Elektronikusan aláírta:
Vanczák Gergely

MICROSEC

e-Szignó Hitelesítés Szolgáltató

eIDAS Rendelet szerinti minősített elektronikus bélyegző tanúsítvány hitelesítési rendek

ver. 2.23

Hatálybalépés: 2021-07-31

Azonosító	1.3.6.1.4.1.21528.2.1.1.181.2.23, 1.3.6.1.4.1.21528.2.1.1.182.2.23, 1.3.6.1.4.1.21528.2.1.1.183.2.23
Verzió	2.23
Első verzió hatálybalépése	2016-07-01
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2021-07-24
Hatálybalépés dátuma	2021-07-31

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság

1033 Budapest, Ángel Sanz Briz út 13.

Verzió	Hatálybalépés	A változás leírása
2.0	2016-07-01	- Új szabályzat az eIDAS követelmények szerint.
2.1	2016-09-05	- Módosítások az NMHH észrevételei alapján.
2.2	2016-10-30	- Módosítások a tanúsító észrevételei alapján.
2.4	2017-09-30	- Éves felülvizsgálat.
2.6	2018-03-24	- Teljes felülvizsgálat. - Közjegyzői személy azonosítás bevezetése. - Kisebb módosítások.
2.7	2018-09-15	- Éves felülvizsgálat.
2.8	2018-12-14	- Változások az auditor javaslatai alapján.
2.11	2019-09-25	- Éves felülvizsgálat.
2.12	2019-12-12	- Változások az auditor javaslatai alapján.
2.13	2020-03-05	- Hatály. - Időbélyegző tanúsítvány leírás módosítása. - Személyes azonosítás szabályai. - Tanúsítvány módosítás. - HSM követelmények. - Kisebb pontosítások.
2.14	2020-05-11	- Kisebb pontosítások. - 2. fejezet átszervezése. - Videotechnológiás természetes személy azonosítás bevezetése a 3.2.3 fejezetben. - A visszavonás feltételeinek kibővítése a 4.9 fejezetben. - 9.4 fejezet kibővítése.
2.15	2020-06-26	- Pontosítások a Távoli kulcsmenedzsment szolgáltatás kapcsán. - Videotechnológiás természetes személy azonosítás megszüntetése a 3.2.3 fejezetben. - Kisebb pontosítások.
2.16	2020-08-14	- OCSP Signing EKU eltávolítása a CA tanúsítványokból. - Kisebb pontosítások.
2.17	2020-10-28	- Pontosítások az auditor és a felügyelő hatóság észrevételei alapján. - Kisebb pontosítások.

Verzió	Hatálybalépés	A változás leírása
2.19	2020-12-28	- Videotechnológiás természetes személy azonosítás bevezetése a 3.2.3 fejezetben. - Szolgáltató által kezdeményezett Tanúsítvány megújítás szabályainak pontosítása. - Open Banking tanúsítványok bevezetése. - Kisebb módosítások.
2.21	2021-03-19	- Szolgáltató kulcsok előálítási szabályainak pontosítása a 6.1.1. fejezetben - A visszavonási lista leírásának pontosítása a 7.2. fejezetben - MD 940 hozzáadása a MALE listához. - Kisebb módosítások.
2.22	2021-06-30	- Elektronikus bélyegző tanúsítványára visszavezetett azonosítás. - Ki kezdeményezheti a visszavonást. - Kulcs kompromittálódás bejelentése. - Megfelelőség értékelés eredményeinek közzététele. - Kisebb pontosítások.
2.23	2021-07-31	- 3 éves tanúsítvány élettartam. - Tanúsítványkérelem benyújtása Ügyféltér fiókon keresztül.

© 2021, Microsec zrt. Minden jog fenntartva.

Tartalomjegyzék

1. Bevezetés **13**
1.1. Áttekintés . . . 13
1.2. Dokumentum neve és azonosítója . . . 13
1.2.1. Hitelesítési rendek . . . 14
1.2.2. Hatály . . . 17
1.2.3. Biztonsági szintek . . . 17
1.3. PKI szereplők . . . 18
1.3.1. Hitelesítés-szolgáltató . . . 18
1.3.2. Regisztráló szervezetek . . . 18
1.3.3. Ügyfelek . . . 19
1.3.4. Érintett felek . . . 19
1.3.5. Egyéb szereplők . . . 19
1.4. A tanúsítvány felhasználhatósága . . . 19
1.4.1. Megfelelő tanúsítvány használat . . . 19
1.4.2. Tiltott tanúsítvány használat . . . 20
1.5. A dokumentum adminisztrálása . . . 20
1.5.1. A dokumentum adminisztrációs szervezete . . . 20
1.5.2. Kapcsolattartó személy . . . 20
1.5.3. A Szolgáltatási szabályzat *Hitelesítési rend*nek való megfelelőségéért felelős személy/szervezet . . . 20
1.5.4. A Szolgáltatási szabályzat elfogadási eljárása . . . 21
1.6. Fogalmak és rövidítések . . . 21
1.6.1. Fogalmak . . . 21
1.6.2. Rövidítések . . . 29

2. Közzététel és adattár felelősségek **29**
2.1. Adattárak . . . 29
2.2. A tanúsítványokra vonatkozó információk közzététele . . . 30
2.3. A közzététel időpontja vagy gyakorisága . . . 31
2.3.1. Kikötések és feltételek közzétételi gyakorisága . . . 31
2.3.2. Tanúsítványok nyilvánosságra hozatalának gyakorisága . . . 31
2.3.3. A megváltozott visszavonási állapot közzétételének gyakorisága . . . 32
2.4. Az adattárak elérésének szabályai . . . 32

3. Azonosítás és hitelesítés **32**
3.1. Elnevezések . . . 32
3.1.1. Név típusok . . . 32
3.1.2. A nevek értelmezhetősége . . . 35

3.1.3. Álnevek használata . . . 35
3.1.4. A különböző elnevezési formák értelmezési szabályai . . . 35
3.1.5. A nevek egyedisége . . . 35
3.1.6. Márkanevek elismerése, azonosítása, szerepük . . . 36
3.2. Kezdeti regisztráció, azonosság hitelesítése . . . 36
3.2.1. A magánkulcs birtoklásának igazolása . . . 36
3.2.2. Szervezet azonosságának hitelesítése . . . 36
3.2.3. Természetes személy azonosságának hitelesítése . . . 37
3.2.4. Nem ellenőrzött alany információk . . . 40
3.2.5. Jogok, felhatalmazások ellenőrzése . . . 40
3.2.6. Együttműködési képességre vonatkozó követelmények . . . 40
3.3. Azonosítás és hitelesítés kulcscsere kérelem esetén . . . 41
3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén . . . 41
3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén . . . 41
3.4. Azonosítás és hitelesítés tanúsítvány megújítás esetén . . . 41
3.4.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén . . . 41
3.4.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén . . . 41
3.5. Azonosítás és hitelesítés tanúsítvány módosítás esetén . . . 42
3.5.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén . . . 42
3.5.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén . . . 42
3.6. Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási kérelem esetén 42
3.7. Ellenőrzött kommunikációs csatorna . . . 42

4. A tanúsítványok életciklusára vonatkozó követelmények 42
4.1. Tanúsítványkérelem . . . 42
4.1.1. Ki nyújthat be tanúsítványkérelmet . . . 43
4.1.2. A bejegyzés folyamata és a résztvevők felelőssége . . . 44
4.2. A tanúsítványkérelem feldolgozása . . . 45
4.2.1. Az igénylő azonosítása és hitelesítése . . . 45
4.2.2. A tanúsítványkérelem elfogadása vagy visszautasítása . . . 45
4.2.3. A tanúsítványkérelem feldolgozásának időtartama . . . 45
4.3. A tanúsítvány kibocsátása . . . 45
4.3.1. A Hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során . . 45
4.3.2. Az Ügyfél értesítése a tanúsítvány kibocsátásáról . . . 46
4.4. A tanúsítvány elfogadása . . . 46
4.4.1. A tanúsítvány elfogadás módja . . . 46
4.4.2. A tanúsítvány közzététele . . . 46
4.4.3. További szereplők értesítése a tanúsítvány kibocsátásról . . . 46
4.5. A kulcspár és a tanúsítvány használata . . . 46

4.5.1. A magánkulcs és a tanúsítvány használata 46
4.5.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata 47
4.6. Tanúsítvány megújítás 47
4.6.1. A tanúsítvány megújítás körülményei 47
4.6.2. Ki kérelmezheti a tanúsítvány megújítást 47
4.6.3. A tanúsítvány megújítási kérelmek feldolgozása 48
4.6.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról 48
4.6.5. A megújított tanúsítvány elfogadása 48
4.6.6. A megújított tanúsítvány közzététele 48
4.6.7. További szereplők értesítése a tanúsítvány kibocsátásáról 49
4.7. Kulcscsere 49
4.7.1. A kulcscsere körülményei 49
4.7.2. Ki kérelmezheti a kulcscserét 49
4.7.3. A kulcscsere kérelmek feldolgozása 49
4.7.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról 49
4.7.5. A kulcscserével megújított tanúsítvány elfogadása 50
4.7.6. A kulcscserével megújított tanúsítvány közzététele 50
4.7.7. További szereplők értesítése a tanúsítvány kibocsátásáról 50
4.8. Tanúsítvány módosítás 50
4.8.1. A tanúsítvány módosítás körülményei 50
4.8.2. Ki kérelmezheti a tanúsítvány módosítást 51
4.8.3. A tanúsítvány módosítási kérelmek feldolgozása 51
4.8.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról 51
4.8.5. A módosított tanúsítvány elfogadása 51
4.8.6. A módosított tanúsítvány közzététele 51
4.8.7. További szereplők értesítése a tanúsítvány kibocsátásáról 51
4.9. Tanúsítvány visszavonás és felfüggesztés 52
4.9.1. A tanúsítvány visszavonás körülményei 52
4.9.2. Ki kérelmezheti a visszavonást 55
4.9.3. A visszavonási kérelemre vonatkozó eljárás 56
4.9.4. A visszavonási kérelemre vonatkozó kivárási idő 56
4.9.5. A visszavonási eljárás maximális hossza 56
4.9.6. Az Érintett felek számára javasolt eljárás a visszavonási információ ellenőrzésére 56
4.9.7. A visszavonási lista kibocsátás gyakorisága 57
4.9.8. A visszavonási lista előállítása és közzététele közötti idő maximális hossza 57
4.9.9. Valós idejű tanúsítvány állapot ellenőrzés lehetősége 57
4.9.10. A valós idejű tanúsítvány állapot ellenőrzésre vonatkozó követelmények . . 57
4.9.11. A visszavonási hirdetmények egyéb elérhető formái 57

4.9.12. A kulcs kompromittálódásra vonatkozó speciális követelmények 57
4.9.13. A felfüggesztés körülményei 58
4.9.14. Ki kérelmezheti a felfüggesztést 58
4.9.15. A felfüggesztési kérelemre vonatkozó eljárás 58
4.9.16. A felfüggesztés maximális hossza 58
4.10. Tanúsítvány állapot szolgáltatások 58
4.10.1. Működési jellemzők 59
4.10.2. A szolgáltatás rendelkezésre állása 59
4.10.3. Opcionális lehetőségek 59
4.11. Az előfizetés vége 59
4.12. Magánkulcs letétbe helyezése és visszaállítása 59
4.12.1. Kulcsletét és visszaállítás rendje és szabályai 59
4.12.2. Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai 60

5. Elhelyezési, eljárásbeli és üzemeltetési előírások 60
5.1. Fizikai követelmények 60
5.1.1. A telephely elhelyezése és szerkezeti felépítése 60
5.1.2. Fizikai hozzáférés 60
5.1.3. Áramellátás és légkondicionálás 61
5.1.4. Beázás és elárasztódás veszély kezelése 62
5.1.5. Tűz megelőzés és tűzvédelem 62
5.1.6. Adathordozók tárolása 62
5.1.7. Hulladék megsemmisítése 62
5.1.8. A mentési példányok fizikai elkülönítése 62
5.2. Eljárásbeli előírások 63
5.2.1. Bizalmi szerepkörök 63
5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok 64
5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés 64
5.2.4. Egymást kizáró szerepkörök 64
5.3. Személyzetre vonatkozó előírások 64
5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények 65
5.3.2. Előélet vizsgálatára vonatkozó eljárások 65
5.3.3. Képzési követelmények 66
5.3.4. Továbbképzési gyakoriságok és követelmények 66
5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága 66
5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei 67
5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények . . . 67

5.3.8. A személyzet számára biztosított dokumentációk 67
5.4. Naplózási eljárások 67
5.4.1. A tárolt események típusai 67
5.4.2. A naplófájl feldolgozásának gyakorisága 70
5.4.3. A naplófájl megőrzési időtartama 71
5.4.4. A naplófájl védelme 71
5.4.5. A naplófájl mentési eljárásai 71
5.4.6. A naplózás adatgyűjtési rendszere 71
5.4.7. Az eseményeket kiváltó alanyok értesítése 71
5.4.8. Sebezhetőség felmérése 72
5.5. Adatok archiválása 72
5.5.1. Az archivált adatok típusai 72
5.5.2. Az archívum megőrzési időtartama 73
5.5.3. Az archívum védelme 73
5.5.4. Az archívum mentési folyamatai 73
5.5.5. Az adatok időbélyegzésére vonatkozó követelmények 74
5.5.6. Az archívum gyűjtési rendszere 74
5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások 74
5.6. Szolgáltatói kulcs cseréje 74
5.7. Kompromittálódást és katasztrófát követő helyreállítás 75
5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások 75
5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok 75
5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások 75
5.7.4. Működés folyamatosságának biztosítása katasztrófát követően 76
5.8. A hitelesítés-szolgáltató vagy a regisztráló szervezet leállítása 76

6. Műszaki biztonsági óvintézkedések 76
6.1. Kulcspár előállítása és telepítése 77
6.1.1. Kulcspár előállítása 77
6.1.2. Magánkulcs eljuttatása az igénylőhöz 79
6.1.3. A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz 80
6.1.4. A szolgáltatói nyilvános kulcs közzététele 80
6.1.5. Kulcsméretek 80
6.1.6. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése 81
6.1.7. A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően) 81
6.2. A magánkulcsok védelme 81
6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások 82
6.2.2. Magánkulcs többszereplős (n-ből m) használata 82

6.2.3. Magánkulcs letétbe helyezése . . . 82
6.2.4. Magánkulcs mentése . . . 82
6.2.5. Magánkulcs archiválása . . . 83
6.2.6. Magánkulcs bejuttatása hardver kriptográfiai eszközbe, vagy onnan történő exportja . . . 83
6.2.7. Magánkulcs tárolása hardver kriptográfiai eszközben . . . 83
6.2.8. A magánkulcs aktiválásának módja . . . 83
6.2.9. A magánkulcs deaktiválásának módja . . . 84
6.2.10. A magánkulcs megsemmisítésének módja . . . 84
6.2.11. A hardver kriptográfiai eszközök értékelése . . . 85
6.3. A kulcspár kezelés egyéb szempontjai . . . 85
6.3.1. Nyilvános kulcs archiválása . . . 85
6.3.2. A tanúsítványok és kulcspárok használatának periódusa . . . 85
6.4. Aktivizáló adatok . . . 87
6.4.1. Aktivizáló adatok előállítása és telepítése . . . 87
6.4.2. Az aktivizáló adatok védelme . . . 87
6.4.3. Az aktivizáló adatok kezelésének egyéb szempontjai . . . 88
6.5. Informatikai biztonsági előírások . . . 88
6.5.1. Speciális informatikai biztonsági műszaki követelmények . . . 88
6.5.2. Az informatikai biztonság értékelése . . . 88
6.6. Életciklusra vonatkozó műszaki előírások . . . 88
6.6.1. Rendszerfejlesztési előírások . . . 88
6.6.2. Biztonságkezelési előírások . . . 89
6.6.3. Életciklusra vonatkozó biztonsági előírások . . . 89
6.7. Hálózati biztonsági előírások . . . 90
6.8. Időbélyegzés . . . 91

7. Tanúsítvány, CRL és OCSP profilok 91
7.1. Tanúsítvány profil . . . 91
7.1.1. Verzió szám(ok) . . . 91
7.1.2. Tanúsítvány kiterjesztések . . . 92
7.1.3. Az algoritmus objektum azonosítója . . . 100
7.1.4. Névformák . . . 100
7.1.5. Névhasználati megkötöttségek . . . 101
7.1.6. A Hitelesítési rend objektum azonosítója . . . 101
7.1.7. A Hitelesítési rend megkötöttségek kiterjesztés használata . . . 101
7.1.8. A Hitelesítési rend jellemzők szintaktikája és szemantikája . . . 101
7.1.9. A kritikus Hitelesítési rend kiterjesztések feldolgozási szemantikája . . . 101
7.2. Tanúsítvány visszavonási lista (CRL) profil . . . 101

7.2.1. Verziószám(ok) . . . 101
7.2.2. Tanúsítvány visszavonási lista kiterjesztések . . . 101
7.3. Online tanúsítvány-állapot válasz (OCSP) profil . . . 103
7.3.1. Verziószám(ok) . . . 104
7.3.2. OCSP kiterjesztések . . . 104

8. A megfelelőség vizsgálata 104
8.1. Az ellenőrzések körülményei és gyakorisága . . . 105
8.2. Az auditor és szükséges képesítése . . . 105
8.3. Az auditor és az auditált rendszerelem függetlensége . . . 106
8.4. Az auditálás által lefedett területek . . . 106
8.5. A hiányosságok kezelése . . . 106
8.6. Az eredmények közzététele . . . 107

9. Egyéb üzleti és jogi kérdések 107
9.1. Díjak . . . 107
9.1.1. Tanúsítvány kibocsátás és megújítás díjai . . . 107
9.1.2. Tanúsítvány hozzáférés díja . . . 107
9.1.3. Visszavonási állapot információ hozzáférés díja . . . 107
9.1.4. Egyéb szolgáltatások díjai . . . 107
9.1.5. Visszatérítési politika . . . 107
9.2. Anyagi felelősségvállalás . . . 107
9.2.1. Pénzügyi követelmények . . . 108
9.2.2. További követelmények . . . 108
9.2.3. Felelősségbiztosítás . . . 108
9.3. Bizalmasság . . . 109
9.3.1. Bizalmas információk köre . . . 109
9.3.2. Bizalmas információk körén kívül eső adatok . . . 109
9.3.3. Bizalmas információ védelme . . . 109
9.4. Személyes adatok védelme . . . 109
9.4.1. Adatkezelési terv . . . 110
9.4.2. Személyes adatok . . . 110
9.4.3. Személyes adatnak nem minősülő adatok . . . 110
9.4.4. Személyes adatok védelme . . . 110
9.4.5. Személyes adatok felhasználása . . . 110
9.4.6. Adatkezelés . . . 110
9.4.7. Egyéb adatvédelmi követelmények . . . 110
9.5. Szellemi tulajdonjogok . . . 110
9.6. Tevékenységért viselt felelősség és helytállás . . . 111

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

A. A rövid hitelesítési rend azonosítók képzési szabályai 120

B. Hivatkozások 121

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zrt. (továbbiakban: Microsec vagy *Hitelesítés-szolgáltató*) által üzemeltetett e-Szignó Hitelesítés Szolgáltató által meghatározott elektronikus bélyegző minősített tanúsítványának kibocsátása szolgáltatásra vonatkozó *Hitelesítési rend*et tartalmazza.

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

1.1. Áttekintés

A *Hitelesítési rend* egy "szabálygyűjtemény, amely egy *Tanúsítvány* felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára". Jelen dokumentum tartalmilag és formailag megfelel az IETF RFC 3647 [30] 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 rend*ek mindegyikére egységesen érvényes, ezt külön nem jelöljük. Az eltérően kezelendő követelmények esetén egyértelműen meghatározásra kerül, hogy az adott követelmény mely *Hitelesítési rend*(ek)re vonatkozik.

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

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

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

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

1.2. Dokumentum neve és azonosítója

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

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	eIDAS Rendelet szerinti minősített elektronikus bélyegző tanúsítvány hitelesítési rendek
Dokumentum verziószáma	2.23
Hatálybalépés ideje	2021-07-31

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

1.2.1. Hitelesítési rendek

A *Hitelesítés-szolgáltató* által kibocsátott valamennyi *Tanúsítvány*nak hivatkoznia kell arra a *Hitelesítési rend*re, amely alapján a kibocsátás történt.

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

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

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

(1.3.6.1.4.1.21528)	MICROSEC Ltd.
(2)	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

1.3.6.1.4.1.21528.2.1.1.181.2.23	Minő/-sített, elektro/-nikus bé/-lyeg/-ző létre/-hozására és ellenőr/-zésére szol/-gáló, nem termé/-szetes szemé/-lyek szá/-mára *Minősített elektronikus bélyegzőt létrehozó eszköz*ön kibo/-csátott *Tanúsítvány*okat szabá/-lyozó, álnevet kizáró hitelesítési rend.	MBJBN
1.3.6.1.4.1.21528.2.1.1.182.2.23	Minő/-sített, elektro/-nikus bé/-lyeg/-ző létre/-hozására és ellenőr/-zésére szol/-gáló, nem termé/-szetes szemé/-lyek szá/-mára *Hardver kriptográfiai eszköz*ön kibo/-csátott *Tanúsítvány*okat szabá/-lyozó, álnevet kizáró hitelesítési rend.	MBJHN
1.3.6.1.4.1.21528.2.1.1.183.2.23	Minő/-sített, elektro/-nikus bé/-lyeg/-ző létre/-hozására és ellenőr/-zésére szol/-gáló, nem termé/-szetes szemé/-lyek szá/-mára szoftve/-resen kibo/-csátott *Tanúsítvány*okat szabá/-lyozó, álnevet kizáró hitelesítési rend.	MBJSN

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

A nem természetes személyek számára kibocsátott *Tanúsítvány*okra vonatkozó *Hitelesítési rend*ek esetén az *Alany* jogi személy.

A *Tanúsítvány*okban szerepeltethető az informatikai rendszer, alkalmazás vagy automatizmus megnevezése is, amely segítségével a *Tanúsítvány*t használják (*Automata tanúsítvány*). A jelen *Hitelesítési rend*ek mindegyike kizárja az álnév használatát, a *Tanúsítvány*ban minden esetben az *Alany* valódi neve szerepel.

A *Minősített elektronikus bélyegzőt létrehozó eszköz* használatát megkövetelő *Hitelesítési rend*ek ([xxxBx])esetén a *Hitelesítés-szolgáltató*nak meg kell győződnie arról, hogy a *Tanúsítvány*hoz tartozó magánkulcs az Európai Unió valamely tagállamában nyilvántartásba vett tanúsító szervezet által kiadott igazolás szerinti *Minősített elektronikus bélyegzőt létrehozó eszköz*ön helyezkedik el.

A *Hardver kriptográfiai eszköz* használatát megkövetelő *Hitelesítési rend*ek ([xxxHx]) esetén a *Hitelesítés-szolgáltató* meggyőződik róla, hogy a *Tanúsítvány*hoz tartozó magánkulcs az alábbi tanúsítvány legalább egyikével rendelkező *Hardver kriptográfiai eszköz*ön helyezkedik el:

- az Európai Unió valamely tagállamában nyilvántartásba vett tanúsító szervezet által kiadott igazolás szerint *Minősített elektronikus bélyegzőt létrehozó eszköz*re vonatkozó tanúsítás;
- legalább EAL-4 szintű Common Criteria [39] tanúsítvány a CEN SSCD PP [41] szerint;
- legalább EAL-4 szintű Common Criteria [39] tanúsítvány a CEN 419 221-5 [26] szerint;
- FIPS 140-2, Level 2 (vagy magasabb szintű) tanúsítvány [38].

Jogszabályban meghatározott informatikai eszköz felhasználásával automatikusan, közvetlen személyi felügyelet nélkül is készíthető minősített *Tanúsítvány*on alapuló fokozott biztonságú elektronikus bélyegző.

A *Minősített elektronikus bélyegzőt létrehozó eszköz* illetve *Hardver kriptográfiai eszköz* használatát megkövetelő *Hitelesítési rend*eknek megfelelő *Tanúsítvány* kibocsátható távoli kulcsmenedzsment szolgáltatás keretében történő felhasználásra is, amennyiben

- a távoli kulcsmenedzsment szolgáltatást egy minősített bizalmi szolgáltató nyújtja,
- a minősített bizalmi szolgáltató a követelményeknek megfelelő *Minősített elektronikus bélyegzőt létrehozó eszköz* illetve *Hardver kriptográfiai eszköz* tanúsítvánnyal rendelkező eszközben kezeli a felhasználók magánkulcsait,
- a távoli kulcsmenedzsment szolgáltatás követelményeknek megfelelő működését egy arra jogosult független tanúsító szervezet által elvégzett megfelelőség értékelés igazolja,
- a minősített bizalmi szolgáltató írásban nyilatkozik, hogy a *Tanúsítvány*ban feltüntetendő nyilvános kulcshoz tartozó magánkulcsot a tanúsításnak megfelelően *Minősített elektronikus bélyegzőt létrehozó eszköz*ben illetve *Hardver kriptográfiai eszköz*ben kezeli.

A *Minősített elektronikus bélyegzőt létrehozó eszköz* használatát megkövetelő minősített *Hitelesítési rend*ek ([xxxBx]) alapján kibocsátott *Tanúsítvány*hoz tartozó magánkulcsot *Minősített elektronikus bélyegzőt létrehozó eszköz* védi. Minősített elektronikus bélyegző csak ilyen *Tanúsítvány*ok alapján készíthető.

Amennyiben egy minősített *Hitelesítési rend* nem követeli meg *Minősített elektronikus bélyegzőt létrehozó eszköz* használatát, a rend szerint kibocsátott *Tanúsítvány* alapján minősített *Tanúsítvány*ra épülő fokozott biztonságú elektronikus bélyegző készíthető.

A minősített elektronikus bélyegzővel vagy minősített *Tanúsítvány*ra épülő fokozott biztonságú elektronikus bélyegzővel ellátott dokumentum a polgári perrendtartásról szóló 1952. évi III. törvény [4] 196. §-a értelmében teljes bizonyító erejű magánokirat.

Jelen *Hitelesítési rend*ek közül:

- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-2 [18] szabványban definiált [QCP-l] *Hitelesítési rend*nek;
- az [MBJBN] *Hitelesítési rend* megfelel a [QCP-l-qscd] *Hitelesítési rend*nek;
- az [MBJHN] *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [17] szabványban definiált [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 *Tanúsítvány*okban csak a magasabb szintű Hitelesítési Rend azonosítója kerül feltüntetésre.

	[QCP-l]	[QCP-l-qscd]	[NCP+]
MBJBN	(x)	X	
MBJHN	X		X
MBJSN	X		

1.2.2. Hatály

Jelen *Hitelesítési rend* gyűjtemény 2021-07-31 -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 szabályzat*okat legalább évente felül kell vizsgálni, és gondoskodni kell az esetlegesen megváltozott követelményekhez illetve igényekhez igazodó módosításukról.

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

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

1.2.3. Biztonsági szintek

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

A *Tanúsítvány Alany* autentikációció erőssége alapján csökkenő sorrendben:

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

A használt hordozó alapján a biztonság szerint csökkenő sorrendben:

- *Minősített elektronikus bélyegzőt létrehozó eszköz*ön kibocsátott *Tanúsítvány*ok [***B*];
- *Hardver kriptográfiai eszköz*ön kibocsátott *Tanúsítvány*ok [***H*];
- egyéb módon, pl. szoftveresen kibocsátott *Tanúsítvány*ok [***S*].

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

- minősített, *Minősített elektronikus bélyegzőt létrehozó eszköz*ön kibocsátott *Tanúsítvány*ok [M**B*];
- minősített, *Hardver kriptográfiai eszköz*ön kibocsátott *Tanúsítvány*ok [M**H*];
- minősített, egyéb módon, pl. szoftveresen kibocsátott *Tanúsítvány*ok [M**S*];

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

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

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

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

1.3. PKI szereplők

1.3.1. Hitelesítés-szolgáltató

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

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

1.3.2. Regisztráló szervezetek

Meghatározását lásd az 1.6 fejezetben.

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

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

1.3.3. Ügyfelek

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

Az *Alany* az a jogi személy, amelynek adatai a *Tanúsítvány*ban szerepelnek.

Az elektronikus bélyegző célú *Tanúsítvány* esetében az *Alany* az *elektronikus bélyegző létrehozója*.

1.3.4. Érintett felek

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

1.3.5. Egyéb szereplők

A megfelelőség értékelést végző független auditor.

A szolgáltatás felügyeletét ellátó hatóság.

Egyéb szereplő nincs.

1.4. A tanúsítvány felhasználhatósága

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

1.4.1. Megfelelő tanúsítvány használat

A *Hitelesítés-szolgáltató* által jelen *Hitelesítési rend*ek valamelyike alapján kibocsátott végfelhasználói *Tanúsítvány*okhoz tartozó magánkulcsok kizárólag elektronikus bélyegző előállítására használhatóak fel, a *Tanúsítvány*ok segítségével az *elektronikus bélyegző létrehozója* igazolhatja az általa lebélyegzett elektronikus dokumentumok hitelességét.

A *Minősített elektronikus bélyegzőt létrehozó eszköz* használatát megkövetelő *Hitelesítési rend*ek esetén ([MBJBN]) a minősített *Tanúsítvány*hoz tartozó magánkulcsot *Minősített elektronikus bélyegzőt létrehozó eszköz* védi, amely az elektronikus bélyegző minősített tanúsítványának kibocsátása szolgáltatás keretén belül kerül kibocsátásra. Az ezen rendek szerint kibocsátott minősített *Tanúsítvány*ok alkalmasak minősített elektronikus bélyegző létrehozására.

Amennyiben egy *Hitelesítési rend* nem követeli meg *Minősített elektronikus bélyegzőt létrehozó eszköz* használatát, a rend szerint kibocsátott minősített tanúsítványon alapuló elektronikus bélyegző minősített tanúsítványra épülő fokozott biztonságú elektronikus bélyegzőnek tekinthető.

A minősített elektronikus bélyegzővel ellátott dokumentum az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény [9] 99. §-a értelmében teljes bizonyító erejű okiratnak minősül.

1.4.2. Tiltott tanúsítvány használat

Szolgáltatói tanúsítványok

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

Végfelhasználói tanúsítványok

A jelen *Hitelesítési rend* alapján kibocsátott *Tanúsítvány*okat, illetve a hozzájuk tartozó magánkulcsokat elektronikus bélyegző előállításától illetve ellenőrzésétől 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 találhatók:

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

1.5.2. Kapcsolattartó személy

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

Kapcsolattartó	Folyamatszervezés részleg vezetője
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13.
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 megfelelőségéért felelős személy/szervezet

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

A *Szolgáltatási szabályzat*ok és a szolgáltatások nyújtása feletti felügyeletet a Nemzeti Média- és Hírközlési Hatóság látja el. A Nemzeti Média- és Hírközlési Hatóság nyilvántartást vezet a követelményeknek megfelelő *Hitelesítési rend*ekről valamint az ezeket alkalmazó *Hitelesítés-szolgáltató*ról.

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

`http://webpub-ext.nmhh.hu/esign2016/`

1.5.4. A Szolgáltatási szabályzat elfogadási eljárása

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

1.6. Fogalmak és rövidítések

1.6.1. Fogalmak

II. hitelesítési osztály	Olyan nem minősített *Hitelesítési rend*ek csoportja, amelyek az *Igénylő* távoli regisztrációja alapján is lehetővé teszik a *Tanúsítvány* kibocsátását.
III. hitelesítési osztály	Olyan nem minősített *Hitelesítési rend*ek csoportja, amelyek a *Tanúsítvány* kibocsátását az *Igénylő* 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 *Tanúsítvány*ban a *Bizalmi szolgáltató* által igazolt azonosságú vagy tulajdonságú jogi személy.
Automata Tanúsítvány	Olyan *Tanúsítvány*, amelyben az *Alany* adatai között feltüntetésre kerül az informatikai eszköz (alkalmazás, rendszer) elnevezése is, amely segítségével az *Alany* a *Tanúsítvány*t használja.
Bélyegző létrehozója (Creator of a Seal)	"Elektronikus bélyegzőt létrehozó jogi személy." (eIDAS [1] 3. cikk 24. pont)
Bizalmi felügyelet	"A *Bizalmi szolgáltatás*ok felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [9] 91.§ 1. bekezdés)

Bizalmi lista (Trusted List)	Az Európai Unió tagállamainak vonatkozásában - az Európai Parlament és a Tanács 910/2014/EU rendelete szerint - egy tagállam által kibocsátott lista, amely információt tartalmaz a tagállam felelőssége alá tartozó bizalmi szolgáltatókra vonatkozóan az általuk nyújtott bizalmi szolgáltatásokra vonatkozó információval együtt, és amely az Európai Bizottság által az Európai Unió Hivatalos Lapjának 2019/C 276/01 számával összhangban kibocsátott központi bizalmi listák jegyzéke alapján hitelesíthető.
Bizalmi szolgáltatás (Trust Service)	"Rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások: • elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy • *Weboldal-hitelesítő tanúsítvány*ok létrehozása, ellenőrzése és érvényesítése; vagy • elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése; " (eIDAS [1] 3. cikk 16. pont)
Bizalmi szolgáltatási rend (Trust Service Policy)	"Olyan szabálygyűjtemény, amelyben egy *Bizalmi szolgáltató*, igénybe vevő vagy más személy valamely *Bizalmi szolgáltatás* használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára. " (2015. évi CCXXII. törvény [9] 1. § 8. pont)
Bizalmi szolgáltató (Trust Service Provider)	"Egy vagy több *Bizalmi szolgáltatás*t nyújtó természetes vagy jogi személy; a *Bizalmi szolgáltató* lehet minősített vagy nem minősített *Bizalmi szolgáltató*." (eIDAS [1] 3. cikk 19. pont)
Elektronikus bélyegző (Electronic Seal)	"Olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét." (eIDAS [1] 3. cikk 25. pont)
Elektronikus bélyegző minősített tanúsítványa (Qualified Certificate for Electronic Seal)	"Elektronikus bélyegző olyan *Tanúsítvány*a, amelyet *Minősített bizalmi szolgáltató* bocsát ki, és amely megfelel az eIDAS [1] III. mellékletében megállapított követelményeknek. " (eIDAS [1] 3. cikk 30. pont)

Elektronikus bélyegző tanúsítványa (Certificate for Electronic Seal)	"Olyan elektronikus tanúsítvány, amely az elektronikus bélyegzőt érvényesítő adatokat egy jogi személyhez kapcsolja, és igazolja az érintett jogi személy nevét. " (eIDAS [1] 3. cikk 29. pont)
Elektronikus bélyegző létrehozásához használt adatok (Electronic Seal Creation Data)	"Olyan egyedi adatok, amelyeket az elektronikus bélyegző létrehozója elektronikus bélyegző létrehozásához használ." (eIDAS [1] 3. cikk 28. pont) Jellemzően kriptográfiai magánkulcs.
Elektronikus bélyegzőt létrehozó eszköz (Electronic Seal Creation Device)	"Elektronikus bélyegző létrehozására használt, konfigurált hardver- vagy szoftvereszköz." (eIDAS [1] 3. cikk 31. 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 kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban. " (eIDAS [1] 3. cikk 33. pont)
Előfizető (Subscriber)	A Szolgáltatóval valamely szolgáltatás igénybevétele érdekében Szolgáltatási szerződést kötő személy vagy szervezet.
Érintett fél (Relying Party)	Az elektronikus dokumentum fogadója, aki egy adott tanúsítványon alapuló elektronikus bélyegzőre hagyatkozva jár el.
Érvényesítés (Validation)	"Olyan folyamat, amelynek keretében ellenőrzik és igazolják, hogy az elektronikus aláírás vagy bélyegző érvényes. " (eIDAS [1] 3. cikk 41. pont)

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 [9] 1. § 21. pont)
Érvényesítési adat (Validation Data)	"Elektronikus aláírás vagy elektronikus bélyegző érvényesítéséhez használt adat." (eIDAS [1] 3. cikk 40. pont)
Felfüggesztés	A *Tanúsítvány* érvényességének ideiglenes megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* felfüggesztése nem végleges, a felfüggesztett *Tanúsítvány* érvényessége visszaállítható.
Fokozott biztonságú elektronikus bélyegző (Advanced Electronic Seal)	"Olyan elektronikus bélyegző, amely megfelel a következő követelményeknek: a/ kizárólag a bélyegző létrehozójához kötött; b/ alkalmas a bélyegző létrehozójának azonosítására; c/ olyan, elektronikus bélyegző létrehozásához használt adatok felhasználásával hozzák létre, amelyeket a bélyegző létrehozója nagy megbízhatósággal kizárólag saját maga elektronikus bélyegző létrehozására használhat; d/ olyan módon kapcsolódik azokhoz az adatokhoz, amelyekre vonatkozik, hogy az adatok minden későbbi változása nyomon követhető; " (eIDAS [1] 3. cikk 26. pont)
Gyökér tanúsítvány (Root Certificate)	Más néven legfelső szintű tanúsítvány. Önhitelesített *Tanúsítvány*, amelyet adott *Hitelesítő egység* saját maga számára bocsátott ki, azaz saját magánkulcsával van aláírva, így a saját – 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 *Bizalmi szolgáltató*, aki/amely a hitelesítés-szolgáltatás keretében azonosítja az igénylő személyét, *Tanúsítvány*t bocsát ki, nyilvántartásokat vezet, fogadja a *Tanúsítvány*okkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a *Tanúsítvány*hoz tartozó szabályzatokat, és a *Tanúsítvány* aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.
Hitelesítő egység	A *Hitelesítés-szolgáltató* rendszerének egy egysége, amely *Tanúsítvány*ok elektronikus aláírását vagy bélyegzését végzi. Egy *Hitelesítő egység*hez mindig egy elektronikus aláírás vagy bélyegző létrehozásához használt adat (magánkulcs) tartozik. Előfordulhat, hogy egy *Hitelesítés-szolgáltató* egyszerre több *Hitelesítő egység*et is működtet.
Hitelesítési rend (Certificate Policy)	"Olyan *Bizalmi szolgáltatási rend*, amely *Bizalmi szolgáltatás* keretében kibocsátott *Tanúsítvány*ra vonatkozik." (2015. évi CCXXII. törvény [9] 1. § 24. pont)
Igénylő	Az a természetes személy, aki az adott *Tanúsítvány* igénylése során eljár.
Képviselt szervezet	Az a *Szervezet*, amelynek a nevében a *Szervezeti ügyintéző* eljár a *Szervezet*hez tartozó *Tanúsítvány*okkal kapcsolatos ügyekben.
Kompromittálódás	Egy kriptográfiai kulcs abban az esetben tekintendő kompromittálódottnak, ha vélelmezhető, hogy illetéktelen személynek is hozzáférése van hozzá.
Köztes hitelesítő egység	Olyan *Hitelesítő egység* amelynek *Tanúsítvány*át egy másik *Hitelesítő egység* bocsátotta ki.
Kriptográfiai kulcs (Cryptographic Key)	Olyan – kriptográfiai transzformációt vezérlő – egyedi digitális jelsorozat, amelynek ismerete szükséges titkosításhoz és dekódoláshoz, illetve elektronikus aláírás vagy bélyegző előállításához és ellenőrzéséhez.
Kulcsgondozás (Key Management)	A kriptográfiai kulcsok előállítása, a felhasználókhoz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, amely szoros kapcsolatban áll az alkalmazott biztonsági eljárásmóddal.

Lenyomat	"Olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti a 2015. évi CCXXII. törvény [9] végrehajtására kiadott rendeletben megfogalmazott követelményeket." (2015. évi CCXXII. törvény [9] 1. § 34. pont) A lenyomat a gyakorlatban olyan rögzített hosszúságú bitsorozat, amely egyértelműen függ az elektronikus dokumentumtól, amelyből származtatják, nagyon kicsi a valószínűsége annak, hogy két különböző dokumentumnak ugyanaz lenne a lenyomata, és gyakorlatilag lehetetlen adott lenyomathoz olyan dokumentumot készíteni, amelynek az a lenyomata.
magánkulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az *Alany*nak szigorúan titokban kell tartania. Elektronikus bélyegző esetében az *elektronikus bélyegző létrehozója* a magánkulcsa segítségével hozza létre a bélyegzőt. A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok kibocsátása során a *Hitelesítő egység* magánkulcsát használja arra, hogy a *Tanúsítvány*t védő elektronikus aláírást vagy bélyegzőt elhelyezze rajta.
Minősített bizalmi szolgáltatás (Qualified Trust Service)	"Olyan *Bizalmi szolgáltatás* amely megfelel az eIDAS Rendeletben foglalt alkalmazandó követelményeknek." (eIDAS [1] 3. cikk 17. pont)
Minősített bizalmi szolgáltató (Qualified Trust Service Provider)	"Olyan *Bizalmi szolgáltató* amely egy vagy több *Minősített bizalmi szolgáltatás*t nyújt, és amelynek minősített státusát a felügyeleti szerv jóváhagyta. " (eIDAS [1] 3. cikk 20. pont)
Minősített elektronikus bélyegző (Qualified Electronic Seal)	"Olyan, fokozott biztonságú elektronikus bélyegző, amelyet minősített elektronikus bélyegzőt létrehozó eszközzel állítottak elő, és amely elektronikus bélyegző minősített tanúsítványán alapul. " (eIDAS [1] 3. cikk 27. pont)
Minősített elektronikus bélyegzőt létrehozó eszköz (Qualified Electronic Seal Creation Device)	"Olyan elektronikus bélyegzőt létrehozó eszköz, amely értelemszerűen megfelel az eIDAS II. mellékletében megállapított követelményeknek." (eIDAS [1] 3. cikk 32. pont)

Minősített elektronikus időbélyegző (Qualified Electronic Time Stamp)	"Olyan elektronikus *Időbélyegző*, amely megfelel az eIDAS Rendelet [1] 42. cikkében megállapított követelményeknek. " (eIDAS [1] 3. cikk 34. pont)
Nyilvános kulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. A nyilvánosságra hozatal jellemzően egy *Tanúsítvány* formájában történik, amely összekapcsolja a szereplő nevét az ő nyilvános kulcsával. Elektronikus bélyegző esetében a bélyegzőt létrehozó fél nyilvános kulcsa szükséges ahhoz, hogy az elektronikus bélyegző hitelességét ellenőrizzük (ez az Érvényesítési adat). A *Tanúsítvány*ok hitelességét az őket kibocsátó *Hitelesítő egység* nyilvános kulcsa segítségével lehet ellenőrizni.
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	Aszimmetrikus kulcsú kriptográfiára épülő infrastruktúra, beleértve a kriptográfiai algoritmusokat, kulcsokat, tanúsítványokat, a rájuk vonatkozó szabványokat és jogszabályokat, a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.
Open Banking	Az EU PSD2 hatókörén kívül eső, de azzal azonos vagy nagyon hasonló követelmények alapján működő pénzforgalmi szolgáltatásokra vonatkozó szabályozott környezet.
Regisztrációs igény	A *Tanúsítványkérelem* és a szolgáltatói szerződés előkészítése céljából az *Ügyfél* által a Szolgáltatónak előzetesen megadott adatok és nyilatkozatok, amelyben többek között felhatalmazza a Szolgáltatót az adatok kezelésére.
Regisztráló szervezet (Registration Authority)	Szervezet, amely ellenőrzi a *Tanúsítvány*ba kerülő adatok valódiságát, az *Igénylő* személy azonosságát, ellenőrzi, hogy a *Tanúsítványkérelem* hiteles-e, és azt egy arra jogosult személy nyújtotta-e be.
Rendkívüli üzemeltetési helyzet	Olyan, a *Hitelesítés-szolgáltató* üzemmenetében zavart okozó rendkívüli helyzet, amikor a *Hitelesítés-szolgáltató* rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
Szervezet	Jogi személy.

Szervezeti tanúsítvány	Olyan *Tanúsítvány*, amelynek *Alany*a *Szervezet*, vagy amely egy természetes személy *Alany* valamely *Szervezet*hez való tartozását mutatja. Ilyen esetben a *Tanúsítvány* "O" mezejében a *Szervezet* neve feltüntetésre kerül. Minden bélyegző tanúsítvány *Szervezeti tanúsítvány*.
Szervezeti ügyintéző	Az *Előfizető* képviseletében eljáró természetes személy, aki jogosult az *Előfizető* nevében a *Tanúsítványkérelem* benyújtására, a *Tanúsítvány* kibocsátás jóváhagyására, az *Előfizető*höz kapcsolódó *Tanúsítvány*ok igénylése, cseréje, felfüggesztése, visszaállítása és visszavonása során eljárni.
Szolgáltatási szabályzat (Trust Service Practice Statement)	"A *Bizalmi szolgáltató* nyilatkozata az egyes *Bizalmi szolgáltatás*ok nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről. " (2015. évi CCXXII. törvény [9] 1. § 41. pont)
Szolgáltatási szerződés	"A *Bizalmi szolgáltató* és a *Bizalmi szolgáltatás*i ügyfél között létrejött szerződés, amely a *Bizalmi szolgáltatás* nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza. " (2015. évi CCXXII. törvény [9] 1. § 42. pont)
Tanúsítvány (Certificate)	"Az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a *Weboldal-hitelesítő tanúsítvány*, valamint mindazon, a *Bizalmi szolgáltatás* 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 [9] 1. § 44.)
Tanúsítványkérelem	Az *Igénylő* által, a Szolgáltató számára a *Tanúsítvány* kibocsátás érdekében benyújtott adatok és nyilatkozatok, amelyekben többek között az *Igénylő* megerősíti a *Tanúsítvány*ba kerülő adatok valódiságát.
Tanúsítványtár	Különböző *Tanúsítvány*okat tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott *Tanúsítvány*okat publikálja, de Tanúsítványtárnak nevezzük az *Alany* illetve az *Érintett fél* számítógépén a használt alkalmazás számára elérhető *Tanúsítvány*okat tartalmazó rendszert is.

Távoli kulcsmenedzsment szolgáltatás	Olyan bizalmi szolgáltatás, amely keretében a szolgáltató biztonságos körülmények között kezeli az Ügyfelek magánkulcsait, biztosítja a szükséges műszaki és eljárási feltételeket annak érdekében, hogy az Ügyfelek – a szolgáltató által tárolt magánkulcsaikkal – kulcs műveleteket végezhessenek el, például elektronikus aláírásokat vagy elektronikus bélyegzőket hozhassanak létre.
Ügyfél	Az *Előfizető* és a hozzá tartozó összes *Igénylő* együttes elnevezése.
Visszavonás	A *Tanúsítvány* érvényességének megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* visszavonása végleges, visszavont *Tanúsítvány* többet nem tehető érvényessé.
Visszavonási állapot nyilvántartás	A *Hitelesítés-szolgáltató* által vezetett belső nyilvántartás a felfüggesztett, illetőleg a visszavont *Tanúsítvány*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 adattár felelősségek

2.1. Adattárak

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

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

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 vagy az *Ügyfél* számára letölthető módon bocsássa az *Ügyfél* rendelkezésére az egyedi Szolgáltatási szerződést, az Általános Szerződési Feltételeket, a *Szolgáltatási kivonat*ot, a *Hitelesítési rend*et és a *Szolgáltatási szabályzat*ot.

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

2.2. A tanúsítványokra vonatkozó információk közzététele

A *Hitelesítés-szolgáltató* tegye közzé a honlapján a

- szolgáltatói *Tanúsítvány*ait;
- a kereszt hitelesített szolgáltatói *Tanúsítvány*okat, amelyek *Alany*a a *Hitelesítés-szolgáltató*, amennyiben a *Hitelesítés-szolgáltató* kérte vagy elfogadta a bizalmi kapcsolat létesítését;
- a végfelhasználói *Tanúsítvány*okat.

Szolgáltatói tanúsítványok

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

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

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

Végfelhasználói tanúsítványok

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

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

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

A *Hitelesítés-szolgáltató* biztosítsa, hogy szolgáltatói *Tanúsítvány*ait, a *Tanúsítványtár*at és a visszavonási információkat közzétevő rendszer rendelkezésre állása éves szinten legalább 99,9% -os legyen és egy kiesés hossza legfeljebb 3 óra legyen.

2.3. A közzététel időpontja vagy gyakorisága

2.3.1. Kikötések és feltételek közzétételi gyakorisága

A szolgáltatás szempontjából leglényegesebb kikötéseket és feltételeket tartalmazza az *Ügyfél* által a szerződéskötés során aláírandó szolgáltatási szerződés, vagy az abban meghivatkozott Általános Szerződési Feltételek [42] dokumentum.

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

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

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

`info@e-szigno.hu`

Érdemi változtatást igénylő észrevétel esetén a dokumentumot megváltoztatja.

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

2.3.2. Tanúsítványok nyilvánosságra hozatalának gyakorisága

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

- az általa működtetett gyökér hitelesítő egységek *Tanúsítvány*ait a szolgáltatás megkezdését megelőzően tegye közzé;
- az általa működtetett köztes hitelesítő egységek *Tanúsítvány*ait a kibocsátást követően 5 munkanapon belül hozza nyilvánosságra;

- a *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítvány*okat a kibocsátást követően haladéktalanul jelenítse meg a *Tanúsítványtár*ban.

2.3.3. A megváltozott visszavonási állapot közzétételének gyakorisága

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

A *Tanúsítvány*ok állapotára vonatkozó információk a *Tanúsítványtár*ban és a *Tanúsítvány visszavonási list*ákon is jelenjenek meg. A *Tanúsítvány visszavonási list*ák kibocsátási gyakoriságával kapcsolatos előírásokat a 4.10. fejezet tárgyalja.

2.4. Az adattárak elérésének szabályai

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

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

3. Azonosítás és hitelesítés

3.1. Elnevezések

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

A *Tanúsítvány* alapmezői között található Kibocsátó azonosító (Issuer), illetve *Alany* azonosító (Subject) mezők feleljenek meg az IETF RFC 5280 [33] illetve IETF RFC 6818 [34] 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

  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 *Tanúsítvány*t használni kívánja (*Automata tanúsítvány*).

  Kitöltése kötelező.

- Surname – OID: 2.5.4.4 – Természetes személy vezetékneve

  Ne kerüljön kitöltésre.

- Given Name – OID: 2.5.4.42 – Természetes személy keresztneve

  Ne kerüljön kitöltésre.

- 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 *Tanúsítvány*ban legalább egy kitöltött "Serial Number" mezőnek kötelezően szerepelnie kell, amely teljesíti az alábbi követelményeket, és ezáltal alkalmas arra, hogy az IETF RFC 4043 [32] ajánlás szerinti "Permanent Identifier" kiterjesztés használata esetén az *Alany* állandó azonosítójának részét képezze:

  – az azonosító értéke a *Tanúsítvány*ban megnevezett, a *Hitelesítés-szolgáltató* által azonosított *Alany*hoz tartozik, és a *Hitelesítés-szolgáltató* rendszerén belül egyedi;
  – a *Hitelesítés-szolgáltató* garantálja, hogy két általa kibocsátott *Tanúsítvány*ban kizárólag akkor szerepel megegyező azonosító érték, ha a két *Tanúsítvány* ugyanahhoz az *Alany*hoz tartozik.

  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

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

  A mező kitöltése kötelező.

  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

  Az "O" mezőben feltüntetett *Szervezet* azonosítója kerülhet ebbe a mezőbe.

  Csak olyan adat kerülhet bele, amelyet a *Hitelesítés-szolgáltató* ellenőrzött.

  A mező kitöltése kötelező.

  Amennyiben az *Ügyfél* kéri az *Alany* Open Banking követelmények, vagy a módosított pénzforgalmi irányelv (PSD2) [2] szerinti adatainak feltüntetését a *Tanúsítvány*ban, 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 [25] szerinti kódolással, vagy a hatóság által elismert egyéb azonosító az ETSI EN 319 412-1 [19] szerinti kódolással.

- Organizational Unit (OU) – OID: 2.5.4.11 – Szervezeti egység elnevezése

  Az "O" mezőben feltüntetett szervezethez kapcsolódó szervezeti egység elnevezése, vagy védjegy vagy egyéb információ kerülhet ebbe a mezőbe.

Csak olyan adat kerülhet bele, amelyet a *Hitelesítés-szolgáltató* ellenőrzött, és amire az adott *Szervezet*nek használati joga van.

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

Kitöltése opcionális.

- CountryName (C) – OID: 2.5.4.6 – Ország azonosítója

  Az "O" mezőben szereplő *Szervezet* székhelye szerinti ország ISO 3166-1 [27] szerinti kétbetűs kódja.

  Kitöltése kötelező.

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

- Street Address (SA) – OID: 2.5.4.9 – Cím adatok

  A szervezet székhelye szerinti cím. Kitöltése opcionális, amennyiben kitöltésre kerül, akkor csak ellenőrzött információ tüntethető fel.

- Locality Name (L) – OID: 2.5.4.7 – Településnév

  A *Szervezet* székhelye szerinti helység neve.

- State or Province Name – OID: 2.5.4.8 – Tagállam, tartomány elnevezése

  A *Szervezet* székhelye szerinti tagállam, megye vagy tartomány neve.

  Kitöltése opcionális.

- Postal Code – OID: 2.5.4.17 – Irányítószám

  A *Szervezet* székhelye szerinti postai irányítószám. Amennyiben kitöltésre kerül, akkor csak ellenőrzött információ tüntethető fel.

  Kitöltése opcionális.

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

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

  Nem lehet kitöltve.

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

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.

  – *Szervezeti tanúsítvány*ok esetében az *Igénylő* kérésére itt kerülhet feltüntetésre a *Szervezet* által jogosan használt védjegy, márkanév, 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.

  – 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" mezejében 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 *Szervezet* nevét a *Hitelesítés-szolgáltató* által a 3.2.2 fejezetben leírtak szerint ellenőrzött formában kell feltüntetni.

3.1.3. Álnevek használata

Bélyegző tanúsítvány nem lehet álneves.

3.1.4. A különböző elnevezési formák értelmezési szabályai

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

3.1.5. A nevek egyedisége

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

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

Eljárások a nevekre vonatkozó vitás kérdések megoldására

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

3.1.6. Márkanevek elismerése, azonosítása, szerepük

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

3.2. Kezdeti regisztráció, azonosság hitelesítése

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

A *Hitelesítés-szolgáltató* saját hatáskörében, külön indoklás nélkül megtagadhatja az igényelt *Tanúsítvány* kibocsátását.

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 *Tanúsítvány*ba kerülő nyilvános kulcshoz tartozó magánkulcsot.

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

Amennyiben az *Alany* magánkulcsát egy másik *Bizalmi szolgáltató* generálja és kezeli, akkor a *Hitelesítés-szolgáltató* köteles meggyőződni arról, hogy a magánkulcs az említett *Bizalmi szolgáltató* birtokában van, és az *Alany* kizárólagos ellenőrzése alatt áll.

3.2.2. Szervezet azonosságának hitelesítése

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

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

A *Szervezeti tanúsítvány*t 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 természetes személy egy *Szervezet* nevében jár el *Szervezeti tanúsítvány* kérelmezése céljából.

Minősített *Tanúsítvány* kibocsátásakor a természetes személy azonosságát az eIDAS Rendelet [1] 24. cikk (1) bekezdése értelmében személyes jelenlét útján vagy azzal egyenértékű biztosítékot nyújtó módszerrel kell ellenőrizni. A *Hitelesítés-szolgáltató* a 24. cikk (1) bekezdésben leírt azonosítási módokat alkalmazhatja az alábbiak szerint.

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

1. **Személyesen történő azonosítás során.**
   - A természetes személynek személyesen meg kell jelennie a személyes azonosítást végző személy előtt, aki az alábbiak valamelyike lehet:
     - *Regisztráló szervezet* tisztviselője,
     - közjegyző, mint 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. [5]) hatálya alá tartozó természetes személyek esetében a Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolvány az Eüt. 82.§ (3) [9] szerint;
     - a Nytv. [5] 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 [6] szerinti úti okmány alapján az Eüt. 82.§ (4) [9] 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) [9] 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 papíralapú 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 *Hitelesítés-szolgáltató* a kezdeti azonosítás során a saját *Regisztráló szervezet*e által végzett azonosítással egyenértékűnek fogadja el a közjegyző által végzett természetes személy azonosítást.

2. **Elektronikus aláírás tanúsítványára visszavezetett azonosítással.**

   Ebben az esetben:

   - Az *Igénylő* a *Tanúsítványkérelmet* elektronikus formában nyújtja be egy nem álneves minősített *Tanúsítvány*án alapuló minősített elektronikus aláírással ellátva.
   - Az elektronikus aláírással ellátott *Tanúsítványkérelem*nek tartalmaznia kell a természetes személy egyértelmű azonosításához szükséges azonosító adatokat.
   - A *Tanúsítványkérelem* hitelességét és sértetlenségét a *Hitelesítés-szolgáltató* ellenőrzi a teljes tanúsítási lánc vizsgálatával.
   - A *Hitelesítés-szolgáltató* csak olyan *Tanúsítvány*on alapuló elektronikus aláírást fogad be, amelyet egy az Európai Uniós fő bizalmi listán publikált nemzeti bizalmi listán szereplő bizalmi szolgáltatás keretében bocsátottak ki, és az aláírás létrehozás időpontjában érvényes volt.
   - A *Hitelesítés-szolgáltató* csak olyan *Tanúsítvány*on alapuló elektronikus aláírást fogad be, amelyet az eIDAS Rendelet [1] 24. cikk (1) bekezdése (a) vagy (b) pontja szerinti személy azonosítás alapján bocsátottak ki.

3. **Nemzeti szinten elismert egyéb azonosítási módszer alkalmazásával**

   A *Hitelesítés-szolgáltató* a természetes személy azonosságának megállapítását a személyes találkozással egyenértékűnek elismert videotechnológiát biztosító elektronikus hírközlő eszköz útján történő azonosítás (a továbbiakban: videotechnológiás azonosítás) felhasználásával is elvégezheti az 541/2020. (XII. 2.) Kormány rendelet [14] szerint.

   Ebben az esetben a *Hitelesítés-szolgáltató* a személyesen történő azonosítás során előírtak szerint jár el azzal a különbséggel, hogy a személyes találkozást olyan videotechnológiás azonosítási eljárással váltja ki, amely során:

   (a) élő telekommunikációs kapcsolat során videofelvétel útján képmást készít az *Ügyfél*ről, majd összeveti az *Ügyfél*ről készített fényképet és az azonosításhoz felhasznált személyazonosság igazolására alkalmas okmányban (a továbbiakban: okmány) szereplő képmást. Az azonosítás akkor megfelelő, ha a *Hitelesítés-szolgáltató* által egyértelműen megállapítható, hogy az okmányban szereplő személy azonos a videofelvételen szereplő *Ügyfél*lel.

   (b) A *Hitelesítés-szolgáltató* a "Tájékoztató az online videóazonosítás feltételeiről" [43] dokumentumban részletesen meghatározza a videótechnológiás azonosítás igénybevételének feltételeit, különösen a videókapcsolat minőségének minimális

követelményeit. A dokumentum a nyilvános szabályzatok között publikálásra kerül a *Hitelesítés-szolgáltató* web oldalán.

A sikeres videotechnológiás azonosítás érdekében célszerű biztosítani az alábbi feltételeket:

- jó állapotban lévő okmány
- megfelelően megvilágított környezet
- csendes, zavarmentes környezet
- idegen személyek jelenlétének kizárása
- IT eszköz kétirányú hang és videó képességgel
- kamera min. 2 megapixel video felbontással
- stabil internetkapcsolat min 1,5Mbps sebességgel.

(c) A *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzat* és a "Tájékoztató az online videóazonosítás feltételeiről" [43] dokumentum bemutatásával és a videofelvétel során biztosítja, hogy az *Ügyfél* a videotechnológiás azonosítás feltételeit részletesen megismerhesse, és azok betartásához kifejezetten hozzájárult, aszerint jár el.

(d) A *Hitelesítés-szolgáltató* a videotechnológiás azonosítás során a *Hitelesítés-szolgáltató* és az *Ügyfél* között létrejött teljes kommunikációt, az *Ügyfél* videotechnológiás azonosítással kapcsolatos részletes tájékoztatását és az *Ügyfél* ehhez történő kifejezett hozzájárulását visszakereshető módon, kép- és hangfelvételen – a kép- és hangfelvétel minőségének romlását kizáró módon – rögzíti, és azt a felvételtől számított legalább 10 évig megőrzi.

(e) A sikeres videotechnológiás azonosítás feltétele, hogy a videotechnológiás azonosítást lehetővé tévő elektronikus hírközlő eszköz képfelbontása és a kép megvilágítása alkalmas legyen az *Ügyfél* nemének, korának, arcjellemzőinek felismerésére, valamint az *Ügyfél*

- úgy nézzen bele a kamerába, hogy arcképe felismerhető és rögzíthető legyen, valamint azonosítható legyen az általa bemutatott okmányon látható arckép alapján,
- érthető módon közölje a videotechnológiás azonosításhoz használt okmány azonosítóját,
- úgy mutassa az okmányát, hogy az azon található biztonsági elemek és adatsorok felismerhetőek, rögzíthetőek és ellenőrizhetőek legyenek, valamint
- okmányán megtalálható adatok megfeleltethetők az *Ügyfél*ről a *Hitelesítés-szolgáltató*nál rendelkezésre álló adatokkal, és az *Ügyfél* a képmása alapján az okmányon felmutatott képmással azonosítható.

(f) A *Hitelesítés-szolgáltató* megbizonyosodik arról, hogy az okmány alkalmas a videotechnológiás azonosítás elvégzésére, így

- az okmány megfelel az okmányt kiállító hatóság előírásainak,
- az egyes biztonsági elemek – különösen a hologram, a kinegram vagy ezekkel megegyező más biztonsági elemek – felismerhetőek és sérülésmentesek, és
- az okmány azonosítója megegyezik az *Ügyfél* által közölt okmányazonosítóval, felismerhető és sérülésmentes.

(g) A videotechnológiás azonosítás során a *Hitelesítés-szolgáltató* megbizonyosodik arról, hogy

- az *Ügyfél* arcképe felismerhető és azonosítható az általa bemutatott okmányon látható arckép alapján, és
- az okmányon megtalálható adatok logikailag megfeleltethetők az *Ügyfél*ről a *Hitelesítés-szolgáltató*nál rendelkezésre álló adatokkal.

(h) Az élő telekommunikációs kapcsolatnak megfelel az is, ha a feltételek vizsgálatát a *Hitelesítés-szolgáltató* gépi úton vagy a telekommunikációs kapcsolat megszűnését követően végzi el, de meggyőződik arról, hogy az *Ügyfél* az azonosítás során élő kapcsolatban van.

A *Hitelesítés-szolgáltató* csak abban az esetben bocsátja ki a *Tanúsítvány*t, ha a videotechnológiás azonosítás maradéktalanul megfelel a fenti követelményeknek.

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

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

3.2.4. Nem ellenőrzött alany információk

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

3.2.5. Jogok, felhatalmazások ellenőrzése

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

Ellenőrizni kell a természetes személy képviseleti jogosultságát.

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

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

3.2.6. Együttműködési képességre vonatkozó követelmények

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

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

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

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

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

3.3. Azonosítás és hitelesítés kulcscsere kérelem esetén

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

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) *Tanúsítvány*okhoz 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 *Tanúsítvány*énál 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 *Tanúsítvány*t. *Tanúsítvány* megújítás csak a Szolgáltatási szerződés érvényessége alatt, és csak még érvényes *Tanúsítvány*okhoz kérhető.

3.4.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

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

A *Hitelesítés-szolgáltató* által kezdeményezett *Tanúsítvány* megújítás esetén a *Hitelesítés-szolgáltató* az ellenőrzés során felhasználhatja az eredeti *Tanúsítvány* kibocsátásakor elvégzett vizsgálatok eredményeit, amennyiben az új *Tanúsítvány* a megújítandó *Tanúsítvány*énál nem későbbi érvényesség vége idővel kerül kiadásra.

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 *Tanúsítvány*t bocsát ki változatlan nyilvános kulccsal, de megváltozott *Alany* azonosító adatokkal.

3.5.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

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

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

3.5.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen *Tanúsítvány* nem módosítható.

3.6. Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási kérelem esetén

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

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

A benyújtott kérelmek hitelességét és a benyújtó jogosultságát ellenőrizni kell.

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

3.7. Ellenőrzött kommunikációs csatorna

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

4. A tanúsítványok életciklusára vonatkozó követelmények

4.1. Tanúsítványkérelem

Új *Tanúsítvány* kiadásához *Tanúsítványkérelem* benyújtására van szükség. Az első *Tanúsítványkérelem* benyújtását megelőzően az *Igénylő Regisztrációs igény*t kell, hogy benyújtson a

*Hitelesítés-szolgáltató*nak, ez történhet a *Hitelesítés-szolgáltató* honlapján keresztül is. A *Regisztrációs igény*ben az *Igénylő* megadja a *Tanúsítvány*ba kerülő adatokat, meg kell jelölnie, hogy pontosan milyen *Tanúsítvány*t igényel, és felhatalmazást kell adnia a *Hitelesítés-szolgáltató* számára a személyes adatainak kezelésére.

A *Hitelesítés-szolgáltató* mindaddig nem tekintheti a *Regisztrációs igény*ben szereplő adatokat hitelesnek, amíg az *Igénylő* a *Tanúsítványkérelem*ben meg nem erősíti azokat. Amennyiben új Szolgáltatási szerződés megkötésére van szükség, a *Hitelesítés-szolgáltató* a *Regisztrációs igény*ben megadott adatok alapján előkészítheti az *Előfizető*vel kötendő Szolgáltatási szerződést.

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

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

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

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

- a *Tanúsítvány*ba kerülő adatok (pl.*Szervezet* neve, szervezeti egység elnevezése, város, ország, email cím);
- az *Alany* képviseletében eljáró személy személyazonosító adatai (teljes név, személyazonosító okmány száma);
- az *Alany* képviseletében eljáró személy elérhetőségei (telefonszám, email cím);
- az *Előfizető* adatai (számlázási adatok).

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

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

4.1.1. Ki nyújthat be tanúsítványkérelmet

Tanúsítványkérelmet természetes személyek nyújthatnak be 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* képviseletére jogosult személy 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 személyes azonosítás megtörténik a találkozás során);
- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájába eljuttatva (ekkor 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.
- Ügyféltér fiókján keresztül beküldve.

Az *Előfizető*nek és az *Alany* képviseletére jogosult személynek a *Tanúsítvány* igénylése során meg kell adniuk elérhetőségi adataikat.

4.1.2. A bejegyzés folyamata és a résztvevők felelőssége

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

A *Szervezet*et is azonosítani kell, illetve meg kell győződni arról, hogy a megjelent személy jogosult a *Szervezet* képviseletére illetve a *Szervezet*hez kapcsolódó *Tanúsítvány* igénylésére (lásd: 3.2.2. fejezet).

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

Az *Alany* képviseletére jogosult személy 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* képviseletére jogosult személy által aláírt *Tanúsítványkérelmet*, amelynek tartalmaznia kell a következőket:

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

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

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

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

Amennyiben az *Alany* képviseletére jogosult személyazonossága vagy a *Szervezet* azonossága 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 korrigálni, 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 összeférhetetlenség elkerülése érdekében biztosítania kell személyi és szervezeti függetlenségét az *Előfizető*kkel szemben. Nem minősül az összeférhetetlenség megsértésének, amikor a *Hitelesítés-szolgáltató* munkatársai számára bocsát ki *Tanúsítvány*t.

A *Hitelesítés-szolgáltató*nak a *Tanúsítvány* kibocsátása előtt ellenőriznie kell a *Tanúsítványkérelem*ben megadott, a *Tanúsítvány*ba 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 szabályzat*ban meg kell határoznia, hogy milyen határidőn belül vállalja a benyújtott *Tanúsítványkérelem* elbírálását.

4.3. A tanúsítvány kibocsátása

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

4.3.1. A Hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során

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

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 *Igénylő*t és az *Előfizető*t, valamint tegye lehetővé az *Igénylő* számára a *Tanúsítvány* átvételét.

4.4. A tanúsítvány elfogadása

4.4.1. A tanúsítvány elfogadás módja

Az *Alany* képviseletére jogosult személynek a *Tanúsítvány* átvétele előtt ellenőriznie kell a *Tanúsítvány*ban szereplő adatok helyességét.

Amennyiben az *Alany* számára a *Hitelesítés-szolgáltató* biztosítja a *Minősített elektronikus bélyegzőt létrehozó eszköz*t is, akkor az *Alany* magánkulcsát tartalmazó *Minősített elektronikus bélyegzőt létrehozó eszköz*, valamint az aktiváláshoz szükséges kód átvétele után az *Igénylő* aláírja a papíralapú átvételi nyilatkozatot, amelyben – többek között – azt igazolja, hogy a *Minősített elektronikus bélyegzőt létrehozó eszköz*t és a hozzá tartozó aktiváló kódokat átvette, valamint azt, hogy ismeri a *Minősített elektronikus bélyegzőt létrehozó eszköz* használatának műszaki és jogszabályi feltételeit.

Az *Alany* a *Tanúsítvány* használatba vételével fogadja el a *Tanúsítvány*t, nincs szükség külön nyilatkozat tételére.

4.4.2. A tanúsítvány közzététele

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

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

4.4.3. További szereplők értesítése a tanúsítvány kibocsátásról

A *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell az *Alany* képviseletére jogosult személyt is.

4.5. A kulcspár és a tanúsítvány használata

4.5.1. A magánkulcs és a tanúsítvány használata

Az *Alany* a *Tanúsítvány*ához tartozó magánkulcsát kizárólag elektronikus bélyegző létrehozására használhatja, más felhasználás nem engedélyezett.

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

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* segítségével igazolt elektronikus bélyegző elfogadása során a *Hitelesítés-szolgáltató* által garantált biztonsági szint megtartásához ajánlott, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, és feleljen meg a *Szolgáltatási szabályzat*ban leírt követelményeknek, különös tekintettel az alábbiakra:

- ellenőrizze a *Tanúsítvány* érvényességét és visszavonási állapotát;
- a bélyegző *Tanúsítvány*okat, illetve az azokhoz tartozó nyilvános kulcsokat kizárólag elektronikus bélyegző ellenőrzésére használja;
- vegyen figyelembe minden korlátozást, amely a *Tanúsítvány*ban vagy a *Tanúsítvány*ban meghivatkozott szabályzatokban szerepel.

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

4.6. Tanúsítvány megújítás

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

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 *Tanúsítvány*hoz tartozó magánkulcs nem kompromittálódott;
- a *Tanúsítvány*ban szereplő *Alany* azonosító adatok érvényben vannak.

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

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

4.6.2. Ki kérelmezheti a tanúsítvány megújítást

A *Tanúsítvány* megújítást az *Előfizető* nevében 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 *Tanúsítvány*ban szereplő *Alany* azonosító adatok érvényben vannak.

A *Hitelesítés-szolgáltató* jogosult a *Tanúsítvány* megújítását kezdeményezni, ha a szolgáltatás nyújtásának belső vagy külső körülményeiben beállt változások ezt szükségessé teszik, például de nem kizárólagosan az alábbi esetekben:

- a külső követelmények megváltozása miatt a *Tanúsítvány* a jelenlegi formájában már nem használható;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány* nem felel meg a hivatkozott *Hitelesítési rend*nek vagy *Szolgáltatási szabályzat*nak;
- ha a *Tanúsítvány* kibocsátásához használt szolgáltatói aláíró kulcsát soron kívül le kell cserélnie.

4.6.3. A tanúsítvány megújítási kérelmek feldolgozása

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

- a benyújtott *Tanúsítvány* megújítási kérelem hiteles;
- a *Tanúsítvány* megújítási kérelem benyújtója rendelkezik a szükséges jogosultságokkal, felhatalmazásokkal;
- a *Tanúsítvány* megújítási kérelem benyújtója nyilatkozott a *Tanúsítvány*ba kerülő *Alany* adatok változatlanságáról és érvényességéről;
- a *Tanúsítvány* megújítási kérelem a *Tanúsítvány* érvényességi ideje alatt került benyújtásra;
- a megújítandó *Tanúsítvány* nincs 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 *Igénylő*t és az *Előfizető*t az új *Tanúsítvány* kibocsátásáról.

4.6.5. A megújított tanúsítvány elfogadása

A *Hitelesítés-szolgáltató* a megújított *Tanúsítvány*t 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 *Tanúsítvány*t.

4.6.7. További szereplők értesítése a tanúsítvány kibocsátásáról

A *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell az *Alany* képviseletére jogosult személyt is.

4.7. Kulcscsere

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

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

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

4.7.2. 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-szolgáltató*nak ellenőriznie kell, hogy:

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

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

4.7.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A *Hitelesítés-szolgáltató* értesítse az *Igénylő*t és az *Előfizető*t 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 *Tanúsítvány*t.

4.7.6. A kulcscserével megújított tanúsítvány közzététele

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

4.7.7. További szereplők értesítése a tanúsítvány kibocsátásáról

A *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell a *Képviselt szervezet Szervezeti ügyintéző*jét is.

4.8. Tanúsítvány módosítás

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

4.8.1. A tanúsítvány módosítás körülményei

A tanúsítvány módosítás szükségessé válik az alábbi esetekben:

- az *Alany Tanúsítvány*ban szereplő adatai megváltoznak;
- a *Hitelesítés-szolgáltató Tanúsítvány* kibocsátó rendszerében megváltozik az adott *Tanúsítvány*t kibocsátó CA valamely a "Subject DN"-ben szereplő azonosító adata vagy a nyilvános kulcsa és így szolgáltatói *Tanúsítvány*a;
- a *Tanúsítvány*ban 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 *Tanúsítvány*hoz tartozó magánkulcs nem kompromittálódott.

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

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

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

4.8.2. 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 Tanúsítvány*ban 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 *Igénylő*t és az *Előfizető*t az új *Tanúsítvány* kibocsátásáról.

4.8.5. A módosított tanúsítvány elfogadása

A *Hitelesítés-szolgáltató* a módosított *Tanúsítvány*t 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 *Tanúsítvány*t.

4.8.7. További szereplők értesítése a tanúsítvány kibocsátásáról

A *Tanúsítvány* kibocsátásáról haladéktalanul értesíteni kell az *Alany* képviseletére jogosult személyt is.

4.9. Tanúsítvány visszavonás és felfüggesztés

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

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

4.9.1. A tanúsítvány visszavonás körülményei

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 *Tanúsítvány*ban lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódott;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban szereplő nyilvános kulcs már nem felel meg a 6.1.5. és 6.1.6. fejezetekben meghatározott követelményeknek;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t 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 *Tanúsítvány*ban szereplő adatokban lényeges változás történt;
- a *Tanúsítvány* módosítása az *Alany*ra vonatkozó adatok változása miatt;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t nem a vonatkozó *Hitelesítési rend* illetve *Szolgáltatási szabályzat* szerint bocsátották ki;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban foglalt bármely adat pontatlan;
- a *Hitelesítés-szolgáltató* már nem jogosult *Tanúsítvány*okat kibocsátani és a meglévő *Tanúsítvány*okra vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodik;

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

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

Szolgáltatói Tanúsítvány visszavonásának okai

A *Hitelesítés-szolgáltató* köteles intézkedni az általa üzemeltetett köztes hitelesítő egység *Tanúsítvány*ának 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-szolgáltató*t 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 *Tanúsítvány*ban szereplő nyilvános kulcs már nem felel meg a 6.1.5 és 6.1.6 fejezetekben meghatározott követelményeknek;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t jogellenesen használták;
- amennyiben a *Tanúsítvány*t nem a vonatkozó *Hitelesítési rend* illetve *Szolgáltatási szabályzat* szerint bocsátották ki vagy a köztes hitelesítő egység működése nem felel meg a rá vonatkozó *Hitelesítési rend*nek vagy *Szolgáltatási szabályzat*nak;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban 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 *Tanúsítvány*okat kibocsátani és a meglevő *Tanúsítvány*okra vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;
- a visszavonást előírja a kibocsátó CA *Hitelesítési rend*je vagy *Szolgáltatási szabályzat*a;
- a *Tanúsítvány* módosítása a hitelesítési egységre, vagy a *Hitelesítés-szolgáltató*ra 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 fentieken kívül egyéb feltételeket is, amelyek esetén a *Hitelesítés-szolgáltató* a *Tanúsítvány*t visszavonja.

Más Szolgáltató által üzemeltetett köztes CA Tanúsítvány visszavonásának okai

A *Hitelesítés-szolgáltató* köteles intézkedni a más hitelesítés-szolgáltató által üzemeltetett köztes hitelesítő egység *Tanúsítvány*ának 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-szolgáltató*t 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 *Tanúsítvány*ban 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 *Tanúsítvány*t jogellenesen használták;
- a kibocsátó *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t nem a vonatkozó *Hitelesítési rend* illetve *Szolgáltatási szabályzat* szerint bocsátották ki vagy a köztes hitelesítő egységet üzemeltető hitelesítés-szolgáltató működése nem felel meg a rá vonatkozó *Hitelesítési rend*nek vagy *Szolgáltatási szabályzat*nak;
- a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*ban 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 *Tanúsítvány*okat kibocsátani és a meglevő *Tanúsítvány*okra vonatkozó CRL és OCSP szolgáltatások fenntartásáról nem gondoskodott;
- a visszavonást előírja a kibocsátó CA *Hitelesítési rend*je vagy *Szolgáltatási szabályzat*a;
- 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 *Tanúsítvány*át kibocsátó *Hitelesítés-szolgáltató* a tevékenységét befejezte;
- a visszavonást jogszabály kötelezővé teszi.

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

4.9.2. Ki kérelmezheti a visszavonást

A *Tanúsítvány* visszavonását írásban kezdeményezhetik az *Ügyfel*ek, részletezve:

- az *Előfizető*;
- az *Előfizető* által bejelentett *Szervezeti ügyintéző*;
- az *Alany* pénzforgalmi szolgáltatási engedélyét kibocsátó hatóság, amennyiben a *Tanúsítvány* az *Alany* Open Banking követelmények, vagy a módosított pénzforgalmi irányelv (PSD2) [2] szerinti adatait tartalmazza;

illetve

- a Távoli kulcs menedzsment szolgáltató által kezelt magánkulcs esetében a Távoli kulcs menedzsment szolgáltató;
- a *Hitelesítés-szolgáltató*.

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

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

4.9.3. A visszavonási kérelemre vonatkozó eljárás

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

- elektronikus formában, a kérelmező nem álneves, a visszavonni kívánt *Tanúsítvány*nál nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) *Tanúsítvány*án alapuló elektronikus aláírásával ellátva;
- elektronikus formában, az *Előfizető* – a visszavonni kívánt *Tanúsítvány*nál nem alacsonyabb biztonsági besorolású (lásd 1.2.3. fejezet) – *Tanúsítvány*ának felhasználásával létrehozott bélyegzőjével ellátva;
- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában ügyfélszolgálati időben, vagy postai úton.

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

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

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

Sikeres visszavonás esetén a *Hitelesítés-szolgáltató* értesítse az *Alany*t és az *Előfizető*t 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 *Tanúsítvány*t.

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 *Tanúsítvány*ok érvényességének ellenőrzésére, a szabályzatok és a kulcshasználat megkötéseire, az egyes *Tanúsítvány*okban meghivatkozott CRL vagy OCSP alapú visszavonási státusz információk ellenőrzésére.

4.9.7. A visszavonási lista kibocsátás gyakorisága

A *Hitelesítés-szolgáltató* legalább naponta egyszer bocsásson ki új *Tanúsítvány visszavonási list*át a végfelhasználói *Tanúsítvány*okat kibocsátó hitelesítési egységeire.

A *Tanúsítvány visszavonási list*ák érvényességi ideje legfeljebb 26 óra lehet.

A *Hitelesítés-szolgáltató* legalább évente egyszer, de visszavonás esetén 24 órán belül bocsásson ki új *Tanúsítvány visszavonási list*át a köztes hitelesítési egységeire. Az ilyen kibocsátott *Tanúsítvány visszavonási list*ák 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* határozza meg *Szolgáltatási szabályzat*ában, hogy milyen követelményeknek kell megfelelniük a *Hitelesítés-szolgáltató* által kiadott *Tanúsítvány*okkal kapcsolatban benyújtottt kulcs kompromittálódási bejelentéseknek.

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

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

4.9.13. A felfüggesztés körülményei

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

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 szabályzat*ban egyértelműen ismertetni kell. Az időtartam elteltét követően a *Hitelesítés-szolgáltató* külön értesítés nélkül jogosult a felfüggesztett *Tanúsítvány* visszavonására.

4.10. Tanúsítvány állapot szolgáltatások

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

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

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

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

A visszavonási vagy felfüggesztési információ nem távolítható el a *Tanúsítvány visszavonási list*áról a visszavont vagy felfüggesztett *Tanúsítvány* lejárati időpontja előtt.

A visszavont *Tanúsítvány*ok a *Tanúsítvány* érvényességének lejárta után se törlődjenek a *Tanúsítvány visszavonási list*ából.

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

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 list*ában kerüljön publikálásra.

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

4.10.1. Működési jellemzők

Nincs megkötés.

4.10.2. A szolgáltatás rendelkezésre állása

A *Hitelesítés-szolgáltató*nak biztosítania kell a *Tanúsítványtár*, valamint a *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány*ok használatára vonatkozó kikötések és feltételek folyamatos elérhetőségét éves szinten legalább 99,9% -os rendelkezésre állás mellett, ahol az eseti szolgáltatáskiesések maximális időtartama legfeljebb 3 óra.

A *Hitelesítés-szolgáltató*nak biztosítania kell a *Visszavonási állapot nyilvántartás*ok és a visszavonás kezelési szolgáltatás éves szinten legalább 99,9% -os rendelkezésre állását, ahol az eseti szolgáltatáskiesések időtartama legfeljebb 3 óra.

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

4.10.3. Opcionális lehetőségek

Nincs megkötés.

4.11. Az előfizetés vége

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

4.12. Magánkulcs letétbe helyezése és visszaállítása

A *Hitelesítés-szolgáltató* a bélyegző *Tanúsítvány*hoz tartozó magánkulcshoz nem nyújthat kulcsletét szolgáltatást.

4.12.1. Kulcsletét és visszaállítás rendje és szabályai

A bélyegző *Tanúsítvány*hoz tartozó magánkulcs nem helyezhető letétbe.

4.12.2. Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

A bélyegző *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 zárak, 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 két – bizalmi szerepkört betöltő, erre feljogosított – munkatárs egyidejű azonosítása után lehet belépni, legalább az egyik munkatársnak rendszer-adminisztrátornak kell lennie;
- az önálló jogosultsággal nem rendelkező személyek csak indokolt esetben, a szükséges ideig tartózkodhatnak a gépteremben megfelelő jogosultságú kísérő személyzettel;
- a belépési logokat folyamatosan archiválják és legalább hetente megvizsgálják.

Az eszközök aktivizáló adatai (jelszavak, PIN kódok) a géptermen belül sem tárolhatók nyílt formában.
Jogosulatlan személyek jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva kell tartani;
- a bejelentkezett terminálokat nem szabad felügyelet nélkül hagyni;
- nem szabad olyan munkafolyamatot végezni, amely során bizalmas adat felfedésre kerülhet.

A gépterem elhagyásakor az adminisztrátornak ellenőriznie kell, hogy:

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

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

5.1.3. Áramellátás és légkondicionálás

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

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

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

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, amelyek automatikusan riasztják a tűzoltóságot. Minden helyiségben jól látható helyen el kell helyezni a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készüléket.

A gépteremben automatikus tűzoltó rendszert kell alkalmazni.

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

A mentett állományokból legalább évente szúrópróbaszerű 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 24/2016. BM rendelet [10] előírásainak megfelelő bizalmi szerepköröket (a rendelet szövegezésében bizalmi munkaköröket) 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 *Tanúsítvány*ok 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-szolgáltató*val munkaviszonyban álló személyek láthatnak el, megbízási szerződés keretében a bizalmi szerepkörök nem láthatók el.

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

5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

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

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

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

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

5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés

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

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

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

5.2.4. Egymást kizáró szerepkörök

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

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

5.3. Személyzetre vonatkozó előírások

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

A *Hitelesítés-szolgáltató* már a felvételi szakaszban foglalkozzon a személyi biztonsággal, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését. Valamennyi bizalmi szerepkör esetén a 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 (matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség);
- legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal.

5.3.2. Előélet vizsgálatára vonatkozó eljárások

A *Hitelesítés-szolgáltató* 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, vétlen 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 naplóznia kell minden olyan biztonsággal kapcsolatos eseményt, amely információt szolgáltathat az informatikai rendszerben vagy annak fizikai környezetében történt eseményekről, változásokról. Minden naplóbejegyzésnél el kell tárolni:

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

Az elmentett naplóbejegyzések nem kerülhetnek módosításra vagy törlésre.

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

Naplózni kell minimálisan az alábbi eseményeket:

- BELSŐ ÓRA

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

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

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

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

- TANÚSÍTVÁNY KEZELÉS
  - szolgáltatói *Tanúsítvány*ok 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 elfogadása és elutasítása;
  - *Tanúsítvány* kibocsátása, állapotváltozása;

- ADATMOZGÁSOK

  - bármilyen, a biztonság szempontjából kritikus adat manuális bevitele a rendszerbe;
  - a rendszer által fogadott, biztonsági szempontból fontos adatok, üzenetek;

- CA KONFIGURÁCIÓ
  - a CA tetszőleges komponensének átparaméterezése, a beállításon történt bármilyen változtatás;
  - felhasználók felvétele, törlése;
  - felhasználói szerepkörök, jogosultságok megváltoztatása;
  - a tanúsítvány profil megváltoztatása;
  - CRL profil megváltoztatása;
  - új CRL lista előállítása;
  - OCSP válasz generálása;
  - *Időbélyegző* generálása;
  - az előírt időpontossági küszöb túllépése;

- *HSM eszköz*
  - *HSM eszköz* installálása;
  - *HSM eszköz* eltávolítása;
  - *HSM eszköz* selejtezése, megsemmisítése;
  - *HSM eszköz* szállítása;
  - *HSM eszköz* tartalmának törlése (nullázás);
  - *HSM eszköz* feltöltése kulcsokkal, tanúsítványokkal;

- KONFIGURÁCIÓ VÁLTOZÁSA
  - hardver;
  - szoftver;
  - operációs rendszer;
  - javító csomag;
  - szoftver telepítése, frissítése vagy eltávolítása a *Hitelesítés-szolgáltató* rendszerében;

- 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 kel értékelni.

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

A kiértékelés során elemezni kell a rendszerek által generált hibaüzeneteket.

Statisztikai módszerekkel elemezni kell a forgalmi adatokban bekövetkezett jelentős változásokat.

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

5.4.3. A naplófájl megőrzési időtartama

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

5.4.4. A naplófájl védelme

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

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

5.4.5. A naplófájl mentési eljárásai

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

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

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

5.4.6. A naplózás adatgyűjtési rendszere

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

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

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

5.4.7. Az eseményeket kiváltó alanyok értesítése

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

5.4.8. Sebezhetőség felmérése

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

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

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

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

5.5. Adatok archiválása

5.5.1. Az archivált adatok típusai

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

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

- a *Hitelesítés-szolgáltató* akkreditációjával kapcsolatos valamennyi irat;
- a *Hitelesítési rend*(ek) 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 *Tanúsítványkérelem*mel együtt benyújtott valamennyi irat;
  - a személyes azonosítás során bemutatott dokumentum(ok) azonosító adatai;
  - Szolgáltatási szerződés(ek);
  - egyéb előfizetői jognyilatkozatok;
  - a kérelmet elbíráló regisztrációs ügyintéző azonosítója;
  - a kérelem elbírálásának körülményei és eredménye;
- a *Tanúsítvány*okkal kapcsolatos valamennyi információ a teljes életciklusra vonatkozóan;
- az *Elektronikus bélyegzőt létrehozó eszköz*ök megszemélyesítésével kapcsolatos információk;
- valamennyi elektronikus és papíralapú naplóbejegyzés.

5.5.2. Az archívum megőrzési időtartama

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

- a *Hitelesítési rend*et a hatályon kívül helyezéstől számított legalább 10 évig;
- a *Szolgáltatási szabályzat*ot a hatályon kívül helyezéstől számított legalább 10 évig;
- Általános Szerződési Feltételeket a hatályon kívül helyezéstől számított legalább 10 évig;
- videotechnológiás személyazonosítás esetén az azonosítás során rögzített teljes kommunikációt legalább a rögzítés időpontjától számított 10 évig;
- a *Tanúsítvány*okkal kapcsolatos valamennyi elektronikus és/vagy papíralapú információt legalább
  - a *Tanúsítvány* érvényességének lejáratától számított 10 évig;
  - a Tanúsítvánnyal előállított elektronikus bélyegzővel kapcsolatos jogvita jogerős lezárásáig;
- minden egyéb archiválandó dokumentomot a keletkezésétől számított legalább 10 évig.

5.5.3. Az archívum védelme

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

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

Az archivált adatok megőrzése során gondoskodni kell az archivált adatok

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

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

5.5.4. Az archívum mentési folyamatai

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

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

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

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

A napi naplóállományokat minősített *Időbélyegző*vel kell ellátni.

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

5.5.6. Az archívum gyűjtési rendszere

A *Hitelesítés-szolgáltató* védett informatikai rendszerén belül kell keletkeznie a naplóbejegyzéseknek, onnan csak az elektronikusan aláírt, minősített *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 *Ügyfel*ek jogosultak a róluk tárolt adatok megtekintésére;
- jogi eljárásokban bizonyíték nyújtása céljából biztosítani kell a szükséges adatokat.

5.6. Szolgáltatói kulcs cseréje

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

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

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

5.7. Kompromittálódást és katasztrófát követő helyreállítás

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

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

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

5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások

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

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

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

5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

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

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

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

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

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

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

5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások

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

- vissza kell vonni a *Hitelesítés-szolgáltató* összes érintett *Tanúsítvány*át;
- új szolgáltatói magánkulcsokat kell generálni a szolgáltatások helyreállításához;

- nyilvánosságra kell hozni a visszavont szolgáltatói *Tanúsítvány*ok 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 szolgáltatási helyszínt az elsődleges telephelytől olyan távol kell elhelyezni, hogy egy valószínűsíthető katasztrófa ne érhesse mindkét helyszínt egyszerre.

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

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

5.8. A hitelesítés-szolgáltató vagy a regisztráló szervezet leállítása

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

A leállítás során kiemelten kezelendő feladatok:

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

6. Műszaki biztonsági óvintézkedések

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

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 [24];
- az Eüt. [9] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

Szolgáltatói kulcspárok előállítása

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

- A szolgáltatói kulcspár előállítását egy kulcsgenerálási forgatókönyv alapján végzi.
- Hitelesítési egység (CA) részére történő kulcspár előállítása esetén egy megfelelő akkreditációval rendelkező auditor független tanúként résztvesz a kulcsgenerálási eseményen, vagy a *Hitelesítés-szolgáltató* videófelvételt készít a teljes CA kulcsgenerálási eseményről.
- Amennyiben a CA kulcspár gyökér hitelesítő egység, vagy idegen szervezet által üzemeltetett köztes hitelesítő egység részére kerül generálásra, a kulcsgenerálási eseményen független tanúként résztvesz egy megfelelő akkreditációval rendelkező auditor.

  A külső auditor egy tanúsítási jelentés kiállításával igazolja, hogy a kulcspár előállítása a *Hitelesítés-szolgáltató* által szabályozott folyamatnak megfelelően történt a kulcspár integritásának és bizalmasságának biztosítása érdekében.
- A szolgáltatói kulcspár előállítását fizikailag védett környezetben (lásd 5.1 pont), legalább két, bizalmi szerepkört (lásd 5.2.1 pont) betöltő, erre feljogosított személy együttes részvételével, a tudásmegosztás elvének alkalmazásával, illetéktelen személyek jelenlétét kizárva végzi.
- A szolgáltatói kulcspár előállítását olyan eszközön belül hajtja végre, amely:
  - megfelel az ISO/IEC 19790 [29] követelményeinek,
  - vagy megfelel a FIPS 140-2 [38] 3-as, illetve annál magasabb szintű követelményeinek,
  - vagy megfelel a CEN 419 221-5 [26] követelményeinek,
  - vagy olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [28] 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 előirányzaton kell alapulnia.

- A kulcsgenerálás folyamatáról részletes naplóbejegyzések készülnek.
- A *Hitelesítés-szolgáltató* a szükséges intézkedések meghozásával és betartásával biztosítja, hogy a magánkulcs az előírt folyamatoknak megfelelően volt előállítva és védve a kulcsgenerálás során.
- Szolgáltatói gyökér és köztes *Tanúsítvány* részére előállított kulcspár esetén a *Hitelesítés-szolgáltató*nak egy kulcselőállítási jegyzőkönyvet kell felvennie, amely igazolja, hogy az eljárás az előre rögzített folyamat szerint zajlott, amely biztosítja a generált kulcsok integritását és bizalmasságát. A jegyzőkönyvet alá kell írnia:
  - szolgáltatói gyökér hitelesítő egység magánkulcsának előállítása esetén a *Hitelesítés-szolgáltató* kulcsmenedzsmentért felelős bizalmi tisztviselőjének, és tanúként egy a *Hitelesítés-szolgáltató* üzemeltetésétől független megbízható személynek (pl. auditor), akik igazolják, hogy a jegyzőkönyvben rögzítettek megfelelnek a végrehajtott folyamatnak;
  - köztes szolgáltatói hitelesítő egység magánkulcsának előállítása esetén a *Hitelesítés-szolgáltató* kulcsmenedzsmentért felelős bizalmi tisztviselőjének, aki igazolja, hogy a jegyzőkönyvben rögzítettek megfelelnek a végrehajtott folyamatnak.

Szolgáltatói infrastruktúrális kulcspárok előállítása

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

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

Végfelhasználói kulcspárok előállítása és ellenőrzése

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

- A kulcsok előállítását fizikailag védett környezetben végzi, kizárólag bizalmi szerepkört betöltő személyek részvételével.
- A *Minősített elektronikus bélyegzőt létrehozó eszköz* illetve *Hardver kriptográfiai eszköz* használatát előíró *Hitelesítési rend*ek esetén a *Hitelesítés-szolgáltató* a magánkulcsot csak a szolgáltatást igénybe vevő *Igénylő Minősített elektronikus bélyegzőt létrehozó eszköz*én vagy a *Hardver kriptográfiai eszköz*én 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.

A *Tanúsítványkérelem* feldolgozása során a *Hitelesítés-szolgáltató* ellenőrzi a kulcspárokat és elutasítja a Tanúsítványkérelmet, ha az alábbi feltételek közül egy vagy több teljesül:

- a kulcspár nem felel meg a 6.1.5. fejezetben és/vagy a 6.1.6. fejezetben előírt követelményeknek;
- egyértelmű bizonyíték van arra, hogy a magánkulcs előállításához használt konkrét módszer hibás volt;
- a *Hitelesítés-szolgáltató* ismer egy bemutatott vagy bizonyított eljárást, amely alapján kompromittálható az *Igénylő* magánkulcsa;
- a *Hitelesítés-szolgáltató* már korábban tudomást szerzett róla, hogy az *Igénylő* magánkulcsa kompromittálódott, például a 4.9.1. fejezetben foglaltak szerint;
- a *Hitelesítés-szolgáltató*nak tudomása van egy bemutatott vagy bizonyított módszerről, amellyel könnyen kiszámítható a *Igénylő* magánkulcsa a nyilvános kulcs (például egy Debian gyenge kulcs, lásd: https://wiki.debian.org/SSLkeys) alapján .

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 *Alany*ok részére generált magánkulcsokat és aktivizáló adatokat a kulcsok átadásáig biztonságos módon tárolja, amely megakadályozza a kulcsok felfedését, lemásolását, módosítását, sérülését, illetéktelenek általi használatát.
- A *Hitelesítés-szolgáltató* biztosítja, hogy a magánkulcsokat és aktivizáló adataikat csak az arra jogosult *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*nak olyan módszerrel kell elérhetővé tennie legfelsőbb szintű szolgáltatói tanúsítványainak nyilvános kulcsait az *Érintett felek* részére, amely lehetetlenné teszi a kulcsok megváltoztatására irányuló támadásokat. Ennek keretében a *Hitelesítés-szolgáltató* legalább a honlapján tegye közzé a szolgáltatói *Tanúsítvány*ait.

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

- A gyökér hitelesítő egységek megnevezését, illetve *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 list*ákon, saját honlapján, valamint az online tanúsítvány-állapot válasz szolgáltatás keretében.
- Az online tanúsítvány-állapot válaszokat aláíró válaszadók számára a *Hitelesítés-szolgáltató* – a legjobb nemzetközi gyakorlatnak megfelelően – rendkívül rövid érvényességi idejű *Tanúsítvány*t bocsásson ki, ezzel kiküszöbölve azt, hogy a *Tanúsítvány* visszavonási állapotát ellenőrizni kelljen. E *Tanúsítvány* visszavonási állapotát a *Hitelesítés-szolgáltató* kizárólag olyan módon tegye közzé, hogy kulcs kompromittálódás vagy bármilyen egyéb probléma esetén az OCSP válaszokat aláíró régi magánkulcshoz ne kerüljön kibocsátásra újabb *Tanúsítvány*. A *Hitelesítés-szolgáltató* az OCSP válaszadói *Tanúsítvány*okat ezt követően új, biztonságos magánkulcshoz bocsássa ki.

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

6.1.5. Kulcsméretek

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

- ETSI TS 119 312 [24];
- az Eüt. [9] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

6.1.6. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A kulcsparaméterek előállítására vonatkozó követelményeket a 6.1.1. fejezet tartalmazza.

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

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

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

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

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

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

A *Hitelesítés-szolgáltató* a végfelhasználói *Tanúsítvány*okban szerepeltesse a "kulcshasználat" (Key Usage) kiterjesztéseket, amelyek meghatározzák a *Tanúsítvány* felhasználási területét és az X.509v3 [37] kompatibilis alkalmazásokban műszakilag is korlátozzák a kulcsok felhasználhatóságát. A mező tartalmára vonatkozó megkötések a 7.1.2 fejezetben szerepelnek.

A bélyegző magánkulcsot az *elektronikus bélyegző létrehozója* kizárólag elektronikus bélyegző létrehozására használhatja fel, a kulcs minden más alkalmazása kifejezetten tiltott.

Az *Időbélyegző egység*ek magánkulcsai csak az *Időbélyegző*k hitelesítésére használhatók fel.

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 eszköz*ök kezelése során a használatból kivont *HSM eszköz*ökben tárolt aláíró magánkulcsokat olyan módon kell törölni, hogy ne legyen lehetséges a kulcsok visszaállítása.

6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

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

- megfelelnek az ISO/IEC 19790 [29] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [38] 3-as, illetve annál magasabb szintű követelményeknek,
- vagy megfelelnek a CEN 14167-2 [40] munkacsoport egyezmény követelményeinek,
- vagy megfelelnek a CEN 419 221-5 [26] követelményeinek,
- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [28] 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 előirányzaton kell alapulnia.

A szolgáltatói magánkulcsok a *HSM eszköz*ön kívül csak kódolt formában tárolhatók. A kódoláshoz csak az Eüt. [9] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozatban foglalt algoritmusok és kulcsparaméterek használhatók, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

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

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

6.2.2. Magánkulcs többszereplős (n-ből m) használata

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

6.2.3. Magánkulcs letétbe helyezése

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

6.2.4. Magánkulcs mentése

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

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

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

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

6.2.5. Magánkulcs archiválása

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

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

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

A magánkulcsok nem létezhetnek nyílt formában a *HSM eszköz*ön kívül.

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

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

6.2.7. Magánkulcs tárolása hardver kriptográfiai eszközben

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

A *HSM eszköz*ön 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.

Az *Alany* részére előállított *Minősített elektronikus bélyegzőt létrehozó eszköz*öket és *Hardver kriptográfiai eszköz*öket 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 az 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 rend*ek esetén a magánkulcsokat az alkalmazott hardver eszköz használati útmutatójában és az eszköz tanúsítvány tanúsítási mellékletében megfogalmazott követelményeknek megfelelően kell használni.

A *Hardver kriptográfiai eszköz*ön 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 *Minősített elektronikus bélyegzőt létrehozó eszköz* csak az *Igénylő* újbóli azonosítása után használható elektronikus bélyegző létrehozására.

A *Minősített elektronikus bélyegzőt létrehozó eszköz* vagy *Hardver kriptográfiai eszköz* használatát nem megkövetelő *Hitelesítési rend*ek 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

Az intelligens kártyán kiadott, használatból kivont magánkulcsok megsemmisítése az intelligens kártya fizikai megsemmisítésével lehetséges, ami az *Igénylő* felelőssége.

A *Hitelesítés-szolgáltató* köteles az *Ügyfél* által részére személyesen átadott intelligens kártyát az *Ügyfél* kérésére jelenlétében, díjmentesen megsemmisíteni.

A *Minősített elektronikus bélyegzőt létrehozó eszköz* használatát megkövetelő *Hitelesítési rend*ek esetén a feleslegessé vált magánkulcsokat az alkalmazott hardver eszköz használati útmutatójában és az eszköz tanúsítvány tanúsítási mellékletében megfogalmazott követelményeknek megfelelően kell megsemmisíteni. A magánkulcsok ennek megfelelő megsemmisítése az *Igénylő* felelőssége.

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

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

A végfelhasználók használatból kivont bélyegző magánkulcsait javasolt megsemmisíteni.

6.2.11. A hardver kriptográfiai eszközök értékelése

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

- ISO/IEC 19790 [29] szerinti tanúsítvánnyal,
- vagy FIPS 140-2 Level 3 [38] szerinti tanúsítvánnyal,
- vagy a CEN 14167-2 [40] munkacsoport egyezmény követelményeinek való megfelelést igazoló legalább EAL-4 szintű Common Criteria alapú tanúsítvánnyal,
- vagy a CEN 419 221-5 [26] 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 *Tanúsítvány*t.

6.3.2. A tanúsítványok és kulcspárok használatának periódusa

A gyökér hitelesítő egységek tanúsítványai és kulcsai

A *Hitelesítés-szolgáltató* gyökér hitelesítő egységeinek *Tanúsítvány*ai 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 *Tanúsítvány*t kibocsátó gyökér vagy köztes szolgáltatói *Tanúsítvány* érvényességi idejét.

A végfelhasználói tanúsítványok

A *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*ok érvényességi ideje:

- legfeljebb a kibocsátástól számított 3 év;
- nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozata szerint biztonságosan felhasználhatók;
- nem haladhatja meg a *Tanúsítvány*t kibocsátó szolgáltatói *Tanúsítvány* érvényességi idejét.

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

Az Időbélyegző egységek tanúsítványai

A *Hitelesítés-szolgáltató* Időbélyegzés szolgáltatók részére kiadhat speciális időbélyegzés szolgáltatói *Tanúsítvány*okat.
A *Hitelesítés-szolgáltató* által kiadott *Időbélyegző egység*ek *Tanúsítvány*ainak érvényességi ideje:

- minősített Időbélyegzés szolgáltató részére kibocsátott *Tanúsítvány* esetében legfeljebb a kibocsátástól számított 12 év;
- nem minősített Időbélyegzés szolgáltató részére kibocsátott *Tanúsítvány* esetében legfeljebb a kibocsátástól számított 135 hónap;
- nem haladhatja meg az alkalmazott kriptográfiai algoritmusok és kulcs paraméterek érvényességi idejét;
- nem haladhatja meg a *Tanúsítvány*t kibocsátó szolgáltatói *Tanúsítvány* érvényességi idejét.

Az Időbélyegző kulcsok életciklusa

Az *Időbélyegző*k hitelesítésére használt magánkulcsok esetében teljesülniük kell az alábbi követelményeknek:

- Az időbélyegzés Szolgáltatónak meg kell határoznia az *Időbélyegző egység*ekben használt magánkulcsok érvényességének végét;

- a kulcs érvényességi ideje nem haladhatja meg a *Tanúsítvány* érvényességi idejét;
- a kulcs érvényességi ideje nem haladhatja meg az alkalmazott kriptográfiai algoritmusok és kulcs paraméterek érvényességi idejét;

A *Tanúsítvány*ok 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 *Tanúsítvány*okat.

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 *Minősített elektronikus bélyegzőt létrehozó eszköz*ök illetve *Hardver kriptográfiai eszköz*ök esetén a *Hitelesítés-szolgáltató*nak:

- az aktivizáló adatokat megfelelő minőségű véletlenszám-generátor segítségével, fizikailag biztonságos körülmények között kell előállítania és a *Minősített elektronikus bélyegzőt létrehozó eszköz*re vagy *Hardver kriptográfiai eszköz*re 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 *Minősített elektronikus bélyegzőt létrehozó eszköz*ök és *Hardver kriptográfiai eszköz*ök esetén:

- a *Hitelesítés-szolgáltató* az aktivizáló adatokat csak abból a célból rögzítheti, hogy azt az *Igénylő* részére átadhassa;

- a *Hitelesítés-szolgáltató*nak az aktivizáló adatokat biztonságos módszer felhasználásával kell az *Igénylő*k 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 felhasználókhoz szerepköröket kell rendelni és biztosítani kell, hogy minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezzen;
- minden tranzakcióról naplóbejegyzést kell előállítani és a naplóbejegyzéseket archiválni kell;
- a biztonságkritikus folyamatok részére biztosítani kell, hogy a *Hitelesítés-szolgáltató* belső hálózati tartományai kellően védettek legyenek a jogosulatlan hozzáféréstől;
- megfelelő eljárásokat kell alkalmazni a kulcsvesztés vagy rendszerhiba 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 eszköz*ök védelméről azok teljes életciklusa alatt.

- Megfelelő tanúsítással rendelkező *HSM eszköz*öket kell használni.
- A *HSM eszköz*ök átvételekor meg kell róla győződni, hogy a szállítás során biztosították a *HSM eszköz*ök feltörés elleni védelmét.

- A tárolás során biztosítani kell a *HSM eszköz*ök feltörés elleni védelmét.
- Az üzemeltetés során folyamatosan be kell tartani a *HSM eszköz*ök biztonsági előirányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket.
- A használatból kivont *HSM eszköz*ökben tárolt magánkulcsokat olyan módon kell törölni, hogy lehetetlenné váljon a kulcsok visszaállítása.
- A használatból kivont *HSM eszköz*öket a biztonsági előirányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeknek megfelelően kell kezelni és megsemmisíteni.

6.7. Hálózati biztonsági előírások

A *Hitelesítés-szolgáltató* tartsa szigorú ellenőrzés alatt az alkalmazott IT rendszereinek konfigurációját, 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 Úniós tagállam bizalmi listáján szereplő minősített időbélyegzés-szolgáltató által biztosított *Időbélyegző*ket kell használnia a naplóbejegyzések és egyéb archiválandó elektronikus állományok hitelesítésére.

7. Tanúsítvány, CRL és OCSP profilok

7.1. Tanúsítvány profil

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

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [37];
- IETF RFC 3739 [31];
- IETF RFC 5280 [33];
- IETF RFC 6818 [34];
- ETSI EN 319 412-1 [19];
- ETSI EN 319 412-3 [21]
- ETSI EN 319 412-5 [23];

7.1.1. Verzió szám(ok)

A *Hitelesítés-szolgáltató* által használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítvány*ai és a *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*ok legyenek az X.509 specifikáció [37] szerinti "v3" *Tanúsítvány*ok.

A *Tanúsítvány*ok alapmezői a következők:

- Verzió (Version)
  A *Tanúsítvány* az X.509 specifikáció [37] szerinti "v3" *Tanúsítvány*oknak felel meg, így a mezőbe a "2" érték kerül.
- Sorozatszám (Serial Number)
  A *Tanúsítvány*t kibocsátó hitelesítő egység által generált egyedi azonosító.

  A végfelhasználói *Tanúsítvány*ok esetében a "Serial Number" mezőnek legalább 8 bájt entrópiájú véletlen számot kell tartalmaznia.

- Algoritmus azonosító (Algorithm Identifier)
  A *Tanúsítvány*t hitelesítő elektronikus aláírás vagy bélyegző készítéséhez használt kriptográfiai algoritmuskészlet azonosítója (OID).

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

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

- Érvényesség (notBefore & notAfter)

  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 [37] 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 *Tanúsítvány*t 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*t tartalmazó tanúsítványláncban használható *Hitelesítési rend*eket. A köztes hitelesítési egység alá tartozó alrendszerekben csak olyan végfelhasználói *Tanúsítvány* adható ki, amely megfelel az itt felsorolt *Hitelesítési rend*ek közül legalább egynek.

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

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

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

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
  OID: 2.5.29.35
  A *Tanúsítvány*t 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 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 *Tanúsítvány*okban szerepeltetni kell legalább egy "Extended Key Usage" értéket az alábbiak szerint:

  A minősített elektronikus bélyegző létrehozására szolgáló *Tanúsítvány*okat kiadó köztes szolgáltatói *Tanúsítvány*okban szereplő értékek:

  - Document Signing (1.3.6.1.4.1.311.10.3.12)
  - Secure E-mail (1.3.6.1.5.5.7.3.4)

  Az *Időbélyegző egység Tanúsítvány*okat kiadó köztes szolgáltatói *Tanúsítvány*okban szereplő értékek:

  - Time Stamping (1.3.6.1.5.5.7.3.8)

- CRL szétosztási pont (CRL Distribution Points) – nem kritikus
  OID: 2.5.29.31
  A mező tartalmazza a CRL elérhetőségét http és/vagy LDAP protokollon keresztül.
  Kitöltése kötelező.

- Szolgáltatói információ elérése (Authority Information Access) – nem kritikus
  OID: 1.3.6.1.5.5.7.1.1
  A *Hitelesítés-szolgáltató* által rendelkezésre bocsátott, a *Tanúsítvány* használatához kapcsolódó egyéb szolgáltatásainak leírása.

  Kötelező a kitöltése, és a mező tartalmazza a következő adatokat:

  - A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást kell nyújtson. Ennek elérhetőségét kell itt szerepeltetni.
  - A tanúsítványlánc felépítésének megkönnyítésére a *Hitelesítés-szolgáltató* adja meg a *Tanúsítvány*t kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.

Más tanúsítvány kiterjesztés nem kerülhet kitöltésre.

Végfelhasználói tanúsítvány

- Hitelesítési rendek (Certificate Policies) – nem kritikus
  OID: 2.5.29.32
  E mező tartalmazza a *Tanúsítvány* kiadása és használata során érvényes *Hitelesítési rend* (lásd 1.2.1.fejezet) azonosítóját, valamint a *Tanúsítvány* alkalmazhatóságára vonatkozó egyéb információkat.

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

  - a *Hitelesítési rend* azonosítója (1.2.1 fejezet szerinti OID) ;
  - a *Szolgáltatási szabályzat* elérhetősége;
  - szöveges [1] figyelmeztetés angol és magyar nyelven, amelyből megállapítható, hogy
    * a *Tanúsítvány* minősített,
    * a *Tanúsítvány*hoz tartozó magánkulcsot *Minősített elektronikus bélyegzőt létrehozó eszköz* védi (kizárólag *Minősített elektronikus bélyegzőt létrehozó eszköz* használatát megkövetelő rendek esetében),

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

    * a *Tanúsítvány*hoz kapcsolódó adatok megőrzési ideje;
  - az ETSI EN 319 411-2 [18] által meghatározott hitelesítési rend azonosítója (OID), amelynek a *Tanúsítvány* szintén megfelel.

    Az ETSI EN 319 411-2 által meghatározott hitelesítési rendek a következők:
    * QCP-l: Jogi személy számára kibocsátott EU minősített *Tanúsítvány*
      OID: 0.4.0.194112.1.1;
    * QCP-l-qscd: Jogi személy számára kibocsátott EU minősített *Tanúsítvány*, ahol a magánkulcs és a hozzá tartozó *Tanúsítvány* *Minősített elektronikus bélyegzőt létrehozó eszköz*ön került kibocsátásra
      OID: 0.4.0.194112.1.3.

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

A "Certificate Policies" mezőt nem tartalmazó végfelhasználói *Tanúsítvány*t teszt *Tanúsítvány*nak 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 *Tanúsítvány*t hitelesítő elektronikus aláírás vagy bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.

  Használata kötelező.

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

- *Alany* kulcsazonosító (Subject Key Identifier) – nem kritikus
  OID: 2.5.29.14
  Az *Alany* nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.
  A mező értéke: a nyilvános kulcs SHA-1 lenyomata.

  Használata kötelező.

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

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

  A kiterjesztés alapértelmezett értéke CA = "FALSE", ezért ez a kiterjesztés nem szerepelhet a végfelhasználói *Tanúsítvány*okban.

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

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

  A végfelhasználói *Tanúsítvány*okban kötelezően beállítandó és kizárólagosan megadandó érték:

  – "nonRepudiation".

- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus
  OID: 2.5.29.37
  A kulcs engedélyezett használati körének további meghatározása.

  Minősített bélyegző végfelhasználói *Tanúsítvány*okban kötelezően beállítandó és kizárólagosan megadandó értékek:

  – "Document Signing (1.3.6.1.4.1.311.10.3.12)"
  – "emailProtection (1.3.6.1.5.5.7.3.4)"

- 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 *Tanúsítvány*ok 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 *Tanúsítvány*ok esetében kötelező a kitöltése, és a mező tartalmazza a következő adatokat:

  – A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást kell nyújtson. Ennek elérhetőségét kell itt szerepeltetni.
  – A tanúsítványlánc felépítésének megkönnyítésére a *Hitelesítés-szolgáltató* adja meg a *Tanúsítvány*t kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.

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

- Minősített tanúsítvánnyal kapcsolatos állítások (Qualified Certificate Statements) – nem kritikus
  OID: 1.3.6.1.5.5.7.1.3
  A mező a minősített *Tanúsítvány*okkal kapcsolatos állítások jelzésére szolgál, azonban van olyan mezője is, amely a nem minősített *Tanúsítvány* esetében is használható.

  Minden minősített végfelhasználói *Tanúsítvány*ban szerepelniük kell a következő állításoknak:

- a *Tanúsítvány* EU minősített *Tanúsítvány* – 'id-etsi-qcs 1' (0.4.0.1862.1.1);
- a *Tanúsítvány*hoz kapcsolódó tranzakciós limit – más néven ügyleti érték vagy pénzügyi tranzakciós korlát – 'id-etsi-qcs 2' (0.4.0.1862.1.2)
  - opcionális;
- azon kijelentés, hogy a Szolgáltató a *Tanúsítvány*hoz kapcsolódó regisztrációs adatokat a *Tanúsítvány* lejárta után 10 évig megőrzi – 'id-etsi-qcs 3' (0.4.0.1862.1.3);
- azon kijelentés, hogy a *Tanúsítvány*hoz tartozó magánkulcs *Minősített elektronikus bélyegzőt létrehozó eszköz*ön helyezkedik el – 'id-etsi-qcs 4' (0.4.0.1862.1.4) – kizárólag *Minősített elektronikus bélyegzőt létrehozó eszköz* használatát megkövetelő hitelesítési rendek esetén;
- a végfelhasználói *Tanúsítvány*ra vonatkozó Szolgáltatási szabályzat rövidített, kivonatolt változatát tartalmazó dokumentum elérhetősége – 'id-etsi-qcs 5' (0.4.0.1862.1.5);
- annak jelzése, hogy a *Tanúsítvány* bélyegzés célra került kibocsátásra – 'id-etsi-qct-eseal' (0.4.0.1862.1.6.2);

A végfelhasználói *Tanúsítvány*ban opcionálisan - az *Ügyfél* kérésére - szerepelhet az *Alany* Open Banking, vagy 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* pénzügyi szolgáltatásainak típusát, valamint az *Alany* pénzforgalmi szolgáltatásait felügyelő hatóság nevét és rövidítését.

Más tanúsítvány kiterjesztés nem kerülhet kitöltésre.

Időbélyegző egység számára kibocsátott tanúsítvány

- Hitelesítési rendek (Certificate Policies) – nem kritikus
  OID: 2.5.29.32
  E mező tartalmazza az *Időbélyegző egység Tanúsítvány*ának kiadása és használata során érvényes *Hitelesítési rend* azonosítóját, valamint az alkalmazhatóságára vonatkozó egyéb információkat. A mező kitöltése kötelező és nem lehet kritikus. A vonatkozó *Szolgáltatási szabályzat* hivatkozása megadható ebben a mezőben.

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
  OID: 2.5.29.35
  A *Tanúsítvány*t 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 *Időbélyegző egység* 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 alapértelmezett értéke CA = "FALSE", ezért ez a kiterjesztés nem szerepelhet az *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban.

  A "pathLenConstraint" mező nem szerepelhet *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban.

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

  Az *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban kötelezően beállítandó és kizárólagosan megadandó érték:

  "nonRepudiation",

  "digitalSignature".

- Kulcshasználati időszak (PrivateKeyUsagePeriod) – nem kritikus
  OID: 2.5.29.16
  A magánkulcs engedélyezett használati időtartamának meghatározása.
  Használata opcionális. Amennyiben alkalmazásra kerül, a "notBefore" és "notAfter" értékek mindegyikét meg kell adni.

- Kiterjesztett kulcshasználat (Extended Key Usage) – kritikus
  OID: 2.5.29.37
  A kulcs további engedélyezett használati körének meghatározása.

  Az *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban kötelezően beállítandó és kizárólagosan megadandó érték:

  "timeStamping (1.3.6.1.5.5.7.3.8)".

- 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
  Hitelesítés-szolgáltató által rendelkezésre bocsátott, az időbélyegző egység *Tanúsítvány*ának használatához kapcsolódó egyéb szolgáltatásainak leírása.

  Kötelező a kitöltése, és a mező tartalmazza a következő adatokat:

  – A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást kell nyújtson. Ennek elérhetőségét kell itt szerepeltetni.

  - A tanúsítványlánc felépítésének megkönnyítésére a *Hitelesítés-szolgáltató* adja meg a *Tanúsítvány*t kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.

- Minősített tanúsítvánnyal kapcsolatos állítások (Qualified Certificate Statements) – nem kritikus
  OID: 1.3.6.1.5.5.7.1.3
  A mező a minősített *Tanúsítvány*okkal kapcsolatos állítások jelzésére szolgál. Az *Időbélyegző egység Tanúsítvány*ában szerepelniük kell a következő állításoknak:

  - a *Tanúsítvány* EU minősített *Tanúsítvány* – 'id-etsi-qcs 1' (0.4.0.1862.1.1);
  - a *Tanúsítvány*hoz kapcsolódó tranzakciós limit – más néven ügyleti érték vagy pénzügyi tranzakciós korlát – 'id-etsi-qcs 2' (0.4.0.1862.1.2)
    - opcionális;
  - azon kijelentés, hogy a Szolgáltató a *Tanúsítvány*hoz kapcsolódó regisztrációs adatokat a *Tanúsítvány* lejárta után 10 évig megőrzi – 'id-etsi-qcs 3' (0.4.0.1862.1.3);
  - azon kijelentés, hogy a *Tanúsítvány*hoz tartozó magánkulcs *Minősített elektronikus bélyegzőt létrehozó eszköz*ön helyezkedik el – 'id-etsi-qcs 4' (0.4.0.1862.1.4) – kizárólag *Minősített elektronikus bélyegzőt létrehozó eszköz* használatát megkövetelő hitelesítési rendek esetén;
  - az *Időbélyegző egység Tanúsítvány*ára vonatkozó Szolgáltatási szabályzat rövidített, kivonatolt változatát tartalmazó dokumentum elérhetősége – 'id-etsi-qcs 5' (0.4.0.1862.1.5);
  - annak jelzése, hogy a *Tanúsítvány* bélyegzés célra került kibocsátásra – 'id-etsi-qcs 6' (0.4.0.1862.1.6) (a mező értéke 'id-etsi-qct-eseal' (2)).

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 szabályzat*ban fel kell sorolni.

7.1.4. Névformák

A *Hitelesítés-szolgáltató* a jelen *Hitelesítési rend*ek alapján kibocsátott *Tanúsítvány*okban egy – az IETF RFC 5280 szabványban [33] illetve az ETSI EN 319 412-2, -3, -4 szabványokban [20], [21], [22] meghatározott attribútumokból összeállított – megkülönböztetett nevet kell használjon az *Alany* azonosítására.

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

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

7.1.5. Névhasználati megkötöttségek

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

7.1.6. A Hitelesítési rend objektum azonosítója

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

7.1.7. A Hitelesítési rend megkötöttségek kiterjesztés használata

Nincs előírás.

7.1.8. A Hitelesítési rend jellemzők szintaktikája és szemantikája

A *Hitelesítés-szolgáltató* a Hitelesítési rend (Certificate Policy) kiterjesztés Irányelv minősítő (Policy Qualifier) mezejében rövid információt helyezhet el a *Tanúsítvány* felhasználhatóságával kapcsolatban. A mezőnek tartalmaznia kell a *Szolgáltatási szabályzat* 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 [33] specifikáció szerinti "v2" verziójú *Tanúsítvány visszavonási list*ákat bocsásson ki.

7.2.2. Tanúsítvány visszavonási lista kiterjesztések

A *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány visszavonási list*ák az alábbi mezőket tartalmazzák:

1. tbsCertList
   Ez a mező tartalmazza a kibocsátó adatait, az érvényességet és egyéb információkat, valamint a visszavont tanúsítványok felsorolását.
   A teljes mező aláírásra kerül a *Hitelesítés-szolgáltató* magánkulcsával.

   (a) Verzió (Version)
   Az IETF RFC 5280 [33] specifikáció szerinti "v2" verziójú *Tanúsítvány visszavonási lista* esetén a mező értéke kötelezően "1".

(b) Aláírás (Signature)
A *Hitelesítő egység* által a *Tanúsítvány*ok kibocsátása során használt aláíró algoritmus azonosítója.
Megegyezik a *Tanúsítvány visszavonási lista* aláírására használt algorimus azonosítóval (lásd. signatureAlgorithm).

(c) Kibocsátó (Issuer Name)
A *Tanúsítvány visszavonási list*át kibocsátó *Hitelesítő egység* egyedi megnevezése ("DN" mező értéke).

(d) Hatálybalépés (thisUpdate)
A *Tanúsítvány visszavonási lista* hatálybalépésének kezdete. UTC szerinti érték az IETF RFC 5280 [33] szerinti "UTCTime" kódolással.

(e) Következő kibocsátás (nextUpdate)
A következő *Tanúsítvány visszavonási lista* kibocsátásának ideje (lásd: 4.10. fejezet). UTC szerinti érték az IETF RFC 5280 [33] szerinti "UTCTime" kódolással.

(f) Visszavont *Tanúsítvány*ok (Revoked Certificates)
A felfüggesztett vagy visszavont *Tanúsítvány*ok listája a *Tanúsítvány*ok sorozatszáma szerint növekvő sorrendbe rendezve. Amennyiben nincs felfüggesztett vagy visszavont *Tanúsítvány*, a *Tanúsítvány visszavonási lista* nem tartalmazza ezt a mezőt.
Minden bejegyzés esetén kötelezően szereplő mezők:

- Tanúsítvány sorozatszám (CertificateSerialNumber)
  A *Tanúsítvány*t kibocsátó hitelesítő egység által generált egyedi azonosító, amely egy egész szám.
- Visszavonás időpontja (revocationDate)
  UTC szerinti érték az IETF RFC 5280 [33] szerinti "UTCTime" kódolással.

A *Hitelesítés-szolgáltató* által használható opcionális *Tanúsítvány visszavonási lista* bejegyzési kiterjesztések (crlEntryExtensions):

- Visszavonás oka (reasonCode) – 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 (InvalidityDate) – nem kritikus
  OID: 2.5.29.24
  Ebbe a mezőbe a magánkulcs megbízhatatlanná válásának ideje kerülhet.
- Útmutató a felfüggesztett *Tanúsítvány*okhoz (holdInstruction) – nem kritikus
  OID: 2.5.29.23
  Ebbe a mezőbe a felfüggesztett *Tanúsítvány* kezelése kerülhet.

(g) CRL kiterjesztések (CRL Extensions)

- Szolgáltatói kulcs azonosítója (AuthorityKeyIdentifier)
  OID: 2.5.29.35
  A *Tanúsítvány visszavonási lista* hitelesítésére használt magánkulcshoz tartozó nyilvános kulcs azonosítója egy "SHA1" formátumú lenyomat formájában.
- CRL sorozatszám (cRLNumber) – nem kritikus
  OID: 2.5.29.20

Ebbe a mezőbe a *Tanúsítvány visszavonási list*ák monoton növekvő sorozatszámai kerüljenek.

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

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

2. Aláíró algoritmus azonosító (signatureAlgorithm)
   A *Tanúsítvány visszavonási list*át 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)

3. Aláírás (signatureValue)
   A *Hitelesítés-szolgáltató* visszavonási listát hitelesítő elektronikus aláírása vagy bélyegzője. A *Tanúsítvány visszavonási list*át az adott hitelesítő egység a *Tanúsítvány*ok aláírására vagy bélyegzésére használt kulcsával kell hitelesítse.

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

7.3. Online tanúsítvány-állapot válasz (OCSP) profil

A *Hitelesítés-szolgáltató*nak az IETF RFC 6960 [35] és IETF RFC 8954 [36] 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 elektronikus aláírás vagy bélyegző 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 elektronikus aláírása vagy bélyegzője.

- 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 [33] szerinti kódolással.

- Következő kibocsátás (nextUpdate)
  A következő OCSP válasz kibocsátásának legkésőbbi ideje. UTC szerinti érték az IETF RFC 5280 [33] 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 [35] szerinti "v1" verziójú online tanúsítvány-állapot kéréseket és válaszokat.

7.3.2. OCSP kiterjesztések

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

- ArchiveCutoff – nem kritikus
  A *Hitelesítés-szolgáltató* az IETF RFC 6960 [35] 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 megfelelőség vizsgálata

A *Hitelesítés-szolgáltató* tevékenységét az Európai Uniós szabályozással összhangban a Nemzeti Média- és Hírközlési Hatóság felügyeli. A Nemzeti Média- és Hírközlési Hatóság évente legalább egyszer átfogó helyszíni ellenőrzést tart a *Hitelesítés-szolgáltató* telephelyén. A helyszíni ellenőrzés előtt a *Hitelesítés-szolgáltató* köteles külső auditor igénybevételével átvilágíttatni üzemeltetését és az átvilágításról készült részletes megfelelőségértékelési jelentést annak kézhezvételétől számított három munkanapon belül a Nemzeti Média- és Hírközlési Hatóságnak benyújtani. Az átvizsgálás során azt kell megállapítani, hogy a *Hitelesítés-szolgáltató* működése

megfelel-e az eIDAS Rendeletben [1] és a vonatkozó magyar jogszabályokban megállapított követelményeknek, valamint az alkalmazott *Hitelesítési rend*(ek)ben és az ennek megfelelő *Szolgáltatási szabályzat*(ok)ban támasztott követelményeknek.

Az átvilágítás tematikája és módszertana feleljen meg az alábbi 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 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [16]
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [15]
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [17]
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; [18]

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

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

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

8.1. Az ellenőrzések körülményei és gyakorisága

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

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

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

8.2. Az auditor és szükséges képesítése

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

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

8.3. Az auditor és az auditált rendszerelem 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-szolgáltató*val;

8.4. Az auditálás által lefedett területek

Az átvizsgálásnak le kell fednie minimálisan az alábbi területeket:

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

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

8.5. A hiányosságok kezelése

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

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

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

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

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

8.6. Az eredmények közzététele

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

9.1.2. Tanúsítvány hozzáférés díja

A *Hitelesítés-szolgáltató* ingyenesen köteles az *Érintett felek* részére 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 *Tanúsítvány*ok visszavonási állapotáról.

9.1.4. Egyéb szolgáltatások díjai

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

9.1.5. Visszatérítési politika

Nincs megkötés.

9.2. Anyagi felelősségvállalás

A *Hitelesítés-szolgáltató*nak a megbízhatóság biztosítása érdekében meg kell felelnie a pénzügyi feltételeknek és teljesítenie kell a felelősségvállalásra vonatkozó követelményeket.

9.2.1. Pénzügyi követelmények

A *Hitelesítés-szolgáltató* a szolgáltatási tevékenységének megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében köteles az alábbi követelmények legalább egyikének megfelelni:

- A *Hitelesítés-szolgáltató* legalább huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával rendelkezik.
- A *Hitelesítés-szolgáltató* a Nemzeti Média- és Hírközlési Hatóság mint jogosult javára pénzügyi intézménynél óvadékot tesz le. Az óvadék összege legalább huszonötmillió forint.
- A költségek megfizetéséért hitelesítés-szolgáltató esetén legalább százmillió forint jegyzett tőkéjű európai uniós vállalkozás készfizető kezességet vállal. A kezességvállalás mértéke legalább huszonötmillió forintig terjed.

9.2.2. További követelmények

Nincs megkötés.

9.2.3. Felelősségbiztosítás

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

meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

9.3. Bizalmasság

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

9.3.1. Bizalmas információk köre

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

9.3.2. Bizalmas információk körén kívül eső adatok

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

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

9.3.3. Bizalmas információ védelme

A *Hitelesítés-szolgáltató* felelősséggel tartozik az általa kezelt bizalmas adatok védelméért.
A *Hitelesítés-szolgáltató* szerződésben vagy titoktartási nyilatkozat aláírásával kell kötelezze alkalmazottait, alvállalkozóit, szerződött partnereit a bizalmas adatok védelmére.
A *Hitelesítés-szolgáltató Szolgáltatási szabályzat*ában tételesen meg kell határozni azon eseteket, amikor a *Hitelesítés-szolgáltató* felfedheti a bizalmas adatokat.
Ilyen esetek például:

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

9.4. Személyes adatok védelme

A *Hitelesítés-szolgáltató*nak gondoskodnia kell az általa kezelt személyes adatok védelméről. Működésének és szabályzatainak meg kell felelniük az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [7] és a 2016/679 EU általános adatvédelmi rendelet [3] rendelkezéseinek.
A *Hitelesítés-szolgáltató* köteles az *Ügyfél*ről nyilvántartott személyes adatokat és információkat a jogszabályi előírásoknak megfelelően

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

9.4.1. Adatkezelési terv

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

9.4.2. Személyes adatok

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

9.4.3. Személyes adatnak nem minősülő adatok

A *Hitelesítés-szolgáltató* az *Igénylő* írásbeli hozzájárulása alapján nyilvánosságra hozhatja az *Alany*ok *Tanúsítvány*ban szereplő adatait.

A *Tanúsítvány*ban a *Hitelesítés-szolgáltató* feltünteti az *Alany*hoz rendelt szolgáltatói egyedi azonosítót.

9.4.4. Személyes adatok védelme

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

9.4.5. Személyes adatok felhasználása

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

9.4.6. Adatkezelés

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

9.4.7. Egyéb adatvédelmi követelmények

Nincs előírás.

9.5. Szellemi tulajdonjogok

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

A *Hitelesítés-szolgáltató* által ügyfelei részére kibocsátott magán- és nyilvános kulcs tulajdonosa az *Előfizető*, 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 *Tanúsítvány*ok teljes jogú felhasználója pedig az *Igénylő*.

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

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

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

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

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

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

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

9.6. Tevékenységért viselt felelősség és helytállás

9.6.1. A szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

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

- a *Hitelesítés-szolgáltató* felelősséget vállal az általa támogatott *Hitelesítési rend*(ek)ben leírt eljárásoknak való megfelelésért;
- a *Hitelesítés-szolgáltató* sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- a *Hitelesítés-szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfel*ekkel szemben a Polgári Törvénykönyv [8] 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 [8] 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* köteles teljesíteni az eIDAS Rendelet [1] 24. cikkének (2) bekezdésében foglalt követelményeket.

A *Hitelesítés-szolgáltató* alapvető kötelezettsége, hogy a szolgáltatást a *Hitelesítési rend*del, a *Szolgáltatási szabályzat*tal, az Általános Szerződési 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 *Tanúsítvány*ok hitelességéért, pontosságáért;
- az általa kibocsátott szabályzatokért, azok jogszabályi megfelelőségéért és betartásáért;
- az általa generált kulcspárok megfelelőségéért, a magánkulcs-nyilvános kulcs és a *Tanúsítvány* összetartozásáért;
- az *Elektronikus bélyegzőt létrehozó eszköz*t 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 szervezet*ektől a jelen *Hitelesítési rend* és a vonatkozó *Szolgáltatási szabályzat* előírásainak maradéktalan betartását.

A *Regisztráló szervezet* felelőssége:

- az *Igénylő* képviseletére jogosult személy személyazonosságának megállapítása;
- a felvett regisztrációs adatok valódiságának garantálása;
- a Szolgáltatási szerződés megkötését megelőzően a szolgáltatások igénybe vevőjének tájékoztatása a *Hitelesítési rend* és a *Szolgáltatási szabályzat* tartalmáról és elérhetőségéről, a szolgáltatás igénybevételének feltételeiről;
- általában kötelezettségeinek maradéktalan betartása.

9.6.3. Az Ügyfél felelőssége és helytállása

Az *Előfizető* felelőssége

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

Az *Előfizető* kötelezettségei

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

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

Az *Igénylő* felelőssége

Az *Igénylő* felelős:

- a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért;
- a *Tanúsítvány*ában szereplő adatok ellenőrzéséért,
- az adataiban bekövetkezett változások haladéktalan bejelentéséért;
- *Elektronikus bélyegzőt létrehozó eszköz*ének, 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 rend*et és a *Szolgáltatási szabályzat*ot;
- a *Hitelesítés-szolgáltató* által kért, a szolgáltatás igénybevételéhez szükséges adatokat hiánytalanul megadni, a valóságnak megfelelő adatokat szolgáltatni;
- amennyiben az *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-szolgáltató*t,
  - kérni a *Tanúsítvány* felfüggesztését vagy visszavonását és
  - megszüntetni a *Tanúsítvány* használatát;
- haladéktalanul megszüntetni a *Tanúsítvány* használatát, amennyiben az *Igénylő* tudomására jut, hogy az általa igényelt *Tanúsítvány*t visszavonták, vagy a kibocsátó CA magánkulcsa kompromittálódott;
- 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 a szolgáltatással kapcsolatos elektronikus bélyegzővel, illetve Tanúsítvánnyal kapcsolatban jogvita indul;
- együttműködni a *Hitelesítés-szolgáltatóval* a *Tanúsítvány* kiadásához szükséges adatok ellenőrzése érdekében, és mindent megtenni azért, hogy az ellenőrzés a lehető leghamarabb befejeződhessen;
- kulcs kompromittálódás vagy nem jogszerű használat gyanújának felmerülése esetében a *Hitelesítés-szolgáltató* megkereséseire a *Hitelesítés-szolgáltató* által megadott időn belül reagálni;
- tudomásul venni, hogy az *Előfizető* jogosult a *Tanúsítvány* visszavonását vagy felfüggesztését kérni;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a *Tanúsítvány*t a *Szolgáltatási szabályzat*ban leírt meghatározott módon, az ott leírt ellenőrzési lépések elvégezése után bocsátja ki;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*okban kizárólag a valóságnak megfelelő adatokat szerepeltet. Ennek megfelelően a *Hitelesítés-szolgáltató* a *Tanúsítvány*ba kerülő adatokat a *Szolgáltatási szabályzat* szerint ellenőrzi;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* jogosult a kibocsátott *Tanúsítvány*t azonnal felfüggeszteni illetve visszavonni, amennyiben
  - tudomására jut, hogy a *Tanúsítvány*ban 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;
  - az *Előfizető* megszegi a Szolgáltatási szerződés vagy az Általános Szerződési Feltételek feltételeit,
  - a visszavonást megköveteli a a *Hitelesítés-szolgáltató Hitelesítési rend*je vagy *Szolgáltatási szabályzat*a;
  - a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t illegális tevékenységhez használták;
  - az *Előfizető* nem fizeti meg határidőre a szolgáltatások díját.

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 *Tanúsítvány*ok elfogadásáról és a felhasználás módjáról. Az érvényesség vizsgálata során a *Hitelesítés-szolgáltató* által garantált biztonsági szint megtartásához szükséges, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, ezért különös tekintettel javasolt:

- a *Hitelesítési rend*ben és a *Szolgáltatási szabályzat*ban megfogalmazott követelmények, előírások betartása;

- megbízható informatikai környezet és alkalmazások használata;
- a *Tanúsítvány* visszavonási állapotának ellenőrzése az aktuális CRL vagy OCSP válasz alapján;
- a *Tanúsítvány* felhasználására vonatkozó valamennyi korlátozás figyelembevétele, amely a *Tanúsítvány*ban, a a *Szolgáltatási szabályzat*ban és a vonatkozó *Hitelesítési rend*ben szerepel.

9.6.5. Egyéb szereplők tevékenységéért viselt felelősség és helytállás

Nincs megkötés.

9.7. Helytállás érvénytelenségi köre

A *Hitelesítés-szolgáltató* kizárja felelősségét, amennyiben:

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

9.8. A felelősség korlátozása

A *Hitelesítés-szolgáltató* korlátozhatja a kártérítési felelősségét

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

9.9. Kártérítési kötelezettség

9.9.1. A szolgáltató kártérítési kötelezettsége

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

9.9.2. Az előfizető kártérítési kötelezettsége

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

9.9.3. Az érintett felek kártérítési kötelezettsége

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

9.10. Érvényesség és megszűnés

9.10.1. Érvényesség

A *Hitelesítési rend* adott verziója 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 *Ügyfel*ekkel 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 rend*et.

9.12.1. Módosítási eljárás

A *Hitelesítés-szolgáltató* évi rendszerességgel illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja a *Hitelesítési rend*et 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 legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre megküldi a Nemzeti Média- és Hírközlési Hatóság részére és publikálja honlapján.

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

`info@e-szigno.hu`

Érdemi változtatást igénylő észrevétel esetén a dokumentumot megváltoztatja.

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

9.12.2. Értesítések módja és határideje

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

9.12.3. Az OID megváltoztatása

A *Hitelesítés-szolgáltató* a *Hitelesítési rend* legkisebb változtatása esetén is új verziószámot ad ki, ami része a dokumentum azonosítónak (OID), így a dokumentum minden változása az OID változását eredményezi, vagyis két eltérő tartalmú – 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 [7];
- 2013. évi V. törvény a Polgári Törvénykönyvről [8].
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól [9];
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről [10];
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről [11];

- 470/2017. (XII. 28.) Kormányrendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről [13];
- 137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről [12];

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 rend*ben és a *Szolgáltatási szabályzat*ban 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: *Minősített elektronikus bélyegzőt létrehozó eszköz*ön kibocsátott *Tanúsítvány Hitelesítési rend*
  - H: *Hardver kriptográfiai eszköz*ön 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] 1952. évi III. törvény a polgári perrendtartásról .

[5] 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról .

[6] 2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról .

[7] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról .

[8] 2013. évi V. törvény a Polgári Törvénykönyvről .

[9] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól .

[10] 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről .

[11] 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről .

[12] 137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről .

[13] 470/2017. (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről .

[14] 541/2020. (XII. 2.) Korm. rendelet a bizalmi szolgáltatások esetében a személyes jelenléttel egyenértékű biztosítékot nyújtó, nemzeti szinten elismert egyéb azonosítási módszerekről

[15] ETSI EN 319 401 V2.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[16] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;.

[17] ETSI EN 319 411-1 V1.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[18] ETSI EN 319 411-2 v2.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;.

[19] Final draft ETSI EN 319 412-1 V1.4.3 (2021-03); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

[20] ETSI EN 319 412-2 V2.2.1 (2020-07); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;.

[21] ETSI EN 319 412-3 V1.2.1 (2020-07); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

[22] 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.

[23] ETSI EN 319 412-5 V2.3.1 (2020-04); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

[24] ETSI TS 119 312 V1.3.1 (2019-02); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[25] ETSI TS 119 495 V1.5.1 (2021-04); Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.

[26] CEN 419 221-5; Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.

[27] ISO 3166-1:2013, Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.

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

[29] ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules.

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

[31] IETF RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile, MARCH 2004.

[32] IETF RFC 4043: Internet X.509 Public Key Infrastructure - Permanent Identifier, May 2005.

[33] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.

[34] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.

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

[36] IETF RFC 8954: Online Certificate Status Protocol (OCSP) Nonce Extension, November 2020.

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

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

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

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

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

[42] e-Szignó Hitelesítés Szolgáltató - Általános Szerződési Feltételek .

[43] Microsec zrt. - Tájékoztató az online videóazonosítás feltételeiről .