- A gyökér hitelesítő egységek megnevezését, illetve *Gyökér tanúsítványaik* lenyomatát a *Szolgáltatási szabályzatban* (lásd: 1.3.1. fejezet). Az állapotváltozásukkal kapcsolatos információk legyenek elérhetőek a *Hitelesítés-szolgáltató* honlapján.
- A köztes (nem gyökér) hitelesítő egységek *Tanúsítványainak* állapotváltozását hozza nyilvánosságra a *Tanúsítvány visszavonási listákon*, saját honlapján, valamint az online tanúsítvány-állapot válasz szolgáltatás keretében.
- Az online tanúsítvány-állapot válaszokat aláíró válaszadók számára a *Hitelesítés-szolgáltató* – a legjobb nemzetközi gyakorlatnak megfelelően – rendkívül rövid érvényességi idejű *Tanúsítványt* bocsásson ki, ezzel kiküszöbölve azt, hogy a *Tanúsítvány* visszavonási állapotát ellenőrizni kelljen.

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

Kulcs kompromittálódás vagy bármilyen egyéb probléma esetén az OCSP válaszokat aláíró régi magánkulcshoz ne kerüljön kibocsátásra újabb *Tanúsítvány*. A *Hitelesítés-szolgáltató*

az OCSP válaszadói *Tanúsítvány*okat ezt követően új, biztonságos magánkulcshoz bocsássa ki.

### Végfelhasználói tanúsítványok

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

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

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

#### 2.2.1. Szolgáltatói információ közzététele

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

A honlapon a hatálybalépés előtt kerüljenek publikálásra a bevezetésre váró új dokumentumok. A honlapon az érvényben levő dokumentumokon kívül legyen elérhető valamennyi dokumentum összes korábbi verziója is.

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

A *Hitelesítés-szolgáltató* a szerződéskötést követően tartós adathordozón bocsássa az *Ügyfél* rendelkezésére a *Hitelesítési rendet*, a *Szolgáltatási szabályzatot* és a *Szolgáltatási szerződést*. A *Hitelesítés-szolgáltató* értesítse *Ügyfeleit* az Általános szerződési feltételek változásáról.

### 2.3. 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, – annak hiányában pedig szükség szerint – késedelem nélkül tegye közzé.

#### 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 listák*on 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, olvasás céljából 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 IETF RFC 5280 [23] illetve IETF RFC 6818 [24] ajánlások szerinti egyedi név formátum előírásainak, ezen kívül a *Hitelesítés-szolgáltató* támogassa a kiterjesztések között található Alternatív név mezők (Subject Alternative Names), (Issuer Alternative Names) kitöltését is.

#### 3.1.1. Név típusok

##### Az *Alany* megnevezése

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

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

Amennyiben az *Alany* természetes személy, akkor a természetes személy *Alany* neve kerüljön ebbe a mezőbe, amelyet a *Hitelesítés-szolgáltató* a 3.2.3 fejezetben leírtak szerint ellenőrzött.

Amennyiben az *Alany Szervezet*, akkor a szervezet teljes vagy rövid elnevezése kerüljön ebbe a mezőbe, amelyet a *Hitelesítés-szolgáltató* a 3.2.2 fejezetben leírtak szerint ellenőrzött.

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

Szerver autentikációs tanúsítvány esetében ebben a mezőben a kért doménnév vagy IP cím szerepeljen. Csak létező és a *Igénylő* által jogosan használt doménnév vagy IP cím tüntethető fel. Szerver autentikációs *Tanúsítványok* esetében csak ebben a mezőben, illetve a Subject Alternative Names mezőben szerepelhet doménnév vagy IP cím. Szerver autentikációs *Tanúsítvány* nem lehet álneves.

Kitöltése kötelező.

- Surname – OID: 2.5.4.4 – Természetes személy vezetékneve

Természetes személy *Alany* esetében az *Alany* vezetékneve kerüljön ebbe a mezőbe, ahol a vezetéknevet a *Hitelesítés-szolgáltató* a CN mezőben szereplő teljes névből képi.

Álneves *Tanúsítvány* esetén nem kerülhet kitöltésre.

Nem álneves *Tanúsítvány* esetén kitöltése kötelező.

Amennyiben a *Tanúsítvány Alanya Szervezet*, akkor ne kerüljön kitöltésre.

Szerver autentikációs *Tanúsítványok* esetében a kitöltése opcionális. Amennyiben kitöltésre kerül, akkor az *Igénylő* vezetékneve kerüljön ide.

- Given Name – OID: 2.5.4.42 – Természetes személy keresztnéve

Természetes személy *Alany* esetében az *Alany* keresztnéve kerüljön ebbe a mezőbe, ahol a keresztnévet a *Hitelesítés-szolgáltató* a CN mezőben szereplő teljes névből képi.

Álneves *Tanúsítvány* esetén nem kerülhet kitöltésre.

Nem álneves *Tanúsítvány* esetén kitöltése kötelező.

Amennyiben a *Tanúsítvány Alanya Szervezet*, akkor ne kerüljön kitöltésre.

Szerver autentikációs *Tanúsítványok* esetében a kitöltése opcionális. Amennyiben kitöltésre kerül, akkor az *Igénylő* keresztnéve kerüljön ide.

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

Kizárólag álneves tanúsítvány esetén kerülhet kitöltésre.

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

A *Tanúsítványban* legalább egy kitöltött "Serial Number" mezőnek kötelezően szerepelnie kell, amely teljesíti az alábbi követelményeket, és ezáltal alkalmas arra, hogy az IETF RFC 4043 [22] ajánlás szerinti "Permanent Identifier" kiterjesztés használata esetén az *Alany* állandó azonosítójának részét képezze:

- az azonosító értéke a *Tanúsítványban* megnevezett, a *Hitelesítés-szolgáltató* által azonosított *Alanyhoz* tartozik, és a *Hitelesítés-szolgáltató* rendszerén belül egyedi;

- a *Hitelesítés-szolgáltató* garantálja, hogy két általa kibocsátott *Tanúsítványban* kizárólag akkor szerepel megegyező azonosító érték, ha a két *Tanúsítvány* ugyanahhoz az *Alanyhoz* tartozik.

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

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

*Szervezeti tanúsítvány* esetében az "O" mezőben kell, hogy szerepeljen a *Szervezet* teljes vagy rövid neve, amelyet a *Hitelesítés-szolgáltató* a 3.2.2 fejezetben leírtak szerint ellenőrzött.

*Szervezeti tanúsítvány* esetében a mező kitöltése kötelező.

Természetes személy részére kiállított *Kódalíró tanúsítvány* esetében a mező kitöltése kötelező, ide írandó a természetes személy neve. Természetes személy részére kiállított egyéb *Tanúsítvány* 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.

Amennyiben az *Alany* jogi személy a mező kitöltése kötelező.

Személyes – szervezethez nem kapcsolódó – *Tanúsítványok* esetében a mező kitöltése tilos.

Amennyiben az *Alany* jogi személy és az *Ügyfél* kéri az *Alany* módosított pénzforgalmi irányelv (PSD2) [2] szerinti adatainak feltüntetését a *Tanúsítványban*, akkor ebbe a mezőbe az *Alany* pénzforgalmi szolgáltatásait felügyelő hatóság által kiosztott engedélyszámát, a hatóság rövidítését és a hatóság illetékessége szerinti ország ISO 3166 szerinti két betűs országkódját tartalmazó azonosító kerüljön az ETSI TS 119 495 specifikáció [16] szerinti kódolással, vagy a hatóság által elismert egyéb azonosító az ETSI EN 319 412-1 [11] szerinti kódolással.

- 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 *Szervezetnek* 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.

- CountryName (C) – OID: 2.5.4.6 – Ország azonosítója  
*Szervezeti tanúsítvány* esetén az "O" mezőben szereplő *Szervezet* székhelye szerinti ország ISO 3166-1 [18] szerinti kétbetűs kódja.  
*Szervezethez* nem kapcsolódó természetes személy *Alany* esetén az *Alany* azonosítására használt személy azonosító dokumentumot kibocsátó ország ISO 3166-1 [18] szerinti 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.  
*Szervezethez* nem kapcsolódó *Tanúsítvány* esetében ne kerüljön kitöltésre.
- State or Province Name – OID: 2.5.4.8 – Tagállam, tartomány elnevezése  
*Szervezeti tanúsítvány* esetében a *Szervezet* székhelye szerinti tagállam, megye vagy tartomány neve.  
Kitöltése opcionális.  
*Szervezethez* nem kapcsolódó *Tanúsítvány* esetében ne kerüljön kitöltésre.
- 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.  
Kitöltése opcionális.  
*Szervezethez* nem kapcsolódó *Tanúsítvány* esetében nem kerülhet kitöltésre.
- Title (T) – OID: 2.5.4.12 – Alany titulusa  
A természetes személy *Alany* szerepe, beosztása vagy hivatása.  
Speciális esetekben a *Tanúsítványban* a *Hitelesítés-szolgáltató* több "Title" mezőt is feltüntethet.
- Email address (EMAIL) – OID: 1.2.840.113549.1.9.1 – Az *Alany* email címe  
Kitöltése opcionális.  
Ha kitöltésre kerül, akkor meg kell egyeznie az *Alany* alternatív neve mezőben szereplő "RFC822name" mezőben szereplő email címmel.

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

### Kiterjesztések

- Az Alany alternatív nevei - "Subject Alternative Names"

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

- Természetes személy *Alanyok* esetében az *Alany* kérésére ide (jellemzően a "Subject Alternative Names" "CN" mezéjébe) kerülhet a "Subject DN / commonName" mezőben szereplőtől eltérő írásmóddal írott neve. E név egyaránt szerepelhet ékezetes vagy ékezet nélküli írásmóddal. A *Hitelesítés-szolgáltató* jogosult jelölni a feltüntetett név jellegét is.

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

- *Szervezeti tanúsítványok* esetében az *Igénylő* kérésére itt kerülhet feltüntetésre a *Szervezet* által jogosan használt védjegy, márkanev, DBA név vagy terméknév (esetleg egyedi azonosítóval kiegészítve). A *Hitelesítés-szolgáltató* jogosult jelölni a feltüntetett név jellegét is.

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

- Szervezeti autentikációs *Tanúsítványok* esetében a "Subject Alternative Names" mezőben szerepelnie kell legalább egy doménnévnek vagy IP címnek.

Kitöltése kötelező. Ebben a mezőben minden domént / IP címet fel kell sorolni, azt is, ami a "CN"-ben szerepel a "domén" mezőben. Csak teljesen minősített doménnév (FQDN) szerepelhet itt, illetve nem szerepelhet lefoglalt tartománybeli IP cím.

A *Tanúsítvány*ban csak itt és a "Subject" mező "CN"-jében szerepelhet doménnév.

- Természetes személy illetve Szervezet számára kibocsátott *Tanúsítványok* esetében az *Alany* alternatív nevei mező "rfc822Name" mezőjében kerülhet megadásra az *Alany* email címe. Amennyiben a *Tanúsítvány*ban szerepel email cím, akkor e mező mindenképpen kerüljön kitöltésre. Ugyanez az email cím opcionálisan megjelenhet a *Tanúsítvány* "EMAIL" mezőjében is.

További *Alany* alternatív nevei mezők használata is megengedett.

#### 3.1.2. A nevek értelmezhetősége

A "SubjectDN" mezőre a következő szabályokat kell alkalmazni:

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



### 3.1.3. Álnevek használata

A *Hitelesítés-szolgáltató* nem ad ki álneves *Tanúsítványt*.

### 3.1.4. A különböző elnevezési formák értelmezési szabályai

Az azonosítók értelmezése érdekében az *Érintett feleknek* a jelen dokumentumban leírtak alapján ajánlott 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 szolgáltatathatja.

### 3.1.5. A nevek egyedisége

Az *Alany*nak a *Hitelesítés-szolgáltató Tanúsítványtárában* 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.

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

### Eljárások a nevekre vonatkozó vitás kérdések megoldására

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

### 3.1.6. Márkanevek elismerése, azonosítása, szerepük

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

## 3.2. Kezdeti regisztráció, azonosság hitelesítése

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

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

### 3.2.1. A magánkulcs birtoklásának igazolása

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

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

### 3.2.2. 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.

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

### 3.2.3. Természetes személy azonosságának hitelesítése

A természetes személy azonosságát igazolni kell:

- amennyiben a kibocsátandó *Tanúsítvány Alanya* a természetes személy;
- amennyiben a természetes személy egy *Szervezet* nevében jár el *Szervezeti tanúsítvány* kérelmezése céljából.

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

#### 1. Személyesen történő azonosítás során.

A III. hitelesítési osztályba tartozó *Tanúsítványok* esetében:

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

- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény (a továbbiakban: Nytv. [4]) hatálya alá tartozó természetes személyek esetében a Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolvány az Eüt. 82.§ (3) [8] szerint;
  - a Nytv. [4] hatálya alá nem tartozó természetes személy esetén a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról, illetve a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló törvény [5] szerinti úti okmány alapján az Eüt. 82.§ (4) [8] szerint;
  - a fenti okmányok egyikével sem rendelkező természetes személyek azonosítása során a *Hitelesítés-szolgáltató* csak európai állampolgárok azonosságának ellenőrzése esetében alkalmazza az Eüt. 82.§ (5) [8] bekezdése szerinti személyazonosság ellenőrzést. Ebben az esetben a természetes személy állampolgársága szerinti európai ország által kibocsátott fényképes személyi igazolványt fogadja el, mint személyazonosság igazolására szolgáló megbízható okmányt.
- A személyazonosság ellenőrzésére szolgáló adatok helyességét a természetes személynek papír alapú írásos nyilatkozatban, saját kezű - az azonosítást végző személy jelenlétében létrehozott - aláírásával igazolnia kell.
  - A személyes azonosítást végző személynek ellenőriznie kell, hogy a bemutatott igazolványokon történt-e módosítás vagy hamisítás.

A II. hitelesítési osztályba tartozó *Tanúsítványok* esetében:

- a természetes személy azonosításához személyes találkozásra nincs szükség, ilyen esetben a *Hitelesítés-szolgáltató* távolról is azonosíthatja az *Igénylőt*;
- az *Igénylő* eljuttatja a *Hitelesítés-szolgáltató*nak valamely személyazonosság igazolására alkalmas hatósági igazolványának másolatát.
- A személyazonosság ellenőrzésére szolgáló adatok helyességét a természetes személynek nyilatkozatban, saját kezű aláírással ellátva igazolnia kell.

## 2. Elektronikus aláírás vagy elektronikus bélyegző tanúsítványára visszavezetett azonosítással.

Ebben az esetben:

- Az *Igénylő* a *Tanúsítványkérelmet* elektronikus formában nyújtja be egy nem álneves – az igényelt *Tanúsítvány*énál nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) – *Tanúsítvány*án alapuló elektronikus aláírással vagy elektronikus bélyegzővel ellátva.
- Az elektronikus aláírással ellátott *Tanúsítványkérelem*nek tartalmaznia kell a természetes személy egyértelmű azonosításához szükséges azonosító adatokat.
- A *Tanúsítványkérelem* hitelességét és sértetlenségét ellenőrizni kell a teljes tanúsítási lánc vizsgálatával.

- A *Hitelesítés-szolgáltató* csak olyan *Tanúsítványon* alapuló elektronikus aláírást vagy elektronikus bélyegzőt fogad be, amelyet egy az Európai Unió fő bizalmi listán publikált nemzeti bizalmi listán szereplő bizalmi szolgáltatás keretében bocsátottak ki, és az aláírás vagy bélyegző létrehozás időpontjában érvényes volt.

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

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

#### 3.2.4. Nem ellenőrzött alany információk

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

#### 3.2.5. Jogok, felhatalmazások ellenőrzése

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

Ellenőrizni kell a természetes személy képviseleti jogosultságát.

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

A *Szervezeti ügyintézőt* az adott *Szervezet* képviseletére jogosult személy jelölheti ki. *Szervezeti ügyintéző* kijelölése nem kötelező, ha nincs kijelölve, akkor az adott *Szervezet* képviseletére jogosult személy láthatja el ezt a feladatot.

#### 3.2.6. Együttműködési képességre vonatkozó követelmények

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

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

Az együttműködő *Hitelesítés-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-szolgáltatónak* közzé kell tennie minden általa kért vagy elfogadott kereszthitelesített *Tanúsítványt*.

### 3.3. Azonosítás és hitelesítés kulcscsere kérelem esetén

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

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

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

A kulcscserével kapcsolatos eljárás részletei a 4.7. fejezetben olvashatóak.

#### 3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

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

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

#### 3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

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

### 3.4. Azonosítás és hitelesítés tanúsítvány megújítás esetén

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

#### 3.4.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

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

#### 3.4.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen *Tanúsítvány* nem újítható meg.

### 3.5. Azonosítás és hitelesítés tanúsítvány módosítás esetén

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

### 3.5.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

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

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

### 3.5.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen *Tanúsítvány* nem módosítható.

## 3.6. Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási kérelem esetén

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

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

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

## 3.7. Ellenőrzött kommunikációs csatorna

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

# 4. A tanúsítványok életrajzára vonatkozó követelmények

## 4.1. Tanúsítványkérelem

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

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

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

A *Hitelesítés-szolgáltatónak* 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 *Tanúsítványkérelemnek* tartalmaznia kell legalább a következő adatokat:

- a *Tanúsítványba* kerülő adatok (pl. név, titulus, *Szervezet* neve, szervezeti egység elnevezése, város, ország, email cím);
- az *Alany* – *Szervezet* esetében a *Szervezet* képviselőjének – személyazonosító adatai (teljes név, személyazonosító okmány száma);
- az *Alany* – *Szervezet* esetében a *Szervezet* képviselőjének – elérhetőségei (telefonszám, email cím);
- *Szervezeti tanúsítvány* igénylése esetében a *Szervezet* adatai (hivatalos elnevezése);
- az *Előfizető* adatai (számlázási adatok).

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

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

#### 4.1.1. Ki nyújthat be tanúsítványkérelmet

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

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

A *Tanúsítványkérelmet* az *Alany – Szervezet* esetében a *Szervezet* képviselője – a következő módokon nyújthatja be:

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

Az *Előfizető*nek és az *Alany*nak – *Szervezet* esetében annak képviselőjének – a *Tanúsítvány* igénylése során meg kell adniuk elérhetőségi adataikat.

#### 4.1.2. A bejegyzés folyamata és a résztvevők felelőssége

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

Amennyiben az *Alany Szervezet*, vagy a *Tanúsítvány*ban feltüntetésre kerül egy *Szervezet* neve is (*Szervezeti tanúsítvány*), akkor a *Szervezet*et is azonosítani kell, illetve meg kell győződni arról, hogy a megjelent személy jogosult a *Szervezet* képviselőjére illetve a *Szervezethez* kapcsolódó *Tanúsítvány* igénylésére (lásd: 3.2.2. fejezet).

Az *Előfizető* határozza meg, hogy mely *Igénylő* mely *Hitelesítési rend* szerinti *Tanúsítvány* jogosult igényelni.

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

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

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

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

- annak megerősítését, hogy a *Tanúsítványkérelemben* megadott adatok pontosak;
- azt, hogy hozzájárul ahhoz, hogy a *Hitelesítés-szolgáltató* a kérelemben megadott adatait nyilvántartsa és kezelje;



- azt, hogy hozzájárul-e a *Tanúsítvány* 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 *Képviselt szervezet*, az *Igénylő* vagy az *Előfizető* benyújtottak.

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

## 4.2. A tanúsítványkérelem feldolgozása

### 4.2.1. Az igénylő azonosítása és hitelesítése

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

### 4.2.2. A tanúsítványkérelem elfogadása vagy visszautasítása

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

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

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

### 4.2.3. A tanúsítványkérelem feldolgozásának időtartama

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

## 4.3. A tanúsítvány kibocsátása

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

### 4.3.1. A Hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során

A *Tanúsítványok* kibocsátásának megfelelően biztonságos módon kell történnie.

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

#### 4.3.2. Az Ügyfél értesítése a tanúsítvány kibocsátásáról

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

#### 4.4. A tanúsítvány elfogadása

##### 4.4.1. A tanúsítvány elfogadás módja

A III. hitelesítési osztályba tartozó *Tanúsítványok* esetén az *Alany*nak – *Szervezet* részére kiállított *Tanúsítvány* esetén az *Alany* képviselőjének – a *Tanúsítvány* átvétele előtt ellenőriznie kell a *Tanúsítványban* szereplő adatok helyességét és erről írásbeli nyilatkozatot kell tennie. A nyilatkozat aláírásával az *Alany* vagy képviselője igazolja a *Tanúsítvány* átvételét.

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

Amennyiben az *Alany* számára a *Hitelesítés-szolgáltató* biztosítja a *HSM* eszközt is, akkor az *Alany* magánkulcsát és *Tanúsítványát* tartalmazó *HSM* eszköz, valamint az aktiváláshoz szükséges kód átvétele után az *Igénylő* aláírja a papíralapú átvételi nyilatkozatot, amelyben — többek között — azt igazolja, hogy az adatok – amelyek alapul vételével a *Hitelesítés-szolgáltató* a *Tanúsítványt* kiállította – helyesek, a *HSM* eszközt és a hozzá tartozó aktiváló kódokat átvette, valamint azt, hogy ismeri a *HSM* eszköz használatának műszaki és jogszabályi feltételeit.

##### 4.4.2. A tanúsítvány közzététele

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

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

##### 4.4.3. További szereplők értesítése a tanúsítvány kibocsátásáról

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

#### 4.5. A kulcspár és a tanúsítvány használata

##### 4.5.1. A magánkulcs és a tanúsítvány használata

Az *Alany* a *Tanúsítványához* tartozó magánkulcsát kizárólag a *Tanúsítványban* szereplő kulcshasználatnak megfelelően használhatja, más felhasználás nem engedélyezett.

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

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

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

#### 4.5.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata

A *Tanúsítvány* felhasználásával végrehajtott műveletek (pl. távoli fél azonosítása, címzett számára dokumentum titkosítása) végrehajtása során a *Hitelesítés-szolgáltató* által garantált biztonsági szint megtartásához ajánlott, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, és feleljen meg a *Szolgáltatási szabályzatban* leírt követelményeknek, különös tekintettel az alábbiakra:

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

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

#### 4.6. Tanúsítvány megújítás

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

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

##### 4.6.1. A tanúsítvány megújítás körülményei

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

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

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

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

#### 4.6.2. Ki kérelmezheti a tanúsítvány megújítást

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

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

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

#### 4.6.3. A tanúsítvány megújítási kérelmek feldolgozása

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

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

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

#### 4.6.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

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

#### 4.6.5. A megújított tanúsítvány elfogadása

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

#### 4.6.6. A megújított tanúsítvány közzététele

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

#### 4.6.7. További szereplők értesítése a tanúsítvány kibocsátásáról

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

## 4.7. Kulcscsere

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

A kulcscsere során kiállított új *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 *Tanúsítványkérelem* benyújtására is.

### 4.7.3. A kulcscsere kérelmek feldolgozása

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

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

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

### 4.7.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

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

### 4.7.5. A kulcscserével megújított tanúsítvány elfogadása

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

#### 4.7.6. A kulcscserével megújított tanúsítvány közzététele

A *Hitelesítés-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 Szervezeti ügyintézőjét* is.

### 4.8. Tanúsítvány módosítás

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

#### 4.8.1. A tanúsítvány módosítás körülményei

A tanúsítvány módosítás szükségessé válik az alábbi esetekben:

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

A tanúsítvány módosítás feltételei:

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

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

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

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

#### 4.8.2. Ki kérelmezheti a tanúsítvány módosítást

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

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

### 4.8.3. A tanúsítvány módosítási kérelmek feldolgozása

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

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

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

### 4.8.7. További szereplők értesítése a tanúsítvány kibocsátásáról

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

## 4.9. Tanúsítvány visszavonás és felfüggesztés

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

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

#### 4.9.1. A tanúsítvány visszavonás körülményei

##### Végfelhasználói tanúsítvány visszavonásának okai

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

- az *Igénylő* vagy az *Előfizető* írásban kéri a *Tanúsítvány* visszavonását;
- az *Igénylő* vagy az *Előfizető* értesíti a *Hitelesítés-szolgáltatót* arról, hogy az eredeti *Tanúsítványkérelmet* nem hagyta jóvá, és utólag sem ad erre jóváhagyást;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódott;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* szereplő nyilvános kulcs már nem felel meg a 6.1.5. és 6.1.6. fejezetekben meghatározott követelményeknek;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* jogellenesen használták;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy az *Előfizető* megszegte a Szolgáltatási szerződés vagy az Általános szerződési feltételek szerinti egy vagy több kötelezettségét;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* szereplő adatokban lényeges változás történt;
- a *Tanúsítvány* módosítása az *Alanyra* vonatkozó adatok változása miatt;
- 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 *Tanúsítványban* foglalt bármely adat pontatlan;
- a *Hitelesítés-szolgáltató* már nem jogosult *Tanúsítványokat* kibocsátani és a meglévő *Tanúsítványokra* vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodik;
- a visszavonást előírja a *Hitelesítés-szolgáltató Hitelesítési rendje* vagy *Szolgáltatási szabályzata*;
- a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* kibocsátó hitelesítő egység magánkulcsa kompromittálódhatott;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy az *Előfizető* nem teljesítette valamely anyagi kötelezettségét a vonatkozó Szolgáltatási szerződésnek megfelelően;
- a *Hitelesítés-szolgáltató* tevékenységét befejezte;



- a visszavonást jogszabály kötelezővé teszi.

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

### **Szolgáltatói Tanúsítvány visszavonásának okai**

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

- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató írásban kéri a *Tanúsítvány* visszavonását;
- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató értesíti a kibocsátó *Hitelesítés-szolgáltatót* arról, hogy az eredeti *Tanúsítvány* kérelmet nem hagyta jóvá, és utólag sem ad erre jóváhagyást;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem a kizárólagos birtokában van;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* szereplő nyilvános kulcs már nem felel meg a 6.1.5 és 6.1.6 fejezetekben meghatározott követelményeknek;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* jogellenesen használták;
- amennyiben a *Tanúsítványt* nem a vonatkozó *Hitelesítési rend* illetve *Szolgáltatási szabályzat* szerint bocsátották ki vagy a köztes hitelesítő egység működése nem felel meg a rá vonatkozó *Hitelesítési rendnek* vagy *Szolgáltatási szabályzatnak*;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* szereplő valamely információ téves vagy félrevezető;
- a kibocsátó CA vagy a köztes CA bármilyen okból megszünteti a tevékenységét, és nem állapodott meg más *Hitelesítés-szolgáltató-val* a *Tanúsítvány* visszavonási szolgáltatás nyújtásáról ;
- amennyiben a *Hitelesítés-szolgáltató* már nem lenne jogosult *Tanúsítványokat* kibocsátani és a meglévő *Tanúsítványokra* vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;
- a visszavonást előírja a kibocsátó CA *Hitelesítési rendje* vagy *Szolgáltatási szabályzata*;
- a *Tanúsítvány* módosítása a hitelesítési egységre, vagy a *Hitelesítés-szolgáltatóra* vonatkozó adatok változása miatt;
- amennyiben a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);
- a *Hitelesítés-szolgáltató* a tevékenységét befejezte;
- a visszavonást jogszabály kötelezővé teszi.

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

### **Más Szolgáltató által üzemeltetett köztes CA Tanúsítvány visszavonásának okai**

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

- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató írásban kéri a *Tanúsítvány* visszavonását;
- a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató értesíti a kibocsátó *Hitelesítés-szolgáltatót* arról, hogy az eredeti *Tanúsítvány* kérelmet nem hagyta jóvá, és utólag sem ad erre jóváhagyást;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a magánkulcs nem a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató kizárólagos birtokában van;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* szereplő nyilvános kulcs már nem felel meg a 6.1.5 és 6.1.6 fejezetekben meghatározott követelményeknek;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* jogellenesen használták;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványt* nem a vonatkozó *Hitelesítési rend* illetve *Szolgáltatási szabályzat* szerint bocsátották ki vagy a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató működése nem felel meg a rá vonatkozó *Hitelesítési rendnek* vagy *Szolgáltatási szabályzatnak*;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítványban* szereplő valamely adat téves vagy félrevezető;
- a kibocsátó CA vagy a köztes CA bármilyen okból megszünteti a tevékenységét, és nem állapodott meg más *Hitelesítés-szolgáltató-val* a *Tanúsítvány* visszavonási szolgáltatás nyújtásáról ;
- amennyiben a *Hitelesítés-szolgáltató* már nem lenne jogosult *Tanúsítványokat* kibocsátani és a meglévő *Tanúsítványokra* vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;
- a visszavonást előírja a kibocsátó CA *Hitelesítési rendje* vagy *Szolgáltatási szabályzata*;
- a *Tanúsítvány* módosítása a hitelesítési egységre, vagy az azt üzemeltető hitelesítés-szolgáltatóra vonatkozó adatok változása miatt;
- amennyiben a *Tanúsítvány* formátuma vagy műszaki tartalma már elfogadhatatlan kockázatot jelent az *Érintett felek* részére (pl. ha egy használt kriptográfiai algoritmus vagy kulcsméret már nem biztonságos);
- a hitelesítési egységet működtető hitelesítés-szolgáltató, vagy a *Tanúsítványát* kibocsátó *Hitelesítés-szolgáltató* a tevékenységét befejezte;

- a visszavonást jogszabály kötelezővé teszi.

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

#### 4.9.2. Ki kérelmezheti a visszavonást

A *Tanúsítvány* visszavonását kezdeményezhetik:

- az *Előfizető*;
- az *Igénylő*
- *Szervezeti tanúsítvány* esetén a *Szervezet* nevében eljárásra jogosult természetes személy;
- az *Előfizető* által bejelentett *Szervezeti ügyintéző*;
- az *Alany* pénzforgalmi szolgáltatási engedélyét kibocsátó hatóság, amennyiben a *Tanúsítvány* az *Alany* módosított pénzforgalmi irányelv (PSD2) [2] szerinti adatait tartalmazza;
- a *Hitelesítés-szolgáltató*.

#### 4.9.3. A visszavonási kérelemre vonatkozó eljárás

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

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

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

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

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

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

#### Tanúsítvánnyal kapcsolatos problémák sürgősségi bejelentése

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

#### 4.9.4. A visszavonási kérelemre vonatkozó kivárási idő

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

#### 4.9.5. A visszavonási eljárás maximális hossza

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

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

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

#### 4.9.7. A visszavonási lista kibocsátás gyakorisága

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

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

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

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

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

#### 4.9.9. Valós idejű tanúsítvány állapot ellenőrzés lehetősége

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

#### 4.9.10. A valós idejű tanúsítvány állapot ellenőrzésre vonatkozó követelmények

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

#### 4.9.11. A visszavonási hirdetmények egyéb elérhető formái

Nincs megkötés.

#### 4.9.12. A kulcs kompromittálódásra vonatkozó speciális követelmények

A *Hitelesítés-szolgáltató* valamely hitelesítési egysége magánkulcsának kompromittálódása esetén tegyen meg minden ésszerű erőfeszítést annak érdekében, hogy az eseményről értesítse az *Érintett 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 *Hitelesítés-szolgáltató* a kockázatok csökkentése érdekében nyújtson lehetőséget a *Tanúsítványok* használhatóságának ideiglenes megszüntetésére arra az esetre, ha feltételezhető, hogy a *Tanúsítvány* visszavonását megalapozó okok valamelyike fennáll.

#### 4.9.14. Ki kérelmezheti a felfüggesztést

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

#### 4.9.15. A felfüggesztési kérelemre vonatkozó eljárás

A *Hitelesítés-szolgáltató* tegye lehetővé a felfüggesztés kezdeményezését az év minden napján a nap minden órájában.

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

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

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

#### 4.9.16. A felfüggesztés maximális hossza

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

### 4.10. Tanúsítvány állapot szolgáltatások

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

- OCSP – online tanúsítvány állapot lekérdezési szolgáltatás;

- CRL – *Tanúsítvány visszavonási lista*.

A *Tanúsítvány visszavonási lista*ban kerüljenek feltüntetésre a visszavont és felfüggesztett *Tanúsítványok*.

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

A visszavonási vagy felfüggesztési információ nem távolítható el a *Tanúsítvány visszavonási listáról* a visszavont vagy felfüggesztett *Tanúsítvány* lejáratási időpontja előtt.

Felfüggesztés, visszaállítás és visszavonás esetén a folyamat sikeres lezárását követően a *Tanúsítvány* új állapota azonnal jelenjen meg a *Hitelesítés-szolgáltató Visszavonási állapot nyilvántartásában*.

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

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

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

#### 4.10.1. Működési jellemzők

Nincs megkötés.

#### 4.10.2. A szolgáltatás rendelkezésre állása

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

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

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

#### 4.10.3. Opcionális lehetőségek

Nincs megkötés.

#### 4.11. Az előfizetés vége

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

#### 4.12. Magánkulcs letétbe helyezése és visszaállítása

A *Hitelesítés-szolgáltató* az autentikációs *Tanúsítvány*hoz tartozó magánkulcshoz nem nyújthat kulcsletét szolgáltatást.

A *Hitelesítés-szolgáltató* a titkosító *Tanúsítvány*okhoz tartozó magánkulcshoz nyújthat kulcsletét szolgáltatást.

##### 4.12.1. Kulcsletét és visszaállítás rendje és szabályai

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

##### 4.12.2. Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Az autentikációs *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, videó megfigyelő rendszer, beléptető rendszer stb. – amelyek együttesen egy erős védelmi szintet biztosítanak a szolgáltatásban részt vevő informatikai rendszerek és a szolgáltató által tárolt bizalmas adatok megóvására.

### 5.1.2. Fizikai hozzáférés

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

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

Az eszközök aktivizáló adatai (jelszavak, PIN kódok) a gépteremben 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 aktíválva 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*ban 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 hálózatról érkező feszültség ingadozások, feszültség kimaradások, tüskék és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramtermelő berendezéssel rendelkezik, amely - üzemanyag utántöltést lehetővé téve - tetszőleges időtartamig képes a szükséges energia biztosítására.

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

A levegő nedvességtartalmát az informatikai rendszerek által megkívánt szintre kell csökkenteni. Megfelelő teljesítményű hűtőrendszert kell használni a szükséges üzemi hőmérséklet biztosítása, az informatikai eszközök túlhevülésének megakadályozása érdekében.

### 5.1.4. Beázás és elárasztódás veszély kezelése

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

### 5.1.5. Tűz megelőzés és tűzvédelem

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

### 5.1.6. Adathordozók tárolása

A *Hitelesítés-szolgáltató*nak védenie kell valamennyi adathordozóját a jogosulatlan hozzáféréstől és a véletlen rongálódástól. Valamennyi 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-szolgáltató*nak a környezetvédelmi előírások betartásával kell gondoskodnia feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről.

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

### 5.1.8. A mentési példányok fizikai elkülönítése

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

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

## 5.2. Eljárásbeli előírások

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

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

A *Hitelesítés-szolgáltató* belső irányítási rendszere biztosítsa a jogszabályoknak és belső szabályzatainak megfelelő működést. Rendszerében minden rendszerelemhez és minden folyamathoz 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 és felfüggesztésének 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-szolgáltatóval* munkaviszonyban álló személyek láthatnak el, megbízási szerződés keretében a bizalmi szerepkörök nem láthatók el.

A bizalmi szerepkörökről naprakész nyilvántartást kell vezetni.

### 5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

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

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

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

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

### 5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés

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

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

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

### 5.2.4. Egymást kizáró szerepkörök

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

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

### 5.3. Személyzetre vonatkozó előírások

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

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

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

#### 5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

A *Hitelesítés-szolgáltató*nál bizalmi szerepkört csak olyan személy tölthet be, akinek a befolyásmentességét és szakértelmét a *Hitelesítés-szolgáltató* igazolni tudja. A bizalmi szerepkört betöltő személyeknek mentesnek kell lenniük az összeférhetetlenségtől, amely veszélyeztethetné a *Hitelesítés-szolgáltató* tevékenységének pártatlanságát.

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

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

#### 5.3.2. Előélet vizsgálatára vonatkozó eljárások

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

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

Kinevezéskor a *Hitelesítés-szolgáltató* vezető munkakört betöltő alkalmazottjának nyilatkozatával, bizalmi szerepkört betöltő alkalmazottjának 3 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, úgy mint előző munkahely, szakmai referenciák, legfontosabb képzettség.

### 5.3.3. Képzési követelmények

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

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

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

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

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

### 5.3.4. Továbbképzési gyakoriságok és követelmények

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

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

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

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

### 5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

Nincs előírás.

### 5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

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

### 5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

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

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

### 5.3.8. A személyzet számára biztosított dokumentációk

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

## 5.4. Naplózási eljárások

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

### 5.4.1. A tárolt események típusai

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

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

Az elmentett naplóbejegyzések nem kerülhetnek módosításra vagy törlésre.

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

Naplózni kell minimálisan az alábbi eseményeket:

- BELSŐ ÓRA

- a belső óra szinkronizációja az UTC időhöz, beleértve az üzemszerű újralibrálásokat is;
- a szinkronizáció elvesztése;

- NAPLÓZÁS

- a naplózó rendszer vagy egyes komponenseinek leállítása, újraindítása;
- a naplózás bármilyen beállításának módosítása, mint pl. gyakoriság, riasztási küszöb érték, vizsgált esemény;
- a tárolt naplózási adatok módosítása vagy törlése;
- a naplózó rendszer hibája miatt végzett tevékenységek;

- RENDSZER BEJELENTKEZÉSEK

- sikeres bejelentkezések, sikertelen bejelentkezési próbálkozások bizalmi szerepkörökbe;
- jelszó alapú azonosítás esetén:
  - \* az engedélyezett sikertelen bejelentkezési próbálkozások számának megváltoztatása;
  - \* az engedélyezett sikertelen bejelentkezési próbálkozások számának elérése felhasználói bejelentkezéskor;
  - \* sikertelen bejelentkezések miatt zárolt felhasználó újbóli engedélyezése;
- az azonosítási technika változtatása (például jelszó alapúról PKI alapúra);

- KULCSKEZELÉS

- a szolgáltatói kulcsok teljes életciklusára vonatkozó valamennyi esemény (kulcsgenerálás, elmentés, betöltés, megsemmisítés stb.);
- a felhasználói kulcsok generálásával, kezelésével kapcsolatos események;
- a *Hitelesítés-szolgáltató* által bármilyen célból tárolt felhasználói magánkulcsok kezelésével kapcsolatos minden esemény;

- TANÚSÍTVÁNY KEZELÉS

- szolgáltatói *Tanúsítványok* kibocsátásával, állapotváltozásával kapcsolatos minden esemény;
- minden kérés, beleértve a *Tanúsítvány* kibocsátást, kulcscserét, megújítást, felfüggesztést és visszavonást;
- a kérések feldolgozásával kapcsolatos események;

- a *Tanúsítvány* kibocsátásával kapcsolatban végrehajtott minden ellenőrzési tevékenység;
  - tanúsítványkérelmek elutasítása;
  - *Tanúsítvány* kibocsátása, állapotváltozása;
- ADATMOZGÁSOK
    - bármilyen, a biztonság szempontjából kritikus adat manuális bevitele a rendszerbe;
    - a rendszer által fogadott, biztonsági szempontból fontos adatok, üzenetek;
- CA KONFIGURÁCIÓ
    - a CA tetszőleges komponensének átparaméterezése, a beállításon történt bármilyen változtatás;
    - felhasználók felvétele, törlése;
    - felhasználói szerepkörök, jogosultságok megváltoztatása;
    - a tanúsítvány profil megváltoztatása;
    - CRL profil megváltoztatása;
    - új CRL lista 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 bizalmi szolgáltatást nyújtó rendszer komponenseket tartalmazó biztonsági területre és onnan kilépése;
    - hozzáférés egy bizalmi szolgáltatást nyújtó rendszer komponenshez;



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

#### 5.4.2. A naplófájl feldolgozásának gyakorisága

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

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

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

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

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

A kiértékelés során elemezni kell a rendszerek által generált hibaüzeneteket.

Statisztikai módszerekkel elemezni kell a forgalmi adatokban bekövetkezett jelentős változásokat.

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

### 5.4.3. A naplófájl megőrzési időtartama

Az online rendszerből való kitörés 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 szabályzat*ban elő kell írni.

### 5.4.6. A naplózás adatgyűjtési rendszere

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

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

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

### 5.4.7. Az eseményeket kiváltó alanyok értesítése

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

### 5.4.8. Sebezhetőség felmérése

A *Hitelesítés-szolgáltató*nak évente sebezhetőség vizsgálatot kell végeznie, amely segítségével feltérképezi a potenciális belső és külső fenyegetettségeket, amelyek jogosulatlan hozzáféréseket

eredményezhetnek, hatással lehetnek a *Tanúsítvány* kiadási folyamatra, vagy lehetővé teszik a *Tanúsítvány*ban tárolt adatok módosítását.

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

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

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

## 5.5. Adatok archiválása

### 5.5.1. Az archivált adatok típusai

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

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

- a *Hitelesítés-szolgáltató* akkreditációjával kapcsolatos valamennyi irat;
- a *Hitelesítési rend(ek)* valamennyi kibocsátott verziója;
- a *Szolgáltatási szabályzat(ok)* valamennyi kibocsátott verziója;
- az Általános szerződési feltételek valamennyi kibocsátott verziója;
- a *Hitelesítés-szolgáltató* működésével kapcsolatos szerződések;
- a regisztrációval kapcsolatos valamennyi információ, beleértve
  - a *Tanúsítványkérelemmel* együtt benyújtott valamennyi irat;
  - a személyes azonosítás során bemutatott dokumentum(ok) azonosító adatai;
  - Szolgáltatási szerződés(ek);
  - egyéb előfizetői jognyilatkozatok;
  - a kérelmet elbíráló regisztrációs ügyintéző azonosítója;
  - a kérelem elbírálásának körülményei és eredménye;
- a *Tanúsítványokkal* kapcsolatos valamennyi információ a teljes életciklusra vonatkozóan;
- valamennyi elektronikus és papíralapú naplóbejegyzés.

### 5.5.2. Az archívum megőrzési időtartama

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

- a *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 lejáratja) gondoskodni kell az adatok hitelességének megőrzéséről.

### 5.5.6. Az archívum gyűjtési rendszere

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

### 5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

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

Az archivált adatállományokat védeni kell a jogosulatlan hozzáféréstől.

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

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

### 5.6. Szolgáltatói kulcs cseréje

A *Hitelesítés-szolgáltató* gondoskodjon arról, hogy az általa üzemeltetett *Hitelesítő egységek* folyamatosan rendelkezzenek a működéshez szükséges érvényes kulccsal és Tanúsítvánnyal. Ennek érdekében a *Tanúsítványuk* lejárta illetve a hozzájuk kapcsolódó kulcsok használati idejének lejárta 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 a biztonsági incidensről – súlyosságának függvényében – 24 órán belül értesíteni kell minden szervezetet, amely felé ilyen jellegű kötelezettség fennáll.

#### 5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások

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

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

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

### 5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

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

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

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

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

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

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

### 5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások

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

- vissza kell vonni a *Hitelesítés-szolgáltató* összes érintett *Tanúsítványát*;
- új szolgáltatói magánkulcsokat kell generálni a szolgáltatások helyreállításához;
- nyilvánosságra kell hozni a visszavont szolgáltatói *Tanúsítványok* adatait a 2.2 fejezetben szabályozott módon;
- 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 szolgáltatói helyszínt az elsődleges telephelytől olyan távol kell elhelyezni, hogy egy valószínűsíthető katasztrófa ne érhesse mindkét helyszínt egyszerre.

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

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

### 5.8. A hitelesítés-szolgáltató vagy a regisztráló szervezet leállítása

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

A leállítás során kiemelten kezelendő feladatok:

- a tervezett leállásról időben értesíteni kell az *Érintett feleket* és az *Előfizetőket*;
- a *Hitelesítés-szolgáltató* tegyen meg mindent annak érdekében, hogy legkésőbb a szolgáltatás leállításáig egy másik szolgáltató átvegye nyilvántartásait és szolgáltatási kötelezettségeit;
- be kell szüntetni az új *Tanúsítványok* kiadását;
- vissza kell vonni a szolgáltatói *Tanúsítványokat* és meg kell semmisíteni a szolgáltatói magánkulcsokat;
- a szolgáltatás megszüntetése után egy teljes rendszermentést és archiválást kell végeznie;

## 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 [15];
- az Eüt. [8] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

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

- A szolgáltatói magánkulcs előállítását fizikailag védett környezetben (lásd 5.1 pont), legalább két, bizalmi szerepkört (lásd 5.2.1 pont) betöltő, erre feljogosított személy együttes részvételével, más illetéktelen személyek jelenlétét kizárva végzi.
- A szolgáltatói magánkulcs előállítását olyan eszközön belül hajtja végre, amely:
  - megfelel az ISO/IEC 19790 [20] követelményeinek,
  - vagy megfelel a FIPS 140-2 [27] 3-as, illetve annál magasabb szintű követelményeinek,
  - vagy megfelel a CEN 419 221-5 [17] követelményeinek,
  - vagy olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [19] 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 előírányaton kell alapulnia.
- A szolgáltatói magánkulcs előállítását egy kulcsgenerálási forгатókönyv alapján végzi.
- Szolgáltatói gyökér hitelesítő egység magánkulcsának előállítása esetén jelen van egy külső auditor. A külső auditor igazolja, hogy a kulcs generálása a forгатókönyv szerint történt.

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

- A kulcsok előállítását fizikailag védett környezetben végzi, kizárólag bizalmi szerepkört betöltő személyek részvételével.
- A *Hardver kriptográfiai eszköz* használatát előíró *Hitelesítési rendek* esetén a *Hitelesítés-szolgáltató* a magánkulcsot csak a szolgáltatást igénybe vevő *Igénylő Hardver kriptográfiai eszközén* generálja, ami lehetetlenné 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 lehetetlenné váljon. A *Hitelesítés-szolgáltató* meggyőződik arról, hogy az előállított kulcspár megfelel a 6.1.5 és 6.1.6 fejezetekben meghatározott követelményeknek és a nyilvános kulcs nem egy ismert gyenge kulcspár tagja.

Az *Igénylő* által előállított kulcspár esetén:

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



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

- szolgáltatói gyökér hitelesítő egység magánkulcsának előállítása esetén a *Hitelesítés-szolgáltató* kulcsmenedzserért 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* kulcsmenedzserért 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 az *Alany* magánkulcsát, akkor az alábbi követelményeknek kell megfelelni:

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

### 6.1.3. A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

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

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

### 6.1.4. A szolgáltatói nyilvános kulcs közzététele

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

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

- A gyökér hitelesítő egységek megnevezését, illetve *Gyökér tanúsítvány*aik lenyomatát tartalmazza a *Szolgáltatási szabályzat*. Az állapotváltozásukkal kapcsolatos információk legyenek elérhetőek a *Hitelesítés-szolgáltató* honlapján.
- A köztes (nem gyökér) hitelesítő egységek tanúsítványainak állapotváltozását hozza nyilvánosságra a *Tanúsítvány visszavonási listák*on, saját honlapján, valamint az online tanúsítvány-állapot válasz szolgáltatás keretében.
- Az online tanúsítvány-állapot válaszokat aláíró válaszadók számára a *Hitelesítés-szolgáltató* – a legjobb nemzetközi gyakorlatnak megfelelően – rendkívül rövid érvényességi idejű *Tanúsítványt* bocsásson ki, ezzel kiküszöbölve azt, hogy a *Tanúsítvány* visszavonási állapotát ellenőrizni kelljen. E *Tanúsítvány* visszavonási állapotát a *Hitelesítés-szolgáltató* kizárólag olyan módon tegye közzé, hogy kulcs kompromittálódás vagy bármilyen egyéb probléma esetén az OCSP válaszokat aláíró régi magánkulchoz ne kerüljön kibocsátásra újabb *Tanúsítvány*. A *Hitelesítés-szolgáltató* az OCSP válaszadói *Tanúsítvány*okat ezt követően új, biztonságos magánkulchoz bocsássa ki.

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

#### 6.1.5. Kulcsméreték

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

- ETSI TS 119 312 [15];
- az Eüt. [8] 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 *Tanúsítványainak* hitelesítésére,
- OCSP válaszadó *Tanúsítványának* 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 *Tanúsítványainak* hitelesítésére,
- végfelhasználói *Tanúsítványok* hitelesítésére,
- *Időbélyegző egység Tanúsítványának* hitelesítésére,
- OCSP válaszadó *Tanúsítványának* hitelesítésére,
- CRL-ek hitelesítésére.

A *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítványok*ban szerepeltesse a "kulcshasználat" (Key Usage) kiterjesztéseket, amelyek meghatározzák a *Tanúsítvány* felhasználási területét és az X.509v3 [26] kompatibilis alkalmazásokban műszakilag is korlátozzák a kulcsok felhasználhatóságát. A mező tartalmára vonatkozó megkötések a 7.1.2 fejezetben szerepelnek.

Az *Alany* a *Tanúsítványához* tartozó magánkulcsát kizárólag a *Tanúsítványban* szereplő kulcshasználatnak megfelelően használhatja, más felhasználás nem engedélyezett.

## 6.2. A magánkulcsok védelme

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

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

### 6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

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

- megfelelnek az ISO/IEC 19790 [20] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [27] 3-as, illetve annál magasabb szintű követelményeknek,
- vagy megfelelnek a CEN 14167-2 [29] munkacsoport egyezmény követelményeinek,
- vagy megfelelnek a CEN 419 221-5 [17] követelményeinek,
- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [19] 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 *HSM* eszközön kívül csak kódolt formában tárolhatók. A kódoláshoz csak az Eüt. [8] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozatban foglalt algoritmusok és kulcsparaméterek használhatók, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

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

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

### 6.2.2. Magánkulcs többszereplős (n-ből m) használata

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

### 6.2.3. Magánkulcs letétbe helyezése

A *Hitelesítés-szolgáltató* csak titkosított formában helyezheti letétbe a szolgáltatói magánkulcsait.

### 6.2.4. Magánkulcs mentése

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

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

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

A végfelhasználói autentikációs magánkulcsokról a *Hitelesítés-szolgáltató* nem készíthet másolatot.

### 6.2.5. Magánkulcs archiválása

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

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

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

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

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

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

### 6.2.7. Magánkulcs tárolása hardver kriptográfiai eszközben

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

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

### 6.2.8. A magánkulcs aktiválásának módja

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

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

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

A *Hitelesítés-szolgáltató* által az *Igénylő* részére *Hardver kriptográfiai eszközön* (pl. intelligens kártyán vagy tokenen) átadott magánkulcsok esetén az eszközt úgy kell konfigurálni és az *Igénylő* részére átadni, hogy:

- egyértelműen megállapítható legyen, hogy az eszközt az átadás előtt nem használták;
- a magánkulcs használata előtt az *Igénylő* kötelezően azonosítsa magát a *Hardver kriptográfiai eszköz* felé.

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

### 6.2.9. A magánkulcs deaktiválásának módja

#### Szolgáltatói magánkulcsok

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

#### Végfelhasználói magánkulcsok

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

A *Hardver kriptográfiai eszközön* átadott magánkulcs esetén az eszköznek biztosítania kell, hogy a magánkulcsok deaktiválódnak az alábbi esetekben:

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

A deaktivált kulcs illetve *Hardver kriptográfiai eszköz* csak az *Igénylő* újbóli azonosítása után használható .

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 *HSM* eszköz felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell elvégezni.

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

##### Végfelhasználói magánkulcsok

A *Hardver kriptográfiai eszköz* használatát megkövetelő *Hitelesítési rendek* esetén a feleslegessé vált magánkulcsokat az alkalmazott hardver eszköz használati útmutatójában és az eszköz tanúsítvány tanúsítási mellékletében megfogalmazott követelményeknek megfelelően kell megsemmisíteni. A magánkulcsok ennek megfelelő megsemmisítése az *Igénylő* felelőssége.

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

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

#### 6.2.11. A hardver kriptográfiai eszközök értékelése

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

- ISO/IEC 19790 [20] szerinti tanúsítvánnyal,
- vagy FIPS 140-2 Level 3 [27] szerinti tanúsítvánnyal,

- vagy a CEN 14167-2 [29] munkacsoport egyezmény követelményeinek való megfelelést igazoló legalább EAL-4 szintű Common Criteria alapú tanúsítvánnyal,
- vagy a CEN 419 221-5 [17] követelményeinek való megfelelést igazoló legalább EAL-4 szintű Common Criteria alapú tanúsítvánnyal,
- vagy a Nemzeti Média- és Hírközlési Hatóság által vagy az Európai Unió valamely tagállamában nyilvántartásba vett, elektronikus aláírási termékek értékelésére jogosult független tanúsító szervezet által erre a célra kiadott igazolással.

### 6.3. A kulcspár kezelés egyéb szempontjai

#### 6.3.1. Nyilvános kulcs archiválása

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

#### 6.3.2. A tanúsítványok és kulcspárok használatának periódusa

##### A gyökér hitelesítő egységek tanúsítványai és kulcsai

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

##### A köztes hitelesítő egységek tanúsítványai és kulcsai

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

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

##### A végfelhasználói tanúsítványok

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

- legfeljebb a kibocsátástól számított
  - *Kódalíró tanúsítványok* esetében 39 hónap;
  - egyéb *Tanúsítványok* esetében 10 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 *HSM* eszköz felhasználói útmutatójában és az eszköz tanúsítványban megfogalmazott eljárásoknak, követelményeknek megfelelő aktiváló módszereket kell alkalmazzon szolgáltatói magánkulcsainak védelmére.

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

A *Hitelesítés-szolgáltató* által az *Igénylő* részére kibocsátott *Hardver kriptográfiai eszközök* esetén a *Hitelesítés-szolgáltató*nak:

- az aktivizáló adatokat megfelelő minőségű véletlenszám-generátor segítségével, fizikailag biztonságos körülmények között kell előállítania és a *Hardver kriptográfiai eszközre* telepítenie;
- az aktivizáló adatokat biztonságos módszer felhasználásával adja át az *Igénylő* részére.

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

Az *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* részére kibocsátott *Hardver kriptográfiai eszközök* esetén:

- a *Hitelesítés-szolgáltató* az aktivizáló adatokat csak abból a célből rögzítheti, hogy azt az *Igénylő* részére átadhassa;
- a *Hitelesítés-szolgáltató*nak 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* saját maga által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használt;
- a *Hitelesítés-szolgáltató* részére megbízható fél által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használtak;

- olyan nyílt forráskódú szoftverek, amelyek teljesítik a biztonsági követelményeket és amelyek megfelelőségét szoftver verifikáció, strukturált fejlesztés és életciklus menedzsment biztosítja.

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

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

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

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

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

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

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

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

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

### 6.6.2. Biztonságkezelési előírások

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

### 6.6.3. Életciklusra vonatkozó biztonsági előírások

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

- Megfelelő tanúsítással rendelkező *HSM* eszközt kell használnia.
- A *HSM* eszköz átvételekor meg kell róla győződni, hogy a szállítás során biztosították a *HSM* eszközök feltörés elleni védelmét.
- A tárolás során biztosítani kell a *HSM* eszközök feltörés elleni védelmét.
- Az üzemeltetés során folyamatosan be kell tartani a *HSM* eszköz biztonsági előírányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket.

- A használatból kivont *HSM* eszközökben tárolt magánkulcsokat olyan módon kell törölni, hogy lehetetlenné váljon a kulcsok visszaállítása.

### 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

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

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

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

## 6.8. Időbélyegzés

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

## 7. Tanúsítvány, CRL és OCSP profilok

### 7.1. Tanúsítvány profil

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

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [26];
- IETF RFC 5280 [23];
- IETF RFC 6818 [24];
- ETSI EN 319 412-1 [11];
- ETSI EN 319 412-2 [12] természetes személyek számára kibocsátott *Tanúsítványok* esetén;
- ETSI EN 319 412-3 [13] nem természetes személyek számára kibocsátott *Tanúsítványok* esetén;

#### 7.1.1. Verzió szám(ok)

A *Hitelesítés-szolgáltató* által használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítványai* és a *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítványok* legyenek az X.509 specifikáció [26] szerinti "v3" *Tanúsítványok*.

A *Tanúsítványok* alapmezői a következők:

- Verzió (Version)  
A *Tanúsítvány* az X.509 specifikáció [26] szerinti "v3" *Tanúsítványok*nak felel meg, így a mezőbe a "2" érték kerül.
- Sorozatszám (Serial Number)  
A *Tanúsítványt* kibocsátó hitelesítő egység által generált egyedi azonosító.  
A végfelhasználói *Tanúsítványok* esetében a "Serial Number" mezőnek legalább 8 bájttal entropiájú véletlen számot kell tartalmaznia.
- Algoritmus azonosító (Algorithm Identifier)  
A *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző készítéséhez használt kriptográfiai algoritmuskészlet azonosítója (OID).

- Aláírás (Signature)  
A *Hitelesítés-szolgáltató* által készített, a *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző, amelyet a *Hitelesítés-szolgáltató* az "Algoritmus azonosító" -ban megadott algoritmuskészlettel hozott létre.
- Kibocsátó (Issuer)  
A *Tanúsítványt* kibocsátó *Hitelesítő egység* megkülönböztetett neve egyedi X.501 név formátum szerint (lásd: 3.1. fejezet).
- Érvényesség (Valid From & Valid To)  
A *Tanúsítvány* érvényességének kezdete és vége.  
Az időpontok UTC szerint és az IETF RFC 5280-nak megfelelő kódolásban kerülnek rögzítésre.
- Az *Alany* azonosítója (Subject)  
Az *Alany* megkülönböztetett neve egyedi X.501 név formátum szerint (lásd: 3.1. fejezet). Mindig kitöltésre kerül.
- Az *Alany* nyilvános kulcsának algoritmus-azonosítója (Subject Public Key Algorithm Identifier)  
Az *Alany* nyilvános kulcsának algoritmus azonosítója.
- Az *Alany* nyilvános kulcsa (Subject Public Key Value)  
Az *Alany* nyilvános kulcsa.
- Kibocsátó egyedi azonosító (Issuer Unique Identifier)  
Nem kitöltött.
- Az *Alany* egyedi azonosítója (Subject Unique Identifier)  
Nem kitöltött.

### 7.1.2. Tanúsítvány kiterjesztések

A *Hitelesítés-szolgáltató* az X.509 specifikáció [26] szerinti tanúsítvány kiterjesztéseket használhat, saját maga által definiált kritikus kiterjesztések használata nem megengedett.

A tanúsítvány kiterjesztéssel kapcsolatos konkrét előírások:

#### Gyökér hitelesítési egység tanúsítványa

- Hitelesítési rendek (Certificate Policies) – nem kritikus  
OID: 2.5.29.32  
Nem szerepelhet ez a mező.
- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus  
OID: 2.5.29.35  
A *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.  
Használata kötelező.  
A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata.

- *Alany* kulcsazonosító (Subject Key Identifier) – nem kritikus  
OID: 2.5.29.14  
Az *Alany* nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.  
A mező értéke: a nyilvános kulcs SHA-1 lenyomata.  
Használata kötelező.
- *Alany* alternatív nevei (Subject Alternative Names) – nem kritikus  
OID: 2.5.29.17  
Kitöltése opcionális.
- Alapvető megkötések (Basic Constraints) – kritikus  
OID: 2.5.29.19  
Annak megadása, hogy a *Tanúsítvány* hitelesítő egység számára lett-e kibocsátva.  
A kiterjesztés kitöltése kötelező és az értéke: CA = "TRUE".  
A *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  
OID: 2.5.29.37  
A kulcs további engedélyezett használati körének meghatározása.  
Nem szerepelhet.

Más tanúsítvány kiterjesztés nem kerülhet kitöltésre.

### **Köztes hitelesítési egység tanúsítványa**

- Hitelesítési rendek (Certificate Policies) – nem kritikus  
OID: 2.5.29.32  
Ez a mező korlátozhatja a köztes *Tanúsítvány* tartalmazó tanúsítványláncban használható *Hitelesítési rendeket*. A köztes hitelesítési egység alá tartozó alrendszerben csak olyan végfelhasználói *Tanúsítvány* adható ki, amely megfelel az itt felsorolt *Hitelesítési rendek* közül legalább egynek.  
A mező kitöltése kötelező és nem lehet kritikus. A *Hitelesítés-szolgáltató* saját köztes hitelesítési egységei számára kibocsátott *Tanúsítványok* esetében szerepelhet "anyPolicy" Identifier ebben a mezőben.  
A vonatkozó *Szolgáltatási szabályzat* hivatkozása megadható ebben a mezőben.  
Más *Hitelesítés-szolgáltató* számára kibocsátott köztes hitelesítési egység *Tanúsítványainak* esetében csak olyan azonosító szerepelhet ebben a mezőben, amely olyan *Hitelesítési rendre*

vonatkozik, amely megfelel a kibocsátó *Hitelesítés-szolgáltató* által alkalmazott valamely *Hitelesítési rendnek*, és nem lehet benne "anyPolicy" azonosító.

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus  
OID: 2.5.29.35  
A *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.  
Használata kötelező.  
A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata.
- *Alany* kulcsazonosító (Subject Key Identifier) – nem kritikus  
OID: 2.5.29.14  
Az *Alany* nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.  
A mező értéke: a nyilvános kulcs SHA-1 lenyomata.  
Használata kötelező.
- *Alany* alternatív nevei (Subject Alternative Names) – nem kritikus  
OID: 2.5.29.17  
Kitöltése opcionális.
- Alapvető megkötések (Basic Constraints) – kritikus  
OID: 2.5.29.19  
Annak megadása, hogy a *Tanúsítvány* hitelesítő egység számára lett-e kibocsátva.  
A kiterjesztés kitöltése kötelező, és az értéke: CA = "TRUE".  
A *Tanúsítványban* szerepelhet a "pathLenConstraint" mező.
- Kulcshasználat (Key Usage) – kritikus  
OID: 2.5.29.15  
A kulcs engedélyezett használati körének meghatározása.  
Kötelezően beállítandó érték:
  - "keyCertSign",
  - "cRLSign".
- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus  
OID: 2.5.29.37  
A kulcs további engedélyezett használati körének meghatározása.  
A 2019-01-01 után kiadandó köztes szolgáltatói *Tanúsítványokban* szerepeltetni kell egy vagy több "Extended Key Usage" értéket az alábbiak szerint:  
Minden köztes *Hitelesítő egység Tanúsítványa* tartalmazza az általa kibocsátott illetve kibocsátható végfelhasználói *Tanúsítványokban* szereplő valamennyi kibővített kulcshasználati bit értéket a 7.1.2 táblázat szerint.
- 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 (1.2.1 fejezet szerinti OID) ;
- a *Szolgáltatási szabályzat* elérhetősége;
- szöveges figyelmeztetés angol és magyar nyelven, amelyből megállapítható, hogy II. vagy III. hitelesítési osztályú *Tanúsítványról* van-e szó, azaz regisztrációkor történt-e személyes azonosítás, a *Tanúsítvány* alanya természetes személy-e, illetve a *Tanúsítványhoz* tartozó magánkulcsot *HSM* eszköz védi-e (ezen információk a *Hitelesítési rend* azonosítója alapján is megállapíthatóak);
- az ETSI EN 319 411-1 [10] által meghatározott hitelesítési rend azonosítója (OID), amelynek a *Tanúsítvány* megfelel az alábbiak szerint:
  - \* DVCP *Tanúsítvány* esetében OID 0.4.0.2042.1.6,
  - \* OVCP *Tanúsítvány* esetében OID 0.4.0.2042.1.7,
  - \* IVCP *Tanúsítvány* esetében OID 0.4.0.2042.1.8.
- *Kódalíró tanúsítvány* esetében a CA/Browser Forum által meghatározott hitelesítési rend azonosítója:
  - \* OID 2.23.140.1.4.1.

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 *Tanúsítványok*ban.  
A "pathLenConstraint" mező nem szerepelhet a végfelhasználói *Tanúsítványok*ban.
- Kulcshasználat (Key Usage) – kritikus  
OID: 2.5.29.15  
A kulcs engedélyezett használati körének meghatározása.  
A különböző felhasználási célú *Tanúsítványok* esetében a következő kulcshasználati bitek kerüljenek beállításra (más érték nem megengedett):

Tanúsítvány típus	keyUsage (kritikus)	ExtKeyUsage
Autentikáció	digitalSignature, keyAgreement (ECC)	clientAuth (1.3.6.1.5.5.7.3.2)
Cisco VPN client	digitalSignature, keyAgreement, keyEncipherment (RSA)	clientAuth (1.3.6.1.5.5.7.3.2), ipsecEndSystem (1.3.6.1.5.5.7.3.5), ipsecIntermediateSystem (1.3.6.1.5.5.8.2.2)
Cisco VPN Server	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	serverAuth (1.3.6.1.5.5.7.3.1), ipsecEndSystem (1.3.6.1.5.5.7.3.5), ipsecIntermediateSystem (1.3.6.1.5.5.8.2.2)
Code Signing	digitalSignature	codeSigning (1.3.6.1.5.5.7.3.3), softwarePublishing (1.3.6.1.4.1.311.2.1.22)
DomainController	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	clientAuth (1.3.6.1.5.5.7.3.2), serverAuth (1.3.6.1.5.5.7.3.1)
RDP Gateway	keyAgreement (ECC), keyEncipherment (RSA)	serverAuth (1.3.6.1.5.5.7.3.1)
SCEP szerver	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	Document Signing (1.3.6.1.4.1.311.10.3.12)
Smartcardlogon	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	clientAuth (1.3.6.1.5.5.7.3.2), smartcardLogon (1.3.6.1.4.1.311.20.2.2)
Titkosító	keyAgreement (ECC), keyEncipherment (RSA)	emailProtection (1.3.6.1.5.5.7.3.4)
VPN Server	digitalSignature, keyAgreement (ECC), keyEncipherment (RSA)	serverAuth (1.3.6.1.5.5.7.3.1)

7.1.2. táblázat

Kulcshasználati bitek és kibővített kulcshasználati bitek

- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus  
OID: 2.5.29.37  
A kulcs engedélyezett használati körének további meghatározása.  
A különböző felhasználási célú végfelhasználói *Tanúsítványok* esetében az előző táblázatban feltüntetett kiterjesztett kulcshasználati bitek kerüljenek beállításra (más érték nem megengedett).
- 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 végfelhasználói *Tanúsítványok* esetében 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.

Végfelhasználói *Tanúsítványok* esetében 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.

A mezőben a *Hitelesítés-szolgáltató* több szolgáltatás illetve hitelesítési egység *Tanúsítvány* elérhetőségi adatait is megadhatja.

- Minősített tanúsítvánnyal kapcsolatos állítások (Qualified Certificate Statements) – nem kritikus

OID: 1.3.6.1.5.5.7.1.3

A mező a minősített *Tanúsítványokkal* kapcsolatos állítások jelzésére szolgál, azonban van olyan mezője is, amely a nem minősített *Tanúsítvány* esetében is használható.

A végfelhasználói *Tanúsítványban* opcionálisan - az *Ügyfél* kérésére - szerepelhet az *Alany* módosított pénzforgalmi irányelv (PSD2) [2] szerinti adatait leíró állítás (azonosítója: 0.4.0.19495.2). Amennyiben ez megjelenik, az értéke egy struktúra, amely tartalmazza az *Alany* PSD2 szerinti szolgáltatásainak típusát, valamint az *Alany* pénzforgalmi szolgáltatásait felügyelő hatóság nevét és rövidítését.

Egyéb esetben a mező nem szerepelhet.

Más tanúsítvány kiterjesztés nem kerülhet kitöltésre.

### 7.1.3. Az algoritmus objektum azonosítója

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

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

### 7.1.4. Névformák

A *Hitelesítés-szolgáltató* a jelen *Hitelesítési rendek* alapján kibocsátott *Tanúsítványokban* egy – az IETF RFC 5280 szabványban [23] illetve az ETSI EN 319 412-2, -3, -4 szabványokban [12], [13], [14] meghatározott attribútumokból összeállított – megkülönböztetett nevet kell használnon az *Alany* azonosítására.

A *Tanúsítvány* 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 *Tanúsítványának* "Subject DN" mezőjében szereplő értékkel.

### 7.1.5. Névhasználati megkötöttségek

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

### 7.1.6. A Hitelesítési rend objektum azonosítója

A *Hitelesítés-szolgáltató*nak a jelen *Hitelesítési rend*ek alapján kibocsátott *Tanúsítványok*ba 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 IETF RFC 5280 [23] specifikáció szerinti "v2" verziójú *Tanúsítvány visszavonási listákat* bocsásson ki.

### 7.2.2. Tanúsítvány visszavonási lista kiterjesztések

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

- Verzió (Version)  
A mező értéke kötelezően "1".
- Algoritmus azonosító (Signature Algorithm Identifier)  
A *Tanúsítvány visszavonási listát* hitelesítő elektronikus aláírás vagy bélyegző készítéséhez használt kriptográfiai algoritmuskészlet azonosítója (OID). A minimálisan támogatandó algoritmuskészletek:
  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)

- Aláírás (Signature)  
A *Hitelesítés-szolgáltató* visszavonási listát hitelesítő elektronikus aláírása vagy bélyegzője. A *Tanúsítvány visszavonási listát* az adott hitelesítő egység a *Tanúsítványok* aláírására vagy bélyegzésére használt kulcsával kell hitelesítse.
- Kibocsátó (Issuer)  
A *Tanúsítvány visszavonási listát* kibocsátó hitelesítő egység egyedi azonosítója.
- Hatálybalépés (thisUpdate)  
A *Tanúsítvány visszavonási lista* hatálybalépésének kezdete. UTC szerinti érték az IETF RFC 5280 [23] szerinti kódolással.
- Következő kibocsátás (nextUpdate)  
A következő *Tanúsítvány visszavonási lista* kibocsátásának ideje (lásd: 4.10. fejezet). UTC szerinti érték az IETF RFC 5280 [23] szerinti kódolással.
- Visszavont *Tanúsítványok* (Revoked Certificates)  
A felfüggesztett vagy visszavont *Tanúsítványok* listája a *Tanúsítvány* sorozatszámával és a felfüggesztés vagy visszavonás idejével.

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

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

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

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

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

- Visszavonás oka (Reason Code) – nem kritikus  
OID: 2.5.29.21  
Ebbe a mezőbe a visszavonás oka kerülhet.  
Felfüggesztett *Tanúsítvány* esetén kötelezően kitöltendő mező, az értéke: "certificateHold (6)".
- Érvénytelenség ideje (Invalidity Date) – nem kritikus  
Ebbe a mezőbe a magánkulcs megbízhatatlanná válásának ideje kerülhet.
- Útmutató a felfüggesztett *Tanúsítványok*hoz (Hold Instruction) – nem kritikus  
Ebbe a mezőbe a felfüggesztett *Tanúsítvány* kezelése kerülhet.

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

### 7.3. Online tanúsítvány-állapot válasz (OCSP) profil

A *Hitelesítés-szolgáltató*nak az IETF RFC 6960 [25] szerinti online tanúsítvány-állapot szolgáltatást kell üzemeltetnie.

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

- Algoritmus azonosító (signatureAlgorithm )  
Az OCSP választ hitelesítő digitális aláírás készítéséhez használt algoritmuskészlet azonosítója (OID). A minimálisan támogatandó algoritmuskészletek:
  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
- Aláírás (Signature)  
A *Hitelesítés-szolgáltató* OCSP választ hitelesítő digitális aláírása.
- Válaszadó azonosítója (responderID)  
Az OCSP választ kibocsátó hitelesítő egység egyedi azonosítója.
- Hatálybalépés (thisUpdate)  
Az OCSP válasz hatálybalépésének ideje. UTC szerinti érték az IETF RFC 5280 [23] szerinti kódolással.
- Következő kibocsátás (nextUpdate)  
A következő OCSP válasz kibocsátásának legkésőbbi ideje. UTC szerinti érték az IETF RFC 5280 [23] szerinti kódolással.  
Kitöltése opcionális.
- *Tanúsítvány* állapot válasz (SingleResponse)  
A válasz tartalmazza a *Tanúsítvány* azonosítóját (CertID) és a *Tanúsítvány* visszavonási állapotát (CertStatus).  
A *Hitelesítés-szolgáltató* a CABF BR követelményeinek megfelelő pozitív OCSP választ nyújt, vagyis a válasz csak akkor tartalmazza a "good" értéket, ha az adott *Tanúsítvány* megtalálható a *Hitelesítés-szolgáltató Tanúsítványtár*ában és nincs felfüggesztett vagy visszavont állapotban.

#### 7.3.1. Verziószám(ok)

A *Hitelesítés-szolgáltató*nak támogatnia kell az IETF RFC 6960 [25] szerinti "v1" verziójú online tanúsítvány-állapot kéréseket és válaszokat.

#### 7.3.2. OCSP kiterjesztések

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

- ArchiveCutoff – nem kritikus  
A *Hitelesítés-szolgáltató* az IETF RFC 6960 [25] specifikáció szerinti szabványos jelöléssel jelezheti, ha a lejárt *Tanúsítvány*okra is szolgáltat visszavonási állapot információt. (Lásd: 4.10. fejezet.)

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

- Visszavonás oka (Reason Code) – nem kritikus  
Ebbe a mezőbe a visszavonás oka kerülhet.  
Felfüggesztett *Tanúsítvány* esetén kötelezően kitöltendő mező, az értéke: "certificateHold (6)".

## 8. A megfelelés vizsgálat

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

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [9]
- ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [10]

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

A megfelelésértékelési jelentés alapján kiállított megfeleléségi tanúsítványt közzé kell tenni a *Hitelesítés-szolgáltató* honlapján.

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

### 8.1. Az ellenőrzések körülményei és gyakorisága

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

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 megfelelést igazoló vizsgálatot olyan szervezet végzi el, amely rendelkezik egy EU tagállam nemzeti akkreditációs szervezete által kiadott erre feljogosító felhatalmazással.

## 8.3. Az auditor és az auditált rendszer elem függetlensége

A külső auditot csak olyan személy végezheti:

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

## 8.4. Az auditálás által lefedett területek

Az átvizsgálásnak le kell fednie minimálisan az alábbi területeket:

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

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

## 8.5. A hiányosságok kezelése

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



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

## 8.6. Az eredmények közzététele

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

## 9. Egyéb üzleti és jogi kérdések

### 9.1. Díjak

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

#### 9.1.1. Tanúsítvány kibocsátás és megújítás díjai

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

#### 9.1.2. Tanúsítvány hozzáférés díja

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

#### 9.1.3. Visszavonási állapot információ hozzáférés díja

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

#### 9.1.4. Egyéb szolgáltatások díjai

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

#### 9.1.5. Visszatérítési politika

Nincs megkötés.

### 9.2. Anyagi felelősségvállalás

Nincs megkötés.

### 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.

## 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 [6] és a 2016/679 EU általános adatvédelmi rendelet [3] rendelkezéseinek.

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

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

#### 9.4.1. Adatkezelési 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 *Tanúsítványból* vagy más nyilvános adatforrásból.

#### 9.4.3. Személyes adatnak nem minősülő adatok

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

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

#### 9.4.4. Személyes adatok védelme

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

#### 9.4.5. Személyes adatok felhasználása

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

#### 9.4.6. Adatkezelés

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

#### 9.4.7. Egyéb adatvédelmi követelmények

Nincs előírás.

## 9.5. Szellemi tulajdonjogok

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

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

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

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

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

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

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

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

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

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

## 9.6. Tevékenységért viselt felelősség és helytállás

### 9.6.1. A szolgáltató felelőssége és helytállása

#### A Szolgáltató felelőssége

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

- a *Hitelesítés-szolgáltató* felelősséget vállal az általa támogatott *Hitelesítési rend(ek)*ben leírt eljárásoknak való megfelelésért;
- a *Hitelesítés-szolgáltató* sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- a *Hitelesítés-szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfelekkel* szemben a Polgári Törvénykönyv [7] a szerződésszegésért való felelősség szabályai szerint felelős;

- a *Hitelesítés-szolgáltató* a vele szerződéses jogviszonyban nem álló harmadik személlyel (ilyen az *Érintett fél* ) szemben a Polgári Törvénykönyv [7] általános felelősségi szabálya szerint felelős;
- a *Hitelesítés-szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött Szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 9.8. fejezet);

### A Szolgáltató kötelezettsége

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

- a szolgáltatásnak megfelelő jogi-, szabályozási-, anyagi-, szerződéses stb. keretek megteremtése;
- magas színvonalú és biztonságos szolgáltatások nyújtása a vonatkozó szabályzatok szerint;
- a szolgáltatásokhoz kapcsolódó szervezetek (hitelesítő szervezet, ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése;
- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése;
- a szolgáltatások biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket;
- a publikus nyilvántartások és saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az interneten keresztül.

### A hitelesítő szervezet felelőssége

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

A hitelesítő szervezet belső működtetését a *Hitelesítés-szolgáltató* belső, operatív szabályzatai határozzák meg. A hitelesítő egységek által kibocsátott szolgáltatói tanúsítványok kezelése (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;
- az *HSM* eszközt aktivizáló kód és az eszközre töltött kulcsok összetartozásáért,
- általában a kötelezettségei betartásáért.

### 9.6.2. A regisztráló szervezet felelőssége és helytállása

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

A *Regisztráló szervezet* felelőssége:

- az *Igénylő* személyazonosságának megállapítása;
- a *Képviselet szervezet* szervezeti azonosságának, a *Képviselet szervezet* nevében eljáró személy személyazonosságának és képviseleti jogosultságának megállapítása;
- a felvett regisztrációs adatok valóságának 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;
- a *Tanúsítvány*ban szereplő adatok ellenőrzéséért,
- az adataiban bekövetkezett változások haladéktalan bejelentéséért;
- magánkulcsának és *Tanúsítvány*ának a szabályzatoknak megfelelő felhasználásáért;
- magánkulcsának és aktivizáló kódjának biztonságos kezeléséért;
- a *Hitelesítés-szolgáltató* haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyekben;
- általában a kötelezettségei betartásáért.

**Az Igénylő kötelezettségei**

Az *Igénylő* köteles:

- a szolgáltatás igénybevétele előtt megismerni a jelen *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 *Tanúsítvány*ban 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;
- 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 *Tanúsítvány* 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
- 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 (pl. adathalászat, csalás, kártékony programok terjesztése) 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 a *Szolgáltatási szabályzatban* és a vonatkozó *Hitelesítési rendben* 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 *Igénylők* nem tartják be a magánkulcs kezelésével kapcsolatos előírásokat;
- az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a nemzetközi mértékadó ajánlások által elfogadott kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

### 9.8. A felelősség korlátozása

A *Hitelesítés-szolgáltató* korlátozhatja a kártérítési felelősségét.

### 9.9. Kártérítési kötelezettség

#### 9.9.1. A szolgáltató kártérítési kötelezettsége

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

#### 9.9.2. Az előfizető kártérítési kötelezettsége

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

#### 9.9.3. Az érintett felek kártérítési kötelezettsége

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

### 9.10. Érvényesség és megszűnés

#### 9.10.1. Érvényesség

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

### 9.10.2. Megszűnés

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

### 9.10.3. A megszűnés következményei

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

## 9.11. A felek közötti kommunikáció

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

## 9.12. Módosítások

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

### 9.12.1. Módosítási eljárás

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

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

### 9.12.2. Értesítések módja és határideje

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

### 9.12.3. Az OID megváltoztatása

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

## 9.13. Vitás kérdések rendezése

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

#### 9.14. Irányadó jog

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

#### 9.15. Az érvényben lévő jogszabályoknak való megfelelés

A jelen *Hitelesítési rend* megfelel az alábbi jogszabályoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [6];
- 2013. évi V. törvény a Polgári Törvénykönyvről [7].
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól [8];

#### 9.16. Vegyes rendelkezések

##### 9.16.1. Teljességi záradék

Nincs megkötés.

##### 9.16.2. Átruházás

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

##### 9.16.3. Részleges érvénytelenség

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

##### 9.16.4. Igényérvényesítés

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

**9.16.5. Vis maior**

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

**9.17. Egyéb rendelkezések**

Nincs megkötés.

## A. A rövid hitelesítési rend azonosítók képzési szabályai

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

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

## B. Hivatkozások

- [1] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről .
- [2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2015/2366 IRÁNYELVE (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről .
- [3] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) .
- [4] 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról .
- [5] 2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról .
- [6] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról .
- [7] 2013. évi V. törvény a Polgári Törvénykönyvről .
- [8] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól .
- [9] ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- [10] ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- [11] ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- [12] 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;.
- [13] 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.
- [14] 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.
- [15] ETSI TS 119 312 V1.3.1 (2019-02); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

- 
- [16] ETSI TS 119 495 V1.3.2 (2019-06); Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.
- [17] CEN 419 221-5; Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.
- [18] ISO 3166-1:2013, Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.
- [19] MSZ/ISO/IEC 15408-2002 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai, 2002 december .
- [20] ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules".
- [21] IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.
- [22] IETF RFC 4043: Internet X.509 Public Key Infrastructure - Permanent Identifier, May 2005.
- [23] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.
- [24] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.
- [25] IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.
- [26] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
- [27] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.
- [28] Common Criteria for Information Technology Security Evaluation, Part 1 - 3.
- [29] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.
- [30] CEN CWA 14169: Secure signature-creation devices "EAL 4+", March 2004.