SZOLGÁLTATÁSI SZABÁLYZAT NEM MINŐSÍTETT TANÚSÍTVÁNYSZOLGÁLTATÁSOKRA

A NETLOCK Kft. nyilatkozata a nem minősített tanúsítványkibocsátásának és a kapcsolódó állapotszolgáltatások valamint a távoli aláírás-szolgáltatás nyújtásának és igénybevételének részletes eljárási és működési szabályairól

NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság

A dokumentum magyar neve:	Szolgáltatási Szabályzat Nem Minősített Tanúsítványszolgáltatásokra
A dokumentum angol neve:	Service Practice Statement for Non-Qualified Certification Service
A dokumentum rövid neve:	SPS-NQC-HU
Verzió:	20260218
Azonosító szám (OID):	1.3.6.1.4.1.3555.1.1.15.0.260218
Jóváhagyás időpontja:	2026.01.19.
Közzététel időpontja:	2026.01.19.
Hatály kezdőnapja:	2026.02.18.
Oldalak száma:	fedlappal együtt 146 oldal
Jóváhagyó:	**Koós Sándor Tamás,** CEO, NETLOCK Kft.

© COPYRIGHT, NETLOCK KFT. 2026. – MINDEN JOG FENNTARTVA

TARTALOM

TARTALOM 2
1. BEVEZETÉS 8
1.1 ÁTTEKINTÉS 8
1.1.1 A Szabványok és előírások 8
1.1.2 A Szolgáltató 9
1.2 A DOKUMENTUM NEVE ÉS AZONOSÍTÁSA 11
1.2.1 Hitelesítési rendek 11
1.2.2 Dokumentum revíziók 15
1.3 A PKI SZEREPLŐK 20
1.3.1 A Hitelesítő Egység és a Kiadó 20
1.3.2 Regisztrációs Egységek 22
1.3.3 Előfizető, Végfelhasználó és Igénylő 23
1.3.4 Érintett Felek 23
1.3.5 Egyéb szereplők 23
1.4 TANÚSÍTVÁNYOK ALKALMAZHATÓSÁGA 24
1.4.1 Megfelelő tanúsítványfelhasználás 24
1.4.2 Tiltott tanúsítványfelhasználás 25
1.5 SZABÁLYZAT ADMINISZTRÁCIÓ 25
1.5.1 A dokumentum adminisztrációját végző szervezet 25
1.5.2 A dokumentum kapcsolattartó személye 25
1.5.3 A szolgáltatási szabályzat szolgáltatási rendnek megfeleléséért felelős szervezet 26
1.5.4 A Szolgáltatási Szabályzat elfogadása 26
1.6 FOGALMAK ÉS RÖVIDÍTÉSEK 26
1.6.1 Fogalmak 26
1.6.2 Rövidítések 36
2. KÖZZÉTÉTEL ÉS TANÚSÍTVÁNYTÁR 39
2.1 ADATTÁRAK 39
2.1.1 A tanúsítványokra vonatkozó információk közzététele 39
2.1.2 Kikötések és feltételek közzététele 40
2.1.3 Nyilatkozatok 40
2.2 A KÖZZÉTÉTEL IDŐPONTJA ÉS GYAKORISÁGA 40
2.3 TANÚSÍTVÁNYTÁR ELÉRÉSÉNEK SZABÁLYAI 41
3. AZONOSÍTÁS ÉS HITELESÍTÉS 42
3.1 ELNEVEZÉSEK 42
3.1.1 Névtípusok 44
3.1.2 A nevek értelmezhetősége 45
3.1.3 Álnevek 46
3.1.4 A különböző elnevezési formák értelmezési szabályai 47
3.1.5 A nevek egyedisége 48
3.1.6 Védjegyek azonosítása, ellenőrzése és szerepe 48
3.2 KEZDETI AZONOSÍTÁS 48
3.2.1 A magánkulcs birtoklásának igazolása 49
3.2.2 Szervezeti azonosság ellenőrzése 50
3.2.3 Természetes személy azonosságának hitelesítése 52
3.2.4 Nem ellenőrzött alany információk 57
3.2.5 Jogok, felhatalmazások ellenőrzése 57
3.2.6 Együttműködési képességre vonatkozó követelmények 59
3.3 AZONOSÍTÁS ÉS HITELESÍTÉS TANÚSÍTVÁNYKEZELÉSI ELJÁRÁS ESETÉN 59
3.3.1 Azonosítás és hitelesítés érvényes tanúsítvány esetén 60
3.3.2 Azonosítás és hitelesítés érvénytelen tanúsítvány esetén 61
3.4 AZONOSÍTÁS ÉS HITELESÍTÉS TANÚSÍTVÁNYÁLLAPOT-VÁLTOZTATÁS ESETÉN 61

4. ÉLETCIKLUS KÖVETELMÉNYEK 62
4.1 TANÚSÍTVÁNYIGÉNYLÉS 62
4.1.1 Ki nyújthat be tanúsítványigénylést? 63
4.1.2 Az igénylés folyamata és a résztvevők felelőssége 63
4.2 TANÚSÍTVÁNYIGÉNYLÉSEK FELDOLGOZÁSA 67
4.2.1 Azonosítás és hitelesítés 67
4.2.2 Tanúsítványigénylések elfogadása vagy visszautasítása 69
4.2.3 A tanúsítványigénylés feldolgozásának időtartama 70
4.3 TANÚSÍTVÁNY KIBOCSÁTÁSA 70
4.3.1 A Szolgáltató tevékenysége a tanúsítvány kibocsátás során 71
4.3.2 Értesítés a tanúsítvány kibocsátásáról 72
4.4 TANÚSÍTVÁNY ELFOGADÁSA 72
4.4.1 A tanúsítványelfogadás módja 72
4.4.2 A tanúsítvány közzététele 73
4.4.3 További szereplők értesítése a tanúsítvány kibocsátásról 73
4.5 KULCSPÁR ÉS TANÚSÍTVÁNY ALKALMAZHATÓSÁGA 73
4.5.1 A magánkulcs és a tanúsítvány használata 73
4.5.2 Az Érintett felek nyilvános kulcs és tanúsítvány használata 74
4.6 TANÚSÍTVÁNYMEGÚJÍTÁS 74
4.6.1 A tanúsítványmegújítás körülményei 74
4.6.2 Ki igényelheti a tanúsítványmegújítást? 75
4.6.3 A tanúsítványmegújítási igénylések feldolgozása 75
4.6.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról 76
4.6.5 A megújított tanúsítvány elfogadása 77
4.6.6 A megújított tanúsítvány közzététele 77
4.6.7 További szereplők értesítése a tanúsítvány kibocsátásáról 77
4.7 KULCSCSERE 77
4.7.1 A kulcscsere körülményei 77
4.7.2 Ki igényelheti a kulcscserét? 77
4.7.3 A kulcscsere igénylések feldolgozása 77
4.7.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról 78
4.7.5 A kulcscserével megújított tanúsítvány elfogadása 78
4.7.6 A kulcscserével megújított tanúsítvány közzététele 78
4.7.7 További szereplők értesítése a tanúsítvány kibocsátásáról 78
4.8 TANÚSÍTVÁNYMÓDOSÍTÁS 78
4.8.1 A tanúsítványmódosítás körülményei 78
4.8.2 Ki igényelheti a tanúsítványmódosítást 78
4.8.3 A tanúsítványmódosítási igénylések feldolgozása 78
4.8.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról 79
4.8.5 A módosított tanúsítvány elfogadása 79
4.8.6 A módosított tanúsítvány közzététele 79
4.8.7 További szereplők értesítése a tanúsítvány kibocsátásáról 79
4.9 VISSZAVONÁS ÉS FELFÜGGESZTÉS 79
4.9.1 A visszavonást és felfüggesztést indukáló körülmények 79
4.9.2 Állapotváltoztatási ügyféligényre jogosultak 81
4.9.3 A visszavonási, felfüggesztési és aktiválási eljárás 81
4.9.4 Az igénylések feldolgozása 82
4.9.5 Állapotváltoztatási igények feldolgozásának maximális ideje 82
4.9.6 Javasolt eljárás a tanúsítványállapot ellenőrzésére 83
4.9.7 A visszavonási lista-kibocsátás gyakorisága 83
4.9.8 A visszavonási lista előállítása és közzététele közötti idő maximális hossza 84
4.9.9 Tanúsítványállapot-szolgáltatás rendelkezésre állása 84
4.9.10 Tanúsítványállapot-szolgáltatásra vonatkozó követelmények 84
4.9.11 A visszavonási hirdetmények egyéb formái 84
4.9.12 Kulcskompromittálódására vonatkozó speciális követelmények 84
4.9.13 A felfüggesztés maximális ideje 85
4.10 VISSZAVONÁSI NYILVÁNTARTÁSOK 85

4.10.1 Működési jellemzők ... 85
4.10.2 Szolgáltatások elérhetősége ... 86
4.10.3 További lehetőségek ... 86
4.11 A SZOLGÁLTATÁSI SZERZŐDÉS MEGSZŰNÉSE ... 86
4.12 KULCSLETÉT ÉS KULCSHELYREÁLLÍTÁS ... 86
4.12.1 Kulcsletét és –helyreállítás rendje és szabályai ... 87
4.12.2 Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai ... 87
5. FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK ... 88
5.1 FIZIKAI ÓVINTÉZKEDÉSEK ... 88
5.1.1 Telephely felépítése ... 88
5.1.2 Fizikai hozzáférés ... 89
5.1.3 Áramellátás, légkondicionálás ... 89
5.1.4 Beázás és elárasztódás veszélyeztetettsége ... 90
5.1.5 Tűzmegelőzés és tűzvédelem ... 90
5.1.6 Adathordozók kezelése ... 90
5.1.7 Hulladékelhelyezés ... 90
5.1.8 Mentés külső helyszínen ... 90
5.2 ELJÁRÁSRENDI BIZTONSÁGI INTÉZKEDÉSEK ... 90
5.2.1 Bizalmi munkakörök ... 91
5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám ... 91
5.2.3 Az egyes szerepkörökhöz tartozó azonosítás és hitelesítés ... 92
5.2.4 Egyes szerepkörök összeférhetetlensége ... 92
5.3 SZEMÉLYZETI BIZTONSÁGI INTÉZKEDÉSEK ... 92
5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények ... 93
5.3.2 Ellenőrzési eljárások ... 94
5.3.3 Képzési követelmények ... 94
5.3.4 Továbbképzési gyakoriságok és követelmények ... 94
5.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága ... 94
5.3.6 Jogosultatlan tevékenységek büntető következményei ... 94
5.3.7 Szerződéses közreműködőkre vonatkozó követelmények ... 95
5.3.8 A személyzet számára biztosított dokumentumok ... 95
5.4 NAPLÓZÁSI ELJÁRÁSOK ... 95
5.4.1 A tárolt események típusai ... 95
5.4.2 A naplófájl feldolgozásának gyakorisága ... 96
5.4.3 A naplófájl megőrzési időtartama ... 96
5.4.4 A naplófájl védelme ... 96
5.4.5 A naplófájl mentési eljárásai ... 96
5.4.6 A naplózás adatgyűjtési rendszere ... 96
5.4.7 Az eseményeket kiváltó Ügyfelek értesítése ... 96
5.4.8 Sebezhetőség felmérése ... 96
5.5 ADATOK ARCHIVÁLÁSA ... 97
5.5.1 Az archiválandó adatok típusai ... 97
5.5.2 Archiválási időtartam ... 97
5.5.3 Az archívum védelme ... 97
5.5.4 Az archívum mentési folyamatai ... 98
5.5.5 Az adatok időbélyegzésére vonatkozó követelmények ... 98
5.5.6 Az archívum gyűjtési rendszere ... 98
5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások ... 98
5.5.8 Egyéb archiválási rendelkezések ... 98
5.6 KULCSCSERE ... 98
5.7 KATASZTRÓFAELHÁRÍTÁS ÉS HELYREÁLLÍTÁS ... 98
5.7.1 Incidens- és kompromittálódás-kezelési eljárások ... 99
5.7.2 IT erőforrások, szoftverek és/vagy adatok meghibásodása ... 99
5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás ... 100
5.7.4 A működés folytonosságának fenntartása katasztrófaesemény után ... 100
5.8 A HITELESÍTŐ VAGY A KÖZPONTI REGISZTRÁCIÓS EGYSÉG MEGSZŰNÉSE ... 101

6. MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK 103

6.1 KULCSPÁR GENERÁLÁS ÉS TELEPÍTÉS 103

6.1.1 Kulcspár előállítása 103
6.1.2 Magánkulcs eljuttatása a Végfelhasználóhoz 105
6.1.3 Nyilvános kulcs eljuttatás a tanúsítvány kibocsátóhoz 105
6.1.4 A szolgáltatói nyilvános kulcs közzététele 105
6.1.5 Kulcsméretek 105
6.1.6 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése 105
6.1.7 A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően 106

6.2 MAGÁNKULCS VÉDELEM ÉS KRIPTOGRÁFIAI MODUL ELŐÍRÁSOK 106

6.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások 106
6.2.2 Magánkulcs többszereplős (n-ből m) használata 107
6.2.3 Magánkulcs letétbe helyezése 108
6.2.4 Magánkulcs mentése 108
6.2.5 Magánkulcs archiválása 108
6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba, vagy onnan történő exportja 108
6.2.7 Magánkulcs tárolása kriptográfiai modulban 108
6.2.8 A magánkulcs aktiválásának módja 108
6.2.9 A magánkulcs deaktiválásának módja 109
6.2.10 A magánkulcs megsemmisítésének módja 109
6.2.11 A kriptográfiai modulok értékelése 109

6.3 A KULCSPÁRKEZELÉS TOVÁBBI SZEMPONTJAI 109

6.3.1 Nyilvános kulcs archiválása 109
6.3.2 Tanúsítvány és kulcspár használati idő 109

6.4 AKTIVÁLÓ ADAT 110

6.4.1 Aktiváló adat generálás és telepítés 110
6.4.2 Aktiváló adat védelme 110
6.4.3 Egyéb aktiváló adattal kapcsolatos előírások 111

6.5 INFORMATIKAI BIZTONSÁGI ELŐÍRÁSOK 111

6.5.1 Speciális informatikai biztonsági műszaki követelmények 111
6.5.2 Informatikai biztonság értékelése 111

6.6 ÉLETCIKLUSRA VONATKOZÓ BIZTONSÁGI ELŐÍRÁSOK 111

6.6.1 Rendszerfejlesztési óvintézkedések 111
6.6.2 Biztonságkezelési előírások 111
6.6.3 Az életciklusra vonatkozó biztonsági előírások 112

6.7 HÁLÓZATI BIZTONSÁG 112

6.8 IDŐBÉLYEGZÉS 112

7. TANÚSÍTVÁNY, CRL, OCSP PROFILOK 113

7.1 TANÚSÍTVÁNYPROFIL 113

7.1.1 Verzió szám(ok) 123
7.1.2 Tanúsítványkiterjesztések 123
7.1.3 Az algoritmus objektum azonosítója 125
7.1.4 Névformák 125
7.1.5 Névhasználati megkötések 125
7.1.6 Hitelesítési Rend azonosítója 125
7.1.7 A szabályzati korlátozás kiterjesztés használata 125
7.1.8 Szabályzatminősítő szintaxis és szemantika 125
7.1.9 A kritikus Hitelesítési Rend kiterjesztés feldolgozása 125

7.2 TANÚSÍTVÁNYVISSZAVONÁSI PROFIL 126

7.2.1 Verziószám(ok) 126
7.2.2 Tanúsítvány visszavonási lista kiterjesztések 126

7.3 TANÚSÍTVÁNYÁLLAPOT-SZOLGÁLTATÁS PROFILOK 126

7.3.1 Verziószám(ok) 126
7.3.2 OCSP kiterjesztések 126

8. A MEGFELELŐSÉG VIZSGÁLATA 129

8.1 AZ ELLENŐRZÉSEK KÖRÜLMÉNYEI ÉS GYAKORISÁGA 129
8.2 AZ ÉRTÉKELŐ ÉS SZÜKSÉGES KÉPESÍTÉSE 130
8.3 AZ AUDITOR ÉS AZ AUDITÁLT ENTITÁS KAPCSOLATA 130
8.4 AZ ÉRTÉKELÉS/AUDIT ÁLTAL LEFEDETT TERÜLETEK 130
8.5 A HIÁNYOSSÁGOK KEZELÉSE 131
8.6 AZ EREDMÉNYEK KÖZZÉTÉTELE 131
9. EGYÉB ÜZLETI ÉS JOGI TUDNIVALÓK 132
9.1 DÍJAK 132
9.1.1 Tanúsítványszolgáltatás díjai 132
9.1.2 Tanúsítvány-hozzáférési díjak 132
9.1.3 A tanúsítványállapot-változtatás és a visszavonási nyilvántartások igénybevételének díjai 133
9.1.4 Egyéb szolgáltatások díjai 133
9.1.5 Visszatérítési politika 133
9.2 PÉNZÜGYI FELELŐSSÉG 133
9.2.1 Biztosítási fedezet 134
9.2.2 Egyéb eszközök 134
9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák 134
9.3 BIZALMAS ÜZLETI INFORMÁCIÓK KEZELÉSE 134
9.3.1 A bizalmas információk köre 135
9.3.2 A bizalmas információk körén kívül eső adatok 135
9.3.3 A bizalmas információk védelme 135
9.4 SZEMÉLYES ADATOK KEZELÉSE 136
9.4.1 Adatkezelési szabályok 136
9.4.2 Személyes adatok 137
9.4.3 Személyes adatnak nem minősülő információk 137
9.4.4 Személyes adatok védelme 137
9.4.5 Személyes adatok felhasználása 137
9.4.6 Adatkezelés 138
9.4.7 Egyéb adatvédelmi követelmények 138
9.5 SZELLEMI TULAJDONHOZ FŰZŐDŐ JOGOK 138
9.6 FELELŐSSÉG ÉS GARANCIÁK 138
9.6.1 A Hitelesítő Egység felelőssége 139
9.6.2 A Regisztrációs Egységek felelőssége 139
9.6.3 Ügyfelek felelőssége és kötelezettségei 139
9.6.4 Érintett felek felelőssége 140
9.6.5 Egyéb résztvevők felelőssége 140
9.7 SZAVATOSSÁG KIZÁRÁSA 140
9.8 FELELŐSSÉG KORLÁTOZÁSA 141
9.9 KÁRTÉRÍTÉS, KÁRTALANÍTÁS 141
9.10 A SZABÁLYZAT HATÁLYA 141
9.10.1 Érvényesség 141
9.10.2 Megszűnés 141
9.10.3 A megszűnés következményei 141
9.11 EGYEDI ÉRTESÍTÉSEK ÉS A RÉSZTVEVŐK KÖZTI KOMMUNIKÁCIÓ 142
9.12 MÓDOSÍTÁSOK 142
9.12.1 A módosítási eljárás 143
9.12.2 Az értesítések módja és határideje 143
9.12.3 A dokumentumazonosító változása 143
9.13 VITÁS KÉRDÉSEK RENDEZÉSE 144
9.13.1 Panaszok kezelésének eljárása 144
9.13.2 9.13.2 Vitás kérdések rendezése békés, tárgyalásos úton 144
9.13.3 9.13.3 Vitás kérdések rendezése peres úton 145
9.14 IRÁNYADÓ JOG 145
9.15 A HATÁLYOS JOGSZABÁLYOKNAK ÉS SZABVÁNYOKNAK VALÓ MEGFELELÉS 145

9.16 VEGYES RENDELKEZÉSEK 147
9.16.1 Teljességi záradék 147
9.16.2 Átruházás 147
9.16.3 Részleges érvénytelenség 147
9.16.4 Igényérvényesítés 147
9.16.5 Vis maior 147
9.17 EGYÉB RENDELKEZÉSEK 147

1. BEVEZETÉS

Jelen dokumentum a NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság (továbbiakban: Szolgáltató) nyilatkozata a nem-minősített bizalmi tanúsítványszolgáltatások nyújtására és igénybevételére vonatkozó követelményeknek való megfelelésről és az alkalmazott részletes eljárási és működési követelményekről (a továbbiakban: Szolgáltatási Szabályzat vagy Szabályzat).

A jelen szolgáltatási szabályzatban rögzített eljárások és az azokra vonatkozó gyakorlati szabályok kizárólag a NETLOCK Bizalmi Szolgáltatási Rend Nem-minősített Tanúsítványszolgáltatásra (a továbbiakban: Szolgáltatási Rend) dokumentum 1.2.1 Hitelesítési rendek fejezetében megadott hitelesítési rendeknek (LCP, NCP, NCP+, NSCP, LSCP, OVCP és EVCP) megfelelő tanúsítványokkal kapcsolatos, a jelen dokumentum 1.1 fejezetében leírt szolgáltatásokra vonatkozik.

Az egyes hitelesítési rendeknek megfelelő tanúsítványok a Szolgáltató kereskedelmi kommunikációban alkalmazott megnevezéseit egy-egy rövid leírással a jelen dokumentum 1.2.1 pontja tartalmazza.
A dokumentumban alkalmazott fogalmak és rövidítések tekintetében lásd az 1.6 fejezetet.

1.1 Áttekintés

Jelen dokumentum a Szolgáltató alábbi bizalmi szolgáltatásaira vonatkozó elvárásokat tartalmazza:

- nem-minősített tanúsítványszolgáltatás,
  - elektronikus aláírás tanúsítványának kibocsátása
  - elektronikus bélyegző tanúsítványának kibocsátása
  - weboldal-hitelesítő tanúsítványok kibocsátása;
- nem-minősített tanúsítványszolgáltatás a DÁP szerinti e-ügyintézést biztosító szervek kiadmányozásra és ügyintézésre jogosult munkatársai valamint a szervek számítógépes rendszerei számára (jelen dokumentum az ilyen tanúsítványokat a továbbiakban egységesen „közigazgatási tanúsítványok”-ként hivatkozza);
- nem-minősített tanúsítványszolgáltatás a NETLOCK SIGN szolgáltatás keretén belül;
- nem-minősített tanúsítványszolgáltatásokhoz kapcsolódó tanúsítványállapot-szolgáltatások.

Az egyes tanúsítványok és hitelesítési rendek közötti kapcsolat tekintetében lásd az 1.2.1 Hitelesítési Rendek fejezetet.

Jelen Szabályzat a Szolgáltató részletes eljárási és működési szabályainak ismertetése mellett ajánlásokat fogalmaz meg a szolgáltatások segítségével létrehozott elektronikus aláírások, bélyegzők és tanúsítványaik, valamint a weboldal-hitelesítő és egyéb tanúsítványok használatához az Érintett Felek számára.

1.1.1 A Szabványok és előírások

Jelen Szolgáltatási Szabályzat a *Szolgáltatási Rend Nem minősített Tanúsítványszolgáltatásokra* dokumentum szerkezetét követve készült, az abban foglalt elvárásoknak való megfelelés módját ismerteti. Az egyes fejezetcímek csak a tartalom adott logikai rend szerinti rendezésére szolgálnak, a rendelkezések értelmezése tekintetében nem irányadók.

A Szabályzat tartalmi vonatkozásokban eleget tesz az eIDAS, a DÁP és a BM rendelet előírásainak és ajánlásainak, és felhasználja az ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412, ETSI TS 119 431-1 és ETSI TS 119 431-2 valamint az x.509 szabvány ajánlásait (lásd 9.15).

A szabályzat alapján kiadott aláíró és bélyegző tanúsítványok, illetve a hozzájuk tartozó

magánkulcsok a közigazgatási hatósági eljárásban (e-ügyintézésben) ügyfélként résztvevő felek által felhasználhatók, valamint alkalmasak az ügyintézésben közreműködő, kiadmányozásra nem jogosult személyek (ügyintézők) által elektronikus aláírások és bélyegző előállítására és ellenőrzésére.

A közigazgatási hatósági eljárásban ügyintézést biztosító állami szervek által használható tanúsítványok megfelelnek a Közigazgatási Rendelet előírásainak.

Az OVCP és EVCP hitelesítési rend szerint kiadott weboldal-hitelesítő tanúsítványok tekintetében Szolgáltató megfelel a CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates című dokumentumnak; az EVCP hitelesítési rend szerint kibocsátottak pedig a Guidelines for Issuance and Management of Extended Validation Certificates című dokumentumnak is, melyek a http://www.cabforum.org címen kerültek publikálásra. Amennyiben jelen szabályzat és e dokumentumok között bármilyen eltérés lenne, akkor e dokumentumok elsőbbséget élveznek a szabályzattal szemben.

A Szolgáltató által használt és alkalmazott jogszabályok, szabványok és előírások a 9.15 pontban kerültek részletezésre.

A NETLOCK Sign szolgáltatás távoli aláírás-szolgáltatására vonatkozó SSASC Policy nem kerül külön dokumentumba, azt a Szolgáltatási Rend tartalmazza. A kulcsmenedzsment szolgáltatásra vonatkozó SSASC Policy előírások szerinti információk a következők:

- A fokozott biztonságú aláírás/bélyegző létrehozására alkalmas nem minősített tanúsítványok tekintetében a szolgáltatás az LSCP és az NSCP szerint is biztosítható.
- A támogatott aláírás formátumok:
  - XADES,
  - PADES,
  - ASIC
- A támogatott aláírási osztályok:
  - B
  - T
  - LT
  - LTA
- Az aláírás dokumentumra és hash lenyomatra egyaránt elhelyezhető.
- Az időbélyegzett formátumok esetén az időbélyegzésre használt szolgáltatás a Szolgáltató Minősített Időbélyeg Szolgáltatása

A kulcsmenedzsment rendszer kezelését bizalmi munkakörben (lásd 5.2.1) nevesített munkatársak végzik.

1.1.2 A Szolgáltató

A jelen Szabályzatban Szolgáltatónak nevezett entitás a NETLOCK Kft.

A Szolgáltató adatai:

Név:	NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság
Rövidített név:	NETLOCK Kft.
Székhely (Ügyfélfogadási helyszín):	1143 Budapest, Hungária körút 17.
Cégjegyzékszám:	01-09-563961
Adószám:	12201521-2-42

TELEFONSZÁM:	(1) 437-6655 (Tanúsítvány állapotváltozás igénylése: 3. menüpont)
WEBOLDAL:	netlock.hu
KIKÖTÉSEK ÉS FELTÉTELEK KÖZZÉTÉTELE:	netlock.hu/aktualis-szabalyzatok
ÜGYFÉLKAPCSOLATI E-MAIL:	info@netlock.hu
MEGRENDELÉSEK, DOKUMENTUMMÁSOLATOK, SZERZŐDÉSEK KÜLDÉSE:	igenylesek@netlock.hu *vagy* kerelmek@netlock.hu
NETLOCK SZABÁLYZATELFOGADÓ EGYSÉG EMAIL CÍME:	szee@netlock.hu
COMPLIANCE EGYSÉG EMAIL CÍME:	compliance@netlock.hu
ÜGYFÉLFOGADÁS / NYITVATARTÁS	A Szolgáltató weboldalán feltüntetett helyen és időintervallumban.

Az Eat.[1] rendelkezéseinek megfelelő nem-minősített szolgáltatóként a Bizalmi Felügyelet 2001. október 27-én vette nyilvántartásba a Szolgáltatót. Regisztrációs szám: FA 6133-5/2001.

A Bizalmi Felügyelet Eat. szerinti szolgáltatásokat tartalmazó nyilvántartásának elérhetősége: http://webpub-ext.nmhh.hu/esign/

Jelen Szolgáltatási Szabályzat az eIDAS és a DÁP rendelkezéseinek megfelelő nem-minősített bizalmi tanúsítványszolgáltatás nyújtásával kapcsolatos eljárási és működési követelményeket tartalmaz, melyek nyújtását Szolgáltató jelen szabályzat hatálybalépésével egyidejűleg kezdte meg. Ezzel kapcsolatban:

- Szolgáltató a DÁP vonatkozó rendelkezései értelmében a Bizalmi Felügyelet által rendszeresített elektronikus űrlapon bejelentette a Felügyeletnek a nem-minősített bizalmi szolgáltatás nyújtásának megkezdését.
- a Szolgáltatási Rend, a Szolgáltatási Szabályzat és az Általános Szerződési Feltételek jóváhagyott nyilvános tervezeteit valamint a 470/2017 Kormányrendelet 2. § (2) bekezdésében meghatározott további dokumentumokat, iratokat és nyilatkozatokat Szolgáltató megküldte a Bizalmi Felügyeletnek a nem-minősített bizalmi szolgáltatás bejelentésekor.
- a Bizalmi Felügyelet felvette a Szolgáltatót és a bizalmi szolgáltatását a nem-minősített bizalmi szolgáltatókat és nem-minősített bizalmi szolgáltatásokat tartalmazó, a DÁP-ban meghatározott nyilvántartásába, valamint
- az eIDAS 22. cikk (1) bekezdésében meghatározott bizalmi listákon (EUTSL) a bizalmi szolgáltatás eIDAS szerinti „nem-minősített" státusza feltüntetésre került (a listák elérhetőségét lásd lentebb).

A jelen Szabályzat szerinti nem-minősített bizalmi szolgáltatások Bizalmi Felügyelethez történő bejelentése jelen nyilvános szabályzatverzió közzétételével egyidejűleg történik.

A Bizalmi Felügyelet eIDAS szerinti nem-minősített szolgáltatókat és szolgáltatásokat tartalmazó közhiteles nyilvántartásának elérhetősége:

http://webpub-ext.nmhh.hu/esign2016/szolgParams/init.do?tipus=fb

A bizalmi felügyelet által gondozott és közzétett magyar bizalmi lista elérhetőségei:

- géppel feldolgozható (xml) formátumban: http://nmhh.hu/tl/pub/HU_TL.xml
- olvasható (pdf) formátumban: http://nmhh.hu/tl/pub/HU_TL.pdf

[1] Az elektronikus aláírásról szóló 2001. XXXV. törvény – már nem hatályos

Az Európai Bizottság által gondozott és közzétett bizalmi listák listája (EU TL) elérhetőségei:

- géppel feldolgozható (xml) formában: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml
- böngészhető, kereshető formában: https://webgate.ec.europa.eu/tl-browser

A listákon feltüntetett szolgáltatások eIDAS szerinti „nem minősített" („fokozott biztonságú") státuszát a „ServiceTypeIdentifier" „CA/PKC" és a „ServiceStatus" „granted" értékei jelzik.

Évente elvégzett önkéntes akkreditációk és egyéb minősítések:

- Tanúsítványszolgáltatás tanúsítása az ETSI EN 319 401, az ETSI EN 319 411 és ETSI EN 319 412-1 szabványok szerint.
- ISO 9001 szabvány
- ISO 27001 szabvány

Lásd még a 8. fejezetet.

1.2 A dokumentum neve és azonosítása

A dokumentum nevét és OID azonosítóját lásd a fedlapon (első számozás nélküli oldal a Szolgáltató logójával) - "A dokumentum magyar neve" és "A dokumentum angol neve" valamint az "Azonosító szám (OID)" sorokban.

A dokumentum többi oldalain a dokumentum magyar neve a fejlécben, OID azonosítója pedig a láblécben kerül feltüntetésre.

A dokumentum jóváhagyásának, közzétételének és hatálybalépésének idejét valamint verziószámát szintén lásd a fedlapon.

Jelen dokumentum egyike a Szolgáltató által kiadott azon dokumentumoknak, amelyek az általa nyújtott szolgáltatások feltételeit együttesen szabályozzák. Ilyen dokumentumok továbbá például az Általános szerződési feltételek, a Szolgáltatási szerződés, a szolgáltatási szabályzatok, az Ügyfelekkel és a Partnerekkel kötött egyéb szerződések.

A jelen dokumentumban Szolgáltatónak nevezett entitás a NETLOCK Kft. - adatait lásd az 1.1.2 pontban.

1.2.1 Hitelesítési rendek

A Szolgáltató a Szolgáltatási Rend 1.2.1 fejezetében meghatározott elsődleges és másodlagos hitelesítési rendek azonosítóit tünteti fel a végfelhasználói tanúsítványok hitelesítési rendek (Certificate Policies) mezőjében (lásd 7.1 Tanúsítványprofil).

A Szolgáltató által forgalmazott végfelhasználói tanúsítványtípusok az alábbi hitelesítési rendek szerint kerülnek kibocsátásra (a hitelesítési rendek és a tanúsítványprofilok kapcsolatát lásd a 7.1 fejezetben). Az alábbi tanúsítványtípusok közül a nyilvános felületeken aktuálisan igényelhetőkről Szolgáltató weboldalán és nyilvános árlistájában ad tájékoztatást.

Amennyiben jelen szabályzatban foglalt egyes eljárások nem egységesen alkalmazandók az aláabb felsorolt összes tanúsítványtípus igénylésére, kibocsátására, kezelésére, az eltérő feltételeket a dokumentum az alábbi nyilvános elnevezések alapján különíti el és amennyiben az egyértelműség megköveteli, zárójelben a hitelesítési rend azonosítót is feltünteti.

Nem minősített aláíró és bélyegző tanúsítványok

NETLOCK tanúsítványok nyilvános felületeken	Hitelesítési Rend	Leírás

megjelenő elnevezései	azonosító[2]	
Expressz személyes aláíró - SW	LCP	Személyes profilú aláíró tanúsítvány szoftveres kulcstárolással, melynek magánkulcsa az eIDAS 26. cikke szerinti fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
Expressz üzleti aláíró - SW	LCP	Üzleti profilú aláíró tanúsítvány szoftveres kulcstárolással, melynek magánkulcsa az eIDAS 26. fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
Expressz bélyegző – SW	LCP	Bélyegző tanúsítvány szoftveres kulcstárolással, melynek magánkulcsa az eIDAS 36. fokozott biztonságú bélyegző létrehozására alkalmas.
Expressz személyes aláíró – SCD	LCP	Személyes profilú aláíró tanúsítvány SCD kulcstárolással és Ügyfél általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
Expressz üzleti aláíró – SCD	LCP	Üzleti profilú aláíró tanúsítvány SCD kulcstárolással és Ügyfél általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
Közigazgatási nem-minősített bélyegző – SCD	NCP+	Közigazgatási bélyegző tanúsítvány SCD kulcstárolással és Ügyfél általi kulcsgenerálással, melynek magánkulcsa az eIDAS 36. és 37. cikke szerinti fokozott biztonságú aláírás létrehozására és a Pp. 197. § alapján magánokirat létrehozására alkalmas.
Expressz személyes aláíró – SCD/CAMS[3]	LCP	Személyes profilú aláíró tanúsítvány SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti nem-minősített tanúsítványon alapuló fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
Expressz üzleti aláíró – SCD/CAMS	LCP	Üzleti profilú aláíró tanúsítvány SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti nem-minősített tanúsítványon alapuló fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
Expressz bélyegző – SCD/CAMS	LCP	Bélyegző tanúsítvány SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 36. cikke szerinti nem-minősített tanúsítványon alapuló fokozott biztonságú aláírás létrehozására alkalmas.
Expressz személyes aláíró – RSCD	LCP, NSCP	Személyes profilú aláíró tanúsítvány menedzselt SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti nem minősített tanúsítványon alapuló fokozott biztonságú

[2] Lásd Szolgáltatási Rend 1.2.1
[3] CAMS: Az Ügyféleszközök megszemélyesítésére a Szolgáltató által alkalmazott rendszer nevének (NETLOCK Card Management System) rövidítése

		aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
Expressz üzleti aláíró –RSCD	LCP, NSCP	Üzleti profilú aláíró tanúsítvány menedzselt SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti nem minősített tanúsítványon alapuló fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
Expressz bélyegző – RSCD	LCP, NSCP	Bélyegző tanúsítvány menedzselt SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 36. cikke szerinti nem minősített bélyegző létrehozására alkalmas.
Közigazgatási nem-minősített aláíró – SCD (CAMS)	NCP+	Üzleti profilú közigazgatási aláíró tanúsítvány SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. és 27. cikke szerinti nem-minősített tanúsítványon alapuló fokozott biztonságú aláírás létrehozására és a Pp. 197. § alapján magánokirat létrehozására alkalmas.
Közigazgatási nem-minősített bélyegző – SCD (CAMS)	NCP+	Közigazgatási bélyegző tanúsítvány SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 36. és 37. cikke szerinti fokozott biztonságú aláírás létrehozására és a Pp. 197. § alapján magánokirat létrehozására alkalmas.

[ECC] Expressz személyes aláíró - SW	LCP	Személyes profilú aláíró tanúsítvány szoftveres kulcstárolással, melynek magánkulcsa az eIDAS 26. cikke szerinti fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
[ECC] Expressz üzleti aláíró - SW	LCP	Üzleti profilú aláíró tanúsítvány szoftveres kulcstárolással, melynek magánkulcsa az eIDAS 26. fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
[ECC] Expressz bélyegző - SW	LCP	Bélyegző tanúsítvány szoftveres kulcstárolással, melynek magánkulcsa az eIDAS 36. fokozott biztonságú bélyegző létrehozására alkalmas.
[ECC] Expressz bélyegző e.v. - SW	LCP	Egyéni vállalkozók számára bélyegző tanúsítvány szoftveres kulcstárolással, melynek magánkulcsa az eIDAS 36. fokozott biztonságú bélyegző létrehozására alkalmas.
[ECC] Expressz álneves aláíró - SW	LCP	Személyes profilú aláíró tanúsítvány szoftveres kulcstárolással, melynek magánkulcsa az eIDAS 26. cikke szerinti fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
[ECC] Expressz személyes aláíró - SCD (kártyás)	LCP	Személyes profilú aláíró tanúsítvány SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
[ECC] Expressz üzleti aláíró -	LCP	Üzleti profilú aláíró tanúsítvány SCD kulcstárolással és

SCD (kártyás)		Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
[ECC] Expressz bélyegző - SCD (kártyás)	LCP	Bélyegző tanúsítvány SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 36. cikke szerinti fokozott biztonságú bélyegző létrehozására alkalmas.
[ECC] Expressz személyes aláíró - RSCD (NLSIGN)	LCP, NSCP	Személyes profilú aláíró tanúsítvány menedzselt SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
[ECC] Expressz üzleti aláíró - RSCD (NLSIGN)	LCP, NSCP	Üzleti profilú aláíró tanúsítvány menedzselt SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
[ECC] Expressz bélyegző - RSCD (NLSIGN)	LCP, NSCP	Bélyegző tanúsítvány menedzselt SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 36. cikke szerinti fokozott biztonságú bélyegző létrehozására alkalmas.

[RSA4096] Expressz személyes aláíró - SCD (kártyás)	LCP	Személyes profilú aláíró tanúsítvány SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
[RSA4096] Expressz üzleti aláíró - SCD (kártyás)	LCP	Üzleti profilú aláíró tanúsítvány SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 26. cikke szerinti fokozott biztonságú aláírás létrehozására alkalmas. A kibocsátásához szükséges azonosítási és hitelesítési eljárásoknak nem része Igénylő (Alany) személyes jelenléten alapuló vagy azzal egyenértékű módon történő személyazonosítása.
[RSA4096] Expressz bélyegző - SCD (kártyás)	LCP	Bélyegző tanúsítvány SCD kulcstárolással és Szolgáltató általi kulcsgenerálással, melynek magánkulcsa az eIDAS 36. cikke szerinti fokozott biztonságú bélyegző létrehozására alkalmas.

Nem-minősített weboldal-hitelesítő tanúsítványok

NETLOCK tanúsítványok nyilvános felületeken megjelenő elnevezései	Hitelesítési Rend azonosító[4]	Leírás
EV weboldal-hitelesítő (SSL) tanúsítvány – SingleDomain	OVCP, EVCP	Az EV tanúsítványkiadásnak is megfelelő eIDAS 3. cikk 38. pontnak megfelelő weboldal-hitelesítő tanúsítvány egyetlen domain név hitelesítésére.
EV weboldal-hitelesítő (SSL) tanúsítvány – MD[5]	OVCP, EVCP	Az EV tanúsítványkiadásnak is megfelelő eIDAS 3. cikk 38. pontnak megfelelő weboldal-hitelesítő tanúsítvány több domain név hitelesítésére.
Weboldal-hitelesítő (SSL) tanúsítvány szervezetek részére – SingleDomain	OVCP	Az eIDAS 3. cikk 38. pontnak megfelelő, OV SSL profilú weboldal-hitelesítő tanúsítvány egyetlen domain név hitelesítésére.
Weboldal-hitelesítő (SSL) tanúsítvány szervezetek részére – MD	OVCP	Az eIDAS 3. cikk 38. pontnak megfelelő, OV SSL profilú weboldal-hitelesítő tanúsítvány több domain név hitelesítésére.

NETLOCK tanúsítványok nyilvános felületeken megjelenő elnevezései	Hitelesítési Rend azonosító[6]	Leírás
[ECC] Nem minősített TLS - SINGLE DOMAIN (EV)	OVCP, EVCP	Az EV tanúsítványkiadásnak is megfelelő eIDAS 3. cikk 38. pontnak megfelelő weboldal-hitelesítő tanúsítvány egyetlen domain név hitelesítésére.
[ECC] Nem minősített TLS - MULTIDOMAIN ÉS WILDCARD (EV)	OVCP, EVCP	Az EV tanúsítványkiadásnak is megfelelő eIDAS 3. cikk 38. pontnak megfelelő weboldal-hitelesítő tanúsítvány több domain név hitelesítésére.
[ECC] Nem minősített TLS - SINGLE DOMAIN (OV)	OVCP	Az eIDAS 3. cikk 38. pontnak megfelelő, OV SSL profilú weboldal-hitelesítő tanúsítvány egyetlen domain név hitelesítésére.
[ECC] Nem minősített TLS - MULTIDOMAIN ÉS WILDCARD (OV)	OVCP	Az eIDAS 3. cikk 38. pontnak megfelelő, OV SSL profilú weboldal-hitelesítő tanúsítvány több domain név hitelesítésére.

Egyedi tanúsítványtípusok

A fenti tanúsítványtípusokon kívül Szolgáltató kibocsáthat más típusú tanúsítványokat is – pl. egyedi ügyféligény alapján. Az egyedileg konfigurált tanúsítványtípusok minden esetben valamely fenti, nyilvános felületeken elérhető típusból származtatott típusok; azaz hitelesítési rendjük szempontjából mindig megfelelnek valamely fenti típusnak (vagy a szolgáltatási rend 1.2.1 pontjában meghatározott egyéb hitelesítési rendeknek).

1.2.2 Dokumentum revíziók

OID	Hatálya	Változás leírása	Készítő
1.3.6.1.4.1.3555.1.59.20160909	2016.09.09-2017.07.20	Az eIDAS rendeletnek megfelelő első nyilvános verzió jogszabályi rendelkezéseknek és a bizalmi felügyelet által tett észrevételek alapján pontosított kiegészített verzió.	Almási János Dr. Barabás Anett Varga Viktor Szabó Zoltán

[4] Lásd Szolgáltatási Rend 1.2.1
[5] MD: Multidomain
[6] Lásd Szolgáltatási Rend 1.2.1

1.3.6.1.4.1.3555.1.59.20170721	2017.07.21- 2017.08.18	A 2017. júniusában hatálybaléptetett új minősített szolgáltatási szabályzat mintájára új nem-minősített szolgáltatási szabályzat készítése.	Varga Viktor Szabó Zoltán
1.3.6.1.4.1.3555.1.59.20170818	2017.08.18- 2017.10.15	Az előző verzió pontosítása a Hatóság észrevételei alapján.	Szabó Zoltán
1.3.6.1.4.1.3555.1.59.20170904	nem hatályosított verzió	Kihelyezett Regisztrációs Egységekkel való együttműködésre vonatkozó kiegészítések és NAIH nyilvántartási szám módosítás illetve egyéb pontosítások.	Szabó Zoltán
1.3.6.1.4.1.3555.1.59.20171012	2017.10.16- 2017.10.26.	Az előző verzió kiegészítése és pontosítása az alábbiakkal. A bizalmi felügyelet észrevételei alapján: - az SSCD és QSCD minősítésű eszközök EU-s listája elérési helyének megadása (1.1.2.) - az alkalmazott eszközök megfelelőségi tanúsítványának elérési helyének megadása (6.2.1.) Valamint: - az LCP hitelesítési rendnek megfelelő új tanúsítványtípusok felvétele (1.2.1) - a kihelyezett regisztrációs egységek működésével és regisztrációs ügyintézőik feladataival kapcsolatos pontosítások (1.3.2., 1.6.1.) - az azonosítási és hitelesítési eljárások szabályainak pontosítása, ezen belül: o nem Magyarországon bejegyzett szervezetek azonosítása (3.2.2. a.) o személyazonosítás szabályai természetes személy adatait nem tartalmazó és LCP hitelesítési rendszerint kiadásra kerülő tanúsítványok esetén (3.2.3. a.) o a személyazonosítási módszerek kiegészítése elektronikus azonosítási eszköz alkalmazásával (3.2.3. a.) o meghatalmazás és egyéb hozzájáruló nyilatkozatok benyújtásának szabályai (3.2.3 b.) o lakcím ellenőrzése személyes tanúsítványok esetén (3.2.3. c.) o a korábban már azonosított/ellenőrzött entitások/adatok újbóli azonosítása/ellenőrzése (3.3.).	Szabó Zoltán
1.3.6.1.4.1.3555.1.59.20171026	2017.10.27- 2018.09.17.	A 3.2.3 fejezet (A természetes személy azonosságának hitelesítése) további pontosítása	Szabó Zoltán
1.3.6.1.4.1.3555.1.59.20180913	2018.09.18- 2019.10.16.	• Dokumentum címének rövidítése. • Fedlap módosítása, kiegészítése. • EU TL elérhetőség pontosítása (1.1.2) • Egyes – értelmezési nehézséget okozó – megfogalmazások javítása (pl. 1.2.1, 9.2 stb.). • Tanúsítványtípusok körének bővítése és egyes esetekben leírásaik pontosítása, kiegészítése (1.2.1).	Szabó Zoltán

		• Weboldal-hitelesítő tanúsítványokhoz kapcsolódó azonosítási és hitelesítési lépések kiegészítése az ún. „Certificate Transparency” eljárással (3.2.5, 4.1.2). • Állapotváltozatási igényre való jogosultság ellenőrzésének kiegészítése (3.4) • A tanúsítványigénylés feldolgozásának maximális idejére vonatkozó szabály pontosítása (4.2.3) • Tanúsítványmegújításhoz szükséges adatellenőrzési eljárás pontosítása (4.6.3) • Felfüggesztett tanúsítvány aktiválására vonatkozó szabályok pontosítása (4.9.2). • Alkalmazott ügyféleszközök listájának bővítése (6.2.1) • Az ún. „Certificate Transparency” eljárásnak megfelelő tanúsítványkiterjesztés felvétele (7.1.2) • Adatkezelési szabályok pontosítása (9.4) • Módosítási szabályok pontosítása (9.12) • Egyes – a közelmúltban változott – jogszabályok hivatkozásának frissítése. • Egyéb, leginkább elütésekből származó kisebb javítások és pontosítások.	
1.3.6.1.4.1.3555.1.59.20191015	2019.10.17- 2020.04.05.	• Kiegészítés SSASC Policy előírások szerinti információkkal a NETLOCK Sign szolgáltatás kapcsán (1.1.1) • Alkalmazott szabványok hivatkozásainak pontosítása a NETLOCK Sign szolgáltatás kapcsán (1.1.1 és 9.15) • Szolgáltató köztes kiadói listájának kiegészítése és pontosítása (1.3.1) • Alkalmazott hitelesítési rendek módosítása (1.2.1) • Eszközhasználati előírások pontosítása (1.4.1, 4.5.1) • A *Regisztrációs ügyintéző* és az *Ügyféleszköz* fogalmának pontosítása és új fogalmak hozzáadása az SSASC Policy előírások kapcsán (1.6.1) • Új rövidítések hozzáadása az SSASC Policy előírások kapcsán (1.6.2) • Kezdeti azonosítási eljárások leírásának kiegészítése (3.2) • A szolgáltatói kulcsok esetleges kompromittálódása esetére előírt eljárás pontosítása (4.9.12) • A visszavonási nyilvántartások elérhetőségével kapcsolatos szabályok pontosítása (4.10.2) • Szolgáltatói tevékenység beszüntetése esetére előírt eljárás pontosítása (5.8) • A Szolgáltató által alkalmazott eszközök listájának pontosítása (6.2.1) • Tanúsítványkiterjesztés-szabályok pontosítása és kiegészítése (7.1)	Szabó Zoltán Varga Viktor

1.3.6.1.4.1.3555.1.59.20200218	nem hatályosított verzió	• A Szolgáltató új telephelyének rögzítése, és a személyes ügyfélfogadás helyszínének módosítása (1.1.2, 1.3.2, 3.2.3)	Varga-Szabó Éva
1.3.6.1.4.1.3555.1.59.20200402	2020.04.06-2020.08.02.	• Új chipkártya felvétele a Szolgáltató által használt és biztosított QSCD Ügyféleszközök közé (6.2.1) • A Közigazgatási Gyökér Hitelesítés-szolgálató új kiadójának felvétele a szabályzatba (1.3.5)	Varga-Szabó Éva
1.3.6.1.4.1.3555.1.59.20200630	2020.08.03-2020.08.30.	• A Szolgáltató személyes ügyfélfogadási helyszínének módosítása (1.1.2, 1.3.2, 3.2.3) • A közigazgatási tanúsítványok ügyfél általi visszaigazolási kötelezettségének megszűntetése (4.3)	Varga-Szabó Éva
1.3.6.1.4.1.3555.1.59.20200731	2020.08.31-2020.09.30.	A Mozilla Root Store Policy weboldal-hitelesítő tanúsítványok érvényességi idejére vonatkozó, legkésőbb 2020. szeptember 1-jétől alkalmazandó korlátozásának implementálása (6.3.2).	Kővári-Szabó Zoltán
1.3.6.1.4.1.3555.1.59.20200901	2020.10.01-2020.12.22.	A szabályzat 3.2.2 pontjának kiegészítése az *EV SSL tanúsítványok szervezeti azonosságának ellenőrzésére használt adatforrások nyilvántartása* nevű dokumentumra való hivatkozással.	Varga-Szabó Éva
1.3.6.1.4.1.3555.1.59.20201119	2020.12.23-2023.11.02.	• CA-Browser Forum változásának implementálása: A nem minősített EV weboldal-hitelesítő tanúsítványprofil Alany mezőinek kiegészítése a *cabfOrganizationIdentifier* mezővel (ld. 7.1)	Varga-Szabó Éva
1.3.6.1.4.1.3555.1.1.15.0.231103	2023.11.03-2023.12.09.	• 1.1.2 Szolgáltató elérhetőségeinek aktualizálása: fax elérhetőség megszűntetése (további pontok: 4.1.2; 9.11.). • 3.2.3 Random acces token érvényességének pontosítása • 4.1.2. Tanúsítvány profil pontosítás • 4.2.2 Tanúsítványigénylések feldolgozási körülményének pontosítása • 5.7.3.c algoritmus változásra vonatkozó kompromittálódás esetén követendő eljárás pontosítása. • 6.2.1 SCD eszközök státuszfigyelés módszertanának pontosítása. • 6.2.1 SCD eszköz nyilvántartás frissítése. • 6.3.2 Weboldal-hitelesítő tanúsítványok élettartamának pontosítása. • CA-Browser Forum változásának implementálása OV és nem minősített EV weboldal-hitelesítő tanúsítványok vonatkozásában (ld. 7.1) • 8.1: Külső partnerek és szolgáltatók ellenőrzése ISO27001 szerint	NETLOCK Compliance

		• 8.4: Audit által lefedett terület pontosítása a konfigurációs ellenőrzéssel • 9.12.3: a dokumentum azonosítójának (OID) megváltozása • 9.15 Szabványoknak való megfelelés kiegészítése az ETSI TS 119 461, ETSI TS 119 511, ETSI EN 301 549 szabvánnyal. • IV SSL tanúsítványtípus kivezetése (1; 1.1.1.;1.2.1; 1.4.1.; 2.1.1.; 2.1.3.; 3.1; 3.1.1; 3.1.2.; 3.1.3.; 3.1.5.; 3.2.3.c; 3.2.5.; 3.3.; 4.1.1.; 4.1.2.; 4.2.2.; 4.3.; 4.9.; 4.9.6.; 4.9.13.;4.10.1.; 4.10.2.; 8.1; 9.15; 7.1 IV SSL tanúsítványprofil fejezetek) • Egyéb formai módosítások: 1.2.1; 1.4.1; 1.6.1; 1.6.2; 3; 3.1; 3.2.2; 3.2.3; 3.3; 4.1; 4.1.2; 4.2.1; 4.9.1; 6.3.2; 7.1; 9.12.2; 9.12.3; 9.15.	
1.3.6.1.4.1.3555.1.1.15.0.231210	2023.12.10- 2024.04.19.	• 1.1.2 – Link eltávolítása • 1.6.1. Fogalmakban link frissítése • 6.2.1: QSCD eszköz felvétele a nyilvántartásba • 7.1. Lábjegyzet eltávolítása	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.15.0.240420	2024.04.20- 2024.06.30.	• 1.2.1 Tanúsítványtípusok frissítése • 1.3.1 Szolgáltató gyökér és köztes kiadóinak frissítése • 1.6.1 Fogalmak frissítése • 3.1.2 Tanúsítvány mező frissítés • 7.1 Tanúsítványprofil frissítés • 7.3.2. OCSP kiterjesztések frissítése • Egyéb formai módosítások: 1.1.1; 1.1.2; 1.2.1; 1.3.1; 1.3.2; 1.3.5.b; 4.1.2.a.ii; 7.3.2	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.15.0.240701	2024.07.01- 2024.07.17.	• 9.15 A hatályos jogszabályoknak és szabványoknak való megfelelés pont frissítése	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.15.0.240714	hatályon kívül helyezett verzió	• 6.2.1. QSCD eszközök frissítése • 6.3.2. Tanúsítvány és kulcspár használati idő pontosítás • 7.3.2 OCSP tanúsítványprofil frissítés • Egyéb formai módosítások: 9.15.	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.15.0.240718	hatályon kívül helyezett verzió	• 1.3.1 Szolgáltatói köztesek frissítése • 6.2.1. QSCD eszközök frissítése • 6.3.2. Tanúsítvány és kulcspár használati idő pontosítás • 7.3.2 OCSP tanúsítványprofil frissítés • Egyéb formai módosítások: 1.3.1, 9.15.	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.15.0.240709	2024.07.09- 2024.07.15.	• 1.1.1 Szolgáltatói elérhetőségek frissítése • 1.2.1 Tanúsítványtípusok frissítése • 1.3.1 Szolgáltatói köztesek frissítése • 6.2.1. QSCD eszközök frissítése • 6.3.2. Tanúsítvány és kulcspár használati idő pontosítás • 7.1.2 Tanúsítványkiterjesztések frissítése	NETLOCK Compliance

		• 7.3.2 OCSP tanúsítványprofil frissítés • Egyéb formai módosítások: 1.3.1, 7, 7.1, 9.15	
1.3.6.1.4.1.3555.1.1.15.0.240716	2024.07.16- 2024.08.31.	• 5.2.1 Bizalmi munkakörök pontosítás • Szabályzat megnevezés pontosítása: 4.3; 5; 5.1; 5.1.6; 5.2.4; 5.4.1; 5.5.8; 5.7.1; 6.1.1; 6.2.2; 6.2.8; 6.2.9; 6.5; 6.5.1; 6.7; 8.4	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.15.0.240901	2024.09.01-től 2025.03.09.ig	• 1.2 Szöveg pontosítása • 1.2.1 Tanúsítványtípusok frissítése • 6.2.1. QSCD eszközök frissítése • Jogszabályváltozás miatti további frissítések: 1.1; 1.1.1; 1.1.2; 1.6.1; 1.6.2; 3.1.3; 3.2; 7.1;9.2.1; 9.3.3; 9.4.6.; 9.15	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.15.0.250409	2025.03.10- 2025.05.16.	• 1.1.2. Székhely módosítás	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.15.0.250517	2025.05.17- 2025.12.27.	A szabályzat 6.2.1 fejezetének módosítása	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.15.0.251228	2025.12.28- 2026.02.17..	A szabályzat 5.7.1 fejezetének módosítása	NETLOCK Compliance
1.3.6.1.4.1.3555.1.1.15.0.260218	2026.02.18-tól visszavonásig vagy új verzió hatálybalépéséig.	• Szolgáltató postafiók címének törlése (1.1.2) • A tanúsítványkérelmekhez tartozó dokumentumok és egyéb bizonyítékfájlok elfogadhatósági határidejének módosítása • Egyéb kisebb pontosítások, formai módosítások	NETLOCK Compliance

1.3 A PKI szereplők

Jelen Szolgáltatási Szabályzat keretében a PKI szereplők alatt a nem-minősített tanúsítványszolgáltatás Ügyfeleit - a tanúsítványok Igénylőit és a szolgáltatás Előfizetőit, a tanúsítványok Végfelhasználóit, a Szolgáltatót és szervezeti egységeit, valamint az Érintett feleket kell érteni.

Lásd még az 1.6.1 Fogalmak fejezet releváns fogalom meghatározásait.

1.3.1 A Hitelesítő Egység és a Kiadó

Szolgáltató egy Hitelesítő Egységet, és annak kezelésében több Kiadót is működtet.

Szolgáltató Kihelyezett Hitelesítő Egységgel nem működik együtt.

A Hitelesítő Egység Szolgáltatási rendben, jelen Szolgáltatási szabályzatban és egyéb Kikötésekben megfogalmazott, a Hitelesítő Egységre vonatkozó követelményeknek megfelelő

működését az egység belső működési szabályzata biztosítja. A Hitelesítő Egység Hitelesítési Ügyintézőket alkalmaz. Szolgáltatónál a Regisztrációs Felelős bizalmi munkakört a Hitelesítési Ügyintézők töltik be. A Hitelesítő Egység munkatársai tevékenységüket a belső működési szabályzatban foglalt előírások szerint végzik.

Szolgáltató az alábbi Kiadókat használja:

- a végfelhasználói és szolgáltatói tanúsítványokat egyaránt hitelesítő Köztes Kiadók, valamint
- legfelső szintű Gyökér Kiadó

amelyek hierarchiába szervezetten működnek.

Szolgáltató olyan Kiadókat és Időbélyegző Kiszolgálókat is hitelesíthet, amelyek Alárendelt Szolgáltatásokhoz kapcsolódnak.

A Hitelesítő Egység feladata, hogy a tanúsítványokat kibocsássa. A Hitelesítő Egység Hitelesítési Ügyintézőket alkalmaz, akik feladata a Regisztrációs Egységek által végzett azonosítás és adatellenőrzés alapján a tanúsítványok kibocsátásával, megújításával, módosításával, állapotváltoztatásával kapcsolatos - nem automatizált - tevékenységek végrehajtása. Lásd a 9.6.1 fejezetet.

Szolgáltató Gyökér Kiadóinak neve és tanúsítványának SHA256 lenyomata:

NetLock Arany (Class Gold) Főtanúsítvány	6C:61:DA:C3:A2:DE:F0:31:50:6B:E0:36:D2:A6:FE:40:19:94:FB:D1:3D:F9:C8:D4:66:59:92:74:C4:46:EC:98
NetLock Platina (Class Platinum) Főtanúsítvány	EB:7E:05:AA:58:E7:BD:32:8A:28:2B:F8:86:70:33:F3:C0:35:34:2B:51:6E:E8:5C:01:67:3D:FF:FF:BB:FE:58

NETLOCK Root ECC CA	00:F1:2C:1E:CF:E2:6D:34:A2:8F:C6:BF:9F:B3:50:85:30:2C:7D:53:A9:AC:35:88:ED:7C:D8:6C:9C:74:23:AA
NETLOCK TLS ECC CA	DC:42:61:66:7A:FE:21:DD:D0:1C:FA:52:D2:CC:AD:FD:70:AB:AF:26:31:5D:C6:A1:5A:32:B7:6C:89:9A:E2:61
NETLOCK TSA ECC CA	18:EC:46:B0:A8:37:8E:D5:44:BF:34:19:81:3B:34:A3:AE:B8:49:A6:2B:85:FF:3A:8F:3E:E3:0D:D3:14:C7:A3
NETLOCK RSA 2048 CA	FE:60:F3:BE:DE:77:B4:31:85:D4:79:95:D6:FB:51:59:16:78:A9:B8:48:48:43:24:E3:09:F0:46:24:F0:8A:FD
NETLOCK RSA 4096 CA	C1:C7:7F:C7:DA:86:51:08:A1:41:B4:F7:9B:7F:C8:54:A4:65:A0:11:AD:A3:AB:3A:0C:03:EC:EE:7E:27:56:4C

A nem-minősített köztes kiadók főbb adatai:

Kiadó neve	Tanúsítvány elérhetőség	Visszavonási lista elérhetőség
NETLOCK Trust Advanced Plus CA	www.netlock.hu/index.cgi?ca=trustap	www.netlock.hu/index.cgi?crl=trustap
NETLOCK Trust Advanced CA	www.netlock.hu/index.cgi?ca=trusta	www.netlock.hu/index.cgi?crl=trusta
NETLOCK Trust EV CA	www.netlock.hu/index.cgi?ca=trustev	www.netlock.hu/index.cgi?crl=trustev
NETLOCK Trust EV CA 2	www.netlock.hu/index.cgi?ca=trustev2	www.netlock.hu/index.cgi?crl=trustev2
NETLOCK Trust EV CA 3	www.netlock.hu/index.cgi?ca=trustev3	www.netlock.hu/index.cgi?crl=trustev3
NETLOCK Üzleti (Class B)	www.netlock.hu/index.cgi?ca=cbca	www.netlock.hu/index.cgi?crl=cbca
NETLOCK Expressz (Class C)	www.netlock.hu/index.cgi?ca=ccca	www.netlock.hu/index.cgi?crl=ccca

Közigazgatási üzleti (Class B)	www.netlock.hu/index.cgi?ca=bkozig	www.netlock.hu/index.cgi?crl=bkozig

NETLOCK Trust Advanced ECC CA	http://aia.ecc.netlock.hu/index.cgi?ca=trustaeccca	http://crl.ecc.netlock.hu/index.cgi?crl=trustaeccca
NETLOCK Trust Advanced Plus ECC CA	http://aia.ecc.netlock.hu/index.cgi?ca=trustapeccca	http://crl.ecc.netlock.hu/index.cgi?crl=trustapeccca
NETLOCK Trust TSA ECC CA	http://aia.ecc.netlock.hu/index.cgi?ca=trusttsaeccca	http://crl.ecc.netlock.hu/index.cgi?crl=trusttsaeccca
NETLOCK Trust Advanced RSA 2048 CA	http://aia.rsa.netlock.hu/index.cgi?ca=trustarsa2048ca	http://crl.rsa.netlock.hu/index.cgi?crl=trustarsa2048ca
NETLOCK Trust Advanced Plus RSA 2048 CA	http://aia.rsa.netlock.hu/index.cgi?ca=trustaprsa2048ca	http://crl.rsa.netlock.hu/index.cgi?crl=trustaprsa2048ca
NETLOCK Trust TSA RSA 2048 CA	http://aia.rsa.netlock.hu/index.cgi?ca=tsarsa2048ca	http://crl.rsa.netlock.hu/index.cgi?crl=tsarsa2048ca
NETLOCK Trust Advanced RSA 4096 CA	http://aia.rsa.netlock.hu/index.cgi?ca=trustarsa4096ca	http://crl.rsa.netlock.hu/index.cgi?crl=trustarsa4096ca
NETLOCK Trust Advanced Plus RSA 4096 CA	http://aia.rsa.netlock.hu/index.cgi?ca=trustaprsa4096ca	http://crl.rsa.netlock.hu/index.cgi?crl=trustaprsa4096ca
NETLOCK Trust TSA RSA 4096 CA	http://aia.rsa.netlock.hu/index.cgi?ca=tsarsa4096ca	http://crl.rsa.netlock.hu/index.cgi?crl=tsarsa4096ca

NETLOCK TLS OV ECC CA	http://aia.ecc.netlock.hu/index.cgi?ca=tlsoveccca	http://crl.ecc.netlock.hu/index.cgi?crl=tlsoveccca
NETLOCK TLS EV ECC CA	http://aia.ecc.netlock.hu/index.cgi?ca=tlseveccca	http://crl.ecc.netlock.hu/index.cgi?crl=tlseveccca

NETLOCK TLS OV ECC CA	http://aia.ecc.netlock.hu/index.cgi?ca=gold	http://crl.ecc.netlock.hu/index.cgi?crl=gold
NETLOCK TLS EV ECC CA	http://aia.ecc.netlock.hu/index.cgi?ca=gold	http://aia.ecc.netlock.hu/index.cgi?ca=gold

További adatokat és kiadókat lásd Szolgáltató weboldalán[7].

1.3.2 Regisztrációs Egységek

A Szolgáltató Központi Regisztrációs Egységet működtet, valamint Kihelyezett Regisztrációs Egységekkel működik együtt. A Központi Regisztrációs Egység Regisztrációs Ügyintézőket, Mobil Regisztrációs Munkatársakat alkalmaz, valamint Kézbesítési Megbízottakkal működik együtt. A Kihelyezett Regisztrációs Egységek legalább egy Regisztrációs Ügyintézőt alkalmaznak.

Szolgáltató Központi Regisztrációs Egységének működési helye Szolgáltató telephelye (ld. 1.1.2), melyet az Ügyfelek a Szolgáltató weboldalán (lásd 1.1.2) közzétett ügyfélszolgálati időpontokban kereshetnek fel személyazonosítás és más regisztrációs ügyintézés céljából.

[7] https://netlock.hu/tanusitvanykiadok/és https://netlock.hu/download/ca_hierarchy/

A Kihelyezett Regisztrációs Egységek csak a Szolgáltatói Partnerrel kötött szerződésben meghatározott ügyfélkör részére nyújtanak regisztrációs szolgáltatásokat. A Kihelyezett Regisztrációs Egységekről, elérhetőségeikről és ügyfélkörükről Szolgáltató a weboldalán (lásd 1.1.2) nyújt tájékoztatást.

A Regisztrációs Egységek feladata a tanúsítvány alanyaként feltüntetett és az igénylésben érintett entitás(ok) azonosítása, adataik és eljárási jogosultságai ellenőrzése, a tanúsítványigénylés rögzítése és hitelesítő egységhez juttatása, a tanúsítványkibocsátási eljárás koordinálása, dokumentálás, a további tanúsítványkezelési és állapotváltoztatási igények végrehajtása, valamint az Ügyfeleszköz átadása is.

Az ügyfélszolgálati teendőket, valamint az Ügyfelekkel való kapcsolattartást a Szolgáltató ügyfélszolgálati munkatársai végzik. Az ügyfélszolgálat a Központi Regisztrációs Egységen belül alkot önálló csoportot. Elérhetőségüket Szolgáltató a weboldalán (lásd 1.1.2) teszi közzé.

A Regisztrációs Egységek a Szolgáltatási rendben, jelen Szolgáltatási szabályzatban és egyéb Kikötésekben megfogalmazott, a Regisztrációs Egységekre vonatkozó követelményeknek megfelelő működését az egységek belső működési szabályzata biztosítja. A Regisztrációs Egységek munkatársai tevékenységüket a belső működési szabályzatban foglalt előírások szerint végzik. A Kihelyezett Regisztrációs Egységeket Szolgáltató a Szolgáltatói Partnerrel kötött szerződésben kötelezi a vonatkozó követelmények betartására.

Lásd még a 9.6.2 fejezetet.

1.3.3 Előfizető, Végfelhasználó és Igénylő

Előfizető és Igénylő a Szolgáltató Ügyfelei, akikkel Szolgáltató szerződéses kapcsolatba kerül.

Végfelhasználó személyét az Előfizető határozza meg.

Lásd még a 1.6 Fogalmak és rövidítések fejezet vonatkozó fogalommagyarázatait.

A Szolgáltató, annak munkatársa, szervezeti egysége vagy Szolgáltatói partnere is lehet a Szolgáltató Ügyfele. Az ilyen ügyfelekre ugyanazok a feltételek vonatkoznak, mint a többi ügyfélre, a szolgáltatási rend és jelen szabályzat előírásaitól és szabályaitól ebben az esetben sem térhet el Szolgáltató. Az ilyen tanúsítványigénylés esetén az Igénylő, Előfizető, Végfelhasználó és Átvevő nem vehet részt a hozzá kötődő igénylés feldolgozása során elvégzett szolgáltatói tevékenységben (regisztráció, személyazonosítás, ügyféleszközzel kapcsolatos teendők, igénylés jóváhagyása, tanúsítvány kibocsátása stb. - részletesen lásd a 4. fejezetet) és arra semmilyen befolyással nem lehet.

1.3.4 Érintett Felek

Az Érintett felek jellemzően nem állnak szerződéses kapcsolatban a Szolgáltatóval, de részükre a jelen Szolgáltatási Rend alapján készült szolgáltatási szabályzat ajánlásokat fogalmazhat meg az általuk igénybevett - jellemzően - nem díjköteles szolgáltatások - jellemzően tanúsítvány-állapotszolgáltatások - kapcsán. A Szolgáltató az Érintett Felekkel elsősorban a tanúsítványtáron keresztül tart kapcsolatot.

Lásd még az 1.6.1 fejezet Érintett Fél fogalmát.

1.3.5 Egyéb szereplők

a. Aláírói partnerek

Az NL Sign szolgáltatás nyújtásába egyedi szerződések kötésével Szolgáltató bevonhat ún. Aláírói partnereket.

Az Aláírói partnerek részt vehetnek a Végfelhasználók regisztrációjának előkészítésében. A

tanúsítványhoz, kulcsokhoz az aktiváló adathoz nem férnek hozzá.

Az Aláírói partnerek a Végfelhasználók magánkulcsával és aktiváló adatával nem kerülhetnek kapcsolatba, azokat meg nem ismerhetik, így Végfelhasználók nevében aláírás vagy bélyegző létrehozására nem lehetnek képesek.

b. Közigazgatási Gyökér Hitelesítés-szolgáltató

Az elektronikus ügyintézést biztosító állami szervek részére kibocsátott ún. közigazgatási végfelhasználói tanúsítványokat Szolgáltató a Közigazgatási Gyökér Hitelesítés-szolgáltató (a továbbiakban KGyHSz) tanúsítványával hitelesített kiadóból adja ki.

A Szolgáltató köztes kiadójának KGyHSz általi hitelesítése igazolja, hogy:

- a Szolgáltató adatait, valamint Bizalmi Szolgáltatási Rendjének és Szolgáltatási Szabályzatának megfelelőségét a KGyHSz ellenőrizte;
- e köztes kiadó alól kibocsátott végfelhasználói tanúsítványok kibocsátása során magára nézve kötelezőnek ismeri el a KGyHSz által kiadott szabályzatokat;
- a Szolgáltató magára nézve kötelezőnek elismeri a KGyHSz felügyeleti, ellenőrzési jogát.

A nem-minősített KGyHSz kiadó főbb adatai:

Kiadó neve	Tanúsítvány elérhetőség	Visszavonási lista elérhetőség
NETLOCK Public Administration CA	www.netlock.hu/index.cgi?ca=paca	www.netlock.hu/index.cgi?crl=paca

1.4 Tanúsítványok alkalmazhatósága

A Szabályzat 1.2.1. Hitelesítési Rendek fejezetében megadott tanúsítványtípusok az alábbi alfejezetekben ismertetett szabályok szerint alkalmazhatók.

A tanúsítványok alkalmazhatósága tekintetében az alábbiakon túl lásd még a másodlagos hitelesítési rend Kulcsfelhasználás mezőjét, valamint a Key Usage mező tartalmát, s a tanúsítványba foglalt egyéb (akár szöveges) korlátozásokat a 7.1.2 Tanúsítványkiterjesztések fejezetben.

1.4.1 Megfelelő tanúsítványfelhasználás

a. Végfelhasználói aláíró és bélyegző tanúsítványok

A jelen Szolgáltatási Szabályzat szerint kibocsátott aláíró és bélyegző tanúsítványokat és a hozzájuk tartozó kulcsokat tilos az elektronikus aláírás vagy bélyeg létrehozásától és ellenőrzésétől eltérő célra felhasználni. Az LCP, NCP és NCP+ szerinti tanúsítványok nem-minősített tanúsítványok, amelyek magánkulcsai az eIDAS 3. cikk 11. pontja szerinti nem-minősített elektronikus aláírás vagy 26. pontja szerinti bélyegző létrehozására alkalmazhatók. Az SCD típusú tanúsítványokhoz (lásd 1.2.1) tartozó magánkulcsok kizárólag SCD eszközön tárolhatók és használhatók (lásd még 4.5.1).

A közigazgatási eljárásban a kiadmányozók és az ügyintézést biztosító számítógépes rendszerek számára kínált tanúsítványokat olyan kiadó adja ki, amelyek tanúsítványát a KGYHSZ felülhitelesítette (lásd 1.3.5). A korlátozás közigazgatási ügyfélre nem vonatkozik.

b. Végfelhasználói weboldal-hitelesítő tanúsítványok

Az OVCP és EVCP hitelesítési rendek szerint kibocsátott tanúsítványok SSL és TLS protokollon

keresztül elért webszerverek azonosítására használhatók.

c. Szolgáltatói tanúsítványok

A Szolgáltató által kibocsátott szolgáltatói tanúsítványok a végfelhasználói és köztes szolgáltatói tanúsítványok ellenőrzésére használhatók fel.

A tanúsítványokhoz tartozó kulcsok felhasználása tekintetében lásd a 6.1.7. A kulcshasználat célja fejezetet. Az egyes tanúsítványtípusoknak megfelelő konkrét korlátozásokat lásd még a tanúsítványtípusokhoz tartozó profiloknál (lásd 7 fejezet).

1.4.2 Tiltott tanúsítványfelhasználás

A Szolgáltató által kibocsátott tanúsítványok előző, 1.4.1 pont szerinti megfelelő tanúsítványhasználattól eltérő alkalmazása tilos, különösképpen a végfelhasználói tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjainak más nyilvános kulcsú tanúsítványok aláírására történő felhasználása, vagy bármilyen bizalmi szolgáltatás nyújtásához történő alkalmazása.

A szolgáltatói gyökér és a végfelhasználói tanúsítványokat hitelesítő köztes tanúsítványokat és kulcsaikat Szolgáltató csak a közzétételüket követően használja tanúsítványok hitelesítésére.

1.5 Szabályzat adminisztráció

Jelen Bizalmi Szolgáltatási Szabályzat kibocsátását és karbantartását a Szolgáltató szabályzatért felelős egysége végzi. A szabályzatelfogadásért felelős egység állandó tagjai a Szolgáltató munkatársai, akiket a Szolgáltató Ügyvezetése írásban jelöl ki. Az Egység működését a Szabályzatelfogadó Egység belső, nem nyilvános működési szabályzata írja le.

1.5.1 A dokumentum adminisztrációját végző szervezet

A Szolgáltató szabályzatokért (kikötésekért) felelős egységének neve NETLOCK Szabályzatelfogadó Egység. A Szabályzatelfogadó Egység állandó tagjai a Szolgáltató munkatársai, akiket a Szolgáltató Ügyvezetése írásban jelöl ki. Az Egység működését a Szabályzatelfogadó Egység belső, nem nyilvános működési szabályzata írja le.

A Szolgáltató szabályzatainak módosításával kapcsolatban lásd a 9.12 fejezetet.

1.5.2 A dokumentum kapcsolattartó személye

Jelen dokumentummal kapcsolatban a Szabályzatelfogadó Egység kapcsolattartásért felelős személye a jelen dokumentum jóváhagyója (lásd a dokumentum fedlapját).

A Szolgáltatási Szabályzattal kapcsolatos kérdésekkel és észrevételekkel az Ügyfelek, a Végfelhasználók és az Érintett felek elektronikus levélben az compliance@netlock.hu címen kereshetik meg a NETLOCK Compliance Egységét.

Szolgáltató munkatársai észrevételeiket egyéb csatornán keresztül is, de szintén csak írásban juttathatják el a Szabályzatelfogadó Egységhez.

A Szabályzatelfogadó Egységnek elektronikus levélben küldött megkeresések (lásd 1.5.1) megválaszolásáért, illetve - amennyiben szükséges az észrevétel nyomán megtenni szükséges egyéb intézkedések megtételéért a kapcsolattartó személy felelős.

A Szabályzatelfogadó Egység részére jelen dokumentummal kapcsolatban eljuttattatott kérdés vagy észrevétel esetén a kapcsolattartó kijelöli az Egység azon munkatársát, aki a megkeresést

feldolgozza. Összetettebb tárgyú megkeresés esetén összehívja a Szabályzatelfogadó Egységet.

A megkeresés feldolgozása során, az Egység vagy munkatársa azonosítja a dokumentum megkereséssel érintett pontját/pontjait, majd az Egység többi munkatársával egyeztetve - és szükség esetén más munkatársak véleményét is kikérve - küld választ elektronikus levélben a megkeresést küldőnek.

Amennyiben a megkeresés nyomán jelen Szolgáltatási Szabályzat vagy más dokumentum módosítása szükségessé válik, a módosítással kapcsolatban a 9.12 fejezet szerint kell Szolgáltatónak eljárnia.

Magánkulcs kompromittálódásának gyanúja esetén, tanúsítványvisszaélés, vagy más típusú csalás, kompromittálás, visszaélés, nem megfelelő magatartás, vagy bármely más, a Tanúsítványokkal kapcsolatos ügyben a compliance.info@netlock.hu címen kereshetik a Szolgáltatót.

1.5.3 A szolgáltatási szabályzat szolgáltatási rendnek megfeleléséért felelős szervezet

A jelen Szolgáltatási Szabályzat alapján nyújtott nem-minősített tanúsítványszolgáltatás nyújtásának és igénybevételének részletes gyakorlati előírásait tartalmazó Szolgáltatási Szabályzat Szolgáltatási Rendnek való megfelelését a NETLOCK Szabályzatelfogadó Egység ellenőrzi. A jelen Szolgáltatási Rend alapján készült szolgáltatási szabályzatot a Szabályzatelfogadó Egység a jelen Szolgáltatási Rendnek való maradéktalan megfelelés esetén hagyhatja jóvá. A Szabályzat vagy nyilvános tervezete közzétételének feltétele, annak jóváhagyása.

1.5.4 A Szolgáltatási Szabályzat elfogadása

Amennyiben a szabályzat módosításra szorul, a módosított új verzió megírása, elfogadása és kibocsátása 9.12.1 fejezetnek megfelelő egységes eljárás szerint és az Egység működési szabályzatában foglaltak szerint történik. Amennyiben az új verzió jóváhagyásáért felelős munkatárs meggyőződött róla, hogy a Szabályzat a módosítást követően is maradéktalanul megfelel a Szolgáltatási Rend előírásainak, jóváhagyja a szabályzatot és haladéktalanul, de legkésőbb az új verzió hatálybalépése előtt gondoskodik annak közzétételéről.

1.6 Fogalmak és rövidítések

1.6.1 Fogalmak

Lásd a Bizalmi Szolgáltatási Rend 1.6.1 fejezetét.

AIA	CAI (Authority Information Access:Certificate Authority Issuers): Az adott tanúsítvány kiadói tanúsítványára vonatkozó elérhetőséget (URL) tartalmazó tanúsítványmező.
Alárendelt szolgáltatás	Szolgáltató szabályzatai alapján működő nem nem-minősített bizalmi szolgáltatás, mely számára Szolgáltató biztosít tanúsítványt.
Aktiváló adat	Olyan a szolgáltató által előállított vagy végfelhasználó által megadott, kizárólag a végfelhasználó által ismert kódsorozat (jelszó, PIN kód), ami a magánkulcsot alkalmazásra képes állapotba helyezi. Tanúsítványaktiváláshoz nincs köze.
Aláírás	Lásd elektronikus aláírás
Aláírás / Bélyegző	Olyan kriptográfiai eszköz, amely minősített aláírás / bélyegző létrehozására nem

Létrehozó eszköz	alkalmas (lásd még 1.6.2. Rövidítések, SCD).
Aláírási szolgáltatás	Az eIDAS szerinti alábbi szolgáltatások: ● elektronikus aláírások és elektronikus bélyegzők létrehozása, ellenőrzése és érvényesítése, ● valamint ezekhez kapcsolódó tanúsítványok ellenőrzése és érvényesítése. Jelen szabályzat keretében e szolgáltatások "felhőalapú" nyújtását értjük, a végfelhasználói aláíró és bélyegző kulcsok szolgáltató által tárolásával és az ügyfelek által webes felületen/protokollon keresztül feltöltött dokumentumok aláírásával/bélyegzésével (beleértve opcionálisan az időbélyeg elhelyezését is).
Aláírói partner	Szolgáltatói partner, aki az aláírási szolgáltatást saját ügyfelei számára biztosítja, amelynek részeként részt vehet a Végfelhasználók azonosításában (akik tekintetében korlátozott információs és adminisztrációs jogokkal bír), s aki az aláírási szolgáltatást saját szolgáltatásával integráltan szolgáltatás nyújtására használja, s aki Előfizetőként vállalja a díjfizetést a végfelhasználók után.
Alany	Lásd a DÁP vonatkozó rendelkezései szerinti meghatározását. Jelen szabályzat keretében a tanúsítvány Subject és SAN mezőit, illetve az ezekben feltüntetésre kerülő adatokat értjük alatta, amelyek utalhatnak egy természetes személyre és/vagy egy szervezetre és/vagy egy védjegyre/terméknévre vagy egy eszköz/rendszer azonosítójára/más elnevezésére vagy egy álnévre. Lásd az Igénylő, Előfizető, Ügyfél és Végfelhasználó entitásokat.
Állapotváltoztatás	Az az eljárás, aminek eredményeként a tanúsítvány állapota (érvényes, felfüggesztett) megváltozik és új értéket vesz fel (érvényes, felfüggesztett, visszavont).
Archiválási szolgáltatás	Az elektronikus dokumentumok hosszú távú megőrzésére vonatkozó szolgáltatás. Olyan elektronikus archiválási szolgáltatás, amelyet valamely minősített bizalmi szolgáltató nyújt, és amely megfelel a 45j. cikkben meghatározott követelményeknek. Jelen szabályzat keretén belül olyan minősített bizalmi szolgáltatás, mely során a Bizalmi Szolgáltató a hozzá archiválás céljából eljuttatott elektronikusan hitelesített (aláírt vagy bélyegzett) dokumentumok aláírása vagy bélyegzője teljes érvényességi láncát létrehozza vagy kiegészíti, az érvényességi láncot archív időbélyeggel ellátja, majd az így kiegészített dokumentumot vagy fájlt biztonságosan eltárolja. Ha az elektronikus aláírással vagy bélyegzővel ellátott elektronikus dokumentum archiválását minősített bizalmi szolgáltató végzi, az ellenkező bizonyításáig vélelmezni kell, hogy az elektronikus dokumentumon elhelyezett elektronikus aláírás, bélyegző vagy időbélyegző és az azokhoz kapcsolódó tanúsítvány az aláírás, bélyegző vagy időbélyegző elhelyezésének időpontjában érvényes volt.
Átvevő	A végfelhasználó valamely kulcsát vagy eszközét (pl. Ügyféleszköz) és aktiváló adatát Szolgáltatótól (személyesen, hagyományos vagy elektronikus kézbesítés útján) átvevő személy, aki az lehet, aki az adott tanúsítvány esetében Igénylő lehet.
Bélyegző	Lásd elektronikus bélyegző
Bizalmi lista	Hatóság vagy szoftvergyártó által kezelt lista, amely a megbízhatónak tartott bizalmi szolgáltatások azonosítóit (jellemzően tanúsítványait) tartalmazza. Egy adott bizalmi listát kezelő szoftver a benne lévő szolgáltatásokra visszavezethető aláírásokat, bélyegzőket és időbélyegzőket elfogadja. Jellemzően az EU bizalmi listát értjük alatta, ahol az eIDAS szerinti nem minősített és minősített szolgáltatások kerülnek feltüntetésre az egyes tagországok felügyeleti szervei által. Lásd: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

Bizalmi Szolgáltatási Rend	NETLOCK Bizalmi Szolgáltatási Rend Nem-minősített Tanúsítványszolgáltatásra
Bizalmi Felügyelet	A DÁP által a bizalmi szolgáltatások felügyeletére kijelölt szerv. Konkrétan a Nemzeti Média- és Hírközlési Hatóság.
Bizalmi munkakör	A szolgáltató informatikai rendszeréért általánosan felelős vezetői munkakör. Lásd az 5.2.1 Bizalmi munkakörök fejezetet.
Bizalmi munkatárs	A Szolgáltatónál vagy Szolgáltatói partnerénél bizalmi munkakört betöltő személy.
Bizalmi szolgáltatás	Az eIDAS 3. cikk 16. Pontja szerint: “Rendszerint díjazás ellenében nyújtott, jelen Szabályzat keretében 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 tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése.” Jelen szabályzat keretén belül a Szolgáltató elektronikus aláírásokhoz, elektronikus bélyegzőkhöz és weboldal hitelesítéshez kapcsolódó, a tanúsítványok kibocsátását és életciklusmenedzsmentjét biztosító, valamint az Időbélyegző szolgáltatását értjük alatta.
Biztonságos zóna:	Olyan (logikailag vagy fizikailag) védett terület, amely védi a titkosságát, integritását és elérhetőségét a Szolgáltató által használt rendszereknek.
CAA ellenőrzés	Olyan ellenőrzés, amikor a DNS bejegyzésben RFC 6844 szerinti CAA rekordokat keres a Szolgáltató. Ha itt arra utaló bejegyzés van, hogy más Szolgáltatóval tart kapcsolatot a domaintulajdonos, akkor nem adható ki tanúsítvány.
Eakta (formátum)	Elektronikus aláírás konténerformátum, amely dokumentumokat, illetve hozzájuk kapcsolódó profilokat (metaadatokat), aláírásokat, ellenjegyzéseket és időbélyegzőket tartalmazhat, szabványos, az ETSI TS 101 903 (XAdES) specifikációnak megfelelően. Lásd bővebben: https://e-szigno.hu/tudasbazis/e-akta-formatum-specifikacioja.html
EV tanúsítvány Extended Validation Certificate (EVC)	Olyan weboldal-hitelesítő tanúsítvány, ami megfelel az EVCG követelményeinek.
Egyéni vállalkozó (e.v.)	2009. évi CXV. törvény az egyéni vállalkozóról és az egyéni cégről.
Elektronikus aláírás	Olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ (eIDAS 3 cikk 10. pont). Jelen szabályzat keretén belül: A Szolgáltató által kibocsátott aláíró tanúsítvány magánkulcs párjával természetes személy által létrehozott elektronikus adat, amelyet az aláírandó elektronikus dokumentumhoz (vagy más elektronikus adatokhoz) csatolnak, s ami a tanúsítvánnyal és a benne foglalt nyilvános kulccsal ellenőrizhető.
Elektronikus bélyegző	Olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét. (eIDAS 3 cikk 25. pont)

	Jelen szabályzat keretén belül: A Szolgáltató által kibocsátott bélyegző tanúsítvány magánkulcs párjával jogi személy által létrehozott elektronikus adat, amelyet az bélyegzendő elektronikus dokumentumhoz (vagy más elektronikus adatokhoz) csatolnak, s ami a tanúsítvánnyal és a benne foglalt nyilvános kulccsal ellenőrizhető. Az elektronikus aláírás jogi személy által létrehozott megfelelője.
Előfizető	Szolgáltató azon szerződéses partnere, aki a szolgáltatási díjak fizetését vállalja. Jogai és kötelezettségei az ÁSZF-ben és a Szolgáltatási szerződésben elkülönülten megjelennek. Tanúsítványszolgáltatás esetén amennyiben a tanúsítvány Alanyként szervezet is megnevezésre került vagy csak egy természetes személy van benne megnevezve, akkor jellemzően azzal megegyezik. NL Sign szolgáltatás esetén megegyezik az Aláírói Partnerrel vagy a Végfelhasználóval. Lásd még az Ügyfél, Igénylő és Végfelhasználó entitásokat, valamint az 1.3.3 Előfizető, Végfelhasználó és Igénylő fejezetet.
Érintett fél	Természetes vagy jogi személy, aki Szolgáltatóval nem kerül szerződéses kapcsolatba, de annak valamely - jellemzően ingyenes - tanúsítvány állapot szolgáltatását igénybe veszi (pl. elektronikus aláírást, bélyegzőt vagy időbélyegzőt ellenőriz és ennek kapcsán az egyes tanúsítványok érvényességi információit vagy szolgáltató szabályzatait ellenőrzi). Lásd az 1.3.4 Érintett felek fejezetet.
Érvényes tanúsítvány	Olyan tanúsítvány, amelynek az érvényességi idejébe esik a mindenkori jelen időpont, és amelynek állapota nem felfüggesztett vagy visszavont (lásd Tanúsítványállapot).
Érvényességi idő(tartam)	Egy kezdeti és végső időpont közötti időtartam, amelyre a tanúsítvány kiadásra került.
Eszközös tanúsítvány	Olyan tanúsítvány, aminek magánkulcsa Kriptográfiai eszközre kerül kiadásra.
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. Általánosabb értelemben egymást hitelesítő tanúsítványok hierarchiája, egészen a gyökér tanúsítványig.
Fokozott biztonságú elektronikus aláírás	Olyan elektronikus aláírás, amely megfelel az eIDAS 26. cikkben meghatározott követelményeknek.
Fokozott biztonságú elektronikus bélyegző	Olyan elektronikus bélyegző, amely megfelel az eIDAS 36. cikkben meghatá-rozott követelményeknek.
Hitelesítési rend	A DÁP vonatkozó rendelkezései szerint: olyan bizalmi szolgáltatási rend, amely bizalmi szolgáltatás keretében kibocsátott tanúsítványra vonatkozik. Szolgáltató szabályzati keretében egy szabványos eljárásrend, ami alapján Szolgáltató tanúsítványt bocsát ki és kezel. Szolgáltató szabályzatai több hitelesítési rendet is magukban foglalnak, megkülönböztetve a nekik megfelelő követelményeket és eljárásokat. Az egyes hitelesítési rendek részletes leírását Szolgáltató a

	Szolgáltatási Rendben teszi közzé.
Hitelesítő egység	Szolgáltató szervezeti egysége, amely a Regisztrációs egység kérelme alapján a tanúsítványok kiadását, publikálását, visszavonását, felfüggesztését, valamint a Tanúsítványvisszavonási lista publikálását végzi. Lásd az 1.3.1 fejezetet.
Hitelesítési Ügyintéző	A Hitelesítő Egységen belül e munkakörben dolgozó munkatársak a tanúsítványok kibocsátásának jóváhagyását végzik.
Hozzáférő	Az archiválásszolgáltatás Előfizetőjének kezdeményezésére a szolgáltatás bizonyos funkcióit a kezdeményező Előfizető által meghatározott dokumetumok tekintetében díjmentesen elérő Érintett fél. Lásd az 1.3.5 Érintett felek fejezetet.
Igénylő	Tanúsítványszolgáltatás esetén a tanúsítványkibocsátási tanúsítványkezelési és állapotváltoztatási eljárásban eljáró, a szolgáltatói szerződést Ügyfél részéről elfogadó természetes személy, aki lehet: ● a tanúsítvány Alanyaként megjelölt természetes személy (Álnév esetén az álnév kérelmezője); ● ennek hiányában a tanúsítvány Alanyaként megjelölt szervezet képviselője vagy meghatalmazottja; ● ezek hiányában a tanúsítvány Alanyaként megjelölt domain név, trademark vagy terméknév tulajdonosa, ill. szervezet tulajdonos esetén annak képviselője vagy meghatalmazottja, illetve a domain név fölött kontrollal rendelkező személy. Előfizetővel megegyezik, amennyiben a tanúsítvány Alanyaként egy természetes személy kerül feltüntetésre (és szervezetnem). NL Sign szolgáltatás esetén megegyezik Végfelhasználóval. Archiválás- és Időbélyegszolgáltatás esetén megegyezik Előfizetővel.
Időbélyegző	Olyan elektronikus adat, amely más elektronikus adatokat egy adott időponthoz köt, amivel igazolja, hogy utóbbi adatok léteztek az adott időpontban.
Időbélyegző Kiszolgáló	A Szolgáltató időbéyegzőket kibocsátó műszaki rendszere.
Időbélyegző szolgáltatás	Szolgáltató azon szolgáltatása, amely a számára küldött elektronikus adatok lenyomata alapján egy időbélyegzőt állít elő, az adott adatokhoz.
Időbélyeg-URL	Az időbélyeg-szolgáltatás elérését biztosító, az Előfizető egyedi azonosítóját tartalmazó virtuális token, melyen keresztül Végfelhasználó időbélyeg kéréseket továbbíthat Szolgáltató felé, Szolgáltató pedig a kérés alapján időbélyeg választ továbbít Végfelhasználó felé.
Kézbesítési Megbízott	Olyan Szolgáltatói partner, aki Szolgáltató megbízásából - Igénylő ilyen irányú igénye esetén - az Igénylővel egyeztetett helyen és időben végzi el a Tanúsítványkibocsátáshoz kapcsolódóan az ügyféleszköz átadását. Adott esetben megegyezhet a Regisztrációs Megbízottal.
KGyHSz	Közigazgatási Gyökér Hitelesítés-Szolgáltató Lásd 1.3.5 és http://www.kgyhsz.gov.hu/
Központi Regisztrációs Egység	A Szolgáltató azon saját szervezetén belül működtetett szervezeti egysége, mely feldolgozza a szolgáltatások igényléseit, azonosítja azok Igénylőjét és Előfizetőjét, ellenőrzi az eljárási jogukat és adataikat.

Kezdeti felfüggesztés	A Tanúsítványfelfüggesztés egy speciális esete, amikor a Szolgáltató a tanúsítványt kibocsátása után azonnal felfüggeszti, így megóvva azt a visszaélésektől arra az időszakra, míg a Tanúsítvány és a magánkulcs biztonságosan eljut az Ügyfélhez.
Képviseleti jog	Teljes vagy részleges képviseleti jog vagy ekként is értelmezhető jogviszony (lásd DÁP).
Kiadó	Szolgáltató tanúsítványokat kibocsátó műszaki rendszere. Szolgáltatónál létezik végfelhasználói és egyes szolgáltatói tanúsítványokat kibocsátó Köztes Kiadó, valamint az ezen egységeket hitelesítő legfelső szintű Gyökér Kiadó, amelyek hierarchiába szervezetten működnek.
Kihelyezett Hitelesítő Egység	A Szolgáltatótól független, önálló szervezet vagy személy (mint Szolgáltatói partner) által, a Szolgáltató előírásai alapján működtetett Hitelesítő Egység.
Kihelyezett Regisztrációs Egység	A Szolgáltatótól független, önálló szervezet vagy személy (mint Szolgáltatói partner) által, a Szolgáltató előírásai alapján működtetett Regisztrációs Egység.
Kikötések (és feltételek)	Szolgáltató azon dokumentumai, amelyek ismertetik, hogy a szolgáltatások nyújtásával kapcsolatosan, milyen elvárásoknak, milyen módon felel meg, s ismertetik a többi szereplő kötelezettségeit és jogait. Ide tartozik a Szolgáltató Szolgáltatási kivonata, Hitelesítési rendje, Szolgáltatási szabályzata, ÁSZF-e, szolgáltatási szerződése, valamint a közöttük létrejött egyéb megállapodások együttesen.
Kriptográfiai eszköz	Olyan biztonságos hardver eszköz, amely a Végfelhasználó magánkulcsát tartalmazza, azt védi a kompromittálódás ellen, s a kulccsal kriptográfiai műveleteket (pl. aláírás, titkosítás) végez a Végfelhasználó számára. Lehet SCD és QSCD, HSM vagy más nem aláírás célú eszköz is. Lehet a Szolgáltató vagy az Ügyfél kezelésében. Utóbbi esetben “Ügyféleszközként” hivatkozunk rá.
Kritikus szolgáltatások	A Szolgáltató tanúsítvány- és kulcselőállítással, az Ügyfelek eszközzel való ellátásával és az állapotváltoztatással kapcsolatos szolgáltatásai.
Kulcscsere	Az a folyamat, amikor a Szolgáltató egy már regisztrált Ügyfél (vagy saját maga) részére bocsát ki új Tanúsítványt és magánkulcsot, annak egy már létező tanúsítványát alapul véve. Az új tanúsítványban a végfelhasználó nyilvános kulcsa megváltozik. Lásd a 4.7 fejezet.
Kulcsletét szolgáltatás	Olyan szolgáltatás, amely a végfelhasználó magánkulcsának megőrzését és annak végfelhasználó számára történő átadását biztosítja (arra az esetre, ha a végfelhasználó kulcs elveszne, megsemmisülne vagy más okból használhatatlanná válna).
Magánkulcs	A szolgáltató vagy ügyfél által generált kulcspár egyik kulcsa, amit végfelhasználó kezel. Lásd nyilvános kulcs. Amennyiben a nyilvános kulcs aláíró vagy bélyegző tanúsítványba kerül, akkor megfelel az eIDAS elektronikus aláírás létrehozásához használt adat és elektronikus bélyegző létrehozásához használt adatok definíciójának.
Minősített Aláírás / Bélyegző Létrehozó eszköz	Olyan kriptográfiai eszköz, amely minősített aláírás / bélyegző létrehozására alkalmas (lásd még 1.6.2. Rövidítések, QSCD).

Minősített tanúsítvány	Olyan tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel az eIDAS Annex I, III vagy IV részének vagy a 1999/93/EC direktívának, attól függően, hogy a tanúsítvány kiadásakor melyik volt hatályban.
Minősített weboldal hitelesítő tanúsítvány	Az eIDAS 3. cikk 39. Pontja szerint: “Olyan weboldal-hitelesítő tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel az eIDAS IV. mellékletben megállapított követelményeknek.” Olyan minősített tanúsítvány, amely a benne megjelölt weboldalak hitelesítésével biztosítja az oldal látogatóit, hogy a mögött egy valódi és legitim szervezet áll.
Mobil Regisztrációs Munkatárs	Olyan regisztrációs ügyintéző, aki - amennyiben személyes találkozó szükséges - az Igénylő azonosítását - ilyen irányú igénye esetén - az Igénylővel egyeztetett helyen és időben végzi el.
NL Sign szolgáltatás	Biztonságos központi kulcstárolási (menedzselt SCD) és kulcsmenedzsment-szolgáltatás, mely webes felületen keresztül feltöltött dokumentumok elektronikus aláírását/bélyegzését (és időbélyegzését) teszi lehetővé. Az NL Sign szolgáltatás keretében használható tanúsítványok igénylése és az ehhez szükséges regisztrációs adatok bekérése valamint a tanúsítvány kibocsátását követően annak használatba vétele az NL Sign szolgáltatás webes felületein történik.
Nyilvános kulcs	A szolgáltató vagy ügyfél által generált kulcspár egyik kulcsa, amit szolgáltató az általa létrehozott tanúsítványban helyez el. Lásd magánkulcs.
Permanens azonosító	Olyan azonosító, mely a tanúsítvány birtokosát egyedileg azonosítja. A tanúsítványban történő megvalósítása az RFC 4043 alapján történik. Lehet szolgáltató által képzett, vagy hivatalos nyilvántartásban szereplő egyedi azonosító adat. A szolgáltató által képzett azonosító egy OID, ami két részből áll: a Szolgáltató (1.3.6.1.4.1.3555) és az Ügyfél egyedi azonosítójából, ami ezt követi. Az Ügyfél egyedi azonosítója 5-tel kezdődik, amelyet egy szám követ, ami a következő értékeket veheti fel: ● 1,6,8,10: személyes vagy üzleti tanúsítványok esetén, amikor az azonosító a természetes személy adataiból képzett. ● 2,7,9,11: szervezeti tanúsítványok esetén, amikor az azonosító a szervezet adataiból képzett. Alkalmazása esetén a tanúsítvány Subject/SerialNumber mezőjébe kerül.
Regisztráció	Kezdeti azonosítási eljárás, amelyet Szolgáltató Igénylő és Előfizető személyazonosságának megállapítására, eljárási joguk ellenőrzésére, valamint adatainak felvételére végez.
Regisztrációs egység	A Szolgáltató azon egysége, amely a szolgáltatások igénylésének feldolgozását, az Igénylő és Előfizető regisztrációját, valamint tanúsítványszolgáltatás esetén a tanúsítványba kerülő adatok ellenőrzését végzi. Létezhet a Szolgáltatón belül (mint belső szervezeti egység) vagy kívül (Kihelyezett Regisztrációs Egység) egyaránt.
Regisztrációs felelős	Bizalmi munkakör. Lásd az 5.2.1 Bizalmi munkakörök fejezetet.
Regisztrációs (validációs és visszavonási) ügyintéző	Szolgáltató bármely Regisztrációs Egységén belül e munkakörben dolgozó munkatársak feladata a tanúsítványigénylések kezelése, Igénylő és Előfizető azonosítása és a tanúsítványigénylésben megadott adatok valódiságának ellenőrzése (lásd 4.2.1 fejezet) valamint a visszavonási igények feldolgozása és végrehajtása (4.9). A Szolgáltató kihelyezett regisztrációs egységeinek regisztrációs ügyintézői a fenti feladatok közül azokat látják el, melyek elvégzésére az egység üzemeltetéséről szóló partnerszerződésben az egységet üzemeltető szolgáltatói partner megbízást kapott a Szolgáltatótól. Amennyiben ez nem fedi le a tanúsítvány kibocsátásához szükséges

	valamennyi ellenőrzési lépést, a fennmaradó feladatokat szükség szerint a Szolgáltató Központi Regisztrációs Egységének Regisztrációs Ügyintézői látják el. A kihelyezett regisztrációs egységek ügyintézői által végzett feladatokat a Szolgáltató Központi Regisztrációs Egységének Regisztrációs felelőse véletlenszerű minatvétel alapján időszakonként utólagosan ellenőrzi. Weboldal-hitelesítő tanúsítványok esetén a tanúsítványba kerülő domain név vagy nevek ellenőrzését minden esetben Szolgáltató Központi Regisztrációs Egységének regisztrációs ügyintézői végzik. Jelen szolgáltatói szerepkör megegyezik a BRG 1.6.1-ben meghatározott „Validation Specialists" fogalmával: az a személy, aki az adatellenőrzési eljárásokat végzi.
SSL tanúsítvány	Weboldal-hitelesítő tanúsítvány
Server Signing Application Service Component (SSASC)	A Szolgáltató olyan szolgáltatási komponense, amely aláíró szervezalkalmazással az Alany nevében készít elektronikus aláírást vagy bélyegzőt. A Szolgáltató a NETLOCK Sign szolgáltatás kulcsmenedzmsent szolgáltatása keretében alkalmaz SSASC-t.
Server Signing Application Service Component Policy (SSASC Policy)	Az SSASC alkalmazására vonatkozó előírások és ajánlások. Jelen szabályzat keretében – a NETLOCK Sign szolgáltatás kulcsmenedzmsent szolgáltatása vonatkozásában – az NSCP és az EUSCP policy-k alkalmazandók. Lásd 1.2.1.
Szabályzatok	Jelen Szolgáltatási Rend és a Szolgáltatási Szabályzat együttes említése.
Szervezet	Tanúsítvány alanya vagy előfizetője tekintetében: jogi személy vagy egyéni vállalkozó vagy egyéni ügyvéd.
Szoftveres tanúsítvány	Olyan tanúsítvány, aminek magánkulcsa nem Kriptográfiai eszközre kerül kiadásra.
Szolgáltatás	Jelen szabályzat keretén belül Szolgáltató bizalmi szolgáltatásai (lásd 1.1 fejezet).
Szolgáltatási Szabályzat, Szabályzat	Szolgáltatási Szabályzat Nem Minősített Tanúsítványszolgáltatásokra. A bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről (lásd DÁP), mely Szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmaz.
Szolgáltatási szerződés	Szolgáltató és Ügyfél között létrejött szerződés, amely a szolgáltatás nyújtására és igénybevételére vonatkozó feltételeket tartalmazza. Megkötése a szolgáltatás igénybevételének előfeltétele.
Szolgáltató	Jelen Szolgáltatási rend szerinti szolgáltatásokat nyújtó NETLOCK.
Szolgáltató szabályzatai	Jelen Bizalmi Szolgáltatási Rend, a Bizalmi Szolgáltatási Szabályzat, az ÁSZF, a szolgáltatási szerződés, a Szolgáltatási kivonat. Valamint egyéb nem nyilvános szabályzatok.
Szolgáltatói partner	Olyan a szolgáltatótól független, önálló természetes vagy jogi személyek, amelyek a Szolgáltatóval való megállapodás alapján a Szolgáltatás nyújtásában részt vesznek.
Szolgáltatói rendszer	Szolgáltató szolgáltatásnyújtást végző rendszereinek együttese.
Szolgáltatói tanúsítvány	Szolgáltató azon tanúsítványai, amelyeket a szolgáltatásnyújtás érdekében használ (pl. Kiadók és Időbélyegző Kiszolgálók tanúsítványai).

Tanúsítvány	Szolgáltató által kibocsátott hiteles igazolás, amely a nyilvános kulcsot az Alanyhoz kapcsolja, és igazolja e Tanúsítványban közzétett adatok valódiságát.
Tanúsítványaktiválás	Az az állapotváltoztatási eljárás, amely felfüggesztett tanúsítvány érvényességét visszaállítja. Aktiválása után a tanúsítvány visszamenőlegesen, azaz a felfüggesztés időtartamára is újra érvényessé válik, mintha a felfüggesztés meg sem történt volna..
Tanúsítványállapot	A szolgáltató által a tanúsítványok érvényességi ideje alatt nyilvántartott érvényes / visszavont / felfüggesztett státusza, amelyről a tanúsítványvisszavonási listán és a Tanúsítványállapot szolgáltatáson keresztül ad tájékoztatást Ügyfelei és az Érintett felek részére.
Tanúsítványállapot-szolgáltatás (OCSP)	Olyan szolgáltatás, ami egy adott tanúsítvány állapotáról ad valós idejű információt az érintett felek számára. Lásd még: tanúsítványvisszavonási lista.
Tanúsítványfelfüggesztés	Az az állapotváltoztatási eljárás, amelyben a Szolgáltató egy még érvényes Tanúsítvány érvényességét átmenetileg megszünteti az eredetileg tervezett érvényességi idő vége előtt. A tanúsítványfelfüggesztés egy átmeneti állapot, a felfüggesztett Tanúsítvány visszavonható, vagy a Tanúsítvány eredeti érvényességi idejében újra érvényessé tehető. A felfüggesztés visszavonása esetén a Tanúsítvány visszamenőleges hatállyal érvényessé válik, mintha a felfüggesztés meg sem történt volna.
Tanúsítványigénylés	Az a folyamat, amikor Igénylő tanúsítványt igényel, azaz a tanúsítvány elkészítéséhez szükséges adatokat megadja és igazolja a Szolgáltatónak, végül pedig Szolgáltatási szerződés Igénylő és - amennyiben nem egyezik Igénylővel - Előfizető általi aláírásával hitelesíti kérelmét az igényelt tanúsítványra vonatkozóan és ezzel felhatalmazza Szolgáltatót az igényelt tanúsítvány kibocsátására.
Tanúsítványkezelési eljárás	Olyan eljárás, ami új tanúsítvány kibocsátását eredményezi egy meglévő tanúsítvány illetve korábbi ügyfél-regisztráció adatai alapján (lásd 3.3 Azonosítás és hitelesítés tanúsítványkezelési eljárás során és 4. Életciklus követelmények fejezeteket).
Tanúsítványszolgáltatás	Szolgáltató azon szolgáltatása, amelynek keretén belül új tanúsítványt állít elő. Ez történhet egy már létező tanúsítvány alapján (követő kibocsátás tanúsítványkezelési eljárással) vagy ilyen előzmények nélkül (eredeti kibocsátás).
Tanúsítványmegújítás	Az a folyamat, amikor a Szolgáltató ugyanarra a nyilvános kulcsra, változatlan Alannyal egy új Tanúsítványt állít ki, új érvényességi időszakra. Lásd a 4.6 fejezet.
Tanúsítványmódosítás	Az a folyamat, amikor a Szolgáltató egy már regisztrált Igénylő részére bocsát ki új Tanúsítványt egy korábban kibocsátott Tanúsítványa alapján, az abban szereplő nyilvános kulccsal, de megváltozott Alany vagy Szolgáltató adatokkal. Lásd a 4.8 fejezet.
Tanúsítványtár	Szolgáltató kibocsátott tanúsítványokat tartalmazó nyilvántartása, amelyen keresztül lekérdezhetők a szolgáltató által kiadott nyilvános tanúsítványok és a Tanúsítványvisszavonási lista.
Tanúsítványtípus	Szolgáltató által kibocsátott különböző tanúsítványok megkülönböztetése valamilyen jellemző szerint, legfőképpen a felhasználási cél alapján. Lásd a Szolgáltatási szabályzat 1.2.1 pontját.
Tanúsítvány-visszavonás	Az az állapotváltoztatási eljárás, amelyben a Szolgáltató a tanúsítvány érvényességét megszünteti az eredetileg tervezett érvényességi idő lejárta előtt. A tanúsítvány-visszavonás visszafordíthatatlan és végleges állapotváltozást jelent, a visszavont tanúsítvány a visszavonás időpontjában érvényességét veszti, s már soha többé nem

	lehet újra érvényes.
Tanúsítványvisszavonási lista (CRL)	Szolgáltató által rendszeres időközönként, valamint állapotváltozások hatására a Tanúsítványtárban közzétett hiteles lista azon tanúsítványokról, amelyek ideiglenesen vagy véglegesen nem érvényesek. A listán szereplő tanúsítványok elfogadása, illetve alkalmazása nem ajánlott. A 24/2016. BM rendelet 17. szerinti visszavonási nyilvántartás egy fajtája.
Teszttanúsítvány	A Szolgáltató által tesztelési célra kibocsátott tanúsítvány, ami tartalmában valamely valódi tanúsítvánnyal egyezik meg, de hitelesítési rend mezője és az Alany elnevezése jelzi a felhasználás teszt voltát. Az ilyen tanúsítványok köztelezettségvállalásra nem használhatók, joghatás nem kapcsolódik hozzájuk, elfogadásuk csak tesztelési céllal lehetséges. Szolgáltató nem vállal felelősséget az ilyen tanúsítványok adattartalma, felhasználása, és a hozzájuk kapcsolódó szolgáltatások rendelkezésre állása tekintetében.
UCC weboldal-hitelesítő tanúsítvány	Olyan weboldal-hitelesítő tanúsítvány, melyben több különböző domain név kerül feltüntetésre (a SubjectAltName/DNSname mezőben).
Ügyfélmenü	A Szolgáltató ügyfelei számára a tanúsítványokkal és hozzájuk kapcsolódó szolgáltatásokkal kapcsolatos különböző igénylések elvégzésére illetve a folyamatban lévő igénylések állapotának megtekintésére biztosított, a Szolgáltató weboldalán keresztül elérhető felület, melybe egyedi felhasználónév és jelszó megadásával lehet belépni (ügyfélmenü regisztrációt követően). A minősített tanúsítványok kezeléséhez a minősített ügyfélmenübe, a nem-minősített tanúsítványok kezeléséhez a fokozott biztonságú ügyfélmenübe kell regisztrálni és bejelentkezni.
Ügyfélmenü regisztráció	Az a folyamat, amikor egy természetes vagy jogi személy adatai megadásával létrehozza saját Ügyfélmenüjét, illetve az Ügyfélmenübe való bejelentkezéshez szükséges bejelentkező nevét és jelszavát.
Ügyfél	A Szolgáltatatóval szerződést kötő fél. Tanúsítványszolgáltatás esetén a tanúsítvány Igénylője és Előfizetője (adott esetben ezek a szereplők meg is egyeznek). NL Sign szolgáltatás esetén az Aláírói Partner és a Végfelhasználó. Lásd még az 1.3.3 Előfizető, Végfelhasználó és Igénylő fejezetet
Ügyféleszköz	Az Ügyfél kezelésében lévő Kriptográfiai eszköz. Ügyféleszköz kizárólag a Szolgáltató által beszerzett, ellenőrzött és az Ügyfél rendelkezésére bocsátott, a Szabályzat 6.2.1 pontjában meghatározott Kriptográfiai eszköz lehet.
Ügyfél-regisztráció	Természetes és nem természetes személyek azonosítása, adataik ellenőrzése és rögzítése az első szolgáltatási szerződés és az első tanúsítványkibocsátás megelőzően. Lásd a 3.2 Kezdeti azonosítás fejezetet.
Végfelhasználó	Az a természetes személy, aki a tanúsítványban szereplő nyilvános kulcs magánkulcs párja felett rendelkezik (kizárólagosan használja vagy a használatáért felelős). NL Sign szolgáltatás esetén az a személy, aki az aláírási szolgáltatás keretén belül a magánkulcsa aktiválásával elektronikus aláírási/bélyegző műveletet hajt végre vagy aki e műveletekért felelős. Lásd még az Ügyfél és Előfizető entitásokat, valamint az 1.3.3 Előfizető,

	Végfelhasználó és Igénylő fejezetet.
Végfelhasználói tanúsítvány, Végfelhasználói kulcs	Az Előfizetők tanúsítványát és kulcsát jelöli, megkülönböztetve a Szolgáltató saját tanúsítványaitól és kulcsaitól.
Weboldal-hitelesítő tanúsítvány	Az eIDAS 3. cikk 38. pontja szerinti tanúsítvány.
Wildcard weboldal-hitelesítő tanúsítvány	Olyan weboldal-hitelesítő tanúsítvány, melyet több aldomain hitelesítésére bocsátott ki szolgáltató (a domain név *.domain.hu formában kerül feltüntetésre, így magában foglalja a domain.hu cím alá tartozó valamennyi aldomaint).

1.6.2 Rövidítések

Hivatkozott jogszabályok rövidítései

eIDAS	Az Európai Parlament és Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről.
DÁP	A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény.
Nytv.	A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény.
Szmtv.	2007. évi I. törvény a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról.
Harmtv.	2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló törvény
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
BM rendelet	A bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI. 30.) BM rendelet.

Műszaki szakkifejezések rövidítései

ASN.1	Abstract Syntax Notation 1
CA	Certification Authority Kiadó
CAA	Certification Authority Authorization

	Bizalmi szolgáltató Felhatalmazás
IP	Internet Protocol
IT	Information Technology
BRG	Baseline Requirements Guidelines
CAB Forum	CA/Browser Forum
CP	Certificate Policy Hitelesítési Rend
CPS	Certification Practice Statement
CRL	Certificate Revocation List Tanúsítványvisszavonási lista
CSP	Certification Service Provider
EAL	Evaluation Assurance Level
EV	Extended Validation
EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
FQDN	Fully qualified domain name
gTLD	Generic top-level domain
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
LSCP	Lightweight SSASC Policy
OCSP	Online Certificate Status Protocol Tanúsítványállapot-szolgáltatás
OID	Object Identifier Azonosító
OVC	Organizational Validation Certificate
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SAN (SubjectAltName)	Subject Alternative Name
SSASC	Server Signing Application Service Component
SCP	Service Component Policy
SCD	Signature / Seal Creation Device Aláírás / Bélyegző Létrehozó eszköz (nem-minősített)
SSL	Secure Socket Layer
TLS	Transport Layer Security

TSP	Trust Service Provider Bizalmi Szolgáltató
QSCD (Korábbi nevén SSCD)	Qualified Signature / Seal Creation Device Minősített Aláírás / Bélyegző Létrehozó eszköz
UN	United Nations
IETF	Internet Engineering Task Force
QC	Qualified Certificate
URL	Uniform Resource Locator

Lásd még a dokumentum 9.15 pontjában foglaltakat.

2. KÖZZÉTÉTEL ÉS TANÚSÍTVÁNYTÁR

Szolgáltató az alábbiak szerint teszi közzé a tanúsítványokra vonatkozó különböző információkat (tanúsítványok, érvényességi információk, szabályzatok és egyéb kikötések).

2.1 Adattárak

Szolgáltató nyilvános tanúsítványtárat és tanúsítványvisszavonási információkat (CRL, OCSP) közlő rendszereket tart fenn, a jelen Szolgáltatási Szabályzat alapján kibocsátható tanúsítványokhoz kapcsolódó Kikötéseket és feltételeket pedig letölthető PDF formátumban teszi közzé weboldalán (lásd 1.1.2).

2.1.1 A tanúsítványokra vonatkozó információk közzététele

Szolgáltató a tanúsítványvisszavonási információkat (CRL, OCSP) HTTP protokollon keresztül szolgáltatja Ügyfelek és Érintett felek számára, legalább éves 99%-os rendelkezésre állással, úgy, hogy az eseti szolgáltatás kiesés hossza pedig egyszerre legfeljebb 3 óra lehet.

A nyilvános tanúsítványtárat Szolgáltató a weboldalán keresztül, HTTPS protokollon keresztül teszi elérhetővé – a nyilvános tanúsítványtárban azon végfelhasználói tanúsítványok alany adatait teszi közzé, melyek ügyfelei a szolgáltatási szerződésben hozzájárultak a közzétételhez. A nyilvános tanúsítványtárban közzétett tanúsítványok bárki számára letölthetők.

Szolgáltató weboldalakat tart fenn a visszavont, lejárt és érvényes weboldal-hitelesítő tanúsítványokkal (OVCP és EVCP) való ellenőrzéshez (teszteléshez).[8]

Szolgáltató weboldalain keresztül lekérdezhetők a tanúsítványtár szolgáltatói tanúsítványai, valamint azon érvényes végfelhasználói tanúsítványok, amelyek közzétételéhez az Ügyfél hozzájárult (lásd 4.4.2 fejezet).

A Szolgáltató az egyes tanúsítványok nyilvánosságra hozatala kapcsán a következő eljárást követi:

- A Kiadók és Időbélyegző Kiszolgálók tanúsítványait Internetes weboldalán teszi közzé (1.1.2 pont)
- Az érvényes végfelhasználói tanúsítványokat a kibocsátást és – amennyiben értelmezett – az aktiválást követően haladéktalanul megjeleníti a nyilvános tanúsítványtárban.
- Szolgáltató teszttanúsítványok kibocsátásával biztosítja, hogy az általa kibocsátott minden tanúsítványtípust ki lehessen próbálni (lásd a 7.1 fejezet).

A Szolgáltató a tanúsítványokkal kapcsolatos állapotinformációkat a következő módszerekkel teszi közzé:

- A Szolgáltató által kibocsátott végfelhasználói tanúsítványokkal, valamint a szolgáltatói tanúsítványokkal kapcsolatos állapotinformációk a tanúsítványállapot-szolgáltatás keretén belül az állapotváltozást követően azonnal elérhetőek.
- A tanúsítványok állapotára vonatkozó információk tanúsítványvisszavonási listákon (CRL) is megjelennek. A visszavonási listák szolgáltató Internetes weboldalán lekérdezhetők, valamint http protokollon keresztül elérhetők az alkalmazások számára is.

A Végfelhasználó az Ügyfélmenübe való bejelentkezéskor a mindenkori tanúsítványai és azok aktuális állapotára vonatkozó információkat elérheti.

A KGyHSz Kiadó a saját gyökér és az általa felülhitelesített szolgáltatók tanúsítványaival kapcsolatos állapotinformációkat saját szabályzatainak megfelelően teszi közzé, melyek a jogszabályok szerint elérhetők tanúsítványtárában, e szabályzat kiadásakor a

[8] Szolgáltató e weboldalak címét közzéteszi a weboldalán (lásd 1.1.2), a technikai adatok között.

http://www.kgyhsz.gov.hu/ Internet címen.

Szolgáltató a weboldalán tájékoztatja Ügyfeleit és az Érintett feleket az egyes tanúsítványtípusok (lásd 1.1.2) kapcsán alkalmazandó eltérő kikötésekről és feltételekről.

2.1.2 Kikötések és feltételek közzététele

Jelen Szolgáltatási szabályzatot és az alapjául szolgáló Szolgáltatási Rendet Szolgáltató – a szükséges Szolgáltatóra specifikus eltérésektől eltekintve – az RFC 3647 szerinti tartalommal és struktúrában teszi közzé.

Szolgáltató weboldalán a hatálybalépés előtt publikálja a Szolgáltatási Rend és Szolgáltatási Szabályzat bevezetésre váró új verzióit valamint az Általános Szerződési Feltételek jelen szabályzat szerinti szolgáltatásokra vonatkozó módosítással érintett új verzióit. A hatályos dokumentumok mellett a weboldalon folyamatosan elérhetők azon korábbi verziók is, melyek alapján kibocsátott tanúsítvány még érvényben van.

Szolgáltató a szolgáltatási szerződés megkötését követően, a tanúsítvány kibocsátásakor a Szolgáltatási Szabályzatot és a szolgáltatási szerződést PDF formátumban megküldi Igénylőnek e-mailhez csatolva, mely a hatályos magyar jogszabályok értelmében tartós adathordozónak tekinthető.

2.1.3 Nyilatkozatok

BRG nyilatkozat

A NETLOCK megfelel a “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” dokumentum aktuális a http://www.cabforum.org oldalon publikált verziójának. Eltérés esetén az OVCP tanúsítványok esetében a Baseline dokumentum a mérvadó.

EVCG nyilatkozat

A NETLOCK megfelel a “CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates” dokumentum aktuális a http://www.cabforum.org oldalon publikált verziójának. Eltérés esetén az EVCP tanúsítványok esetében a EVCG dokumentum a mérvadó.

2.2 A közzététel időpontja és gyakorisága

Szolgáltató a Szolgáltatási Szabályzatot új verziójának hatálybalépése előtt legalább 30 nappal nyilvános tervezetként weboldalán közzéteszi, hogy azt Ügyfelei és az Érintett felek megismerhessék és hatálybalépése előtt észrevételeket tehessenek Szolgáltató felé a tervezettel kapcsolatban (lásd az 1.5.2 A dokumentum kapcsolattartó személye és a 9.12.1 A módosítási eljárás fejezetek).

Szolgáltató Szabályzatelfogadó Egysége évente legalább egyszer felülvizsgálja a Szolgáltatási Szabályzatot és a Szolgáltatási Rendet és szükség esetén módosítja azokat (lásd 9.12).

Jelen Szabályzattal kapcsolatos új verziók közzététele a 9.12 fejezetben ismertetett eljárásoknak megfelelően történik. A Szolgáltatási Szabályzat új verzióinak közzététele tekintetében szintén lásd a 9.12 fejezetet.

Szolgáltató egyéb szabályzatai és szerződéses feltételei, illetve ezek újabb változatai szükség esetén kerülnek kibocsátására.

Szolgáltató a rendkívüli információkat – amikor arra szükség van – a jogszabályi előírásoknak megfelelően, ennek hiányában késlekedés nélkül közzéteszi.

A Hitelesítő és Időbélyegző Kiadók tanúsítványai legkésőbb a szolgáltatás megindításakor kerülnek közzétételre.
A tanúsítványvisszavonási listák kibocsátási gyakoriságával kapcsolatosan lásd a 4.9.7 fejezetet.

2.3 Tanúsítványtár elérésének szabályai

A Szolgáltató által közzétett kikötések és feltételek, rendkívüli információk, tanúsítványok és állapotinformációk nyilvános információk. Olvasás céljából bárki elérheti ezeket az információkat, a közlő közegek sajátosságainak megfelelően.

Szolgáltató tanúsítványtára szabványos HTTP és HTTPS protokollokkal is elérhető.

A tanúsítványtár elérhetőségét Szolgáltató folyamatosan (az év minden napján, 0–24h) biztosítja a karbantartáshoz szükséges idők kivételével. A Szolgáltató a tervezett karbantartásokat lehetőség szerint munkaidőn kívüli időszakokra ütemezi. A tanúsítványtár kizárólag szolgáltató weboldalán keresztül érhető el szabályosan, egyedi manuális lekérdezések keretében. Más jellegű (pl. automatizált) lekérdezés csak szolgáltató írásbeli engedélyével lehetséges.

Az online szolgáltatások (tanúsítványtár, OCSP) nem rendelkeznek hozzáférési korlátozással, de a túlzott használat esetén szolgáltatásvédelmi okokból egy határ átlépése esetén korlátozhatók a kérések. A korlátozások feltételei közzétételre kerülnek a Szolgáltató weboldalán.

A szolgáltatások rendelkezésre állása tekintetében lásd a 2.1.1 és a 4.9.9 fejezetet.

3. AZONOSÍTÁS ÉS HITELESÍTÉS

A végfelhasználói nem-minősített tanúsítványok kibocsátásával kapcsolatban előírt, illetve a szolgáltatási szerződés megkötéséhez szükséges Ügyfélazonosítási és adatellenőrzési eljárások részleteit az alábbi alfejezetek tartalmazzák.

3.1 Elnevezések

A Szolgáltató által kibocsátott tanúsítványok Kibocsátó azonosító (Issuer) és Alany azonosító (Subject) mezői megfelelnek az ITU-T X.509 és az RFC 5280 és az ETSI EN 319 412 ajánlások név formátum előírásainak.

A tanúsítványokban található Alany mezőkben (Subject és SAN) feltüntetett adatok azonosítják azt az entitást, amely a tanúsítványba foglalt nyilvános kulcshoz tartozó magánkulcsot birtokolja, azaz aki számára a tanúsítvány ki lett bocsátva. Az Alany mezők több különböző azonosítót tartalmaznak, az alábbi tartalommal.

Az adat neve és azonosítója (Szabványos név, OID azonosító, magyar név)	**Tartalom**
Subject mező	
CN id-at-commonName 2.5.4.3 Név	Személyes és üzleti tanúsítvány esetén az Igénylő természetes személy teljes nevét tartalmazza, az adatforrásban szereplő formában.
	Szervezeti tanúsítvány esetén a szervezet teljes vagy rövidített neve / DBA / Trademark / Termékazonosító DBA esetén tartalma lehet: 1. Cégformát nem tartalmazó cégnév Az ellenőrzött cégnév hosszú vagy rövid neve szerepelhet benne, a cégforma (Kft, Bt. stb.) megjelölése nélkül. 2. Domain név 3. Termék azonosító Terméknév amit egy cégnév/DBA/Trademark előz meg.
	Álneves tanúsítvány esetén a pseudonym mezővel egyező tartalmú.
	Weboldal-hitelesítő (OVCP, EVCP) tanúsítvány esetén a weboldal neve A commonName csak egy FQDN-t tartalmazhat, aminek a SAN/DNSName mezőben szintén szerepelnie kell.
SN Id-at-surname 2.5.4.4 Vezetéknév	A tanúsítvány CN mezőjében megnevezett természetes személy teljes nevének vezetéknév része. A felbontás a vonatkozó MELASZ ajánlás alapján kerül elvégzésre.

G id-at-givenName 2.5.4.42 Keresztnevek	A tanúsítvány CN mezőjében megnevezett természetes személy teljes nevének keresztnév része. A felbontás a vonatkozó MELASZ ajánlás alapján kerül elvégzésre.
Id-at-pseudonym 2.5.4.65 Pseudonym	Az álnevet az Igénylő választja, a Szolgáltató az álnevet nem ellenőrzi, az Előfizető az esetleges álnévvel kapcsolatos (szerzői jogi stb.) problémákért maga felel. Álneves tanúsítványt a Szolgáltató az álneves tanúsítványprofil szerint bocsátja ki, amelyben a „CN=CommonName” és „Pseudonym” mezők egyező módon tartalmazzák az álnevet, s az álnév mellett jogi/természetes személy nem tüntethető fel.
id-at-serialNumber 2.5.4.5 Sorozatszám	A tanúsítvány CN mezőjében megnevezett természetes/jogi személyhez tartozó globálisan egyedi sorozatszám.
id-at-countryName 2.5.4.6 Ország	Előfizető székhelye vagy lakhelye szerinti ország. ISO 3166-1 szerinti kétbetűs országkód.
L id-at-localityName 2.5.4.7	Előfizető székhelye, telephelye vagy lakhelye szerinti város
id-at-stateOrProvinceName 2.5.4.8	Előfizető székhelye vagy lakhelye szerinti megye, vagy állam
id-at-organizationName 2.5.4.10	Üzleti, szervezeti és OV, EV weboldal-hitelesítő tanúsítvány esetén Előfizető szervezet teljes vagy rövidített neve
id-at-organizationalUnitName 2.5.4.11	Üzleti és szervezeti tanúsítvány esetén Előfizető szervezeten belüli szervezeti egységének a neve. A tanúsítványba foglaláshoz Előfizetőnek igazolnia kell a létezését.
organizationIdentifier 2.5.4.97	Üzleti, szervezeti és OV, EV weboldal-hitelesítő tanúsítvány esetén Előfizető nyilvántartásban szereplő adóazonosító száma, az ETSI EN 319 412-1 által meghatározott szemantikus formában. Egy hivatalos nemzeti vagy más azonosító rendszerben kapott egyedi azonosítót tartalmazhat kötött formátumban, az alábbiak szerint: 1. Ha a szervezet rendelkezik adószámmal, akkor VAT előtag, majd a szervezetet bejegyző ország kódja, kötőjel, és az szervezet adószáma változatlan formában. Magyar szervezet

	esetén a „VATHU-„ előtagot követheti belföldi vagy a “VATEU-” előtagot közösségi adószám változatlan formában. 2. Ha előző pont nem alkalmazható, akkor Cégjegyzékszám kerül feltüntetésre "NTRHU-" előtagot követve. 3. Ha előző pontok nem alkalmazhatók, akkor nemzeti bejegyzett séma alapján "XX:HU" értékkel, amelyben az „XX” a nemzeti vagy EU-s azonosítási séma két karakteres jelölése. 4. Ha előző pontok nem alkalmazhatók, akkor más egyedi hivatalos azonosító kerül alkalmazásra 5. Ha egyik említett azonosító sem áll rendelkezésre, az alapító okirat azonosítója és az alapító jogszabály megnevezése is kerülhet ide. Más országok azonosítórendszerei esetében a Szolgáltató az ISO 3166 szerinti országkódokat alkalmazza.
Id-at-title 2.5.4.12 Titulus	Üzleti tanúsítvány esetén Igénylő beosztása vagy titulusa Előfizető szervezetén belül. Opcionális.
subject/EMAIL	Tartalma megegyezik a SubjectAlternateName:emailaddress mezővel.
SAN mező	
SAN SubjectAlternateName:DNSName	Weboldal-hitelesítő tanúsítvány esetén Egy vagy több domain nevet tartalmaz Ha a CN DNS bejegyzést tartalmaz, az itt is szerepel.
SAN SubjectAlternateName:emailaddress	A CN-ben megadott entitáshoz igazoltan tartozó email cím RFC 822 előírásai szerint Weboldal-hitelesítő tanúsítvány esetén nem szerepel.
SAN SubjectAlternateName:otherIdentifier	Szolgáltató egyedi azonosítója (mely a permanens azonosító szolgáltatói részével megegyezik).

A tanúsítvány fenti Alany (Subject és SAN) mezőinek kitöltésére vonatkozó tanúsítványprofilonként eltérő előírásokat és a Kibocsátó (Issuer) mező tartalmát a lásd a 7.1 fejezetben.

3.1.1 Névtípusok

Szolgáltató a tanúsítványok Subject mezőinek képzése esetén az RFC 5280 szabványnak megfelelően az X.500 distinguished name előírásait követi. Szolgáltató az alábbi névtípusokat különbözteti meg a végfelhasználói tanúsítványok esetén, s hozzájuk az alábbi profilokat kapcsolja:

Névtípus (Alany típusa)	**Tanúsítványprofil**
Természetes személy	Személyes
Jogi személy	Szervezeti

DBA / Trademark / Termékazonosító és jogi személy együttesen	Szervezeti
Álneves	Álneves
Természetes és jogi személy együttesen	Üzleti
Weboldal és DBA / Trademark együttesen	OV SSL
Weboldal és jogi személy együttesen	OV és EV weboldal-hitelesítő tanúsítvány

A tanúsítványprofilok leírását lásd a jelen Szabályzat 7. fejezetében.

3.1.2 A nevek értelmezhetősége

Természetes személyek számára kibocsátott aláíró tanúsítvány *Subject* mezője a következő adatot tartalmazza kötelezően:

- commonName (Név)
- givenName és surName vagy pseudonym (Vezeték és Családnév)
- countryName (Országkód)
- serialNumber (Alany egyedi azonosítója)
- emailAddress (E-mail cím);

Jogi személyek számára kibocsátott bélyegző és weboldal-hitelesítő (OVCP és EVCP) tanúsítvány *Subject* mezője a következő adatot tartalmazza kötelezően:

- commonName (Név)
- countryName (Országkód)
- localityName (Város)
- organizationName (Szervezet neve)
- organizationIdentifier (szervezetazonosító).

Amennyiben a tanúsítvány Alanyaként kizárólag jogi személy kerül feltüntetésre, Szolgáltató minden esetben feltünteti a szervezet egyedi azonosítóját a tanúsítvány Subject/organizationIdentifier mezőjében.

Amennyiben a tanúsítvány Alanyaként természetes személy és szervezet egyaránt feltüntetésre kerül (üzleti tanúsítványprofil, lásd 7.1), a Szolgáltató abban az esetben nem tünteti fel kötelezően a szervezet egyedi azonosítóját a tanúsítvány Subject/organizationIdentifier mezőjében, ha a tanúsítvány igénylője ügyvéd vagy ügyvédi iroda – egyéb esetben a szervezetazonosító kötelezően feltüntetésre kerül.

A weboldal-hitelesítő (OVCP és EVCP) tanúsítványok SAN mezője kötelezően tartalmazza a commonName mezőben feltüntetett domain nevet is, valamint UCC tanúsítvány esetén a további domain neveket.

A Subject mezőre vonatkozó részletes leírást a 3.1 tartalmazza.

A tanúsítványban szereplő természetes és jogi személy nevét a Szolgáltató közhiteles nyilvántartásban, annak hiányában hivatalos azonosító dokumentumban ellenőrzi, s az azokban szereplő írásmóddal azonosan tünteti fel.

Amennyiben *Subject/Serialnumber* mező tartalma egy hivatalos (okmány alapján ellenőrzött) nemzeti azonosító, akkor annak kötelező formátuma: <REF>HU-<igazolványszám>, ahol a <REF> helyére három karakter kerül a következők szerint:

1. "PAS" útlevélszám esetében (pl. PASHU-AE123456)
2. "IDC" személyazonosító igazolvány vagy vezetői engedély számának esetén (pl. IDCHU-123456AB (személyazon. ig.) vagy IDCHU-AB123456 (vezetői engedély))
3. "TIN" adóazonosító jel esetében (pl. TINHU-1234567890)

Egyedi azonosítórendszerek esetén a <REF> helyére „XX:" formátumú karaktersorozat kerül, amelyben az „XX" a nemzeti vagy EU-s azonosítási séma két karakteres jelölése (pl. EI:HU-200007292386 vagy AT:EU-BH16251).

Amennyiben a tanúsítvány több serialnumber értéket tartalmaz, a további serialnumber mezőkre nincs formai előírás - amennyiben azok nem a fenti igazolványok alapján kerülnek.

A tanúsítvány azonosító mezői („Subject" és „Issuer") az X.500 egyedi névformátum előírásainak felelnek meg. A „*Subject*" és „*Issuer*" mezőre vonatkozó további szabályok:

- A tanúsítványban az adatok speciális és vezérlő karakterek nélkül szerepelnek.
- A nevek alapértelmezetten tanúsítványban az alábbiak szerint kerülnek feltüntetésre: a személyazonosság igazolására a hatósági igazolványban foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve a CN, SN és G mezőkben az UTF-8 kódolást használva. A nevek egyes egységeit szóköz választja el.
- A tanúsítványban a vonatkozó szabványok szerinti meghatározott maximális karakterszámot meghaladó elnevezések esetén rövidítés használata lehetséges.

A Subject/organizationIdentifier mezőben egy hivatalos nemzeti vagy más azonosító rendszerben kapott egyedi azonosító szerepelhet kötött formátumban, amelyet az ETSI EN 319 412-1 5.1.4 definiál (*REFCO-szervezetazonosító* formában szerepel, ahol a REF és CO helyére három és két karakter kerül az alábbiak szerint).

Kitöltése:

1. Ha a szervezet rendelkezik adószámmal, az alapján kell kitölteni a mezőt: magyar adószám esetén "VATHU", EU-s adószám esetében "VATEU" értékkel.
2. Ha előző pont nem alkalmazható, akkor Cégjegyzékszámmal "NTRHU" értékkel.
3. Ha előző pontok nem alkalmazhatók, akkor nemzeti bejegyzett séma alapján "XX:HU" értékkel, amelyben az „XX" a nemzeti vagy EU-s azonosítási séma két karakteres jelölése.
4. Ha előző pontok nem alkalmazhatók, akkor más egyedi hivatalos azonosító is alkalmazható.
5. Ha egyik említett azonosító sem áll rendelkezésre, az alapító okirat azonosítója és az alapító jogszabály megnevezése is kerülhet ide.

Más országok azonosítórendszerei esetében az ISO 3166 szerinti országkód alkalmazandó a HU országkód helyett.

A teszttanúsítványok Subject mezője felveheti bármely a szolgáltató által kibocsátott tanúsítvány formáját, de a commonName mezőben minden esetben jelölésre kerül a teszt jelleg a "TEST" vagy "TESZT" felirattal, amit egyéb névadatok is követhetnek, nem megtévesztő, s valódi személlyel össze nem keverhető módon.

3.1.3 Álnevek

Az eIDAS 5 cikk (2) bekezdése, valamint a DÁP vonatkozó rendelkezései alapján Szolgáltató Álneves nem-minősített tanúsítványt is kibocsát. Álneves tanúsítványt kizárólag saját maga számára igényelheti Igénylő. Az álnevet az Igénylő választja, a Szolgáltató az álnevet nem

ellenőrzi, az Előfizető az esetleges álnévvel kapcsolatos (szerzői jogi stb.) problémákért maga felel.

Álneves tanúsítványt a Szolgáltató az álneves tanúsítványprofil szerint bocsátja ki, amelyben a „CN=CommonName” és „Pseudonym” mezők egyező módon tartalmazzák az álnevet, s az álnév mellett jogi/természetes személy nem tüntethető fel.

A Szolgáltató az Álnevet használó aláíró esetén jogerős bírósági végzés kivételével kizárólag az Ügyfél beleegyezésével adhatja át a hatóságoknak vagy bármely más harmadik személynek az Ügyfél valódi azonosságára vonatkozó adatokat. A Szolgáltató saját hatáskörében jogosult a jogi problémákba (akár valószínűsíthetően) ütköző álneves tanúsítvány kiadását megtagadni, a kiadott tanúsítványokat visszavonni.

Álneves weboldal-hitelesítő (OVCP és EVCP) tanúsítvány nem igényelhető.

3.1.4 A különböző elnevezési formák értelmezési szabályai

A Szolgáltató által kibocsátott tanúsítványoknak nem célja, hogy az Alanyként megjelölt természetes személyek, jogi személyek számára digitális igazolványként funkcionáljon, illetve hogy személyüket kizárólag a tanúsítványban feltüntetett adatok alapján azonosítani lehessen.

Az üzleti profilú tanúsítvány (lásd 7.1) önmagában képviseleti jogosultságot nem igazol. Amennyiben Szolgáltató olyan tanúsítványt bocsát ki, melynek teljes vagy részleges képviseleti jog vagy ekként is értelmezhető jogviszony igazolása is célja, ezt a jogviszonyt Szolgáltató közhiteles adatbázis vagy ennek hiányában közokirat alapján ellenőrzött tisztség feltüntetésével jelzi a tanúsítványban. A tisztséget Szolgáltató a tanúsítvány Subject/Title mezőjében tünteti fel, valamint a 7.1.8 pont alapján a tanúsítvány certificatePolicies/policyQualifier mezőjében az alábbi nyilatkozatot is feltünteti: „Szolgáltató a tanúsítvány kibocsátása előtt hiteles információk alapján ellenőrizte a Tanúsítvány Subejct/CN mezőjében feltüntetett természetes személy jogosultságát a Subejct/O mezőben megjelölt szervezet képviseletére.”

Az azonosítók értelmezése érdekében az Érintett Felek részére a jelen Szabályzatban leírtak szolgálnak tájékoztatásul (lásd különösen a 7.1.5 pont). Amennyiben az azonosító, illetve a tanúsítványban foglalt adatok értelmezésével kapcsolatban az Érintett Félnek segítségre van szüksége, akkor a Szolgáltatóval közvetlenül is felveheti a kapcsolatot (lásd 1.1.2 fejezet).

A Szolgáltató az Alany(ok) adatairól többlettájékoztatást – a tanúsítványban feltüntetett adatok értelmezését segítő információn kívül – csak az erre vonatkozó felhatalmazást adó jogszabályok alapján ad ki.

Kibocsátó azonosító

A kibocsátó azonosító úgy értelmezendő, hogy a tanúsítványt a Szolgáltató adta ki egy adott szolgáltatói (köztes/gyökér) tanúsítvány segítségével.

A szolgáltatói tanúsítvány *Issuer* mezője a tanúsítvány kibocsátójának székhely szerinti országkódját (*Country*) és városát (*Locality*), a szervezet nevét (*Organization*), szervezeti egységét (*Organization Unit*) és az adott tanúsítványt kiadó Kiadó megnevezését (*Common Name*) tartalmazza.

Alanyazonosító

A *Subject mező* úgy értelmezendő, hogy a tanúsítvány az *Organization* nevű természetes vagy jogi személyhez illetve, azon belül O*rganization-unit* szervezeti egységhez tartozó *Common Name* nevű természetes személyhez / jogi személyhez / weboldalhoz (domain név) / DBA-hoz / terméknévhez tartozik.

A természetes személy lakóhelye, illetve a szervezet székhelye vagy telephelye a *Country* (ország), a *State* (ország/megye) és a *Locality* (település) mezők szerinti helyen található. Ennél

pontosabb helymeghatározást a tanúsítvány nem tartalmaz.

3.1.5 A nevek egyedisége

Szolgáltató a végfelhasználói aláíró és bélyegző tanúsítványok esetében a tanúsítványok Alanyait (Subject mező) egymástól egyértelműen megkülönbözteti. Ennek érdekében a Szolgáltató minden Ügyfél számára egy egyedi alanyazonosítót (OID alapú Permanens azonosító) ad, melyet a tanúsítvány Subject/Serialnumber mezőjében tüntet fel (lásd 7.1 fejezet). Ez az azonosító egyedileg azonosítja a tanúsítványban szereplő természetes vagy jogi személyt. Egy Alanynak lehet több azonosítója, viszont ezt az azonosítót soha nem kaphatja meg más Alany.

A fentiek mellett a Szolgáltató egy további Subject/Serialnumber mezőben más egyedi azonosítót is feltüntethet (pl. személyazonosító igazolvány szám, hatósági kártya azonosítója stb.).

Weboldal-hitelesítő tanúsítványok (OVCP és EVCP) esetén a Permanens azonosító nem értelmezett.

3.1.6 Védjegyek azonosítása, ellenőrzése és szerepe

Szolgáltató a tanúsítványban védjegyet is feltüntethet az Ügyfél birtokában/tulajdonában lévő DBA, trademark, terméknév vagy termékazonosító alapján. Ezen adatok a tanúsítvány Subject/CN és/vagy a SubjectAltName/dirname mezőben kerülhetnek feltüntetésre. Ellenőrzésüket lásd a 3.2.2 fejezetben.

Az Ügyfél részéről egy védjegy megszerzése nem tekinthető olyan eseménynek, amely a tanúsítvány módosítását eredményezi.

3.2 Kezdeti azonosítás

A végfelhasználói nem minősített tanúsítványok kibocsátása előtti ügyfél-regisztrációt, beleértve a DÁP vonatkozó rendelkezései által előírt ellenőrzéseket Szolgáltató a jelen (3.2) fejezet alfejezeteiben részletezett azonosítási és hitelesítési eljárásokkal végzi, amennyiben azokat Szolgáltató még nem végezte el korábban vagy a korábban elvégzett eljárás már nem tekinthető megbízhatónak. Szolgáltató kizárólag a 3.3 fejezetben megadott esetekben tekinthet el a jelen (3.2) fejezet alfejezeteiben részletezett eljárások elvégzésétől.

Szolgáltató a kezdeti azonosítás keretében az alábbi eljárásokat végzi:

1. azonosítja Igénylő személyét, ellenőrizve személyes adatait, eljárási jogosultságát és a tanúsítványban feltüntetésre kerülő egyéb adatok használatára való jogosultságát is;
2. amennyiben eltér Igénylőtől, azonosítja az Előfizetőt, ellenőrizve legalább a tanúsítványba foglalandó teljes nevét és egyedi azonosító adatát valamint a tanúsítványban feltüntetésre kerülő egyéb adatok használatára való jogosultságát;
3. azonosítja Előfizető képviseletére jogosult vagy jogosultak személyét;
4. azonosítja Előfizető képviselője vagy képviselői meghatalmazottjának személyét és ellenőrzi a meghatalmazást;
5. ellenőrzi a tanúsítvány Alanyaként feltüntetésre kerülő adatokat;
6. ellenőrzi a tanúsítványba foglalandó nyilvános kulcs magánkulcs párjának birtoklását, valamint
7. rögzíti az ellenőrzött adatokat és dokumentálja az azonosítási, ellenőrzési eljárásokat.

Az 1.-5. pontok szerinti ellenőrzésekhez a Szolgáltató olyan hiteles és érvényes hivatalos okmányokat, dokumentumokat és/vagy megbízható központi nyilvántartásokat vagy adatbázisokat használ, amelyek kellő biztonsággal igazolják az Igénylő és Előfizető által benyújtott adatok

valódiságát és érvényességét, így:

- az Alanyként feltüntetésre kerülő természetes és/vagy jogi személy azonosságát;
- Igénylő és Előfizető képviselőjének eljárási jogosultságát,
- a tanúsítványba foglalandó képviseleti jog meglétét (ilyen tény igazolására alkalmas tanúsítvány igénylése esetén),
- a tanúsítvány által igazolt címtartomány (domain) vagy a tanúsítványban feltüntetendő IP-cím fölötti rendelkezési jogot (weboldal-hitelesítő - OVCP és EVCP - tanúsítvány igénylése esetén),
- a tanúsítványba foglalandó szabályozott szakma gyakorlására való jogosultságot (szabályozott szakma megnevezését feltüntető tanúsítvány igénylése esetén) és
- a személyazonosság megállapításához használt azonosító adatok és dokumentumok valódiságát.

Amennyiben az ellenőrzésekhez nem áll rendelkezésre hivatalos okmány, dokumentum vagy megbízható adatforrás, Szolgáltató ezek ellenőrzését teljes bizonyító erejű magánokiratba foglalt nyilatkozat alapján ellenőrzi.
Az eljárások akkor tekinthetők sikeresnek, ha az Igénylő és Előfizető által benyújtott adatok pontosan megegyeznek az okmányokban, dokumentumokban és/vagy megbízható adatforrásokban vagy nyilatkozatban szereplő adatokkal.

Mielőtt Szolgáltató bármilyen nyilvántartást vagy adatbázist megbízható adatforrásként kezd el alkalmazni, értékeli annak megbízhatóságát, pontosságát, és a módosításnak vagy hamisításnak való ellenállását. Szolgáltató figyelembe veszi a következőket az értékelése során:

1. A biztosított információk származási ideje,
2. Az információforrás frissítési gyakorisága,
3. Az adatszolgáltató és az adatgyűjtés célja,
4. Az adatok nyilvános elérhetősége,
5. Az adatok meghamisításának vagy megváltoztatásának relatív nehézsége.

Amennyiben a nyilvántartás vagy adatbázis jogszabály szerint közhiteles adatokat tartalmaz, Szolgáltató nem végzi el a fenti értékelést és az ilyen adatbázist vagy nyilvántartást megbízható adatforrásnak tekinti.

Szolgáltató az ellenőrzött adatok rögzítése mellett eltárolja az adatforrás által igazolt érvényességi időt is, amennyiben ilyen értelmezhető (pl. okmány érvényességi ideje). A kibocsátott tanúsítvány érvényességi ideje meghaladhatja ezt az érvényességi időt, de a Szolgáltatási szerződés aláírásakor az adatforrásnak érvényesnek kell lennie.

Az azonosítási és ellenőrzési eljárásokat végző munkatársai számára Szolgáltató részletes belső működési szabályzatban írja elő az entitásazonosítási és adatellenőrzési eljárások módját, az elvégzendő gyakorlati lépéseket, továbbá részletes leírást biztosít számukra ezek elvégzéséhez.

A végfelhasználói tanúsítvány Igénylője, Előfizetője Szolgáltató munkatársa, partnere is lehet, de esetében ugyanúgy kell eljárnia Szolgáltatónak, mint bármilyen más Ügyfél esetén. A Szolgáltató munkatársa, partnere az Igénylő / Előfizető szerepen túl semmilyen formában sem vehet részt a számára biztosított szolgáltatás igénylésében és kiszolgálásában.

3.2.1 A magánkulcs birtoklásának igazolása

Amennyiben az Igénylő állítja elő a tanúsítványhoz tartozó kulcspárt, úgy Szolgáltató gondoskodik mindazon technikai és műszaki eljárás alkalmazásáról, melynek révén megbizonyosodhat arról, hogy az Igénylő ténylegesen birtokolja a tanúsítványba foglalandó nyilvános kulcshoz tartozó magánkulcsot. Ennek igazolása történhet egyebek mellett az Ügyfél által előállított szabványos elektronikus tanúsítványkérelemmel (pl. PKCS#10 vagy SPKAC CSR) vagy önaláírt tanúsítványon alapuló igényléssel és annak Szolgáltató felé átadásával.

Az NL Sign szolgáltatás keretében, a Szolgáltató biztonságos és védett informatikai rendszerének tanúsított HSM (Hardware Security Module) moduljában generált kulcsok esetében a Szolgáltató technikai úton meggyőződik arról, hogy a magánkulcs kizárólag Végfelhasználó befolyása alatt áll. A Szolgáltató tanúsított rendszere biztosítja, hogy a kulcsok generálása kizárólag akkor lehetséges, ha Végfelhasználó a rendszerbe bejelentkezett és a korábban általa generált aktiváló adat megadásával jóváhagyja a tanúsítványigénylést. Szolgáltató az így generált magánkulccsal hitelesített PKCS#10 formátumú tanúsítványkérelem alapján bizonyosodik meg a magánkulcs Végfelhasználó általi birtoklásáról.

A magánkulcs birtoklásának fenti módokon történő igazolása mindaddig érvényes, amíg a magánkulcshoz érvényes tanúsítvány kapcsolódik.

3.2.2 Szervezeti azonosság ellenőrzése

Előfizető azonosítása

Nem természetes személy Előfizetők tanúsítványban feltüntetendő teljes nevének és egyedi azonosítójának ellenőrzésére, valamint képviselője személyének megállapítására Szolgáltató közhiteles nyilvántartást vagy a bejegyzését és az előbbieket igazoló közokiratot vesz igénybe. Ezek hiányában az ellenőrzés alapja más megbízható adatforrás vagy jogszabály lehet.

A nem természetes személyek azonosítása kapcsán Szolgáltató elsősorban az alábbi közhiteles vagy megbízható adatbázisokat használja:

- a Ptk. szerinti gazdasági társaságok esetén a Ctv. 1. §-ban meghatározott Céginformációs és az Elektronikus Cégeljárásban Közreműködő Szolgálat online céginformációs szolgáltatása által biztosított online cégnyilvántartás;
- a Civil tv. hatálya alá eső szervezetek esetén a Ctv 84. §-ban meghatározott Országos névjegyzékben;
- az Ügyvédi tv. hatálya alá tartozó ügyvédek esetén az Ügyvédi tv. 116. §-ában meghatározott, a Magyar Ügyvédi Kamara weboldalán online elérhető nyilvántartásban;
- a Köznev. törvény hatálya alá tartozó köznevelési intézmények esetén az Oktatási Hivatal weboldalán elérhető, a 229/2012 Korm. rendeletben meghatározott köznevelési információs rendszer intézménytörzsi nyilvántartásának közérdekű adataira vonatkozó intézménykeresőben;
- az Áht. hatálya alá tartozó költségvetési szervek, köztestületek, önkormányzatok és egyéb törzskönyvi jogi személyek esetén a Magyar Államkincstár weboldalán elérhető, az Áht-ben meghatározott Törzskönyvi nyilvántartásban.
- az egyéni vállalkozóról és az egyéni cégről szóló törvény hatálya alá eső vállalkozások esetén a Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság által működtetett, a törvényben meghatározott online Egyéni vállalkozók nyilvántartásában.

Az EV SSL tanúsítványok szervezeti azonosságának ellenőrzésére használt adatforrások a Szolgálató *EV SSL tanúsítványok szervezeti azonosságának ellenőrzésére használt adatforrások nyilvántartása* nevű dokumentumában kerülnek közzé tételre a Szolgáltató weboldalán (lásd 1.1.2).

Amennyiben a fenti nyilvántartások nem elérhetők, illetve egyéb szervezetforma vagy nem Magyarországon bejegyzett nem természetes személyek esetén Szolgáltató más vonatkozó közhiteles vagy megbízható adatforrást használ, amennyiben pedig ilyenek nem elérhetők vagy a hozzáférés és ellenőrzés költsége aránytalanul magas, az ellenőrzés alapja alapító vagy létesítő valamint kinevezési közokirat vagy más, a nem természetes személy nevét és egyedi azonosítóját, valamint képviselője személyét igazoló közokirat lehet.

Nem Magyarországon bejegyzett nem természetes személy esetén Szolgáltató a nem természetes

személy nevét és egyedi azonosítóját, valamint képviselője személyét igazoló dokumentum(ok) közjegyző által hitelesített magyar vagy angol nyelvű fordítása alapján végzi az ellenőrzést. Amennyiben a dokumentum eredeti nyelve angol, fordítás nem szükséges és ebben az esetben az eredeti dokumentum(ok) közjegyző által hitelesített másolata szolgál az ellenőrzés alapjául.

Szolgáltató a nem természetes személyek egyedi azonosítójaként elsősorban adószámot tüntet fel a végfelhasználói tanúsítványban; ennek ellenőrzését – amennyiben a fentebb sorolt nyilvántartások nem tartalmazzák, Szolgáltató a magyar adószámok vonatkozásában a Nemzeti Adó és Vámhivatal weboldalán elérhető hatósági nyilvántartásban az adóalanyok lekérdezésével, vagy közösségi adószámok esetén az Európai Unió hivatalos weboldalán elérhető Közösségi adószám-megerősítő oldalán ellenőrzi. Cégjegyzékszám egyedi azonosítóként való feltüntetése esetén, azt a fentebb megadott cégnyilvántartásban ellenőrzi.

A nem természetes személy képviselője nevében meghatalmazott is eljárhat. A meghatalmazott jogosultságát Szolgáltató a 3.2.3 b. pont szerint ellenőrzi.

A nem természetes személy egyéb tanúsítványba foglalandó adatait a fentiekhez hasonló módon egyéb megbízható adatforrás, egyéb hivatalos dokumentumok vagy okiratba foglalt meghatalmazás alapján ellenőrzi. Előfizető tanúsítványban feltüntetésre kerülő szervezeti egységének valódiságát (Subject/organizationalUnitName), amennyiben az előbbi ellenőrzési lehetőségek nem állnak rendelkezésre, Előfizető szolgáltatási szerződésben tett nyilatkozata biztosítja.

Szolgáltató a tanúsítványigénylés (lásd 4.1) során eredeti dokumentumok vagy hiteles elektronikus igazolások bemutatását várhatja el Igénylőtől és Előfizetőtől.

Előfizető adatainak megőrzése

Előfizető tanúsítványalanyként feltüntetendő és Szolgáltató nyilvántartásában tárolásra kerülő következő adatait Szolgáltató saját rendszerében letárolja (lásd a 9.4 fejezetet):

- Előfizető azonosító adatait (teljes és rövid neve, hivatalos címe, adószáma, cégjegyzékszáma, szervezeti egység neve);
- Ezek ellenőrzésére használt dokumentumok adatai (mint pl. dokumentumok típusa, azonosítószáma, érvényességi ideje) és eredeti/másolati példányai VAGY elektronikus bélyegzője és annak ellenőrzéséhez használt adatok;
- Előfizető képviselőinek képviseleti jogosultságai (egyéb képviselő adatok kapcsán lásd a 3.2.3 fejezetet);
- Szolgáltatási szerződés és egyéb nyilatkozatok (pl. meghatalmazások) aláírt példánya;
- Különböző nyilvántartásokban való lekérdezések és az arra adott válaszok adatai;
- Kapcsolatfelvételhez szükséges adatok (pl., telefonszám, email cím).

Egyéb nem személyes alanyadatok ellenőrzése

Amennyiben Igénylő a tanúsítvány Alanyaként egy eszköz, rendszer vagy termék nevének, illetve azonosítójának vagy DBA / Védjegy vagy más egyedi elnevezésének feltüntetését igényli (önállóan vagy egy természetes vagy jogi személy mellett), akkor Szolgáltató meggyőződik arról, hogy az Ügyfél jogosan birtokolja a nevet és/vagy azonosítót, s az nem megtévesztő. Az ellenőrzés hivatalos dokumentumon, megbízható adatforráson vagy az azonosítót kezelő hivatalos szervvel való egyeztetésen alapul, amennyiben ilyen elérhető.

A tanúsítványigényléssel és elfogadással az Ügyfél kifejezi, hogy a benne foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik személy jogait.

Szervezetazonosítás közigazgatási tanúsítványok esetén

A közigazgatási tanúsítványok esetén Igénylőnek meg kell adnia az ügyfél-regisztrációt kérő ügyintézést biztosító állami szerv, valamint az ügyintézési célú elektronikus bélyegzőhöz rendelt

eszköz egyértelmű azonosításához szükséges, a tanúsítványban szerepeltetendő adatokat és az ügyintézést biztosító állami szervnél a kapcsolattartásért felelős személy elérési adatait.

3.2.3 Természetes személy azonosságának hitelesítése

Igénylő személyazonosságának ellenőrzése

Amennyiben az igényelt tanúsítvány természetes személy adatait tartalmazza (ide nem értve az Expressz tanúsítványtípusokat – LCP, lásd 1.2.1), Igénylő személyazonosságának ellenőrzésére Szolgáltató az alábbi, i., ii. és iii. pontokban részletezett módszerek valamelyikét alkalmazza – az i. és iii. pontok alkalmazása esetén a iv. pontban megadott adatellenőrzési eljárással kiegészítve.
EV weboldal-hitelesítő tanúsítvány (EVCP – lásd 1.2.1) igénylése esetén az Igénylőt Szolgáltató az i. pont szerinti eljárások valamelyikével azonosítja, a iv. pontban megadott adatellenőrzési eljárással kiegészítve.
Amennyiben az igényelt tanúsítvány természetes személy adatait nem tartalmazza (ide nem értve az EV weboldal-hitelesítő tanúsítványokat) valamint az Expressz tanúsítványtípusok (LCP - lásd 1.2.1) esetén, Igénylő személyazonosságának ellenőrzésére Szolgáltató alapértelmezetten kizárólag a iv. pontban megadott adatellenőrzési eljárást végzi el, melyet esetenként kiválthat az i., ii. és iii. pontokban részletezett – nagyobb biztonságot nyújtó – eljárások valamelyikével.

i. Megjelenésen alapuló (és azzal egyenértékű) hitelesítések:

Igénylő személyazonosításához személyes megjelenésére van szükség Igénylő választása alapján:

- Központi Regisztrációs Egység munkatársa előtt a Szolgáltató telephelyén (lásd 1.1.2), vagy
- Kihelyezett Regisztrációs Egység munkatársa előtt a Szolgáltatói Partner által megjelölt helyen (a Kihelyezett Regisztrációs Egység előtti személyazonosítás kizárólag a Szolgáltatói Partnerrel kötött szerződésben meghatározott ügyfélkör számára elérhető), vagy
- Mobil Regisztrációs Munkatárs előtt, az ÁSZF-ben és a Szolgáltató weboldalán (lásd 1.1.2) közétett feltételek mellett az Ügyfél által kért helyen és időben, vagy
- közjegyző előtt.

A Szolgáltató előtti megjelenés esetére:
Szolgáltató (Központi Regisztrációs Egység munkatársa, Mobil Regisztrációs munkatárs vagy Kihelyezett Regisztrációs Egység munkatársa) előtt való megjelenés esetén Igénylő személyazonosító dokumentuma Szolgáltató munkatársának való bemutatásával azonosítja magát. Amennyiben a bemutatott dokumentum valódiságával kapcsolatban nem merül fel kétség, a Szolgáltató munkatársa a személyazonosító dokumentum fényképét és aláírását, a megjelent személy arcával és a Szolgáltatási szerződésen található aláírással összehasonlítva állapítja meg Igénylő személyazonosságát. A személyazonosító igazolványban szereplő fénykép alapján Igénylőnek egyértelműen felismerhetőnek kell lennie, s a dokumentumon szereplő aláírásának meg kell egyeznie a Szolgáltatási szerződésen tett aláírásával. Amennyiben kétség merül fel a bemutatott dokumentum valódisága illetőleg a fénykép vagy az aláírás megfeleltethetősége kapcsán, a Szolgáltató megtagadja a tanúsítványkibocsátási Igénylés teljesítését.

Közigazgatási tanúsítvány igénylése esetén a regisztrációs ügyintéző aláírásával igazolja, hogy a személyazonosító igazolványon szereplő arckép megfeleltethető az igénylő arcának és az igazolványban szereplő aláírás azonos Igénylő Szolgáltatási szerződésen szereplő aláírásával.
Szolgáltató az előtte bemutatott személyazonosító dokumentumban - vagy a hozzá eljuttatott másolatában - annak érvényességét és hitelességét, valamint az Igénylő által megadott adatok valódiságát ellenőrzi.

A Szolgáltató a személyes megjelenés során elsősorban az alábbi személyazonosító dokumentumok bemutatását igényli:

- személyazonosító igazolvány vagy fényképes vezetői engedély (magyar és EU állampolgárok esetén)
- útlevél (nem EU állampolgárok esetén)

Nem magyar EU állampolgárok, valamint izlandi, norvég és svájci állampolgárok esetén a bemutatott személyazonosító dokumentum valódiságát Szolgáltató munkatársa az Európai Tanács által biztosított „PRADO" elnevezésű online adatbázisban található dokumentumminta alapján ellenőrzi.

Egyéb állampolgárok esetén Szolgáltató hasonló megbízható online adatbázis segítségével vagy más, dokumentálható és igazolható módon ellenőrzi a bemutatott dokumentum valódiságát. Ilyen esetben az ellenőrzés módját jegyzőkönyvben rögzíti, a jegyzőkönyvet pedig a tanúsítványok kibocsátásával kapcsolatban megőrzendő adatokkal együtt megőrzi (lásd 3.2.3. e).

A dokumentum bemutatását követően a Szolgáltató – Igénylő hozzájárulásával – elektronikus másolatot készít a dokumentumról (vagy elkéri az Igénylő által készített másolatot). Amennyiben a másolatkészítéshez Igénylő nem járul hozzá, a dokumentum adatait tartalmazó adategyeztető űrlap aláírásával kell igazolnia az okmány adatait.

A dokumentummásolat vagy adategyeztető űrlap alapján a dokumentum érvényességét és adatait Szolgáltató a iv. pont szerint ellenőrzi, majd a dokumentummásolatot vagy adategyeztető űrlapot a tanúsítványok kibocsátásával kapcsolatban megőrzendő adatokkal együtt megőrzi (lásd 3.2.3. e).

Amennyiben a dokumentum valódiságával kapcsolatban, illetve az okmányfénykép vagy az aláírás megfeleltethetősége kapcsán Szolgáltató részéről nem merül fel kétség, valamint a iv. pont szerinti ellenőrzés alapján a dokumentum és adatai érvényesek, Szolgáltató sikeresnek tekinti a személyazonosítást.

A közjegyző előtti megjelenés esetére:
Közjegyző előtt történő megjelenés esetén Igénylőnek az aláírt Szolgáltatási szerződést közjegyzői ténytanúsító okiratba kell foglaltatnia, melyben a közjegyző tanúsítja, hogy ellenőrizte Igénylő személyazonosságát és aláírását. Igénylőnek az okirat eredeti példányát kell eljuttatnia a Szolgáltatóhoz a fentebb megadott személyazonosító okmánya másolatával együtt.
Ez esetben a személyazonosítás alapjául a közjegyzői okirat ellenőrzése, illetve a dokumentummásolat alapján a dokumentum érvényességének és adatainak iv. pont szerinti ellenőrzése szolgál.
Amennyiben a közjegyzői okirat valódiságával és érvényességével kapcsolatban Szolgáltató részéről nem merül fel kétség, valamint a iv. pont szerinti ellenőrzés alapján a dokumentum és adatai érvényesek, személyazonosítást sikeresnek tekinti.

ii. Elektronikus azonosító eszköz használatával történő hitelesítés

Az eIDAS 24. cikk (1) bekezdés b) pontjának megfelelően a természetes személyek azonosítására Szolgáltató az Európai Unió Hivatalos Lapjában[9] közzétett listán szereplő, „jelentős", illetve a „magas" biztonsági szinttel rendelkező elektronikus azonosítási rendszert is alkalmazhat, amennyiben az azonosító eszköz kibocsátásához személyes megjelenés volt szükséges. Amennyiben Igénylő vagy Előfizető képviselője vagy maghatalmazottja személyazonosítására Szolgáltató számára elérhető ilyen elektronikus azonosító rendszer, a tanúsítványkibocsátást megelőző személyazonosítás elvégzéséhez nem szükséges a természetes személy jelenléte.

[9] http://eur-lex.europa.eu/oj/direct-access.html

iii. Elektronikus hitelesítés

Szolgáltató Igénylő és Előfizető képviselője vagy meghatalmazottja azonosítását elektronikus hitelesítéssel is végezheti. Ilyen esetben a Szolgáltatási szerződés, illetve a meghatalmazás elektronikus aláírásának ellenőrzése szolgál a személyazonosítás alapjául. Amennyiben az aláírás tanúsítványa nem igazolja egyértelműen aláíró személyazonosságát (pl. mert a tanúsítványt nem Szolgáltató bocsátotta ki és/vagy abban egyértelmű személyazonosító adat nem található) Szolgáltató igényt tarthat Igénylő / Előfizető képviselője vagy meghatalmazottja személyazonosító okmányának másolatára, melyen annak kézi aláírását külön is kérheti a másolaton feltüntetni. (Ez esetben – az elektronikus aláírás ellenőrzése mellett – az okmány eredeti és rajta elhelyezett kézi aláírásának egyezése is a személyazonosítás alapja.) Szolgáltató a tanúsítvány Alanyaként feltüntetett természetes személy nevének és egyéb személyes adatainak pontos egyezését várja el a személyazonosító okmány adataival.

Igénylő érvényes elektronikus aláírását Szolgáltató abban az esetben fogadja el, ha aláíró tanúsítványát szabványos NCP, NCP+, QCP-n vagy QCP-n-qscd hitelesítési rend szerint bocsátotta ki egy az EU Bizalmi listáján szereplő szolgáltató és ezt a Szolgáltató egyértelműen meg tudja állapítani. Szolgáltató indoklás nélkül megtagadhatja a nem általa kiadott nem-minősített tanúsítványon alapuló aláírás elfogadását a személyazonosításhoz.

Az elektronikus aláírásba foglalt tanúsítványadatokat Szolgáltató felhasználhatja hiteles adatként, de kérhet az Igénylő és Előfizető részéről további adatszolgáltatását is (pl. az i. pont szerinti személyazonosító dokumentum másolatát), illetve az adatokat (és adott esetben a dokumentum érvényességét) a iv. pont szerint ellenőrzi.

Amennyiben az elektronikus aláírás ellenőrzése sikeres és tanúsítványa megfelel a fentieknek, illetve – adott esetben – az okmánymásolaton szereplő aláírások egyezősége kapcsán Szolgáltató részéről nem merül fel kétség, valamint a iv. pont szerinti ellenőrzés alapján a dokumentum és/vagy adatai érvényesek, Szolgáltató sikeresnek tekinti a személyazonosítást.

iv. Személyazonosító dokumentumok és adatok ellenőrzése

Amennyiben az igényelt tanúsítvány természetes személy adatait nem tartalmazza (ide nem értve az EV weboldal-hitelesítő tanúsítványt), valamint az Expressz tanúsítványtípusok (LCP - lásd 1.2.1) esetén, Szolgáltató Igénylő i. pontban foglaltaknak megfelelő személyazonosító dokumentumának másolatára tart igényt – személyes jelenlét és az eredeti dokumentumok bemutatása nem szükséges. Ebben az esetben a dokumentum és adatai érvényességének alábbiak szerinti ellenőrzése a személyazonosítás alapja; a dokumentum és adatai érvényességének esetén Szolgáltató a személyazonosítást sikeresnek tekinti.

Amennyiben az igényelt tanúsítvány természetes személy adatait tartalmazza (ide nem értve az Expressz tanúsítványtípusokat – LCP, lásd 1.2.1) és Szolgáltató Igénylőt az i. vagy a iii. pont szerint azonosítja, a dokumentum és/vagy adatai érvényességének alábbiak szerinti ellenőrzése része a személyazonosításnak és az érvényesség megállapítása szükséges ahhoz, hogy a személyazonosítást a Szolgáltató sikeresnek tekintse.

EV weboldal-hitelesítő tanúsítvány (EVCP) igénylése esetén Igénylő i. pont szerinti azonosításán túl, az azonosításhoz használt dokumentum és adatai érvényességének alábbiak szerinti ellenőrzése is része a személyazonosításnak és az érvényesség megállapítása szükséges ahhoz, hogy a személyazonosítást a Szolgáltató sikeresnek tekintse.

Szolgáltató a bemutatott és/vagy másolatban hozzá eljuttatott vagy részére átadott személyazonosító dokumentum érvényességét és hitelességét, valamint az abban szereplő adatokat közhiteles vagy más megbízható központi nyilvántartásban ellenőrzi (kivéve az OV weboldal-hitelesítő tanúsítványokat, melyek esetében a másolat alapján történik a dokumentum érvényességének ellenőrzése). Magyar állampolgárok esetén ez a Belügyminisztérium Polgárok személy- és lakcímnyilvántartása. A dokumentummásolatokat és az ellenőrzés eredményét Szolgáltató rögzíti (lásd 3.2.3. e).

Amennyiben – például nem magyar állampolgárságú természetes személy esetén – ilyen

nyilvántartás Szolgáltató számára nem elérhető vagy elérhetősége nem ismert vagy a hozzáférés és ellenőrzés költsége aránytalanul magas, a Szolgáltató ezt a tényt rögzíti, és a rendelkezésére álló okmányok, dokumentumok és/vagy adatforrások alapján dönt arról, hogy az adott tanúsítványt az Igénylő részére kibocsátja-e. Ilyen esetben, amennyiben a Szolgáltató a tanúsítvány kibocsáthatósága mellett dönt, az ellenőrzés módját, az ahhoz használt okmányokat, dokumentumokat és/vagy adatforrásokat jegyzőkönyvben rögzíti, a jegyzőkönyvet pedig a tanúsítványok kibocsátásával kapcsolatban megőrzendő adatokkal együtt megőrzi.

Előfizető képviselője, meghatalmazottja személyazonosságának ellenőrzése

Amennyiben Előfizető, illetve annak képviselője eltér Igénylőtől, akkor a Szolgáltatási szerződést Előfizető képviselőjének / meghatalmazottjának is alá kell írni. Személyes megjelenés ehhez nem szükséges.

Előfizető képviselője (együttes képviselet esetén képviselői) személyének megállapítása a 3.2.2 szerinti jogszabály, közhiteles nyilvántartás vagy bejegyzést igazoló közokirat, létesítő okirat vagy megbízható, rendszeresen frissített adatforrás alapján történik meg. Előfizető meghatalmazottja személyének megállapítása a képviselő(k) által aláírt meghatalmazás alapján történik. Szolgáltató a Ptk. 6:16. § szerinti teljes bizonyító erejű magánokiratba, vagy közokiratba foglalt általános meghatalmazást vagy a Szolgáltató által a weboldalán közzétett mintának megfelelő, tanúsítványigénylésre és -kezelésre feljogosító, egyszerű magánokiratként kibocsátott meghatalmazást fogad el.

Előfizető képviselőinek / meghatalmazottjának a Szolgáltatási szerződésen és meghatalmazáson található aláírása hiteles aláírásminta (pl. közjegyző által készített aláírási címpéldány, ügyvéd által készített aláírásminta vagy hivatalos okmányon szereplő aláírás, meghatalmazott esetében pedig a meghatalmazáson szereplő aláírása) alapján kerül ellenőrzésre.

A meghatalmazásokat és az aláírásmintákat Igénylő egyszerű elektronikus másolatként is benyújthatja, de Szolgáltató igényt tarthat az eredeti dokumentumokba való betekintésre is. Az elektronikus másolatot Szolgáltató a tanúsítványok kibocsátásával kapcsolatban megőrzendő adatokkal együtt megőrzi (lásd 3.2.3. e).

A jogosultságok és felhatalmazások kapcsán lásd még a 3.2.5 fejezetet.

A Szolgáltatási szerződés és meghatalmazás Igénylőtől eltérő Előfizető általi hitelesítése történhet a képviselő(k) elektronikus aláírásával vagy az Előfizető bélyegzőjével is, illetve a Szolgáltatási szerződés a Meghatalmazott elektronikus aláírásával is hitelesíthető. Előfizető érvényes bélyegzőjét, illetve képviselőjének vagy meghatalmazottjának érvényes elektronikus aláírását Szolgáltató abban az esetben fogadja el, ha azok tanúsítványát szabványos QCP-n, QCP-l, QCP-n-qscd vagy QCP-l-qscd hitelesítési rend szerint bocsátotta ki egy az EU Bizalmi listáján szereplő szolgáltató és ezt a Szolgáltató egyértelműen meg tudja állapítani. A Szolgáltató által korábban, személyes találkozó útján kiadott nem minősített tanúsítványok is elfogadhatók igénylésre.

Egyéb alanyadatok ellenőrzése

Szabályozott szakmára vonatkozó titulusok, valamint cégjegyzésre való jogosultságra vonatkozó információ feltüntetése esetén az erre vonatkozó adatokat Szolgáltató ellenőrzi (amennyiben értelmezett szakmai igazolvány vagy a 3.2.2 fejezet szerinti közhiteles vagy megbízható adatforrások vagy okiratok vagy szakmai kamara vagy más hiteles vagy megbízható nyilvántartás adatai alapján).
A tanúsítványba kerülő vagy amennyiben nem kerül feltüntetésre a tanúsítványban a kapcsolattartáshoz megadott email címről Szolgáltató üzenetküldést vár Igénylő részéről az email címhez tartozó postafiókhoz való hozzáférés igazolására, az alábbiak szerint.

- A NETLOCK Sign szolgáltatás esetén az email cím ellenőrzése automatizáltan, az alábbiak

szerint történik:
    - randomizált linket (random access token) tartalmazó e-mail küldése Igénylőnek,
    - Igénylő az e-mail-ben a linkre kattintva validálja azt;
    - a random access token érvényessége 120 óra.
- Egyéb esetben tanúsítványok esetén:
    - random adatot tartalmazó email küldése Igénylőnek
    - Igénylő válasz e-mail-ben a random adatot az visszaküldi
    - amennyiben az ellenőrzés 60 napnál nem régebbi, az ellenőrzés elfogadható.

Személyes profilú (lásd 7.1) tanúsítvány igénylése esetén, a tanúsítvány alanyadatai között feltüntetésre kerül az Igénylő lakhelye szerinti ország és helység neve, melyek igazolására Szolgáltató igényt tarthat Igénylő lakcímet igazoló hatósági igazolványának másolatára. Igénylő lakhelye szerinti helyadatokat és amennyiben annak másolatát bekérte, a lakcímet igazoló hatósági igazolvány érvényességét Szolgáltató közhiteles vagy más megbízható központi adatbázisban ellenőrzi. Magyar állampolgárok esetén ez a Belügyminisztérium Polgárok személy- és lakcímnyilvántartása. A dokumentummásolatokat és az ellenőrzés eredményét Szolgáltató rögzíti (lásd 3.2.3. e). Amennyiben – például nem magyar állampolgárságú természetes személy esetén – ilyen nyilvántartás nem elérhető vagy elérhetősége Szolgáltató számára nem ismert vagy a hozzáférés és ellenőrzés költsége aránytalanul magas, Igénylő eredeti lakcímet igazoló hatósági igazolványának bemutatását várja el Igénylőtől. Szolgáltató a bemutatott dokumentum valódiságának ellenőrzése és másolatának megőrzése kapcsán a 3.2.3 a. i. pontban foglaltaknak megfelelően jár.

Átvevő azonosítása

Amennyiben Igénylő nem jelent meg személyesen a Szolgáltató előtt (vagy ha az átvétel nem a személyazonosítást követően azonnal történik), és Szolgáltató át kívánja adni Ügyfélnek az általa generált magánkulcsot tartalmazó Ügyféleszközt, akkor Átvevőt a Kézbesítési megbízott személyes találkozás során azonosítja fényképes személyazonosító igazolványa alapján.

Igénylő, Előfizető, képviselő és meghatalmazott adatainak rögzítése

Szolgáltató a tanúsítvány Alanyaként feltüntetendő adatokat a fenti ellenőrzések során felhasznált adatforrások alapján rögzíti, illetve az adatforrásokban való ellenőrzést dokumentálja

Igénylő, Előfizető és képviselőjének, valamint meghatalmazottjának, illetve Átvevőnek alábbi adatait, dokumentumait és az ellenőrzés megtörténtének egyéb bizonyítékait Szolgáltató saját rendszerében letárolja (lásd a 9.4 fejezetet):

- Igénylő, Előfizető képviselője és meghatalmazottja, valamint Átvevő egyértelmű személyazonosságának megállapításához szükséges adatai hiteles okmány alapján;
- természetes személy részére kibocsátott tanúsítvány esetén Igénylő lakcíme hiteles okmány alapján;
- Igénylő kapcsolatfelvételhez szükséges adatai (pl. postacím, telefonszám, email cím).
- Szolgáltatási szerződés aláírt példánya;
- elektronikus aláírás ellenőrzéséhez használt adatok;
- különböző nyilvántartásokban való lekérdezésekre adott válaszok adatai;
- az azonosításra és ellenőrzésére használt dokumentumok adatai (mint pl. dokumentumok típusa, azonosítószáma, érvényességi ideje);
- az Igénylés során bemutatott okmányok, igazolások, nyilatkozatok és meghatalmazások Igénylő által beadott másolati vagy Szolgáltató által szkennelt példányai.

Egyéb rendelkezések

Az azonosítási eljárás során biztosított adatok valódiságát a Szolgáltatási szerződés aláírásával Igénylőnek és Előfizetőnek el kell ismerniük.

A teszttanúsítványok Alanyaként (ha a tanúsítvány tartalma alapján egyértelműen jelzésre kerül annak teszt jellege) Szolgáltatónak nem kell valódi természetes vagy jogi személyt feltüntetni, ezért az ilyen alanyadatok ellenőrzése értelemszerűen nem elvárt.

3.2.4 Nem ellenőrzött alany információk

A Szolgáltató által kibocsátott tanúsítványban csak olyan alanyadatok szerepelnek, amelyeket a Szolgáltató a jelen (3.2) fejezet egyéb alpontjai szerint ellenőrzött, vagy – amennyiben ez nem lehetséges – amelyek valódiságáról az Előfizető/Igénylő előzetesen írásban, büntetőjogi felelősségének tudatában nyilatkozott. Amennyiben a Szolgáltató nem tud hitelt érdemlő módon meggyőződni az adatok valódiságáról és helyességéről, a tanúsítványkibocsátást megtagadhatja (lásd 4.2.2 fejezet).

3.2.5 Jogok, felhatalmazások ellenőrzése

Amennyiben Előfizető nem természetes személy, akkor a nevében egy természetes személy járhat el Szolgáltató előtt Igénylőként. Ez a természetes személy lehet a jogi személy hivatalos képviselője/képviselői vagy az általuk meghatalmazott másik személy. E személyek azonosítása és ellenőrzése a 3.2.3 pont vagy a 3.3 pont alapján történik, és az ellenőrzés eredményét Szolgáltató rögzíti.

Meghatározott időre adott meghatalmazás esetén minden esetben ellenőrizni kell a meghatalmazás lejárati időpontjának meg nem haladását, valamint (jogi személyek esetén) a meghatalmazó képviseleti jogának fennállását.

Amennyiben a tanúsítvány Alanyaként a jogi személy Előfizető mellett természetes személy Végfelhasználó kerül megnevezésre, akkor Előfizető képviselőjének/képviselőinek vagy a meghatalmazottjuknak, az adott jogi és természetes személy nevének és egyéb adatainak a tanúsítványban való feltüntetetéséhez hozzá kell járulni.

Amennyiben a tanúsítvány teljes vagy részleges képviseleti jogot vagy ekként is értelmezhető jogviszonyt is tartalmaz (a továbbiakban együtt: képviseleti jog), a Szolgáltató köteles a tanúsítvány kibocsátása előtt a képviseleti jog fennállásáról és annak a tanúsítványból kiolvasható tartalmáról jogszabály, közhiteles nyilvántartás, létesítő okirat vagy ezek hiányában meghatalmazás alapján meggyőződni és az ellenőrzés eredményét rögzíteni.

Jogok, felhatalmazások ellenőrzése weboldal-hitelesítő tanúsítványok esetén (OVCP és EVCP)

Amennyiben a tanúsítvány Alanyaként (Subject és SAN mezők) domain név kerül feltüntetésre, a Szolgáltató ellenőrzi, hogy Előfizető a domain nevet jogosan használja és a fölött megfelelő technikai kontrollal bír.

A domain feletti kontrol ellenőrzésére Szolgáltató a következő technikai megoldásokat alkalmzza:

1. Konstruált e-mail a domain kontaktnak (BRG 3.2.2.4.4), melynek lépései:
    a. randomizált linket (random access token) tartalmazó e-mail küldése Igénylő számára az általa megjelölt fő vagy konkrét aldomainre;
    b. az email címek lokális tagja a következő lehet: 'admin', 'administrator', 'webmaster', 'hostmaster', vagy 'postmaster'

c. Igénylő az emailben a linkre kattintva validálja azt.

A random access token érvényessége 30 nap. A fő domain hitelesítése alkalmas aldomainekre tanúsítvány kibocsátásra.

2. Egyeztetett weboldal módosítás (BRG 3.2.2.4.6), melynek lépései:
   a. randomizált adathalmazt tartalmazó e-mail küldése Igénylő számára
   b. Igénylő a webszerverén elhelyezi az adatot a /.well-known/pki-validation könyvtárban a tanúsítani kívánt domainben (al vagy fő domain)
   c. Igénylő az ügyfélmenüjében gombnyomással jelzi, hogy elhelyezte a kódot, melynek hatására Szolgáltató rendszere automatikusan ellenőrzi a kód elhelyezését.

   A random access token érvényessége 30 nap. A fő domain hitelesítése alkalmas aldomainekre tanúsítvány kibocsátásra.

3. DNS változtatás (DNS TXT rekord) (BRG 3.2.2.4.7), melynek lépései:
   a. randomizált adathalmazt tartalmazó e-mail küldése Igénylő számára
   b. Igénylő a domainhez tartozó DNS TXT bejegyzésbe elhelyezi a kódot, úgy, hogy a kód előtagja: „netlock=” legyen
   c. Igénylő az ügyfélmenüjében gombnyomással jelzi, hogy elhelyezte a kódot, melynek hatására Szolgáltató rendszere automatikusan ellenőrzi a DNS TXT rekordban található kód ellenőrzését.

   A random access token érvényessége 30 nap. A fő domain hitelesítése alkalmas aldomainekre tanúsítvány kibocsátásra.

4. DNS CAA Contact Email (BRG 3.2.2.4.13), melynek lépései:
   a. randomizált linket (random access token) tartalmazó e-mail küldése Igénylő számára a DNS CAA ContactEmail tulajdonságban megjelölt email címre.
   b. Igénylő az e-mailben a linkre kattintva validálja azt.

   A random access token érvényessége 30 nap. A fő domain hitelesítése alkalmas aldomainekre tanúsítvány kibocsátásra. A DNS bejegyzés formátuma a következő kell legyen: „CAA 0 contactemail user@domain.hu”

5. DNS TXT Record Email contact (DNS TXT rekord) (BRG 3.2.2.4.14), melynek lépései:
   a. randomizált linket (random access token) tartalmazó e-mail küldése Igénylő számára a DNS TXT-ben megadott e-mail contact email címére.
   b. Igénylő az e-mailben a linkre kattintva validálja azt.

   A random access token érvényessége 30 nap. A fő domain hitelesítése alkalmas aldomainekre tanúsítvány kibocsátásra.

   A DNS TXT bejegyzés formátuma a következő kell legyen:

   - A tanúsítani kívánt domain alá aldomain-ként, fel kell venni a „validation-contactemail”-t;
   - ehhez az aldomainhez a TXT rekordban szerepelnie kell egy e-mail címnek (RFC 6532 3.2 szerint; kizárólag egy email cím, és csak e-mail cím szerepelhet benne).

Amennyiben Előfizető a hivatalos doamin regiszter alapján nem tulajdonosa a domain névnek (MultiDomain típusú tanúsítvány esetén a domain neveknek), akkor a tanúsítvány kiállításához az összes tulajdonos hiteles hozzájárulása szükséges. Ennek ellenőrzése során Szolgáltató a képviseletek és meghatalmazások ellenőrzéséhez hasonlóan jár el (lásd 3.2.3 b. pont). A

szolgáltató az igényelt domain neveket technikai úton is ellenőrizheti.
A weboldal-hitelesítő tanúsítványok minél szélesebb körű böngészőelfogadottsága érdekében valamint a lehetséges visszaélések elkerülése valamint a domainek és az azokra kiadott tanúsítványok kapcsolatának ellenőrizhetősége érdekében a Szolgáltató a weboldal-hitelesítő tanúsítványokat – kibocsátásuk előtt – aláveti az ún. „Certificate Transparency" (CT)[10] eljárásnak. Ennek keretében a Szolgáltató a jelen (3.2) fejezetben foglalt azonosítási és hitelesítési eljárásokat követően – azok sikeressége esetén – a tanúsítványt – kiadása előtt – az RFC 6962 ajánlásnak megfelelően hitelesített előtanúsítványként közzétételre továbbítja egy nyilvánosan hozzáférhető ún. CT nyilvántartás felé, melyben új bejegyzésként rögzítésre kerül a tanúsítvány. A bejegyzés rögzítéséről – azaz az „előtanúsítvány" közzétételéről a CT nyilvántartás aláírt, időbélyegzett bizonylatot küld vissza a Szolgáltatónak. A visszaküldött bizonylatra a Szolgáltató – kibocsátása előtt – a tanúsítvány megfelelő mezőjében (lásd 7.1) hivatkozást helyez el.
A domain-ellenőrzés a weboldal-hitelesítő teszttanúsítványok kiadásának is feltétele.

3.2.6 Együttműködési képességre vonatkozó követelmények

A Szolgáltató a szolgáltatás nyújtása során együttműködhet más Szolgáltatókkal, akik magukra kötelező érvényűnek ismerik el a Bizalmi Szolgáltatási Rendbe foglalt követelményeket.

A Szolgáltató a weboldalán közzétesz minden kereszthitelesített tanúsítványt, amely Alanyaként vagy kibocsátójaként szerepel.

3.3 Azonosítás és hitelesítés tanúsítványkezelési eljárás esetén

Olyan eljárás esetén, ami új tanúsítvány kibocsátását eredményezi (lásd a 4. Életciklus követelmények fejezetet, különösen a 4.6 Tanúsítványmegújítás, 4.7. Kulcscsere, 4.8 Tanúsítványmódosítás alfejezeteket), Szolgáltató a 3.2 fejezetben ismertetett kezdeti azonosítási eljárás szerint azonosítja és ellenőrizi az Ügyfelet vagy ügyfeleket és az igénylésben szereplő adatokat.

Abban az esetben, amennyiben

- Igénylő azonosítását, személyes adatainak és eljárási jogosultságának ellenőrzését;
- Előfizető azonosítását és azonosító adatainak, valamint a tanúsítványban feltüntetésre kerülő egyéb adatok használatára való jogosultságának ellenőrzését;
- Előfizető képviseletére jogosult vagy jogosultak személyének azonosítását;
- Előfizető képviselője vagy képviselői meghatalmazottjának azonosítását és a meghatalmazás ellenőrzését;
- a tanúsítvány Alanyaként feltüntetésre kerülő és Szolgáltató nyilvántartásában eltárolt adatok ellenőrzését; valamint
- a magánkulcs birtoklásának ellenőrzését

Szolgáltató korábban már elvégezte, akkor ezen eljárásokat Szolgáltató csak akkor köteles megismételni a 3.2 fejezetben ismertetett kezdeti azonosítási eljárásrend szerint, amennyiben a korábbi ellenőrzése már elavult vagy nem megbízható, vagy ha a korábban felvett Igénylői, Előfizetői, vagy Alany adatok megváltoztak.

A 3.2 fejezetben ismertetett azonosítási és hitelesítési eljárásokat egy újabb igénylés esetén Szolgáltató az alábbi feltételekkel tartja megbízhatónak:

- a 3.2.3. a. i., ii. és iii. pontok szerinti személyazonosítási eljárások eredményét az igényelt

[10] Az ún. „Certificate Transparency" programról bővebb információ: https://www.certificate-transparency.org

tanúsítvány érvényessége esetén;

- a természetes és nem természetes személyek azonosító adatainak 3.2.2. és 3.2.3. pontok szerinti ellenőrzését
    - közhiteles vagy más megbízható adatforrásban történő ellenőrzés esetén az ellenőrzés napját követő 60 naptári napig;
    - eredeti közokirat bemutatása alapján történő ellenőrzés esetén az irat bemutatása napját követő 60 naptári napig;
    - az eredeti közokirat közjegyző által hitelesített fordítása vagy másolata esetén a közjegyzői hitelesítés napját követő 60 naptári napig;
- a 3.2.3 b. és 3.2.5 szerinti meghatalmazásokat és más jellegű hozzájáruló nyilatkozatokat, valamint az aláírásmintákat abban az esetben, ha Szolgáltatónak nincs tudomása azok visszavonásáról vagy érvényességük megszűnéséről.

Amennyiben e feltételek nem állnak fenn, az eljárások eredményét Szolgáltató elavultnak tekinti és azokat a 3.2 fejezet szerint megismétli.

A 3.2 fejezetben megadott igénylői és előfizetői, valamint a tanúsítványban feltüntetésre kerülő alanyadatok vagy azok jogos felhasználásának igazolására és ellenőrzésére szolgáló dokumentumokat vagy másolataikat Igénylőnek csak abban az esetben kell ismét eljuttatnia a Szolgáltatóhoz, ha azok érvényessége lejárt vagy az azokban foglalt adatok valamelyike megváltozott a korábbi igénylés során végzett ellenőrzési eljárások óta.

Amennyiben az igénylés új aláíró vagy bélyegző nyilvános kulcsot tartalmaz és/vagy új Ügyféleszköz igénylésére is kierjed, akkor a 3.2.1 fejezet szerinti rendelkezéseket minden esetben be kell tartani.

Weboldal-hitelesítő tanúsítványok (OVCP és EVCP) kezelésére irányuló igények esetén az adatok ellenőrzését és az azonosítást Szolgáltató legalább 13 havonta (EVCP) vagy 27 havonta (OVCP) megismétli.

3.3.1 Azonosítás és hitelesítés érvényes tanúsítvány esetén

Amennyiben Igénylő személyazonosítása egy korábbi tanúsítványigénylés kapcsán már megtörtént és ez a tanúsítvány az újabb igényléskor még érvényes a 3.2.3. a. szerinti személyazonosítási eljárásokat csak abban az esetben folytatja le a Szolgáltató, ha az újabb igényléssel érintett tanúsítvány kibocsátáshoz a korábbinál nagyobb biztonságot nyújtó személyazonosítási eljárás szükséges.

Amennyiben az igényelt tanúsítvány kibocsátásához ellenőrizni szükséges adatok megegyeznek a Szolgáltató által az Ügyfél részére korábban kiadott tanúsítvány kibocsátását megelőzően ellenőrzött adatokkal és ez a tanúsítvány az újabb igényléskor még érvényes, Szolgáltató ezen adatok vonatkozásában dokumentumok bemutatását vagy másolatuk megküldését nem igényli, de a korábban rögzített dokumentumok és adatok közhiteles vagy más megbízható adatbázisban való ellenőrzését megismétli (kivéve, ha a legutóbbi ellenőrzés 60 napon belül történt).

Amennyiben Igénylő egy korábbi tanúsítványigénylése kapcsán az előfizetői adatok ellenőrzéséhez eredeti vagy közjegyző által hitelesített dokumentum volt szükséges, az újabb igénylés kapcsán e dokumentumokat Igénylőnek újból be kell mutatnia vagy át kell adnia (kivéve, ha az eredeti okirat bemutatása vagy a másolat/fordítás közjegyzői hitelesítése 60 napon belül történt).

3.3.2 Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Amennyiben Igénylő személyazonosítása és adatainak ellenőrzése korábban már megtörtént, de az ez alapján kiadott tanúsítvány már nem érvényes, Szolgáltató a 3.2 szerinti azonosítási és hitelesítési eljárásokat teljes egészében megismétli. Amennyiben az igénylői, előfizetői és a tanúsítványba kerülő alanyadatok nem változtak, és ellenőrzésükhöz rendelkezésre áll közhiteles vagy más megbízható adatforrás valamint a korábban rögzített megahatalmazás vagy más jellegű hozzájáruló nyilatkozat érvényes, e dokumentumok bemutatásától és/vagy másolataik megküldésétől Szolgáltató ebben az esetben is eltekinthet.

Érvénytelen tanúsítvánnyal aláírt vagy bélyegzett szolgáltatási szerződést meghatalmazást vagy más dokumentumot a Szolgáltató nem fogadja el.

3.4 Azonosítás és hitelesítés tanúsítványállapot-változtatás esetén

Szolgáltató tanúsítvány-visszavonási, -felfüggesztési és -újraaktiválási szolgáltatásokat egyaránt nyújt. Az állapotváltoztatás igénylőjét a Szolgáltató minden esetben azonosítja és meggyőződik az adott művelethez való jogosultságáról.

Az igénylő jogosultsága a 4.9.2 fejezet szerint kerül ellenőrzésre, a művelet pedig a 4.9.4 fejezet szerint kerül feldolgozásra. Az állapotváltoztatás igénylőjének azonosítását a Szolgáltató az alábbiak szerint végzi, a tanúsítvány Igénylője és Előfizetője esetén:

CSATORNA	ÁLLAPOTVÁLTOZÁST IGÉNYLŐ AZONOSÍTÁSA
Ügyfélmenü (Kizárólag felfüggesztési igény esetén)	Felhasználónév és jelszó megadása.
Telefon	Az ügyfélmenü regisztrációban rögzítésre került személyes adatok közül legalább három adat egyeztetése szükséges. Az azonosítás akkor tekinthető sikeresnek, ha az igénylő által közölt mindhárom adat egyezik az ügyfélmenü regisztrációban rögzítettekkel.
Email	Szolgáltató a hozzá emailben érkezett állapotváltoztatási igények igénylőit az email feladójának email címe alapján azonosítja. Amennyiben az állapotváltoztatási igény Szolgáltatóhoz az annak tárgyát képező a tanúsítványban rögzített email címről érkezik, az azonosítás sikeres. Amennyiben az állapotváltoztatási igény Szolgáltatóhoz *nem* az annak tárgyát képező a tanúsítványban rögzített email címről érkezik, az azonosítás nem lehetséges. Ebben az esetben Szolgáltató a vonatkozó tanúsítvány vonatkozásában állapotváltoztatási igénylésre jogosulttal megkísérli telefonon felvenni a kapcsolatot, hogy azonosítása után – lásd fentebb –erősítse vagy cáfolja az igényt.

Hatóság megkeresése esetén az azonosítást a szerv hivatalos (elektronikus vagy hagyományos) bélyegzője vagy elektronikus aláírása alapján végzi.

4. ÉLETCIKLUS KÖVETELMÉNYEK

Jelen (4.) fejezet a Szolgáltató által kibocsátott tanúsítványok életciklusát kezelő műveleteket írja le.

A tanúsítvány életciklusa a tanúsítvány igénylésétől és kiadásától annak lejártáig vagy visszavonásáig terjed. Ezen időtartamban van lehetőség - amennyiben adott hitelesítési rend (lásd 1.2.1. fejezet) vagy kulcshasználat (lásd 7.1.2 fejezet) esetén elérhető - a tanúsítvány felfüggesztésére, aktiválásra, illetve a tanúsítvány módosítására vagy a hozzá tartozó kulcsok cseréjére. Szolgáltató biztosítja, hogy Érintett felek tesztelési célú tanúsítványokat (lásd 7.1. fejezet) is igényelhessenek. Jelen (4.) fejezetben foglalt szabályok közül csak azon szabályok értelmezhetők a teszt tanúsítványokra, amelyeknél ezt a szabályzat szövege kifejezetten jelzi.

NL Sign szolgáltatás esetén a tanúsítvány életciklusát kezelő Ügyféligénylések a szolgáltatásba integráltan valósulnak meg. Lásd 6.8 fejezet.

4.1 Tanúsítványigénylés

A jelen szabályzatban megadott feltételekkel és módon kizárólag az 1.1 fejezetben megadott szolgáltatások keretében, az 1.2.1 fejezet szerinti tanúsítványok igényelhetők.

Jelen (4.1.) fejezet kizárólag az eredeti tanúsítványigénylésre vonatkozó eljárásokat ismerteti. A megújítási, módosítási vagy kulcscsere igénylések keretében történő tanúsítványkibocsátásokat a megfelelő (4.6.-8.) fejezetek írják le.

Minden új végfelhasználói tanúsítvány kibocsátásához az Igénylő által a Szolgáltató Központi vagy Kihelyezett Regisztrációs Egységéhez (lásd: 1.3.2 fejezet) előzőleg eljuttatott tanúsítványigénylés szükséges (lásd 4.1.2 fejezet).

A Szolgáltató szabályzataiban és/vagy weboldalán (lásd 1.1.2 fejezet) közérthető írásos tájékoztatást nyújt:

- az igényelhető tanúsítványok nem-minősített voltáról és az alkalmazásukhoz kapcsolódó joghatásokról;
- alkalmazhatóságukról (lásd az 1.4 fejezetben foglaltakat);
- a szolgáltatással kapcsolatos üzleti és jogi tudnivalókról (lásd a 9 fejezetben foglaltakat);
- a Szolgáltatási Szerződés megkötésének feltételeiről;
- a felek jogairól és kötelezettségeiről;
- a Szolgáltató Általános Szerződési Feltételeinek (ÁSZF) a tanúsítványokkal kapcsolatos szolgáltatásokra vonatkozó részeiről;
- a magánkulcs használatával kapcsolatosan szükséges biztonsági intézkedésekről;
- az Ügyféleszköz használatáról, amennyiben Igénylő azt a Szolgáltatótól szerzi be.

Szolgáltató a szabályzatait és egyéb tájékoztató dokumentumait weboldalán nem szerkeszthető, PDF formában teszi közzé, illetve közvetlen a weboldalon megjelenített tartalmak útján is közöl információkat.
Legkésőbb a szerződéskötést követően Szolgáltató elektronikus levélbe illesztett link(ek)en keresztül elérhetővé teszi az Ügyfél számára a szolgáltatási szerződést, a szolgáltatási rendet és a szabályzatot.

4.1.1 Ki nyújthat be tanúsítványigénylést?

Végfelhasználói tanúsítványt az igényelt profil szerint az alábbi felek igényelhetik:

TANÚSÍTVÁNY PROFIL (lásd 7.1 fejezet)	IGÉNYLŐ
SZEMÉLYES PROFIL	A tanúsítvány Alanyaként megjelölt természetes személy saját maga részére.
ÁLNEVES PROFIL	A tanúsítvány Alanyaként megjelölt álnevet az Igénylés során megadó természetes személy saját maga részére.
ÜZLETI PROFIL	A tanúsítvány Alanyaként megjelölt természetes személy saját maga részére, igazolva, hogy a szintén a tanúsítvány alanyaként megjelölt szervezet hozzájárult a tanúsítványigényléshez. *VAGY* A Szolgáltató és Ügyfél közötti előzetes megállapodás szerint a tanúsítvány Alanyaként megjelölt szervezetképviselője vagy annak meghatalmazottja, megjelölve a természetes személyt, akinek adatait szintén a tanúsítvány alanyaként kívánja feltüntetni. *VAGY* Közigazgatási tanúsítványok esetén az elektronikus ügyintézést biztosító állami szerv.
SZERVEZETI PROFIL	A tanúsítvány Alanyaként megjelölt jogi személy képviselője vagy meghatalmazottja. *VAGY* A tanúsítvány Alanyaként megjelölt trademarkot birtokló jogi személy képviselője vagy meghatalmazottja.
NEM-MINŐSÍTETT OV és EV WEBOLDAL-HITELESÍTŐ PROFIL	A tanúsítvány Alanyaként a domain mellett megjelölt, a domaint birtokló vagy azt jogosan használó szervezet képviselője vagy annak meghatalmazottja.

Tesztelési célú tanúsítványt (lásd 7.1 fejezet) bármely profillal bármely természetes személy igényelhet saját maga, általa képviselt szervezet vagy eszköze számára.

Szolgáltató kockázatlistát kezel azon természetes és jogi személyekről, akik esetében a tanúsítványigényléssel kapcsolatban kockázatokat tart nyilván, valamint külső adatforrásokat is felhasználhat a kockázatértékeléshez. Szolgáltató a kockázatértékelés alapján visszautasíthatja a tanúsítványigényléseket.

Menedzselt SCD szolgáltatás esetén a Végfelhasználók regisztrációja és az NL Sign aláírási szolgáltatás igénylése a tanúsítványszolgáltatásra vonatkozó megfelelő eljárásokkal (lásd 4. fejezet) együttesen is történhet.

4.1.2 Az igénylés folyamata és a résztvevők felelőssége

A tanúsítványigénylés folyamata az Igénylő által a Szolgáltató Központi vagy Kihelyezett Regisztrációs Egységéhez eljuttatott igényléssel kezdődik és a tanúsítvány kibocsátásával végződik. A folyamat során az Igénylő az igénylésben megadott adatok helyességéért, a Szolgáltató pedig azok ellenőrzéséért és a tanúsítvány alanyadatainak helyes megjelenítéséért felelős.

A tanúsítványigénylés folyamata

Tanúsítványigénylés a Szolgáltató weboldalán elérhető Ügyfélmenüben történő regisztrációt (lásd alább) követően az Ügyfélmenübe bejelentkezve a tanúsítványigénylés funkció kiválasztásával és a rendszer által kért adatok (lásd alább) megadásával kezdeményezhető.

Tesztelési célú tanúsítvány (lásd 7.1. fejezet) igénylését Ügyfél a Szolgáltató Regisztrációs Egységéhez eljuttatott e-mailben (lásd 1.1.2 fejezet) kezdeményezheti. Az ügyféllel egyeztetett

igény a Szolgáltató jogi osztályának jóváhagyásával teljesíthető. Belső tesztelési célra a Szolgáltató bármely munkatársa a Szolgáltató Belső ellenőrével való egyeztetést követően igényelhet teszt tanúsítványt.

NL Sign szolgáltatás esetén a tanúsítványigénylést a szolgáltatás rendszerében kell elvégeznie Igénylőnek.

Az ÁSZF szerinti szolgáltatáscsomagok esetén az Igénylés a Szolgáltató weboldalán elérhető csomagmegrendelő űrlapok kitöltésével és elküldésével kezdeményezhető. Ebben az esetben az Ügyfélmenü regisztráció (lásd alább) és az igénylés Szolgáltató rendszerében való rögzítése (lásd alább) a Szolgáltatóhoz beküldött megrendelő űrlapon megadott adatok alapján jön létre.

A tanúsítványigénylés fent leírt módjaitól Ügyféllel vagy Kihelyezett Regisztrációs Egység közreműködése esetén a Szolgáltatói partnerrel történő külön megállapodás alapján Szolgáltató eltérhet (pl. tömeges tanúsítványigénylés vagy speciális tanúsítványtípus esetén).

A tanúsítványigénylési folyamat során a Szolgáltató a tanúsítványigénylés során megadott adatok alapján elkészíti, és elektronikus formában eljuttatja Igénylőhöz az igényelt tanúsítvány kiadására vonatkozó Szolgáltatási szerződést.

A tanúsítványigényléshez szükséges tanúsítványigénylési eljárás részben automatizált folyamat, részben pedig humán beavatkozással zajlik. Az ennek során az Igénylő részéről megtenni szükséges lépéseket részletesen a Szolgáltató weboldaláról letölthető útmutatók tartalmazzák.

i. Az Ügyfélmenü regisztrációkor rögzített adatok

Szolgáltató tanúsítványigénylésekhez, illetve az Igénylővel és Előfizetővel való kapcsolattartáshoz szükséges adatokat rögzíti.

Igénylő személyes Ügyfélmenü regisztrációjakor Szolgáltató az alábbi adatokat rögzíti és őrzi meg informatikai rendszerében:

- név (kötelező);
- személyazonosító igazolvány száma (kötelező)
- lakcím ország (kötelező);
- lakcím város (kötelező);
- lakcím irányítószám, utca, házszám (opcionális);
- telefon (kötelező);
- email cím (kötelező);
- bejelentkező név (kötelező);
- jelszó (kötelező);
- jelszó emlékeztető (opcionális).

Amennyiben jogi személy részére történik tanúsítványigénylés (szervezeti, üzleti, OV SSL vagy EV SSL profil esetén, lásd 7.1), az alábbi adatok rögzítése is szükséges:

- név (kötelező);
- székhely országa (kötelező);
- székhely városa (kötelező);
- székhely irányítószáma, utca, házszám (opcionális);
- telefon (opcionális);
- email cím (kötelező).

Weboldal-hitelesítő tanúsítvány (OVCP és EVCP) esetén Szolgáltató informatikai rendszerében az alábbi adatokat rögzíti és őrzi meg.

- szerver elnevezése (kötelező);
- ország (kötelező);
- város (kötelező);
- domain nevet tartalmazó URL (kötelező).

ii. Tanúsítványigényléskor megadandó és rögzített adatok

Tanúsítványigénylés az igényelt tanúsítványprofil szerint az alábbi adatok benyújtásával kezdeményezhető. A tanúsítványprofiltól függetlenül megadandók továbbá az Előfizető szerződéskötéshez és számlázáshoz szükséges adatai, valamint Igénylő bejelentkező neve és jelszava.

TANÚSÍTVÁNY-PROFIL (lásd 7.1. fejezet)	**BENYÚJTANDÓ ADATOK**⁕
SZEMÉLYES PROFIL	A tanúsítvány Alanyaként feltüntetésre kerülő Igénylő természetes személy adatai: ● személyazonosító okmányának száma; ● személyazonosító okmányában szereplő családi és utóneve vagy utónevei; ● lakcímet igazoló hatósági igazolványában szereplő lakcíme vagy tartózkodási helye; ● saját email címe.
ÁLNEVES PROFIL	● A tanúsítványt Igénylő természetes személy adatai a személyes profillal megegyezően; ● a tanúsítványban használni kívánt álneve.
ÜZLETI PROFIL	● A tanúsítvány Alanyaként feltüntetésre kerülő Igénylő természetes személy adatai a személyes profillal megegyezően (kivéve lakcím). ● A tanúsítvány Alanyaként feltüntetésre kerülő szervezet és képviselőjének/meghatalmazottjának adatai a szervezeti profillal megegyezően.
SZERVEZETI PROFIL	A tanúsítvány Alanyaként feltüntetésre kerülő szervezet adatai: ● azonosító dokumentumban szereplő neve; ● azonosító dokumentumban szereplő székhelye; ● szervezeti egységének megnevezése (opcionálisan, kivéve weboldal-hitelesítő tanúsítványok esetén); ● email címe; ● adószáma; ● a szervezet képviselőjének/képviselőinek vagy meghatalmazottjának ○ neve ○ e-mail címe.
OV és EV WEBOLDAL-HITELESÍTŐ PROFIL	A szervezeti profilnál megadott valamennyi adat valamint a tanúsítvány Alanyaként feltüntetésre kerülő domian név vagy domain nevek megadása is szükséges, valamint Igénylőnek tanúsítványkérelem fájlt (Certificate Signing Request - CSR) is át kell adnia.
⁕ *A bekért adatok köre esetenként bővebb is lehet.*	

Tesztelési célú tanúsítvány (lásd 7.1. fejezet) igénylésekor Igénylőnek a tesztelés célját és a tesztelendő tanúsítvány profilját kell megadnia.

iii. Dokumentumok benyújtása

Amennyiben a 3. fejezet alapján Igénylő személyazonosításához személyazonosító dokumentumának másolatára tart igényt Szolgáltató, azt Igénylőnek a tanúsítványigénylése rögzítését követően mihamarabb el kell küldenie Szolgáltató erre dedikált email címre (lásd 1.1.2).

Amennyiben a 3. fejezet szerint valamely tanúsítványigénylésben szereplő entitás azonosításához, jog vagy felhatalmazás illetve tanúsítványba kerülő adat ellenőrzéséhez – közhiteles vagy más megbízható adatforrás hiánya vagy aránytalanul magas költséggel járó elérése esetén – közokirat vagy más hivatalos dokumentum szükséges, Igénylőnek az igénylés benyújtását követően ezen dokumentumokat be kell mutatnia vagy azok közjegyző által hitelesített másolatát vagy fordítását el kell juttatnia Szolgáltatónak. A dokumentumok egyszerű elektronikus másolatát Igénylő előzetesen megküldheti elektronikus formában az erre dedikált email címre (lásd 1.1.2), mellyel az igénylési folyamat előrehaladását segítheti.

A dokumentumokról Szolgáltató az Igénylés rögzítését követően emailben küld pontos tájékoztatást Igénylőnek.

iv. További feltételek tanúsítványigénylés kapcsán

1. Az Igénylőnek a fentieken kívül meg kell adnia
   a. a tanúsítvány tervezett felhasználási célját,
   b. az Előfizető típusát (magánszemély, vállalat, kormányzat vagy egyéb),
   c. valamint a 4.2.1 pontban leírtak szerint hitelesített Szolgáltatási szerződést át kell adnia a Szolgáltatónak.
2. Az Ügyfél a Szolgáltatási szerződés aláírásával nyilatkozik az alábbiakról:
   a. a szerződésben szereplő személyes adatai a valóságnak megfelelőek és azokat önkéntesen adta meg a Szolgáltatónak;
   b. megismerte, érti és elfogadja a Szolgáltató Általános Szerződési Feltételeit, az igényelt tanúsítványra vonatkozó jelen Szolgáltatási szabályzatot és a Szolgáltató Bizalmi Szolgáltatási Rendjét, melyek elérhetők a Szolgáltató weboldalán;
   c. a szerződéskötést megelőzően a szerződés megkötéséhez szükséges jogszabályok szerinti tájékoztatást megkapta, és a tanúsítványra vonatkozó korlátozásokat (pl. kulcshasználat vagy szolgáltatói felelősségvállalás,) megismerte;
   d. weboldal-hitelesítő tanúsítvány esetén hozzájárul, hogy Szolgáltató a tanúsítványt – kibocsátása előtt – közzétegye egy nyilvánosan elérhető „Certificate Transparency” nyilvántartásban (lásd 3.2.5) és elfogadja, hogy a tanúsítványa kibocsátása kizárólag e közzétételt követően lehetséges;
   e. felhatalmazza Szolgáltatót a Szolgáltatási szerződésben megjelölt tanúsítvány kibocsátására.
3. Az Ügyfél a Szolgáltatási szerződés aláírásával továbbá igazolja, hogy
   a. hozzájárul az Ügyfélmenü regisztráció és az Igénylés során megadott adatok kezeléséhez;
   b. kéri a szerződés szerinti nyilvános kulcs hitelesítését és a tanúsítvány nyilvános tanúsítványtárba való felvételét, tárolását és kezelését (lásd még 4.4.2. fejezet);
   c. ismeri a szerződő felek jogait és kötelezettségeit.
4. Amennyiben a tanúsítvány alanyaként szervezet feltüntetésre kerül, a képviselőjének vagy meghatalmazottjának a Szolgáltatási szerződésben, vagy - ha a Szolgáltatási szerződéshez külön került csatolásra - a Szolgáltatási szerződéshez tartozó mellékletben nyilatkozik az alábbiakról:
   a. a tanúsítványigénylés tudtával és hozzájárulásával történik;
   b. meghatalmazza Igénylőt, hogy a tanúsítvány igénylésével, illetve
      i. felfüggesztésével, visszavonásával, aktiválásával (4.9),
      ii. megújításával (4.6),
      iii. módosításával (4.8),
      iv. a kulcsok cseréjével (4.7) kapcsolatban eljárjon;
   c. vállalja a szerződés kapcsán felmerülő szolgáltatási díjak megfizetését;
   d. megismerte, érti és elfogadja az ÁSZF-et, az igényelt tanúsítványra vonatkozó jelen Szolgáltatási szabályzatot és a Bizalmi Szolgáltatási Rendet, melyek elérhetők a Szolgáltató weboldalán (lásd 1.1.2 pont).

Ügyfelek felelőssége

Az igénylés során Igénylő felelőssége a jelen (4.1.2) fejezetben részletezett adatok pontos megadása, a Szolgáltató által emailben küldött tájékoztatók megismerése valamint a Szolgáltató által kért lépések megtétele. Amennyiben jelen szabályzat az igényelt tanúsítvány kibocsátásához előírja, Igénylő felelős személyazonossága igazolásáért a 3. fejezet szerint.

A Szolgáltatási szerződést az Igénylőnek és Előfizetőnek - a 4.2.1 fejezetben foglaltak szerint kell

aláírnia.

4.2 Tanúsítványigénylések feldolgozása

Jelen (4.2.) fejezet szabályai mind az új tanúsítványigénylés (4.1. fejezet), mind pedig a megújítási (4.6. fejezet), a módosítási (4.8. fejezet) vagy a kulcscsere (4.7. fejezet) igénylések feldolgozására egyaránt vonatkoznak - beleértve a Tanúsítványkibocsátást megelőző azonosítási-hitelesítési eljárást, a kiadott tanúsítvány Ügyfél általi elfogadását vagy visszautasítását és a feldolgozás időtartamát. Amennyiben Szolgáltató valamely igény feldolgozására a jelen fejezetben foglaltaktól eltérő szabályokat alkalmaz, azokat a megfelelő fejezetek tartalmazzák.

A tanúsítványigénylések feldolgozása során az elektronikus megrendelő űrlap kitöltésével megadott személyes és szervezeti adatok ellenőrzését, az Igénylő azonosítását és eljárási jogának ellenőrzését, valamint – eszköz igénylése esetén – a kulcspár generálását a Központi vagy Kihelyezett Regisztrációs Egységek munkatársai végzik. A Szolgáltatási Szerződés – az igénylés módjától függően – automatizmussal vagy a Regisztrációs Egységek munkatársainak közreműködésével készül.

A NETLOCK SIGN szolgáltatás igénybevétele esetén a kulcsgenerálásban a Központi vagy Kihelyezett Regisztrációs Egység nem vesz részt. A kulcsgenerálást a felhasználók végzik, a tanúsítványigénylést követően, a NETLOCK SIGN védett környezetében.

A Szolgáltató az Igénylés során ellenőrzi a megadott email cím valódiságát is, innen kéri a tanúsítványigénylés megerősítését, valamint utasításokat és információkat továbbít ide, melyek Igénylő általi teljesítése és megismerése elengedhetetlen a tanúsítványigénylési eljárás lefolytatásához.

Amennyiben a magánkulcs generálása az igénylés vagy szolgáltatói ajánlat alapján Szolgáltató által biztosított Ügyféleszközre történik, a Szolgáltató az igénylés feldolgozása során elvégzi a kulcsgenerálást (lásd 6.1 fejezet), majd ezt követően összeállít egy csomagot, mely tartalmazza

- az Ügyféleszközt és amennyiben használatához szükséges, az Ügyféleszköz-olvasót;
- az Ügyféleszköz első használatbavételéhez szükséges tájékoztatót.

A csomag (Ügyféleszköz, olvasó és tájékoztató) elkészültéről a Szolgáltató az Igényléskor megadott email címen értesíti az Ügyfelet, melyet ezután az Átvevő az emailben megadott helyen és módon átvehet.

4.2.1 Azonosítás és hitelesítés

A Tanúsítványkibocsátást megelőzően elvégzendő azonosítási és hitelesítési feladatokat a Szolgáltató Regisztrációs Egységei abban az esetben végzik el, ha a tanúsítványigénylés során Igénylő az összes adatot és információt megadta, illetve ezek igazolására az összes szükséges okmány és dokumentum másolatát megküldte, melyet jelen szabályzat értelmében a Szolgáltató részére az igényelt tanúsítványprofilnak megfelelően meg kell adnia, illetve el kell küldenie (lásd 4.1.2. fejezet).

Az igénylés során megadott vagy beszerzett adatokat, illetve Igénylő személyazonosságát és eljárási jogát a Szolgáltató Regisztrációs Egységei a 3. fejezetben írtak szerinti független forrásokból ellenőrzik. A Regisztrációs Ügyintézők és Regisztrációs Felelősök a Regisztrációs Egységek belső működési szabályzatában foglalt munkafolyamatokra vonatkozó előírásokat betartva végzik az azonosítási és hitelesítési eljárást. E működési szabályzatok további - jelen szabályzatban nem tárgyalt - előírásokat tartalmazhatnak a Szolgáltató által kiemelt kockázatúnak minősített tanúsítványigénylések azonosítására és ezek kiegészítő ellenőrzési eljárására vonatkozóan.

Igénylő és Előfizető azonosítása tekintetében lásd a 3.2 és 3.3 fejezeteket.

Szolgáltatási szerződés hitelesítése és Szolgáltatóhoz való eljuttatása

Szolgáltatási szerződés hitelesítése minden tanúsítványkibocsátást megelőzően szükséges az Igénylő és adott esetben az Előfizető részéről, akkor is, ha a tanúsítványkibocsátás alapja egy korábban végzett adatellenőrzés.

A Szolgáltatási szerződés tartalmazza az Igénylő és Előfizető nyilatkozatát arra vonatkozóan, hogy a kötelezettségeiket megismerték és azok betartását vállalják.

A Szolgáltatási szerződés hitelesíthető és benyújtható papír alapon kézi aláírással és elektronikus úton, elektronikus aláírással és adott esetben bélyegzővel ellátva.

A papír alapú Szolgáltatási szerződést Igénylőnek a személyazonosító okmányban rögzített kézi aláírással megegyezően kell aláírnia. Előfizetőnek - amennyiben személye eltér az Igénylő személyétől - a papír alapú meghatalmazást képviselője vagy meghatalmazottja útján a benyújtott hiteles aláírásmintán (lásd 3.2.3) szereplő aláírással megegyezően kell aláírnia.

A Szolgáltatási szerződés elektronikus hitelesítése esetén az aláíráshoz használt tanúsítványban feltüntetett személyazonosító adatoknak meg kell egyezniük a Szolgáltatási szerződésben megjelölt Igénylő / Előfizető képviselő vagy meghatalmazott személyes adataival vagy a meghatalmazásban megjelölt egyértelmű tanúsítványazonosító adatokkal. Előfizető bélyegzőt is használhat a hitelesítéshez. Ez esetben a bélyegzőben feltüntetett szervezetazonosító adatoknak meg kell egyezniük a Szolgáltatási szerződésben megjelölt Előfizető adataival.

Amennyiben a meghatalmazás nem a Szolgáltatási szerződés részét képezi, hanem külön dokumentum, a szerződés és a meghatalmazás aláírásának módja eltérő is lehet, azaz lehet az egyik papír alapú, míg a másik elektronikus.

A Szolgáltatási szerződés aláírására Igénylő nem adhat meghatalmazást másnak, Előfizető nevében azonban meghatalmazott is aláírhatja a Szolgáltatási szerződést.

A Szolgáltatási szerződés aláírására Igénylő nem adhat meghatalmazást másnak, Előfizető nevében azonban meghatalmazott is aláírhatja a Szolgáltatási szerződést. Az Előfizető nevében meghatalmazottként eljáró személy Igénylő is lehet, ebben az esetben a szolgáltatási szerződést Ügyfél részéről kizárólag Igénylő írja alá, mellyel saját nevében és Előfizető nevében egyaránt nyilatkozik. Szolgáltató a szolgáltatási szerződést, annak elfogadását követően saját elektronikus bélyegzőjével vagy a Regisztrációs Egység erre meghatalmazással rendelkező munkatársa elektronikus vagy kézi aláírásával hitelesíti. Elektronikus aláírás vagy bélyeg esetén annak tanúsítványa NCP, NCP+ vagy QCP hitelesítési rendek alapján kerül kiadásra. Szolgáltató, miután maga részéről hitelesítette a szolgáltatási szerződést, azt elektronikus másolatként is eljuttathatja Igénylőhöz.

CAA ellenőrzés (OVCP és EVCP)

A Szolgáltató – weboldal-hitelesítő tanúsítványok (OVCP és EVCP) esetén – CAA ellenőrzést végez.

A CAA ellenőrzés során lekéri a domain CAA rekordját.

Szolgáltató engedélyezettnek tekinti maga számára a tanúsítványkiadást, amennyiben:

- nem wildcard domain estén a CAA rekord issue tartalma „netlock.hu”, „netlock.net” vagy „netlock.eu”;
- wildcard domain estén a CAA rekord issuewild tartalma „netlock.hu”, „netlock.net” vagy „netlock.eu”.
- CAA rekord nem elérhető.

Amennyiben a CAA rekordban issue vagy issuewild szerepel, de üres, Szolgáltató a tanúsítvány kibocsátását megtagadja.

4.2.2 Tanúsítványigénylések elfogadása vagy visszautasítása

Az Igénylés beérkezését a Szolgáltató elektronikus úton küldött automatikus válaszlevélben igazolja vissza az Igénylés során megadott email címre. Az automatikus visszaigazolás nem jelenti az Igénylés Szolgáltató általi elfogadását, mindössze arról tájékoztatja Ügyfelet, hogy az Igénylés beérkezett a Szolgáltató valamely Regisztrációs Egységéhez és megkezdi annak feldolgozását.

A Szolgáltató Regisztrációs Egységei a tanúsítványigénylés feldolgozása során döntenek annak elfogadásáról vagy visszautasításáról. A tanúsítványigénylést a Regisztrációs Egységek akkor fogadják el, ha a 4.2.1. fejezet szerinti azonosítási és hitelesítési lépések sikeresen lezajlottak, azaz:

- Igénylő személyazonosítása sikeres;
- a tanúsítvány alanyaként feltüntetésre kerülő adatok valódiságának ellenőrzése sikeres és az adatok valódiak;
- a Szolgáltatási szerződés megfelelően aláírásra került.

Amennyiben az azonosítás és hitelesítés sikeresen megtörténik, valamint az aláírt Szolgáltatási szerződés elfogadásra került, az ellenőrzést végző munkatárs jóváhagyja a tanúsítványigénylést.

A Szolgáltató Igénylőt hiánypótlásra szólítja fel, amennyiben a 4.2.1. fejezet szerinti azonosítási és hitelesítési lépések eredménytelenek, és ennek oka, hogy

- az igénylés feldolgozásához a Szolgáltatónak nem áll rendelkezésre minden szükséges adat, illetve dokumentum (lásd 4.1.2 fejezet), *vagy*
- a rendelkezésre álló adat nem hiteles illetve hitelessége nem állapítható meg, *vagy*
- Igénylő jogosultsága a tanúsítványigénylésre nem állapítható meg.

A Szolgáltató a tanúsítványigénylést visszautasítja vagy törli, amennyiben a 4.2.1. fejezet szerinti azonosítási és hitelesítési lépések eredménytelenek vagy sikertelenek, és ennek oka, hogy

- az igényléskor megadott adatok nem valódiak, *vagy*
- az Igénylő nem jogosult az adott tanúsítványigénylés beadására.

További körülmények, melyek a tanúsítványigénylés visszautasítását vagy törlését eredményezhetik:

- Általános, üzleti, jogi körülmények:
  - az Igénylő a Szolgáltató hiánypótlási, pontosítási felszólításának határidőben nem tesz eleget;
  - a szolgáltatás díjának kiegyenlítése nem történik meg az ÁSZF-ben meghatározott határidőre;
  - Előfizetőnek valamely jelen szabályzat szerinti szolgáltatással kapcsolatos díjtartozása van;
  - az Ügyféleszközt az arra jogosult nem veszi át az első értesítést követő 60 napon belül;
  - a kérelem beadás dátumától számított 60 naptári napon belül bármely okból nem teljesülnek a tanúsítványkiadáshoz szükséges feltételek;
  - a tanúsítvány alanyaként feltüntetésre kerülő szervezet ellen jogerős felszámolási vagy végelszámolási határozat van hatályban;
  - a tanúsítvány alanyaként feltüntetésre kerülő entitás(ok) és/vagy az Igénylő lakhelye/székhelye az Európai Unió vagy Magyarország által technológiai vagy gazdasági embargóval sújtott országban van.
- Azonosítással és hitelesítéssel kapcsolatos körülmények:
  - NL Sign szolgáltatás esetén a Végfelhasználó nem hagyta jóvá az igénylést;
  - a tanúsítvány alanyaként feltüntetésre kerülő entitás(ok) és Igénylő/Előfizető kapcsolata nem egyértelmű;
  - Igénylő jogosultsága a tanúsítvány igénylésére nem egyértelmű;
  - a tanúsítványigénylésben megadott adatok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel;

- a tanúsítványigénylésben megadott adatok igazolása céljából bemutatott vagy másolatban elküldött okmányok/dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel;
- Igénylő és/vagy Előfizető nem járul hozzá a tanúsítványigénylésben megadott adatok igazolása céljából bemutatott okmányokról, dokumentumokról való másolatkészítéshez és/vagy a másolatok eltárolásához;
- a tanúsítványigénylés tárgya jogi személyiséggel nem rendelkező szervezet vagy társulás adatait tartalmazó tanúsítvány kibocsátása;
- egyéb a szolgáltató szabályzatit sértő körülmény.

Az elutasított igényekről az Igénylő értesítést kap, melyben szerepel az elutasítás indoka.

A Szolgáltató egyes - belső működési szabályzatában meghatározott - domain végződések esetén és belső domain nevekre nem ad ki weboldal-hitelesítő (OVCP és EVCP) tanúsítványt, az ilyen domain nevet tartalmazó igényléseket automatikusan elutasítja.

4.2.3 A tanúsítványigénylés feldolgozásának időtartama

A Tanúsítványigénylés akkor tekinthető feldolgozottnak, ha a tanúsítvány kibocsátásra került, vagy az igénylést a Szolgáltató elutasította.

A Szolgáltató a tanúsítványigényléshez szükséges, az Igénylő által küldött dokumentumok kézhezvételétől vagy az eredeti dokumentumok Igénylő általi bemutatásától számított 14 munkanapon belül feldolgozza a tanúsítványigénylést. A Szolgáltató a tanúsítványt a tanúsítvány kibocsátásához szükséges feltételek teljesülése esetén alapesetben további 3-5 munkanapon belül bocsátja ki.

Hiánypótlási felszólítás esetén a hiánypótlás időtartama nem számít be a tanúsítványigénylés feldolgozásának határidejébe.

4.3 Tanúsítvány kibocsátása

Jelen (4.3.) fejezet szabályai mind az új tanúsítványigénylés (4.1. fejezet), mind pedig a megújítási (4.6. fejezet), a módosítási (4.8. fejezet) vagy a kulcscsere (4.7. fejezet) igénylések feldolgozására vonatkoznak - beleértve a Szolgáltató tanúsítványkibocsátás során végzett tevékenységeit és a Végfelhasználó értesítését a tanúsítvány kibocsátásáról. Amennyiben Szolgáltató a módosítási, megújítási vagy kulcscsere igények alapján végzett tanúsítványkibocsátásra a jelen fejezetben foglaltaktól eltérő szabályokat alkalmaz, azokat a megfelelő fejezetek tartalmazzák.

A tanúsítvány kibocsátásának időpontja az az időpont, amikor a Szolgáltató az aláírt tanúsítványt elérhetővé teszi az Ügyfélmenüben - a tanúsítvány érvényességének kezdete ettől eltérő időpont is lehet.

Végfelhasználói tanúsítványok kibocsátása

Végfelhasználói tanúsítványok kibocsátásának feltétele egy előzőleg Igénylő által a Szolgáltatóhoz eljuttatott 4.1. fejezet szerinti tanúsítványigénylés. A tanúsítványt a Szolgáltató csak akkor bocsájtja ki, ha az igénylés a 4.2. fejezetben foglaltak szerint feldolgozásra került.

A Szolgáltató Központi vagy Kihelyezett Regisztrációs Egysége által jóváhagyott tanúsítványigénylés Szolgáltató Hitelesítési Egységéhez kerül, amely gondoskodik a tanúsítványkibocsátás megtörténtéről. A tanúsítványt kizárólag az Igénylés feldolgozása során ellenőrzött adatokkal adhatja ki a Szolgáltató.

A díjfizetés az ÁSZF-ben meghatározott módon a tanúsítvány kibocsátása előtt esedékes. A Szolgáltató Előfizetővel ettől eltérően is megállapodhat: ebben az esetben Szolgáltató a szolgáltatási díj kiegyenlítése előtt előállíthatja és kibocsáthatja a tanúsítványt, emellett pedig meghatározza, hogy mely időpontig kell Előfizetőnek a szolgáltatás díját kiegyenlítenie.

Végfelhasználó a kulcsokat a tanúsítvány kibocsátását követően tudja használatba venni az alábbiak szerint.

TANÚSÍTVÁNY	KULCSOK ÉS A TANÚSÍTVÁNY HASZNÁLATBA VÉTELE
SZOFTVERES TANÚSÍTVÁNY	Szoftveres tanúsítvány esetén Igénylő kulcsot saját maga generálta a számítógépén. Kibocsátását követően a tanúsítványt Végfelhasználónak telepítenie kell számítógépére a Szolgáltató weboldaláról letölthető útmutató alapján. A kulcsok és a tanúsítvány ezt követően vehetők használatba.
ESZKÖZÖS TANÚSÍTVÁNY	Szolgáltató csak arra jogosult Átvevőnek adja át az igényelt Ügyféleszközt. A tanúsítványt - kibocsátását követően - Végfelhasználónak fel kell töltenie az ügyféleszközre a Szolgáltató weboldaláról letölthető útmutató alapján. A kulcsok és a tanúsítvány ezt követően vehetők használatba. Amennyiben a tanúsítványban szereplő kulcsokat az igénylés során a Szolgáltató generálta, a tanúsítvány kiadására csak abban esetben kerül sor, amennyiben Szolgáltató meggyőződött arról, hogy az Ügyféleszközt az arra jogosult Átvevő átvette. Igénylővel történő előzetes megállapodás alapján azonban Szolgáltató az eszköz átadását megelőzően is kibocsáthatja és az ügyféleszközre felfüggesztett állapotban feltöltheti a tanúsítványt. Ebben az esetben Végfelhasználónak az átvétel után haladéktalanul, de legkésőbb a 4.9.13 pontban meghatározott időn belül aktiválnia kell a tanúsítványt. A kulcsok és a tanúsítvány ezt követően vehetők használatba. Közigazgatási tanúsítványok esetén Előfizetőnek a tanúsítvány kibocsátását követően az Ügyféleszköz átvételét vissza kell igazolnia, melyről a Szolgáltató emailben tájékoztatja Igénylőt. Amennyiben a sikeres kézbesítést visszaigazolása a tanúsítvány kibocsátását követő 60 napon belül nem történik meg, a tanúsítványt a Szolgáltató visszavonja.
OV, EV SSL	SSL tanúsítvány esetén Igénylő a kulcspárt saját maga generálta a hitelesítendő szerveren. Ebben az esetben a tanúsítvány szerverre telepítését követően vehetők használatba a kulcsok és a tanúsítvány.
NL SIGN SZOLGÁLTATÁS KERETÉBEN KIBOCSÁTOTT TANÚSÍTVÁNY	NL Sign szolgáltatás esetén Igénylő a kulcsot saját maga generálja a NETLOCK Sign rendszerben. A tanúsítvány kibocsátását követően azonnal használatba vehetők a kulcsok és a tanúsítvány.

Szolgáltatói tanúsítványok kibocsátása

A szolgáltatói tanúsítványok kiadása a Szolgáltató Információbiztonsági Szabályzatában meghatározott módon, legalább két bizalmi munkatársának kontrollja mellett jegyzőkönyvezetten történik. A szolgáltatói tanúsítványokat a Szolgáltató a 2.2 pontban meghatározott módon és időtartam alatt teszi közzé.

4.3.1 A Szolgáltató tevékenysége a tanúsítvány kibocsátás során

Végfelhasználói tanúsítványok

A Szolgáltató az igénylés során megadott adatok alapján informatikai rendszerében létrehozza, majd a Szolgáltatási szerződés aláírása és elfogadása után szolgáltatói tanúsítványával hitelesíti, és Végfelhasználó számára elérhetővé teszi a tanúsítványt. Az Igénylő ellenkező nyilatkozatát kivéve a tanúsítvány ezt követően a nyilvános tanúsítványtárban is elérhetővé válik (lásd. 4.4.2. fejezet). E tevékenységek - azaz a kibocsátás - során a Szolgáltató biztosítja a teljes folyamat biztonságát, megakadályozva a tanúsítványok hamisíthatóságát.

Szolgáltató és Előfizető előzetes ellenkező megállapodását kivéve a tanúsítvány kibocsátása csak

a szolgáltatás díjának kiegyenlítését követően lehetséges, ezért Szolgáltató a tanúsítvány kibocsátását megelőzően az igénylés során megadott számlázási adatok alapján elkészíti a szolgáltatás díjának kiegyenlítéséhez szükséges papír vagy elektronikus számlát vagy díjbekérőt és eljuttatja azt igényléskor megadott számlázási/email címre (lásd még ÁSZF).

Szolgáltatói tanúsítványok

A tanúsítvány elérhetővé tételével egy időben a Szolgáltató weboldalán rövid leírást tesz közzé a végfelhasználói tanúsítványokat hitelesítő szolgáltatói tanúsítvány céljáról. Az Időbélyeg-válaszokat hitelesítő és egyéb szolgáltatói tanúsítványok a Szolgáltató nyilvános tanúsítványtárából tölthetők le. A kibocsátás során a Szolgáltató biztosítja a teljes folyamat biztonságát, megakadályozva a tanúsítványok hamisíthatóságát.

4.3.2 Értesítés a tanúsítvány kibocsátásáról

A tanúsítvány kibocsátásáról - legkésőbb a tanúsítvány érvényességének kezdőnapján - a Szolgáltató a tanúsítványban szereplő e-mail címen értesíti Ügyfelet.

A Szolgáltató a kibocsátásáról értesítő emailben tájékoztatást nyújt a tanúsítvány letöltéséről és telepítéséről vagy aktiválásáról.

Speciális rendelkezések a közigazgatási ügyintézőkre és a kiadmányozókra vonatkozóan

Szolgáltató a magánkulcs előállításának tényéről és a tanúsítvány kibocsátásáról értesíti az Igénylőt meghatalmazó hatóságot is. Az értesítés e-mailben, a hatóság által az Igénylés során megadott email címre történik.

4.4 Tanúsítvány elfogadása

Jelen (4.4) fejezet szabályai mind az új tanúsítványigénylés (4.1. fejezet), mind pedig a megújítási (4.6. fejezet), a módosítási (4.8. fejezet) vagy a kulcscsere (4.7. fejezet) igénylések alapján kiadott tanúsítványokra egyaránt vonatkoznak. Amennyiben Szolgáltató a módosítási, megújítási vagy kulcscsere igények alapján kiadott tanúsítványokra a jelen fejezetben foglaltaktól eltérő szabályokat alkalmaz, azokat a megfelelő fejezetek tartalmazzák.

4.4.1 A tanúsítványelfogadás módja

A tanúsítvány letöltése vagy aktiválása illetve a magánkulcs használatba vétele előtt Ügyfélnek kötelessége ellenőrizni a tanúsítványban feltüntetett adatok helyességét. A tanúsítvány adatait a Végfelhasználó az Ügyfélmenübe bejelentkezve tekintheti meg. Amennyiben bármilyen rendellenességet, eltérést talál, a tanúsítványt és a magánkulcsot nem veheti használatba, kifogását pedig azonnal jeleznie kell a Szolgáltató Ügyfélszolgálata felé és intézkednie kell a tanúsítvány visszavonása/felfüggesztése érdekében (lásd 4.9 fejezet).

Ügyfélnek ellenőriznie kell a magánkulcs és a tanúsítvány összetartozását, a kulcs felhasználási célja szerinti művelet végrehajtásával, majd a művelet tanúsítvánnyal való ellenőrzésével.

Eszközös tanúsítvány esetén a tanúsítványt, a hozzá tartozó nyilvános kulcsot és annak magánkulcs párját a Szolgáltató elfogadottnak tekinti, amennyiben az Ügyféleszköz átvételét követő 5 munkanapon belül Ügyfél nem jelez a Szolgáltatónak a tanúsítvánnyal kapcsolatos kifogást vagy nem kezdeményezi annak visszavonását vagy felfüggesztését. Egyéb esetben a tanúsítvány kibocsátását követő 5 munkanap elteltével tekinti a Szolgáltató Ügyfél által elfogadottnak a végfelhasználói tanúsítványt.

Speciális szabályok a közigazgatási ügyintézőkre és a kiadmányozásra jogosultakra

A tanúsítványt igénylő hatóság a magánkulcs és a tanúsítvány átvételének tényét írásban köteles igazolni. Amennyiben az átvétel vagy annak igazolása a felhívást követő 60 napon belül nem valósul meg, a Szolgáltató a tanúsítványt visszavonja.

4.4.2 A tanúsítvány közzététele

A Szolgáltató a végfelhasználói tanúsítvány kiadását követően közzéteszi azt a nyilvános tanúsítványtárában, kivéve, ha a tanúsítvány Igénylője másként nyilatkozott. Igénylő ilyen nyilatkozatot a tanúsítványigénylés feldolgozása során e-mailben tehet a Szolgáltató Regisztrációs Egységei felé.

4.4.3 További szereplők értesítése a tanúsítvány kibocsátásról

Végfelhasználói tanúsítványok

A Szolgáltató a 4.3.2 pontban meghatározottakon túl további szereplőket a tanúsítvány kibocsátásáról külön nem értesít.

Szolgáltatói tanúsítványok

Szolgáltató a szolgáltatói tanúsítványok kiadásáról weboldalán (lásd. 1.1.2. fejezet) tesz közzé tájékoztatást.

4.5 Kulcspár és tanúsítvány alkalmazhatósága

4.5.1 A magánkulcs és a tanúsítvány használata

A Tanúsítvány és a benne szereplő nyilvános kulcshoz tartozó magánkulcs a Tanúsítvány “KeyUsage” és “Extended KeyUsage” mezőjében megadott célokra használható a 7.1 fejezet szerint, az 1.4 fejezetben foglaltakkal is összhangban.

Egyéb megkötések a tanúsítvány használatával kapcsolatban:

- Amennyiben a kulcsgenerálás kriptográfiai eszközre történt, Végfelhasználó a magánkulcsot kizárólag azon az eszközön aktiválhatja és használhatja, melyre a kulcsot generálták (lásd még 1.4.1).
- Amennyiben a kulcsgenerálás SCD kriptográfiai eszközre történt, Végfelhasználó a magánkulcsot kizárólag azon a SCD eszközön aktiválhatja és használhatja, melyre a kulcsot generálták (lásd még 1.4.1).
- Amennyiben a kulcsgenerálás nem kriptográfiai eszközre történt, Végfelhasználó a magánkulcsot csak kizárólagosan a saját befolyása alatt álló eszközön aktiválhatja és használhatja.
- A magánkulcs a Végfelhasználó kizárólagos befolyása alatt kell, hogy álljon.
- Lejárt érvényességű, visszavont vagy felfüggesztett állapotú tanúsítvány és kapcsolódó kulcsok használata nem megengedett.
- Amennyiben a Végfelhasználó a magánkulcsról másolatot készít, akkor azt ugyanolyan gondossággal köteles kezelni, mint az eredeti példányt.
- Végfelhasználó azonnal köteles értesíteni a Szolgáltatót, amennyiben az alábbi esetek valamelyike bekövetkezik a tanúsítvány érvényességének vége előtt, és egyúttal köteles azonnal beszüntetni a magánkulcs alkalmazását:
  - a magánkulcs elvesztése, ellopása, kompromittálódása

  - a magánkulcs feletti kizárólagos kontroll elvesztése (pl. az aktiválási adat kompromittálódása) miatt
  - a tanúsítványban feltüntetett adatok pontatlansága vagy változása.
- A végfelhasználói tanúsítványt aláíró szolgáltatói kulcs kompromittálódása esetén a Végfelhasználó azonnal köteles beszünteti a magánkulcs és a tanúsítvány alkalmazását.
- A tanúsítvány érvényességének lejárta vagy visszavonása esetén lásd 6.2.10 fejezet.

Az NL Sign szolgáltatás keretében kibocsátott tanúsítványok kizárólag a NETLOCK Sign rendszerben használhatók.

4.5.2 Az Érintett felek nyilvános kulcs és tanúsítvány használata

A tanúsítvány felhasználása során a Szolgáltató által garantált biztonsági szint megtartásához szükséges, hogy az Érintett Felek megfelelő körültekintéssel járjanak el, a Szolgáltató szabályzataiban leírt követelményeknek megfelelően, különös tekintettel az alábbiakra:

- a nyilvános kulcsokat csak olyan felhasználás esetén fogadja el, amelyek összhangban vannak a Tanúsítvány “KeyUsage” és “Extended KeyUsage” mezőinek tartalmával (lásd 7.1 fejezet);
- ellenőrizze a tanúsítvány érvényességét, és állapotát (lásd 4.9.6 fejezet);
- vegyen figyelembe minden korlátozást, amely a tanúsítványban vagy a tanúsítványban hivatkozott szabályzatokban szerepel (lásd 1.4 és 6.1.7 fejezetek);
- a kulcsok és a tanúsítványok használatára csak megbízható szoftvereket alkalmazzon.

Amennyiben az Érintett fél nem a Szolgáltató szabályzataiban leírtaknak megfelelően jár el, az ebből eredő károkért a Szolgáltató nem vállal felelősséget.

4.6 Tanúsítványmegújítás

Ügyfélnek lehetősége van a Szolgáltató által kibocsátott tanúsítványa érvényességi idejének lejárta előtt igényelni annak megújítását. A megújítás során a Szolgáltató a megújítandó tanúsítványban szereplő nyilvános kulccsal és Alanyadatokkal előállít egy új tanúsítványt.

Megújítás esetén az Ügyfél nem igényelheti az Alanyadatok módosítását, ugyanakkor a tanúsítvány egyéb adatai változhatnak (pl. tanúsítvány sorszám és érvényességi idő, Szolgáltatói adatok, CRL/OCSP elérhetőség).

A végfelhasználói tanúsítványok megújítását a Szolgáltató bármikor kezdeményezheti saját hatáskörben.

A végfelhasználói tanúsítványok többször is megújíthatók, de Szolgáltató jogosult a megújítási igények elutasítására.

4.6.1 A tanúsítványmegújítás körülményei

Ügyfél tanúsítványa megújítását az alábbi feltételek fennállása esetén igényelheti:

- a tanúsítvány érvényes;
- a tanúsítvány lejárata legfeljebb 30 napon belül esedékes;
- a tanúsítványban szereplő nyilvános kulcs kriptográfiailag még biztonságosnak tekinthető és vélhetően az is marad a megújított tanúsítvány érvényességi ideje alatt is;
- a tanúsítványban szereplő nyilvános kulcshoz tartozó magánkulcs nem kompromittálódott.

Szolgáltató a tanúsítvány lejáratát megelőzően legfeljebb 30 nappal a tanúsítványban szereplő e-mail címre értesítést küld, melyben tájékoztatja Ügyfelet a tanúsítvány közelgő lejártáról és a tanúsítványmegújítás / új tanúsítvány igénylésének folyamatáról.

Tanúsítványmegújítás a Szolgáltató weboldaláról letölthető útmutató leírását követve vagy előzetes megállapodás alapján más, írásos módon igényelhető.

Szolgáltató saját hatáskörben az alábbi feltételek fennállása esetén kezdeményezheti végfelhasználói tanúsítvány megújítását:

- a tanúsítvány érvényes;
- a tanúsítványt valamely külső körülmény (pl. jogszabályváltozás vagy felügyeleti határozat) miatt az eredeti érvényesség lejárta előtt vissza kell vonni és a megújítással biztosítható a tanúsítvány új feltételeknek való megfelelése;
- a tanúsítványban szereplő nyilvános kulcs kriptográfiailag még biztonságosnak tekinthető és vélhetően az is marad a megújított tanúsítvány érvényességi ideje alatt is.

A Szolgáltató által kezdeményezett végfelhasználói tanúsítványmegújításról Szolgáltató minden esetben értesítést küld tanúsítványban szereplő e-mail címre.

Szolgáltatói tanúsítványok megújításának feltétele, hogy a megújítandó tanúsítvány érvényes legyen.

4.6.2 Ki igényelheti a tanúsítványmegújítást?

Végfelhasználói tanúsítványok megújítását a megújítandó tanúsítvány Igénylője vagy Előfizetője és a Szolgáltató igényelheti.

4.6.3 A tanúsítványmegújítási igénylések feldolgozása

A tanúsítványmegújítási igénylés beérkezését a Szolgáltató elektronikus úton küldött automatikus válaszlevélben igazolja vissza a tanúsítványban szereplő email címre. Az automatikus visszaigazolás nem jelenti az Igénylés Szolgáltató általi elfogadását, mindössze arról tájékoztatja Igénylőt, hogy az igénylés a Szolgáltató valamely Regisztrációs Egységéhez beérkezett és megkezdi annak feldolgozását.

A tanúsítványmegújítási eljárás részben automatizált folyamat, részben pedig humán beavatkozással zajlik. A Szolgáltató a megújítási igénylés során a megújítandó tanúsítványban szereplő email címre utasításokat és információkat továbbít, melyek Igénylő általi teljesítése és megismerése elengedhetetlen a megújítási eljárás lefolytatásához. A megújítás során az Igénylő részéről megtenni szükséges lépéseket részletesen a Szolgáltató weboldaláról letölthető útmutatók is tartalmazzák.

Igénylőnek a megújítási igénylés során számlázási és az új Szolgáltatási szerződés elkészítéséhez szükséges adatokat kell megadnia. A szolgáltatási szerződést Szolgáltató elektronikus formában juttatja el Igénylőhöz.

Azonosítás és hitelesítés

Tanúsítványmegújítási igénylés esetén az Igénylő azonosítása, valamint a megújított tanúsítvány kibocsátásához szükséges Szolgáltatási szerződés aláírása és a Szolgáltatóhoz való eljuttatása a 4.2.1. fejezet szerint történik, az alábbi eltérésekkel.

Aláíró tanúsítvány esetén, amennyiben Igénylő a vonatkozó szolgáltatási szerződést a megújítás alapjául szolgáló tanúsítványával hitelesíti, a megújított tanúsítványban feltüntetésre kerülő adatokat Szolgáltató a megújítás alapjául szolgáló tanúsítvány alapján ellenőrzi; közhiteles vagy más megbízható adatforrás vagy okirat alapján történő ellenőrzést ebben az esetben a Szolgáltató nem végez, mivel a megújítás alapjául szolgáló tanúsítvány – érvényessége esetén – hitelesen igazolja a tanúsítványba kerülő adatokat.

Megújítás esetén a Szolgáltatási szerződés aláírásával Igénylő az alábbiakról is nyilatkozik:

- az eredeti tanúsítványának kibocsátáskor ellenőrzött adatai változatlanok;
- az adatai valódiságát akkor igazoló dokumentumai még érvényesek;
- nincs tudomása a tanúsítványhoz tartozó magánkulcsa kompromittálódásáról.

A megújítási igénylések elfogadása vagy visszautasítása

A Szolgáltató a megújítási igénylés feldolgozása során dönt annak elfogadásáról vagy visszautasításáról. A tanúsítványigénylést a szolgáltató akkor fogadja el, ha a 4.6.3.1. fejezet szerinti azonosítási és hitelesítési lépések sikeresen lezajlottak.

A megújítási igénylés a Szolgáltatási szerződés érvényes aláírásával tekinthető teljesnek és hitelesnek. A Szolgáltató a Szolgáltatási szerződést nem írja alá, a Szolgáltatási szerződés elfogadását a megújított tanúsítvány kibocsátásával jelzi.

A megújítási igény teljességének és a Szolgáltatási szerződés helyességének és hitelességének ellenőrzését a Szolgáltató Regisztrációs Egységeinek munkatársai végzik. Amennyiben megújítási igényléskor megadott adatok hiányosak és/vagy a Szolgáltatási szerződés helytelen, nem megfelelően hitelesített vagy hitelessége nem állapítható meg, a Szolgáltató Regisztrációs Egysége Igénylőt hiánypótlásra szólítja fel.

A tanúsítványmegújítási igényt Szolgáltató az alábbi körülmények fennállása esetén elutasíthatja:

- a Szolgáltató által kért hiánypótlás a megújítandó tanúsítvány lejártáig nem történik meg;
- az igénylés feldolgozása során a Szolgáltató tudomást szerez a megújítandó tanúsítvány kibocsátásakor ellenőrzött adatok érvénytelenné válásáról - ebben az esetben a megújítandó tanúsítványt a Szolgáltató visszavonja (lásd. 4.9. fejezet);
- Szolgáltatónak a megújítási eljárás során tudomására jut, hogy a megújítandó tanúsítványhoz tartozó magánkulcs kompromittálódott - ebben az esetben azonnal intézkedik a tanúsítvány visszavonásáról is.
- a tanúsítványigénylés visszautasítását eredményező bármely a megújításra is alkalmazható körülmény fennállása;
- az Ügyfélnek kiegyenlítetlen lejárt fizetési határidejű számlája van a Szolgáltató bármely szolgáltatása kapcsán;
- a megújítandó tanúsítvány nem azonosítható egyértelműen.

Szolgáltató egyéb írásbeli indokkal (pl. felügyeleti határozat) is megtagadhatja a tanúsítvány megújítását.

A megújítási igény visszautasítása esetén Ügyfél új tanúsítvány igénylésével tarthatja fenn a szolgáltatás igénybevételének folytonosságát.

A megújítási igény feldolgozásának időtartama

A Szolgáltató a tanúsítványmegújítási igénylést a 4.2.3 pontban meghatározott időtartam alatt dolgozza fel. Hiánypótlási felszólítás esetén a hiánypótlás időtartama nem számít be a megújítási igénylés feldolgozásának idejébe.

A megújított tanúsítvány kibocsátása

A megújított tanúsítványt a feltételek fennállása esetén Szolgáltató az eredeti tanúsítvány érvényességének lejáratát megelőző 2-10 munkanappal bocsájtja ki – a Szolgáltató és az Ügyfél erre vonatkozó megállapodását kivéve.

Szolgáltató nem vállal felelősséget azért, ha a megújított tanúsítvány nem kerül kibocsátásra az eredeti tanúsítvány lejárta előtt és ezzel a szolgáltatás folytonossága megszakad, abban az esetben, ha ehhez az Ügyfél mulasztása vagy késedelme vezetett.

Lásd még 4.3. fejezet.

4.6.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A megújított tanúsítvány kiadásáról Szolgáltató a 4.3.2. fejezet szerint értesíti ügyfelet.

4.6.5 A megújított tanúsítvány elfogadása

A megújított tanúsítvány elfogadására a 4.4.1 pont rendelkezései alkalmazandók.

4.6.6 A megújított tanúsítvány közzététele

A megújított tanúsítvány közzétételére a 4.4.2 pontban foglalt rendelkezések alkalmazandók.

4.6.7 További szereplők értesítése a tanúsítvány kibocsátásáról

A további szereplők értesítésére a 4.4.3 rendelkezései alkalmazandók.

4.7 Kulcscsere

Ügyfélnek lehetősége van a Szolgáltató által kibocsátott tanúsítványa érvényességi idejének lejárta előtt tanúsítványában szereplő nyilvános kulcs és az ahhoz tartozó magánkulcs cseréjét igényelni. A kulcscsere során az Ügyfél saját maga, vagy a Szolgáltató az Ügyfél részére új kulcspárt generál, majd a kulcscsere igénylés alapjául szolgáló tanúsítványban szereplő alanyadatokkal Szolgáltató előállít egy új tanúsítványt, benne az új nyilvános kulccsal. Ügyfélnek a visszavont tanúsítványhoz tartozó magánkulcsot meg kell semmisítenie. (lásd 6.2.10 fejezet).

Kulcscsere esetén az Ügyfél nem igényelheti a kulcson kívül más adat módosítását, ugyanakkor a tanúsítványban változhatnak egyéb adatok (pl. sorszám és érvényességi idő, szolgáltatói adatok, CRL/OCSP elérhetőség).

A kulcscserét Ügyfél írásban igényelheti, melynek módjáról a Szolgáltató weboldalán található tájékoztatás. Az írásos igény mellett a kulcscsere folyamat elindításához Igénylőnek új tanúsítványigénylést is kell kezdeményeznie a 4.1.2. fejezet szerint.

A végfelhasználói tanúsítványok kulcscseréjét a Szolgáltató bármikor kezdeményezheti saját hatáskörben. Saját hatáskörben végzett kulcscseréről a Szolgáltató a tanúsítványban szereplő email címen tájékoztatja az Ügyfelet.

A kulcscserére sor kerülhet érvényes és visszavont (pl. kulcskompromittálódás miatt) tanúsítvány esetén egyaránt.

4.7.1 A kulcscsere körülményei

Ügyfél a tanúsítványhoz tartozó kulcspár cseréjét a tanúsítvány érvényességi idejében kezdeményezheti.

Szolgáltató saját hatáskörben akkor kezdeményezheti végfelhasználói tanúsítvány kulcsainak cseréjét, ha a kulcspár kriptográfiailag már biztonságosnak nem tekinthető vagy valamely külső körülmény (pl. jogszabályváltozás vagy felügyeleti határozat) erre kényszeríti.

A Szolgáltató által kezdeményezett végfelhasználói kulcscseréről a Szolgáltató minden esetben értesítést küld tanúsítványban szereplő e-mail címre.

4.7.2 Ki igényelheti a kulcscserét?

A kulcscsere igénylésére a 4.6.2 pont rendelkezései alkalmazandók.

4.7.3 A kulcscsere igénylések feldolgozása

Az igények feldolgozására a 4.6.3 pont rendelkezései alkalmazandók azzal a különbséggel, hogy az érintett tanúsítvány érvényes állapota, illetve a hozzá tartozó magánkulcs kompromittálódás-mentessége nem elvárás.

4.7.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

Az Ügyfél értesítésére a 4.3.2 pont rendelkezései alkalmazandók.

4.7.5 A kulcscserével megújított tanúsítvány elfogadása

A tanúsítvány elfogadására a 4.4.1 pont rendelkezései alkalmazandók.

4.7.6 A kulcscserével megújított tanúsítvány közzététele

A tanúsítvány közzétételére a 4.4.2 pontban foglalt rendelkezések az alkalmazandók.

4.7.7 További szereplők értesítése a tanúsítvány kibocsátásáról

A további szereplők értesítésére a 4.4.3 pont rendelkezései az alkalmazandók.

4.8 Tanúsítványmódosítás

Ügyfélnek a Szolgáltató által kibocsátott tanúsítványa érvényességi idején belül igényelni kell annak módosítását, amennyiben a tanúsítvány alanyadatai a tanúsítvány érvényességi idején belül megváltoznak.

A tanúsítványmódosítás során a Szolgáltató a módosítandó tanúsítványban szereplő nyilvános kulccsal és az igénylés szerint módosított alanyadatokkal előállít egy új tanúsítványt. Amennyiben az adatok megváltozása miatt a módosítási igénylés alapjául szolgáló tanúsítványban érvénytelen adatok szerepelnek, a Szolgáltató a módosítási folyamat során azt visszavonja (lásd 4.9. fejezet).

Abban az esetben, ha a módosítási igény az igénylés alapját képező tanúsítvány érvényességének lejárta előtti 30 napban történik a módosítás egyúttal megújításnak (lásd 4.6. fejezet) is tekinthető. Ebben az esetben az új tanúsítvány érvényességi idejére vonatkozóan a 4.6. fejezet az irányadó.

Módosítás esetén az alanyadatok igény szerinti módosításán kívül a tanúsítvány egyéb adatai is változhatnak (pl. tanúsítvány sorszám és érvényességi idő, szolgáltatói adatok, CRL/OCSP elérhetőség).

A végfelhasználói tanúsítványok módosítását a Szolgáltató is bármikor kezdeményezheti saját hatáskörben. Erről a Szolgáltató a tanúsítványban szereplő email címen értesíti Ügyfelet. Ebben az esetben az új tanúsítvány érvényességi idejét Szolgáltató határozza meg.

Tanúsítványmódosítás a Szolgáltató weboldaláról letölthető útmutató leírását követve vagy előzetes megállapodás alapján más, írásos módon igényelheti Ügyfél.

A végfelhasználói tanúsítványok többször is módosíthatók, de Szolgáltató jogosult a módosítási igények elutasítására.

4.8.1 A tanúsítványmódosítás körülményei

A tanúsítványmódosítás körülményeire a 4.6.1 pont rendelkezései alkalmazandók, azzal a különbséggel, hogy módosítási igény a tanúsítvány érvényességi idején belül bármikor kezdeményezhető.

4.8.2 Ki igényelheti a tanúsítványmódosítást

A tanúsítványmódosítás igénylőjére a 4.6.2 pont rendelkezései alkalmazandók.

4.8.3 A tanúsítványmódosítási igénylések feldolgozása

A tanúsítványmódosítási igények feldolgozására a 4.6.3 pont rendelkezései alkalmazandók az alábbi a különbségekkel:

- a megváltozott alanyadatokat a Szolgáltató Központi vagy Kihelyezett Regisztrációs Egysége a 4.2.1 fejezet szerint ellenőrzi;
- az alanyadatok változatlanságáról és az eredeti ellenőrzéskor bemutatott dokumentumok érvényességéről szóló nyilatkozat nem vonatkozik a megváltozott adatokra;
- Szolgáltató nem utasítja el az igényt az eredeti tanúsítvány kibocsátásakor ellenőrzött adatok érvénytelensége miatt.

4.8.4 Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A módosított tanúsítvány kiadásáról Szolgáltató a 4.3.2. fejezet szerint értesíti ügyfelet.

4.8.5 A módosított tanúsítvány elfogadása

A megújított tanúsítvány elfogadására a 4.4.1 pont rendelkezései alkalmazandók.

4.8.6 A módosított tanúsítvány közzététele

A módosított tanúsítvány közzétételére a 4.4.2 pontban foglalt rendelkezések az alkalmazandók.

4.8.7 További szereplők értesítése a tanúsítvány kibocsátásáról

A további szereplők értesítésére a 4.4.3 pont rendelkezései az alkalmazandók.

4.9 Visszavonás és felfüggesztés

Ügyfélnek lehetősége van tanúsítványa érvényességi idején belül az tanúsítványállapot megváltoztatását igényelni. Az állapotváltoztatási igény irányulhat a tanúsítvány felfüggesztésére, aktiválására és visszavonására (lásd *Bizalmi Szolgáltatási Rend, 1.6.1. Fogalmak*).

Állapotváltoztatási igény esetén a Szolgáltató az igénylés alapján megváltoztatja az igénylés tárgyát képező tanúsítvány állapotát az alábbiak szerint:

- felfüggeszteni csak érvényes tanúsítványt lehet;
- aktiválni csak felfüggesztett tanúsítványt lehet;
- visszavonni érvényes és felfüggesztett tanúsítványt lehet.

A felfüggesztés meghatározott időtartamra szól, ezen időszakon belül az Ügyfél a tanúsítványt visszavonja vagy újraaktiválja vagy az időszak végén Szolgáltató a tanúsítványt visszavonja. A felfüggesztett tanúsítvány az aktiválást követően újra érvényessé válik, s ezután a felfüggesztés időtartamára is érvényesnek tekintendő. A visszavonás véglegesen érvénytelenné teszi a tanúsítványt a visszavonás (vagy az azt megelőző felfüggesztés) pillanatától.

A visszavonás vagy felfüggesztés vonatkozhat végfelhasználói és szolgáltatói tanúsítványra egyaránt.

Weboldal hitelesítő tanúsítványok (OVCP és EVCP) esetén a felfüggesztés és aktiválás nem értelmezett.

4.9.1 A visszavonást és felfüggesztést indukáló körülmények

A Szolgáltató a végfelhasználói tanúsítvány visszavonására/felfüggesztésére vonatkozó igényt az igény beérkezését követő legfeljebb 24 órán belül az alábbi körülmények figyelembevételével elbírálja, és ennek alapján a tanúsítványt visszavonja vagy felfüggeszti, illetve a visszavonási/felfüggesztési igényt elutasítja.

A végfelhasználói tanúsítványok visszavonását vagy felfüggesztését az alábbi körülmények indukálhatják. Az alábbi esetekben a Szolgáltatónak az Igény beérkezését követő legfeljebb 24

órán belül vissza kell vonnia vagy fel kell függesztenie a tanúsítványt:

- Ügyfél szabályos igénylése (Állapotváltoztatási ügyféligény);
- Ügyfél jelzi a szolgáltatónak, hogy az eredeti tanúsítványigénylés nem volt engedélyezett és azt utólag sem engedélyezi;
- Ügyfél kötelezettségeinek be nem tartása;
- Harmadik fél bejelentése talált ügyféleszközről;
- az ÁSZF által meghatározott egyéb körülmény;
- a tanúsítványban lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódása;
- a tanúsítványt hitelesítő szolgáltatói magánkulcs kompromittálódása;
- jogszerűtlen név- vagy adathasználat,
- a tanúsítványban hibásan rögzített adatok vagy az adatok valótlansága, megváltozása, félrevezetésre alkalmassága;
- Ügyfél nem kérte a tanúsítvány aktiválását a felfüggesztési időn belül;
- a tanúsítvány rosszhiszemű felhasználása;
- bíróság vagy hatóság erre vonatkozó jogerős és végrehajtható határozata;
- a tanúsítvány műszaki jellemzői a mértékadó szakmai ajánlások alapján az elfogadhatónál nagyobb kockázatot jelentenek bármely félnek (pl. kulcshossz ajánlottnál kisebb mérete);
- a szolgáltatási szerződés megszegése vagy megszűnése;
- a tanúsítvány nem a vonatkozó szabályzatok szerint lett kibocsátva;
- a szolgáltató tudomására jut, hogy a tanúsítványban szereplő valamely név (pl. FQDN) használatára az Ügyfél nem jogosult;
- a szolgáltató tudomására jut a tanúsítványban feltüntetett képviseleti jogosultság megszűnése;
- amennyiben a tanúsítványra vonatkozó érvényességi információs szolgáltatások fenntartása megszűnik;
- a bizalmi szolgáltatás megszűnése, kivéve, ha a Szolgáltató korábban gondoskodott az általa kibocsátott tanúsítványok vonatkozásában a CRL és OCSP szolgáltatások fenntartásáról;
- jogszabály teszi kötelezővé.

A tanúsítványok felfüggesztésének lehetséges okai:

- a tanúsítvány kiadását követő kezdeti felfüggesztés a szállítás biztonságának növelésére;
- a tanúsítvány visszavonását indukáló bármely körülményre vonatkozó alapos vélelem.

Weboldal-hitelesítő tanúsítványok (QCP-w és EVC) esetén a felfüggesztése nem értelmezett.

A Szolgáltató legfeljebb 7 napon belül köteles intézkedni a szolgáltatói tanúsítványának visszavonásáról az alábbi esetekben:

- a Hitelesítő Egység szabályos, írásbeli igénylése (kihelyezett kiadó esetén);
- a Hitelesítő Egység jelzi a szolgáltatónak, hogy az eredeti kiadó tanúsítványigénylés nem volt hiteles és azt utólag sem hitelesíti, illetve engedélyezi (kihelyezett kiadó esetén);
- a tanúsítványban lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódása;
- a tanúsítványt hitelesítő szolgáltatói magánkulcs kompromittálódása;
- a tanúsítvány rosszhiszemű felhasználása;
- a tanúsítványban hibásan rögzített adatok vagy az adatok valótlansága, megváltozása, félrevezetésre alkalmassága;
- amennyiben a tanúsítványra vonatkozó érvényességi információs szolgáltatások fenntartása megszűnik;
- a tanúsítvány műszaki jellemzői a mértékadó szakmai ajánlások alapján az elfogadhatónál nagyobb kockázatot jelentenek bármely félnek (pl. kulcshossz ajánlottnál kisebb mérete);
- bíróság vagy hatóság erre vonatkozó jogerős és végrehajtható határozata;
- a bizalmi szolgáltatás megszűnése;

- jogszabály teszi kötelezővé.

4.9.2 Állapotváltoztatási ügyféligényre jogosultak

A tanúsítványfelfüggesztést, -visszavonást és -aktiválást a Szolgáltató, bíróság, a felügyelet vagy más hatóság, valamint végfelhasználói tanúsítványok esetén azok Igénylője és Előfizetője kezdeményezhetik. Szabályozott szakmák esetén a szakmai Kamara abban az esetben, ha az Ügyfél jogosultsága a tanúsítványban jelölt szabályozott szakma gyakorlására megszűnt.

Tanúsítvánnyal történő visszaélés harmadik fél általi bejelentése esetén a Szolgáltató megvizsgálja a körülményeket, és saját hatáskörben dönt a tanúsítvány felfüggesztéséről.

Tanúsítványaktiválást Ügyfél abban az esetben jogosult igényelni, amennyiben a felfüggesztést Igénylő vagy Előfizető igényelte és az igényt indukáló körülmények már nem állnak fenn. Amennyiben Szolgáltató saját hatáskörben függesztette fel a végfelhasználói tanúsítványt, a felfüggesztést indukáló körülmények megszűnésével haladéktalanul aktiválja a tanúsítványt.

4.9.3 A visszavonási, felfüggesztési és aktiválási eljárás

A visszavonási és a felfüggesztési eljárás

A visszavonási vagy felfüggesztési eljárás a visszavonásra vagy felfüggesztésre vonatkozó állapotváltoztatási igény Szolgáltatóhoz történő beérkezésével vagy a Szolgáltató döntésével, illetve utasításával kezdődő és a tanúsítvány visszavonásával vagy felfüggesztésével, illetve nem megfelelő igénylés esetén az igénylés visszautasításával záródó folyamat.

A visszavonásra és felfüggesztésre irányuló igényeket a Szolgáltató más igényeket megelőzően, soron kívül bírálja el.

Visszavonást, felfüggesztést és aktiválást az arra jogosultak (lásd 4.9.2 pont) emailben és telefonon igényelhetnek. A visszavonási, felfüggesztési és aktiválási igénynek legalább a következő adatokat kell tartalmaznia:

- a tanúsítvány sorszáma,
- a visszavonást / felfüggesztést kérő (természetes és adott esetben jogi személy) megnevezése,
- a visszavonást / felfüggesztést kérő elérhetősége,
- a visszavonás / felfüggesztés időpontja (ha nem azonnali),

Felfüggesztést az arra jogosultak saját ügyfélmenüjükbe bejelentkezve is igényelhetnek, mely esetben a felfüggesztés automatikusan megtörténik.

Kulcskompromittálódás vagy -vesztés esetén Szolgáltató kulcscsere eljárást folytatja le (lásd 4.7 fejezet). A visszavonásra irányuló ügyféligényeket Szolgáltató az igény feldolgozásának idejére felfüggesztéssel is kezelheti.

A felfüggesztett tanúsítványhoz tartozó magánkulcs használatát a felfüggesztés ideje alatt szüneteltetni kell. A visszavont tanúsítványhoz tartozó magánkulcsot a visszavonást követően azonnal meg kell semmisíteni, amennyiben ez lehetséges (lásd 6.2.10).

A tanúsítványok állapotának változásaival kapcsolatban felmerülő tanúsítványelfogadásból származó károkra az alábbi felelősségi szabályok vonatkoznak:

- A visszavonási vagy felfüggesztési igény Szolgáltatóhoz történő megérkezéséig az Ügyfél a felelős az esetlegesen felmerülő károkért.
- A felfüggesztési vagy visszavonási igény Szolgáltatóhoz való beérkezését követően, a tanúsítvány megváltozott állapotának közzétételéig a Szolgáltató felel az esetleges felmerülő károkért.
- Amennyiben a Szolgáltató már közzétette a tanúsítvány érvénytelen (visszavont vagy

felfüggesztett) állapotát, a Szolgáltató semmilyen felelősséget nem vállal azért, ha bármely Érintett Fél mégis érvényesnek tekinti a tanúsítványt.

Lásd a 9.6 és 9.8 fejezeteket.

A tanúsítványaktiválási eljárás

A felfüggesztett tanúsítvány (újbóli) érvénybe helyezését azon személyek igényelhetik, akik az adott tanúsítvány tekintetében felfüggesztési és visszavonási igénylésre jogosultak. Az igénylés a 4.9.3.1 pontban meghatározott módon történhet azzal, hogy az Ügyfélmenüben nem kezdeményezhető a tanúsítvány aktiválása. Amennyiben a felfüggesztés 4.9.13 pont szerinti időtartama alatt a tanúsítvány aktiválására nem kerül sor, a felfüggesztési időtartam leteltével a tanúsítvány automatikusan visszavonásra kerül.

4.9.4 Az igénylések feldolgozása

A Szolgáltató az állapotváltoztatási igényeket végrehajtásuk előtt az alábbiak szerint ellenőrzi:

1. Igénylő azonosítása: lásd a 3.4. fejezetben foglaltakat
2. Igénylő jogosultsága: lásd a 4.9.2. fejezetben foglaltakat
3. Az igénylés helyessége: lásd 4.9.3.1 fejezetben foglaltakat

Az állapotváltoztatási igények végrehajthatósága:

- Visszavonási igény esetén: amennyiben a tanúsítvány érvényes vagy felfüggesztett.
- Felfüggesztési igény esetén: amennyiben a tanúsítvány érvényes.
- Aktiválási igény esetén: a tanúsítvány felfüggesztett állapotban van és a felfüggesztést indukáló körülmények már nem állnak fenn.

A Szolgáltató Központi vagy Kihelyezett Regisztrációs Egysége, amennyiben meggyőződött az Igénylő jogosultságáról valamint az igény teljességéről és hitelességéről, haladéktalanul elvégzi a vonatkozó tanúsítvány felfüggesztését/visszavonását.

Amennyiben a fenti elvárások nem teljesülnek, akkor az igénylést a Szolgáltató visszautasítja, egyébként további mérlegelés és halasztás nélkül intézkedik a tanúsítvány visszavonása, felfüggesztése vagy aktiválása érdekében. A visszavonási igényt a visszavonáshoz vezető körülmények tisztázása céljából Szolgáltató ideiglenesen a tanúsítvány felfüggesztésével is kezelheti.

A Szolgáltató minden végrehajtott és visszautasított felfüggesztési, visszavonási és tanúsítványaktiválási igénylésről e-mailben értesíti a tanúsítvány Igénylőjét és Előfizetőjét.

A tanúsítványok állapotának változását a Szolgáltató visszavonási nyilvántartások keretében közzéteszi (lásd 4.9.7.-10 és 4.10. fejezetek).

4.9.5 Állapotváltoztatási igények feldolgozásának maximális ideje

A visszavonási/felfüggesztési/aktiválási igények feldolgozási ideje az igényléshez használt csatorna szerint az alábbi lehet:

CSATORNA	FELDOLGOZÁS IDEJE	FELDOLGOZÁS MAXIMÁLIS IDŐTARTAMA
ÜGYFÉLMENÜ (kizárólag felfüggesztés)	Az igény feldolgozása és végrehajtása folyamatosan 7X24 órában és automatikusan történik.	legfeljebb 24 óra
TELEFON (lásd 1.1.2. fejezet)	Az igények feldolgozása folyamatosan, 7x24 órában történik.	

Amennyiben ezen időszak alatt a Szolgáltató nem képes a visszavonási, felfüggesztési vagy aktiválási igény jogszerűségéről – a benyújtó személy jogosultságáról - megbizonyosodni, úgy a továbbiakban – ellenkező tény tudomására jutásáig – a visszavonási, felfüggesztési, illetve aktiválási igényt illetéktelen személytől származónak tekinti, és a visszavonási vagy felfüggesztési, illetve aktiválási folyamatot eredménytelenként lezárja.

Az állapotváltoztatási igények végrehajtását követően a Szolgáltató a változást érvényesíti:

- a tanúsítványállapot-szolgáltatásban (OCSP) azonnal;
- új visszavonási lista legkésőbb a változást követő 1 órán belül kerül kiadásra;
- a nyilvános tanúsítványtárában legkésőbb a változást követő 1 órán belül.

4.9.6 Javasolt eljárás a tanúsítványállapot ellenőrzésére

A Tanúsítványban foglalt információk elfogadásánál és felhasználásánál szükséges, hogy az Érintett felek - az 1.4. és a 4.5. fejezetek előírásait illetve a 7.1. fejezet tanúsítványprofilok, hitelesítési rendek és a felhasználási célok összefüggéseit bemutató táblázatban foglaltakat is figyelembe véve - megfelelően gondosan járjanak el. Így különösen javasolt:

- a végfelhasználói tanúsítvány érvényességi idejét ellenőrizni;
- a végfelhasználói tanúsítványt hitelesítő köztes Kiadó tanúsítványának (szolgáltatói tanúsítvány) érvényességi idejét ellenőrizni;
- a köztes Kiadó tanúsítványát hitelesítő legfelső szintű gyökér Kiadó tanúsítványának (szolgáltatói tanúsítvány) érvényességi idejét ellenőrizni;
- a végfelhasználói és szolgáltatói tanúsítványok tanúsítványállapotát ellenőrizni a tanúsítványokban hivatkozott CRL vagy OCSP alapú tanúsítványállapot információk lekérésével.

A tanúsítvány akkor tekinthető érvényesnek, ha az ellenőrzési idő (pl. az aláírás vagy bélyegzés ideje) szerinti időpont a tanúsítvány érvényességi idejébe esik, s a tanúsítvány állapota ebben az időpontban érvényes volt, s ugyanezek igazak, az érvényességi lánc minden tanúsítványára.

Lejárt érvényességi idejű tanúsítványok múltbeli érvényességének megállapításához a múltbéli időpontban aktuális visszavonási lista vagy OCSP válasz szükséges (ezek pl. egy elektronikus aláírásba vagy bélyegzőbe beágyazásra kerülhetnek a hitelesítés időpontjában).

A weboldal-hitelesítő tanúsítványok (OVCP és EVCP) érvényességét a weboldal hitelesítésének pillanatára kell megállapítani.

Az Érintett Felek az egyes tanúsítványok aktuális állapotáról a visszavonási nyilvántartások (lásd 4.10. fejezet) igénybevételével kaphatnak információkat. Szolgáltató weboldalán található nyilvános tanúsítványtárban csak az aktuálisan érvényes tanúsítványok kereshetők - amennyiben a keresett tanúsítvány Igénylője hozzájárult a tanúsítvány egyes adatainak nyilvánosságra hozatalához. A felfüggesztett és visszavont vagy lejárt érvényességű tanúsítványok a nyilvános tanúsítványtárban nem érhetők el.

4.9.7 A visszavonási lista-kibocsátás gyakorisága

A visszavonási listákon (CRL) alapvetően azon visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre, amelyeknek az érvényességi ideje még nem járt le a lista kibocsátásakor, de Szolgáltató kibocsáthat olyan visszavonási listákat is, melyeken érvényességi idejüktől függetlenül az összes, a Szolgáltató által kibocsátott visszavont és aktuálisan felfüggesztett tanúsítvány feltüntetésre kerül. A felfüggesztett tanúsítványok az újraaktiválás hatására kerülhetnek ki a listából. A visszavonási listákat a Szolgáltató saját elektronikus aláírásával hitelesíti.

Két egymást követően kibocsátott végfelhasználói tanúsítványokra vonatkozó visszavonási lista kibocsátása közt általában 4, de legfeljebb 24 óra telik el; a listák érvényességi ideje legfeljebb 24 óra. A szolgáltatói tanúsítványokra vonatkozó új visszavonási listák általában 24 óránként, de

legfeljebb 12 havonta kerülnek kiadásra (kereszthitelesített tanúsítvány esetén legfeljebb 31 naponta); a listák érvényességi ideje legfeljebb 12 hónap. Ezen időközönként visszavonási lista akkor is kibocsátásra kerül, ha a legutóbbi kibocsátás óta nem történt tanúsítványvisszavonás, -felfüggesztés vagy -aktiválás. A visszavonási listák mindig tartalmazzák a következő lista kibocsátásnak legkésőbbi idejét.

4.9.8 A visszavonási lista előállítása és közzététele közötti idő maximális hossza

Szolgáltató a visszavonási listát (CRL) az állapotváltoztatási igény jóváhagyása után legfeljebb egy órán belül előállítja, majd ezt követően azonnal közzéteszi.

4.9.9 Tanúsítványállapot-szolgáltatás rendelkezésre állása

Szolgáltató a tanúsítványok állapotának ellenőrzéséhez Tanúsítványállapot-szolgáltatást (OCSP) is nyújt a 4.10. fejezetben foglaltak szerint.

4.9.10 Tanúsítványállapot-szolgáltatásra vonatkozó követelmények

A Szolgáltató a tanúsítványállapot-információk lekéréséhez az RFC 2560 vagy az RFC5019 által meghatározott 'GET' és POST paraméterrel érkező Online Certificate Status Protocoll (OCSP) kéréseket támogatja. Lásd. 4.10. fejezet.

OCSP kérésekre bármely Érintett fél jogosult. A megfelelően paraméterezett kéréseket a Szolgáltató minden esetben kiszolgálja a 6.5. fejezetben foglaltak figyelembevételével. A kérések feldolgozása és az OCSP válaszok küldése automatikusan történik. Szolgáltató az OCSP válaszokat saját, erre a célra dedikált szolgáltatói tanúsítványával (OCSP válaszadói tanúsítvánnyal) hitelesíti. A tanúsítvány érvényességét OCSP szolgáltatással ellenőrző Érintett félnek az OCSP válasz aláírását is ellenőriznie kell.

A Szolgáltató által kibocsátott OCSP válasz a kérdéses tanúsítvány érvényessége esetén "good" állapotinformációt tartalmaz, amennyiben

- az OCSP kérés egy a Szolgáltató által kibocsátott tanúsítványra vonatkozik;
- az OCSP kérés a tanúsítványban feltüntetett OCSP elérhetőségre irányul.

4.9.11 A visszavonási hirdetmények egyéb formái

Érintett felek a nyilvános tanúsítványtárat is felhasználhatják tanúsítványállapot-információ szerzésre: ha egy adott, Szolgáltató által kibocsátott tanúsítványt itt nem találnak meg, akkor az nem érvényesnek tekinthető.

Amennyiben a Szolgáltató a gyökértanúsítványa használatát megszünteti, ennek tényét weboldalán teszi közzé.

4.9.12 Kulcskompromittálódására vonatkozó speciális követelmények

Szolgáltató minden esetben értesíti az Ügyfelet vagy Ügyfeleit a végfelhasználói tanúsítványban feltüntetett email címen, ha a végfelhasználói kulcs vagy kulcsok kompromittálódásának veszélyéről vagy bármely 4.9.1 fejezet szerinti körülmény fennállásának lehetőségéről értesül.

A vélelmezett vagy bizonyosságot nyert kulcskompromittálódás esetén a visszavonási eljárás lépéseit hajtja végre (4.9.1.1 pont). Kompromittálódott magánkulcs soha többet nem használható, lehetőség szerint intézkedni kell a megsemmisítéséről és a megsemmisítésig ugyanolyan felügyeletben és védelemben részesítendő, mint egy érvényes magánkulcs (lásd 6.2.10 fejezet).

Az Ügyfélnek kötelessége minden intézkedés megtétele az esetleges károk megelőzése vagy enyhítése érdekében, beleértve a kompromittálódott magánkulcs által esetlegesen Érintett Felek értesítését is.

A Köztes Kiadók szolgáltatói magánkulcsainak kompromittálódása vagy annak veszélye esetén szintén a visszavonási eljárás lépései kerülnek végrehajtásra (4.9.1.2 pont).

A Gyökér Kiadó (rootCA) magánkulcsainak kompromittálódása vagy annak veszélye esetén Szolgáltató a Gyökér Kiadó tanúsítványát és kulcsait haladéktalanul megsemmisíti és erről értesítést tesz közzé weboldalán, e-mail címmel rendelkező ügyfelei számára elektronikus levélben értesítőt küld, valamint tájékoztatja erről a Bizalmi felügyeletet illetve azon böngészőgyártókat, melyek ún. "root program"-jában a gyökértanúsítvány szerepel.

4.9.13 A felfüggesztés maximális ideje

Tanúsítvány felfüggesztett állapotban addig lehet, míg a visszavonáshoz vezető körülmények fennállásának gyanúja bizonyítást vagy cáfolatot nem nyer, de legfeljebb 30 naptári napig. A tanúsítvány visszavonásáról, vagy aktiválásáról Szolgáltatónak a lehető leghamarabb intézkednie kell. A felfüggesztett állapot kezdő időpontja a felfüggesztési igény elfogadásától, azaz a 4.9.3.1 pontban foglaltaknak megfelelő igénylés elvégzésétől számítandó, mely időpont a CRL-ben feltüntetésre kerül. Ha ez idő alatt a visszavonáshoz vezető körülmények gyanúja cáfolatot nem nyer, Szolgáltató a tanúsítványt automatikusan visszavonja.

Weboldal-hitelesítő tanúsítványok (OVCP és EVC) esetén a felfüggesztése nem értelmezett.

4.10 Visszavonási nyilvántartások

A Szolgáltató az Érintett felek számára biztosítja a jelen szabályzat alapján kibocsátott tanúsítványok állapotának (érvényes, felfüggesztett, visszavont) ellenőrzéséhez szükséges szolgáltatásokat.

4.10.1 Működési jellemzők

Az egyes tanúsítványokra vonatkozó tanúsítványvisszavonási lista és tanúsítványállapot-szolgáltatás a tanúsítvány crlDistributionPoints és authorityInfoAccess:OCSP tanúsítványkiterjesztés mezőiben található URL-eken érhetők el (lásd 7.1.2. fejezet). E nyilvántartásokban az érvényességi idejükön belül ellenőrizhetők a tanúsítványok. A tanúsítvány “notAfter” mezőjében szereplő időpontot követően

- az aktuálisan kibocsátott tanúsítványvisszavonási lista akkor sem tartalmazza a tanúsítványt, ha az korábban visszavonásra/felfüggesztésre került.
- OCSP kérés esetén a tanúsítvány érvényességi idején belüli utolsó tanúsítványállapotot adja válaszul a Szolgáltató.

A tanúsítvány érvényességi idejének lejártát követően a tanúsítvány állapota a korábbi visszavonási listákban tekinthető meg, amelyek (egyedi kérelem útján) beszerezhetők a szolgáltatónál.

A visszavonási nyilvántartások működtetése során Szolgáltató az alábbiak szerint jár el:

- biztosítja a tanúsítványállapot-információk folyamatos, napi 24 órában, heti 7 napban való online elérhetőségét (a tanúsítvány megfelelő mezőiben megadott URL-eken és a Szolgáltató weboldalán);
- A CRL-en és OCSP válaszban feltüntetésre kerülő időpontadatok legalább naponta egyszer szinkronizálásra kerülnek az egyezményes koordinált világidővel (UTC).
- PKI alapú aláírással biztosítja a tanúsítványállapot-információk sértetlenségét és hitelességét;
- biztosítja, hogy a visszavonási információk legalább a tanúsítvány eredeti érvényességi idejéig szerepeljenek az aktuálisan kibocsátott tanúsítványállapot-információk között;

- a lejárt tanúsítványokkal kapcsolatos visszavonási információk a tanúsítvány érvényességi ideje alatt kibocsátott archív visszavonási listák között érhetők el;
- a tanúsítványállapot ellenőrzésére tanúsítványvisszavonási lista (CRL) és tanúsítványállapot-szolgáltatást (OCSP) nyújt;
- gondoskodik arról, hogy CRL és az OCSP szolgáltatások egymással összhangban működjenek és a tanúsítvány állapotának változásáról szóló információk mindkét szolgáltatásban elérhetőek legyenek és megegyezzenek;
- biztosítja, hogy a tanúsítványvisszavonási információk nyilvánosak és nemzetközileg is elérhetőek legyenek;
- biztosítja, hogy a tanúsítványállapot-jelzések között egymástól megkülönböztethető módon megjelenjen a visszavont és felfüggesztett tanúsítványállapot;
- biztosítja, hogy a felfüggesztett tanúsítványok az aktiválás hatására lekerülnek a tanúsítványvisszavonási (CRL) listából;
- kulcskompromittálódás miatti tanúsítványfelfüggesztés vagy -visszavonás esetén, az állapotváltozás bejegyzése után a Szolgáltató rendkívüli visszavonási listát (CRL) bocsát ki; más okból történő visszavonás vagy felfüggesztés esetén az állapotváltozás legkésőbb a következő tervezett visszavonási listában kerül publikálásra.
  A weboldal-hitelesítő tanúsítványokra (OVCP és EVCP) vonatkozó visszavonási lista méretét szolgáltató - lehetőség szerint - 7MB alatt tartja, a gyors letölthetőség érdekében.

4.10.2 Szolgáltatások elérhetősége

Szolgáltató a tanúsítványszolgáltatáson belül a végfelhasználói tanúsítványok visszavonásának és felfüggesztésének igénylését és a visszavonási nyilvántartások elérhetőségét folyamatosan (7x24) biztosítja az alábbiak szerint.

A Szolgáltató

- a visszavonási nyilvántartások;
- a Szolgáltató által kibocsátott tanúsítványok használatára vonatkozó egyéb kikötések és feltételek; *valamint*
- az állapotváltozással kapcsolatos szolgáltatások elérhetősége kapcsán

a 4.9. fejezetben foglaltakat is figyelembe véve

- biztosítja az éves szinten 99%-os rendelkezésre állást;
- garantálja, hogy az eseti szolgáltatáskiesések maximális időtartama legfeljebb 3 óra.

A weboldal-hitelesítő tanúsítványokhoz (OVCP és EVCP) nyújtott CRL és OCSP szolgáltatások válaszideje normál terhelés esetén legfeljebb 10 másodperc.
Szolgáltató a végfelhasználói tanúsítványok aktiválását munkanapokon a weboldalán (lásd 1.1.2) közzétett ügyfélfogadási időben biztosítja.

Szolgáltató biztosítja, hogy az általa kibocsátott CRL-ek a kibocsátásuktól számított két évig az eredeti URL-en elérhetők legyenek, a két évnél régebbi CRL-ek elérhetősége (URL) megváltozhat.

4.10.3 További lehetőségek

A tanúsítványállapot-szolgáltatásra vonatkozóan a Szolgáltató további előírást nem alkalmaz.

4.11 A szolgáltatási szerződés megszűnése

A szolgáltatási szerződés megszűnését Szolgáltató az ÁSZF-ben ismerteti.

4.12 Kulcsletét és kulcshelyreállítás

Az NL Sign szolgáltatás keretében kiadott végfelhasználói tanúsítványok magánkulcsait

Szolgáltató tárolja, de a kulcshelyreállítási szolgáltatás nem értelmezett, mivel a magánkulcs tárolása úgy valósul meg, hogy ahhoz Szolgáltató semmilyen módon ne férjen hozzá. Egyéb esetben a végfelhasználói tanúsítványok magánkulcsait Szolgáltató semmilyen módon nem tárolja vagy menti el, így azok visszaállítását sem tudja biztosítani, amennyiben végfelhasználói oldalon az elveszik vagy megsérül.

4.12.1 Kulcsletét és -helyreállítás rendje és szabályai

A végfelhasználói tanúsítványok magánkulcsai esetében a Szolgáltató nem biztosít sem kulcsletét- sem kulcshelyreállítás szolgáltatást.

A Ügyfél a saját végfelhasználói magánkulcsáról abban az esetben készíthet másolatot, ha biztosítani tudja a másolat megfelelő tárolását és védelmét. A végfelhasználói magánkulcsok Ügyfél által készített másolataira ugyanolyan szintű biztonsági előírások vonatkoznak, mint az eredeti magánkulcsra (lásd 6.2 fejezet). A magánkulcsokról legfeljebb annyi másolatot szabad készíteni, ami elégséges a szolgáltatás fenntartásához.

Szolgáltató a saját, szolgáltatói magánkulcsait elmentve is tárolja.

4.12.2 Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Szolgáltató nem tárol és állít vissza szimmetrikus kulcsokat.

5. FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

A kockázatok csökkentése érdekében Szolgáltató az általa biztosított szolgáltatásokhoz szükséges hardver, szoftver, illetve egyéb eszközeit két, fizikailag egymástól elkülönült helyszínen, egy elsődleges és egy másodlagos helyszínen tárolja. A két helyszínre vonatkozó előírások megegyezőek, az esetleges eltérések a megfelelő pontoknál feltüntetésre kerültek.

A szolgáltatói rendszerek konfigurációját a Szolgáltató rendszeresen ellenőrzi a biztonsági előírásokat sértő változások kiszűrése érdekében.

A hitelesítő és regisztrációs egységek eszközeit kizárólag az erre felhatalmazott, megfelelően kioktatott és ellenőrzött tudású személyzet kezeli.

Az egységek adatállományairól biztonsági mentések készülnek (ld. 6.5 alfejezet). A mentéseket a Szolgáltató az 5.5.2 pontban meghatározott ideig megőrzi.

A Szolgáltató a fizikai, eljárásbeli és személyzeti előírásokat rendszeresen elvégzett kockázatelemzéssel vizsgálja. A Szolgáltató az általa használt eszközök (beleértve az információs vagyont is) tekintetében vagyonnyilvántartást vezet.

Szolgáltató nem nyilvános Információbiztonsági Szabályzata tartalmazza az információbiztonsági szabályozással kapcsolatos előírásokat.

Az Információbiztonsági szabályzatot és a vagyonnyilvántartást a Szolgáltató rendszeres időközönként, vagy jelentős változás esetén haladéktalanul felülvizsgálja azok folyamatos alkalmazhatósága, megfelelősége és eredményessége tekintetében.

5.1 Fizikai óvintézkedések

A fizikai óvintézkedések célja a Szolgáltató bizalmas információira és fizikai körleteire (szerverterem, illetve szerverszoba) irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása. A fizikai hozzáférés tekintetében Szolgáltató megfelelő jogosultságrendszert alkalmaz az ellenőrzött hozzáférés érdekében és azokat rendszeres időközönként felülvizsgálja.

Az értékek elvesztésének, sérülésének, kompromittálódásának, valamint a működési tevékenység megzavarásának elkerülésére a Szolgáltató az Információbiztonsági Szabályzatban meghatározott intézkedéseket követi.

A kritikus és érzékeny információt feldolgozó szolgáltatások megvalósítására és a kriptográfiai modulok alkalmazására és tárolására biztonságos helyszíneken került sor. A biztosított védelem arányban áll a Szolgáltató által végzett kockázatelemzésben megállapított kockázatokkal.

5.1.1 Telephely felépítése

Szolgáltató a telephelyén, egy védett számítógépteremben valósítja meg a leginkább veszélyeztetett szolgáltatásokat. A számítógépteremben a fizikai hozzáférés, beléptetés ellenőrzése és felügyelete, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása, telekommunikációs hálózat elérhetősége, elektromágneses kisugárzás stb. védelmi szempontok egységes érvényesítésére került sor. Illetéktelen személyek a számítógépterembe nehezen juthatnak be, a biztonsági őrség viszont rövid idő alatt meg tudja közelíteni riasztás esetén. A biztonsági körletnek nincs ablaka, a bejárati ajtókon kívül csak a különösen erős fal bontásával lehetne behatolni ide. A helyiség redundáns klíma-, automata tűzoltó, továbbá illetéktelen behatolást jelző (riasztó) berendezéssel van ellátva. Az eszközök többszörösen túlbiztosított elektromos energiaellátással rendelkeznek.

A Szolgáltató másodlagos helyszíne egy védett számítógépterem szerverszéfjében található, melynek biztonsági szintje megegyezik a telephely biztonságával.

A Szolgáltató Központi Regisztrációs Ügyintézői a tanúsítványok kulcsgenerálását, illetve a kulcstároló eszközökkel kapcsolatos előkészítő műveleteket, a tanúsítvány kibocsátását, valamint az állapotváltozás kezelését egy külön erre a célra kialakított, védett szerverszobában valósítják meg. A védett szerverszoba kifejezetten erre a célra készült.

5.1.2 Fizikai hozzáférés

A biztonsági körletek pontos paramétereit, illetve a belépni jogosultak listáját a mindenkori belső operációs dokumentumok tartalmazzák. A biztonsági körletekbe bizalmi munkakört betöltő munkatársakon kívül más személyek csak külön felhatalmazással és kísérettel léphetnek be. A számítógépterembe a belépés személyhez kötött elektronikus kártyával történik a belépések fizikai és elektronikus naplózása mellett. A számítógéptermen belül a szolgáltatói rendszerek egy olyan elkülönült részen kerültek kialakításra, ahova biometrikus azonosítást követően lehet belépni. A biztonsági körlet beléptető előhelységét, illetve magát a számítógéptermet 24 órás videó kamerás megfigyelő rendszer is védi.

A másodlagos helyszín beléptetési rendszere biometrikus azonosítással nem rendelkezik, de az egyenszilárdság megőrzésére, a másodlagos helyszínt biztonságát állandó élőerős védelem is biztosítja. A szerverszobába az arra jogosult munkatársak kártyás azonosítást követően léphetnek be; a be-, illetve kilépések folyamatos naplózásra kerülnek. A szerverszoba 24 órás videós kamerás megfigyelő rendszer is védi.

A Szolgáltató kockázatelemzése a kritikus szolgáltatások keretében foglalkozik a fizikai hozzáférés szabályozásával, a természeti katasztrófa elleni védelemmel, a villámvédelemmel, a tűzbiztonsági tényezőkkel, a támogató eszközök (különösen áram és klíma) meghibásodásával, az építmény összeomlásával, vízvezeték szivárgással, talajvíz elleni védelemmel, lopás, betörés és behatolás elleni védelemmel, valamint a katasztrófa utáni helyreállítással.

A Szolgáltató a szolgáltatói tanúsítványokat a normál operációtól elkülönítetten tárolja, ahhoz kizárólag a bizalmi munkatársak férhetnek hozzá.

5.1.3 Áramellátás, légkondicionálás

A Szolgáltató védett számítógép termének zavartalan áramellátása kiemelten fontos a folyamatos üzemeltetés biztosítása érdekében, melynek érdekében a Szolgáltató az alábbi intézkedéseket alkalmazza/alkalmaztatja:

- szünetmentes energiaellátás,
- zárlati leoldásra szelektív áramkörök,
- villamos zavar, villám és túlfeszültség védelem.

A szünetmentes energiaellátást biztosító rendszer felépítése a következő:

- dízel gépes áramfejlesztő,
- lokális akkumulátoros szünetmentes tápegység,
- redundáns tápválasztó.

Az alkalmazott üzemmód pedig az alábbi:

- az üzemi táp kimaradása vagy csökkenése esetén a rendszer átkapcsol a tartalék tápra,
- ezalatt a rendszer elindítja az áramfejlesztőt,
- amikor az üzemi táp ismét használható (5 percen keresztül folyamatosan), akkor a rendszer visszatér rá.

Zárlati leoldásra szelektív áramkörök segítségével a gépteremben több egymástól független működésű rendszer lett kialakítva a folyamatos üzemeltetés támogatására. Az elosztó hálózat úgy lett megtervezve, hogy egy eszközcsoport zárlata esetén csak a zárlatot okozó eszközcsoport legyen áramtalanítva, a többi hibátlan eszközcsoport üzemben maradjon.

A szerverteremben biztosított a géptermek épülettől független légkondicionálása. A védett számítógépterem a bejutó levegő tisztaságát megfelelő szűrőrendszerrel biztosítja, gondoskodik a levegőből a különféle szennyeződések kiszűréséről, tovább biztosítja a kezelőszemélyzet részére

szükséges levegőt. A levegő nedvességtartalma és hőmérséklete folyamatosan ellenőrzött. A légkondicionáló berendezések biztosítják az informatikai rendszerek megfelelő hűtését. A folyamatos üzemvitelt egy második (tartalék) klímaberendezés is támogatja, mely szükség esetén működésbe lép. A klímaberendezések elhelyezésének módja biztosítja, hogy azok karbantartása ne okozzon zavart a gépterem működésében.

5.1.4 Beázás és elárasztódás veszélyeztetettsége

A Szolgáltató szolgáltatási helyszínei védettek a beázástól és az elárasztódástól. A védett számítógépteremben a biztonságot növeli az álpadló alkalmazása.

5.1.5 Tűzmegelőzés és tűzvédelem

A Szolgáltató szolgáltatási helyszínei a tűzvédelmi előírásoknak megfelelően működnek. A helyszínek tűz és füstérzékelőkkel, kézi és automata oltó berendezésekkel rendelkeznek. A kézi oltó berendezések helye és a menekülési útvonal jól látható helyen jelzésre került.

5.1.6 Adathordozók kezelése

Szolgáltató adathordozóinak biztonságos tárolására biztonsági körlet, illetve egy bérelt banki széf szolgál. A kritikus adatokról Szolgáltató több mentési példánnyal rendelkezik. A Szolgáltató folyamatosan gondoskodik és megfelelő intézkedéseket tesz az adathordozó avulás megakadályozására.

Szolgáltató az érzékeny adatokat tartalmazó adathordozókat az Információbiztonsági Szabályzatban előírt módon semmisíti meg, amennyiben azokra már nincs szükség. A selejtezett eszközök tartalmát Szolgáltató véglegesen törli, vagy az eszközt helyreállíthatatlanul tönkreteszi.

5.1.7 Hulladékelhelyezés

A fizikailag megsemmisítés kapcsán a Szolgáltató az alábbiak szerint jár el:

- a papíralapú dokumentumok zúzógéppel felaprításra kerülnek,
- a hajlékony lemezek (házából való kibontás után) zúzógéppel felaprításra kerülnek,
- egyéb más mágneses adathordozók demagnetizálás után összetörésre kerülnek;
- egyéb más adathordozók összetörésre kerülnek.

5.1.8 Mentés külső helyszínen

Szolgáltató az üzemmenet folytonossága és az adatvesztés elkerülése érdekében mentéseket végez és biztosítja az informatikai rendszer egészének szükség esetén való helyreállíthatóságát. A mentéseket védi a jogosulatlan hozzáféréstől, módosítástól és törléstől, és a megsemmisüléstől. A rendkívüli helyzetekre való felkészülés magában foglalja a kidolgozott tervek adott esetekre történő alkalmazását és tesztelését is.

A megőrzendő adatok biztonságos tárolását Szolgáltató csak írható médiával, távoli helyen tárolt mentéssel vagy több tárolási helyen történő távoli párhuzamos tárolással végzi.

5.2 Eljárásrendi biztonsági intézkedések

Szolgáltató gondoskodik rendszerei biztonságos, szabályszerű, a meghibásodás minimális kockázata melletti üzemeltetéséről. Ennek érdekében elegendő számú és megfelelő képzettséggel, műszaki tudással, tapasztalattal rendelkező személyzetet alkalmaz.

A szolgáltatások esetében Szolgáltató a jogszabályoknak és szabályzatainak megfelelő naprakész belső irányítási és ellenőrzési eljárásrendet és kapcsolódó felelősségi rendszert működtet. A rendszer megfelelő működését a független rendszervizsgáló ellenőrzési tevékenység is biztosítja.

Szolgáltató külső, független rendszervizsgáló által folyamatosan ellenőrzött minőségirányítási és információbiztonsági irányítási rendszerrel rendelkezik.

Szolgáltató a szolgáltatás nyújtása során létrejövő és kezelt adatot a jogszabályok és a szolgáltatási szabályzatban meghatározott kockázatelemzés alapján biztonsági osztályba sorolja, és gondoskodik azok megfelelő nyilvántartásáról, ellenőrzéséről, védelméről, valamint az ehhez szükséges felelősségi rendszer működtetéséről.

5.2.1 Bizalmi munkakörök

Szolgáltatónál bizalmi munkakört (lásd Bizalmi Szolgáltatási Rend 5.2.1 fejezet) olyan személy tölt be, akinek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét, szakértelmét szakmai gyakorlat, végzettség és szakképesítés igazolja.

- Informatikai rendszerért általánosan felelős vezető;
- Biztonsági tisztviselő: A szolgáltatás biztonságáért általánosan felelős személy;
- Rendszeradminisztrátor: A szolgáltató informatikai rendszer telepítését,
- konfigurálását, karbantartását végző személy;
- Rendszerüzemeltető: A szolgáltató informatikai rendszerének 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 tanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.

Az informatikai rendszerért általánosan felelős munkakört olyan személy tölti be, aki szakirányú felsőfokú végzettséggel[11] és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik.

Szolgáltató a bizalmi munkakört betöltő személyt munkaviszonyban foglalkoztatja, és a bizalmi munkakört betöltő személy független minden olyan érdektől, amely hátrányosan érintheti a szolgáltatás megbízhatóságát és biztonságát. Szolgáltató gondoskodik arról, hogy a szolgáltatások nyújtásával kapcsolatban álló személy a szükséges és megfelelően naprakész tudással és tapasztalattal rendelkezzen. Szolgáltató valamennyi bizalmi munkakör betöltését biztosítja.

A Szolgáltató a bizalmi munkakörökről naprakész nyilvántartást vezet, változás esetén a változás tényét haladéktalanul bejelenti a Bizalmi Felügyeletnek.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám

Szolgáltató az alábbi tevékenységeket legalább kettő arra kijelölt és közvetlen felhatalmazással rendelkező bizalmi munkatárs együttes fizikai jelenlétével, egy fizikailag védett környezetben végzi:

- szolgáltatói kulcspárok generálása
- köztes kiadó tanúsítványának kibocsátása;
- szolgáltatói magánkulcsok mentése és visszaállítása;
- szolgáltatói magánkulcsok megsemmisítése.

[11] szakirányú felsőfokú végzettség a matematikusi, fizikusi egyetemi végzettség vagy műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség

5.2.3 Az egyes szerepkörökhöz tartozó azonosítás és hitelesítés

A Szolgáltató valamennyi, bizalmi munkakört betöltő munkatársa a zárt körletbe csak megfelelő azonosítást és hitelesítést követően léphet be, amely az informatikai rendszerekhez való hozzáférésnél további azonosítással egészül ki. Sikeres azonosítás és hitelesítés nélkül a zárt körletbe való bejutás, illetve rendszerhozzáférés nem lehetséges, így egyetlen biztonság szempontjából kritikus tevékenység sem végezhető el.

Szolgáltató informatikai rendszerének minden felhasználóját és az adminisztratív folyamatok minden szereplőjét személy szerint azonosítja, kivéve a nyilvános adatszolgáltatásához kizárólag olvasási jogosultsággal rendelkező felhasználókat. Informatikai rendszereihez csak az arra felhatalmazott személyek férhetnek hozzá. A szolgáltató adminisztrálja a Rendszeradminisztrátorok, Rendszerüzemeltetők és Független rendszervizsgálók rendszerhozzáférését, beleértve a felhasználói fiók kezelését, alkalmi módosítását és adott esetben a hozzáférés megszüntetését.

Az egyes alkalmazásokhoz való hozzáférések korlátozásra kerülnek. A rendszer el tudja különíteni az egyes bizalmi munkaköröket, így különösen a Rendszeradminisztrátori és Rendszerüzemeltetői hozzáféréseket.

A személyzetet azonosításra és hitelesítésre kerül a szolgáltatások szempontjából kritikus alkalmazások használata előtt, s tevékenységükkel kapcsolatban elszámoltathatók.

A bizalmi munkakörhöz tartozó jogosultsági szinteket a Szolgáltató a Személyzeti Politikájában rögzíti.

5.2.4 Egyes szerepkörök összeférhetetlensége

Szolgáltató a rendszereiben olyan biztonsági előírásokat alkalmaz, illetve jogosultsági szinteket határoz meg, amely minimalizálja az azonosítatlan vagy nem szándékolt módosításokat, illetve csökkenti a visszaélési lehetőségeket.

A feladatkörök elhatárolása végett

- a biztonsági tisztviselő nem látja el a független rendszervizsgáló és az informatikai rendszerért általánosan felelős vezető feladatait;
- a független rendszervizsgáló nem látja el az informatikai rendszerért általánosan felelős vezető feladatait;
- a biztonsági tisztviselő nem látja el a rendszeradminisztrátor feladatait; és
- a független rendszervizsgáló nem látja el a regisztrációs felelős és a rendszeradminisztrátor feladatait.

Szolgáltató szigorú ellenőrzési eljárásokkal biztosítja a regisztrációs feladatok elkülönítését, azaz, hogy a tanúsítvány kibocsátásához szükséges adatok érvényesítését és tanúsítványkibocsátás jóváhagyását ne ugyanaz a bizalmi munkatárs végezze. Az ellenőrzési eljárások auditálhatók.

Az összeférhetetlenségre vonatkozó részletszabályokat Szolgáltató Információbiztonsági Szabályzata tartalmazza.

5.3 Személyzeti biztonsági intézkedések

A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a lehetőségekkel való visszaélés kockázatának csökkentése.

Ennek érdekében Szolgáltató a személyi biztonsággal már a felvételi szakaszban foglalkozik, majd az alkalmazás során történő ellenőrzésekkel biztosítja.

Szolgáltató pontosan és részletesen kidolgozott, folyamatosan karbantartott Személyzeti Politikával rendelkezik. A Személyzeti Politikájában meghatározott ideiglenes és állandó szerepköröket és felelősségeket munkaleírásokban dokumentálja, amelyek tartalmazzák:

- a szerepkörök információkezelési lehetőségei és a különböző hitelesítési folyamatokra való hatásai alapján felmérhető kockázati besorolását,
- a szükséges szakismereti és tapasztalati követelményeket,
- a munkakörrel és a munkatárs feladataival összefüggő tevékenységek leírását, a felelősségek körét és mértékét, továbbá a kapcsolódó munkakörök megnevezését.

A Szolgáltató munkavállalói mindaddig nem tölthetnek be bizalmi munkakört, amíg a személyükkel kapcsolatos ellenőrzések végrehajtása és a szükséges nyilatkozatok megtétele meg nem történt, és a megfelelő képzésben és tapasztalatszerzésben részt nem vettek.

A Szolgáltató vezető tisztségviselői, vezető beosztású munkatársai, bizalmi munkaköröket betöltő munkatársai függetlenek minden olyan kereskedelmi, pénzügyi és egyéb hatástól, ami hátrányosan befolyásolhatja a Szolgáltató által nyújtott szolgáltatások iránti bizalmat.

5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények

Szolgáltató olyan munkatársakat és adott esetben olyan alvállalkozókat alkalmaz, akik megbízhatóak, rendelkeznek a szükséges szakértelemmel, tapasztalattal és képesítésekkel, valamint megfelelő képzésben részesültek a biztonságra és a személyes adatok védelmére vonatkozó szabályokkal kapcsolatban, továbbá olyan igazgatási és ügyvezetési eljárásokat alkalmaz, amelyek megfelelnek az európai és nemzetközi szabványoknak.

A Regisztrációs Egységek bármely bizalmi munkakörére jelölt személy (emberi megbízhatósága és szakmai alkalmassága ellenőrzése céljából) kezdeti ellenőrzésen megy keresztül. E biztonsági alapellenőrzés során az ellenőrzést végző szakemberek: az életrajzban megadott adatokat (életrajzi elemek, referenciák, szakmai előmenetel stb.) ellenőrzik. Ennek során:

- a képzettségre vonatkozó adatokat egybevetik a jelölt által benyújtandó bizonyítványokkal, diplomákkal,
- a gyakorlati tapasztalatra vonatkozó állításokat személyes referenciákon keresztül, publikációkra alapozva, illetve egyéb úton igazolják.

Szolgáltató biztosítja, hogy a Regisztrációs Ügyintézők és Felelősök elegendő ismerettel rendelkezzenek tevékenységük szabályzatnak megfelelő végzéséhez, ennek érdekében képzést biztosít a Regisztrációs Ügyintézők és Felelősök számára az alábbi témakörökben:

- alapvető PKI ismeretek;
- a Szolgáltatási Rendben és Szabályzatban foglalt azonosítási és hitelesítési alapelvek és eljárások;
- adathalász és más, az azonosítási és hitelesítési eljárás megbízhatóságát veszélyeztető technikák.

Szolgáltató a képzésekről nyilvántartást vezet.

A Regisztrációs Ügyintézők és Felelősök a fenti ismeretek hiányában nem végezhetik a tevékenységüket, ezért a Szolgáltató sikeres vizsga letételét követeli meg a Regisztrációs Ügyintézőktől és Felelősöktől.

A Regisztrációs Ügyintézők és Felelősök ismerik a forgalomban lévő hatósági, illetve azonos funkciójú dokumentumokat, azok fajtáit, ismertetőjegyeit, képesek az átadott iratok érvényességének megállapítására.

Valamennyi bizalmi munkakört betöltő munkatársnak a biztonsági alapellenőrzésen túl időszakos biztonsági ellenőrzéseken is át kell átesniük.

Nem tölthet be bizalmi munkakört az a személy, aki akár az alap, akár egy időszakos biztonsági ellenőrzésen a „magas biztonsági kockázat” minősítést kapja. Bizalmi munkakört csak büntetlen előélettel rendelkező személy tölthet be, amit a felvételi eljárás során 3 hónapnál nem régebbi

erkölcsi bizonyítvánnyal kell igazolni.

Az időszakos biztonsági ellenőrzésre évente kerül sor valamennyi bizalmi munkakört betöltő (lásd 5.2.1 pont) munkatárs esetén.

A Regisztrációs felelősök kijelölésüket követően a munkakörük betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt, aminek a végén vizsgázniuk kell. Ennek a képzési formának a fő célja a szolgáltatásra vonatkozó egységes biztonságpolitika megismerése, megértése, az ezen alapuló aktuális eljárások későbbi helyes alkalmazása érdekében. További részletek a Személyzeti Politikában találhatók.

A bizalmi munkakört a munkatársak a megfelelő gyakorlati tapasztalat megszerzését követően tölthetnek be.

5.3.2 Ellenőrzési eljárások

A felvételi eljárás során a Szolgáltató a személyek személyazonosságáról fizikai jelenlétük során vagy fényképes személyazonosító okmányaik ellenőrzésével győződik meg. Mindezek mellett a Szolgáltató a felvételi eljárás során figyelembe veszi a korábbi munkahelyekre, releváns végzettséget és szakmai referenciákra vonatkozó információkat is.

A bizalmi munkakör munkatársai az ellenőrzés lefolytatását megelőzően nem kaphatnak hozzáférést a Szolgáltató rendszereihez.

5.3.3 Képzési követelmények

A bizalmi munkakört betöltő munkatársaknak rendelkezniük kell a feladataik ellátásához szükséges tudással. Ennek érdekében a bizalmi munkakört betöltő munkatársaknak kinevezésüket megelőzően tudásuk igazolására vizsgát kell tenniük. Amíg sikeres vizsgát nem tesznek, nem férhetnek hozzá a szolgáltatói rendszerekhez. A vizsga és a képzés a bizalmi munkakör típusától függően a következő ismeretekre terjed ki:

- PKI alapismeretek;
- Hitelesítés és ellenőrzési szabályok és eljárások;
- Biztonsági és adatvédelmi szabályok;
- Általános fenyegetések az információhitelesítési eljárásokra (beleértve az adathalász és egyéb social engineering taktikákat);
- A Szolgáltatási Szabályzat és egyéb szabályzatok előírásai;
- Egyes tevékenységük jogi következményei;
- Szolgáltató informatikai rendszerének sajátosságai és kezelésének módja.

5.3.4 Továbbképzési gyakoriságok és követelmények

A Szolgáltató továbbképzésre és oktatásra vonatkozó gyakorlatát az éves továbbképzési tervben határozza meg.

Abban az esetben, amikor a bizalmi szolgáltatásban jelentős változás következik be, valamennyi munkatárs a szükséges felépítésű és szintű moduláris továbbképzésben részesül, illetve megkapja a szükséges dokumentációkat.

5.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága

A vonatkozó szabályokat a Szolgáltató Személyzeti Politikája tartalmazza.

5.3.6 Jogosultatlan tevékenységek büntető következményei

A szolgáltató rendszerének nem engedélyezett használatára, illetve a szolgáltatás nyújtása közben

elkövetett hibákra, mulasztásokra, károkozásokra vonatkozó szankciókat a Szolgáltató a bizalmi munkakört betöltő személyek munkaszerződésében rendezi.

5.3.7 Szerződéses közreműködőkre vonatkozó követelmények

A Szolgáltató nem munkaviszonyban dolgozó szerződéses közreműködőire ugyanazok a biztonsági szabályok vonatkoznak, mint a munkaviszonyban dolgozókra.

5.3.8 A személyzet számára biztosított dokumentumok

A Szolgáltató folyamatosan biztosítja a szolgáltatásnyújtásban közreműködő személyek részére a szerepkörük ellátásához szükséges aktuális szabályzatokat és dokumentációkat.

5.4 Naplózási eljárások

Szolgáltató hitelesítési rendszere a jogszabályi, illetve az egyes szabványokban, előírásokban meghatározott követelményeknek megfelelő, széleskörű naplózási tevékenységet folytat a tanúsítványokra és az Ügyféleszközök elkészítésére vonatkozó műveletek és az ezek során felhasznált adatok megőrzése érdekében. A napló tartalmazza a bejegyzés pontos idejét, a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény típusát, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét, az esemény végrehajtás sikerességét, illetve sikertelenségét. A Szolgáltató a naplókban feltüntetett időt olyan gyakorisággal szinkronizálja, hogy a saját idő és a valódi idő közti eltérés ne haladja meg az 1 másodpercet. Az esetleges ennél nagyobb eltérések szintén naplózásra kerülnek.

A Szolgáltató egyéb rendszerei szintén naplóznak. E naplózások tulajdonságai az adott alkalmazások függvényei. A naplózások elemei elkülönülten keletkeznek a különböző modulokban. A több komponensből álló rendszer miatt a napló állományok nem egy helyen keletkeznek, de feldolgozásuk egy központi helyen történik.

Szolgáltató a naplóállomány minden bejegyzését védi a módosítástól és a jogosulatlan hozzáféréstől. A naplót úgy kezeli, hogy kizárható a napló megsemmisítése, a napló bejegyzéseinek törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása. Szolgáltató a naplóról rendszeres mentést készít, valamint gondoskodik a naplóadatok folyamatos értékeléséről és ellenőrzéséről.

Operatív szinten az egyes rendszerek üzemeltetési leírásai szabályozzák a napló adatok kezelését.

5.4.1 A tárolt események típusai

Szolgáltató által alkalmazott rendszer minden jogszabályban előírt eseményt és hibát regisztrál, amely a szolgáltatások szempontjából kritikus. A naplóállományok automatikusan vagy manuálisan kerülnek rögzítésre. A naplóállományok mellett a Szolgáltató egyes események rögzítésére jegyzőkönyvet használ.

A Szolgáltató az Információbiztonsági Szabályzatban részletezi, hogy az egyes események kapcsán pontosan milyen adatokat/eseményeket rögzít.

A naplózott események időponttal ellátott bejegyzésként kerülnek napló állományba. A Szolgáltató a napló minden bejegyzését elektronikus aláírás és biztonsági másolat és mentés alkalmazásával védi a módosítástól, illetéktelen hozzáféréstől, megsemmisítéstől, a napló bejegyzéseinek törlésétől, a bejegyzések sorrendjének bármilyen módon történő megváltoztatásától.

A naplóban lehetséges az esemény típusa és/vagy a felhasználó személye szerinti keresés. A naplóbejegyzések szöveges formátumúak.

5.4.2 A naplófájl feldolgozásának gyakorisága

Szolgáltató naplóbejegyzéseinek átvizsgálása napi rendszerességgel megtörténik az arra megfelelő szakértelemmel és jogosultsággal rendelkező független rendszervizsgálók által. A kiértékelésre manuálisan és szoftvereszközök segítségével kerül sor.

A kiértékelés során az értékelő elemzi a rendszerek által generált hibaüzeneteket, a forgalmi adatokban bekövetkezett jelentős változásokat, a szokásostól eltérő mintákat, valamint a gyanús aktivitásokat. A kiértékelés tényét és eredményét, valamint az esetleges szükséges intézkedéseket az értékelő, illetve a szoftvereszköz rögzíti.

Szolgáltató hálózati védelmi rendszerei automatikus riasztási funkciókkal is el vannak látva az erőforrásokhoz történő jogosulatlan hozzáférés észlelésének jelzésére. Ilyen riasztási esetekben a naplóbejegyzések soron kívül átvizsgálásra kerülnek. Rendellenességek észleléskor, reklamációkor vagy egyéb megkeresések kapcsán is sor kerülhet a napló adatok rendkívüli átvizsgálására.

5.4.3 A naplófájl megőrzési időtartama

A napló állományok keletkezésük helyén tárolódnak, illetve archiválásra kerülnek (ld. 5.5.2 pont), és a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított 10 évig, illetőleg a velük kapcsolatban felmerült és bejelentett jogvita jogerős lezárásáig megőrződnek. A naplófájlok a Független rendszervizsgálók számára hozzáférhetők.

5.4.4 A naplófájl védelme

Szolgáltató hitelesítési rendszerének naplóbejegyzései a Szolgáltató elektronikus aláírásával ellátva, a törlések és beszúrások észrevétlen végrehajtását kizáró módon kerülnek tárolásra.

A napló állományt a véletlen és szándékos rongálások ellen biztonsági mentések védik. A személyes adatokat tartalmazó naplóbejegyzések esetében Szolgáltató gondoskodik az adatok bizalmas tárolásáról. A napló állományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán szükségük van (jellemzően Független rendszervizsgálók). Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi.

5.4.5 A naplófájl mentési eljárásai

A naplóállományok rendszeresen mentésre kerülnek az 5.1.6 és 5.1.8 pontban meghatározott módon. Amennyiben a naplóbejegyzés egy helyen keletkezik, a Szolgáltató 24 (huszonnégy) órán belül gondoskodik a biztonsági másolat létrehozásáról.

5.4.6 A naplózás adatgyűjtési rendszere

A naplóbejegyzéseket az alkalmazások automatikusan gyűjtik és tárolják a napló állományokban. A mentett médiákat Szolgáltató napi rendszerességgel begyűjti. A médiákat Szolgáltató saját munkatársai szállítják a megőrzési helyre.

5.4.7 Az eseményeket kiváltó Ügyfelek értesítése

A naplóbejegyzéseket kiváltó személyeket, egységeket és alkalmazásokat Szolgáltató nem értesíti, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az esemény kiváltásában közreműködőknek a Szolgáltatóval fennálló szerződéses viszony vagy jogszabály rendelkezése esetén kötelessége a Szolgáltatóval való együttműködés.

5.4.8 Sebezhetőség felmérése

A naplóbejegyzések feldolgozása során Szolgáltató a naplózott események alapján a

sebezhetőségre vonatkozó felméréseket végez. A napi rendszerességgel végzett feldolgozáson túl Szolgáltató szakemberei havonta áttekintik a rendkívüli eseményeket és ezek alapján a sebezhetőségre vonatkozó elemzéseket végeznek. Ezen elemzések alapján a Szolgáltató lépéseket tesz a rendszer biztonságának javítására.

A Szolgáltató évente kockázatértékelést végez, amely segítségével azonosítja, értékeli és kockázati osztályba sorolja az olyan előrelátható külső és belső fenyegetettségeket, amelyek lehetővé tehetik a tanúsítványkezelési folyamatok jogosulatlan elérését, nyilvánosságra hozatalát, megváltoztatását, megsemmisítését vagy más visszaélést (pl. aláírási szolgáltatás vagy kulcsletét esetén ügyfél magánkulcsok elérését). A kockázatelemzés a bekövetkezés esetén a várható kárra is kiterjed. A kockázatelemzés a fentiek mellett tartalmazza a fenyegetettségek elhárítására a Szolgáltató által alkalmazott folyamatok, védelmi intézkedések leírását is.

5.5 Adatok archiválása

A Szolgáltató a szolgáltatással kapcsolatos adatokat a jelen fejezetben meghatározott módon és ideig őrzi meg. Szolgáltató a megőrzéssel együtt olyan eszközt is biztosít, amellyel a kibocsátott tanúsítvány tartalma megállapítható. Szolgáltató az archivált adatállomány minden bejegyzését védi a jogosulatlan módosítástól, törléstől, megsemmisüléstől és jogosulatlan hozzáféréstől. Az elektronikus formában tárolt archivált adatállományt legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel, és időbélyegzővel látja el. Szolgáltató biztosítja, hogy mindaddig, amíg az adatokat őrzi, azok hitelesek, az arra jogosult személyek számára hozzáférhetők és értelmezhetők legyenek.

5.5.1 Az archiválandó adatok típusai

A Szolgáltató az általa kiadott tanúsítványokhoz kapcsolódó adatokat - különösen az előállításukkal és kibocsátásukkal összefüggőket - beleértve a személyes adatokat is – meg kell őriznie. Így tárolásra kerül:

- a tanúsítványigénylés során az Igénylő és Előfizető által megadott adatok (lásd 4.1.2.1 fejezet);
- az azonosítási és hitelesítési eljárások (lásd 4.2.1 fejezet) során a Szolgáltató birtokába jutott elektronikus vagy papír alapú dokumentumok vagy azok másolatai;
- az igénylést elfogadó (lásd 4.2.2) regisztrációs ügyintéző azonosítója;
- az azonosítást és hitelesítést végző Regisztrációs Egység megnevezése;
- a tanúsítványállapot változási eljárás során közzétett információk (lásd 4.9.3 pont);
- a jelen Szabályzat szerinti naplózott információk (5.4 pont).

Az elektronikus adatokat Szolgáltató elektronikus úton őrzi meg. A papír alapon rendelkezésre álló dokumentumokat Szolgáltató elektronikus másolatként vagy eredeti papír alapú formájában őrzi meg.

5.5.2 Archiválási időtartam

Szolgáltató a tanúsítványokkal kapcsolatos elektronikus és papír alapú információkat és személyes adatokat legalább a tanúsítvány érvényességének tanúsítványban megadott lejártától számított tíz évig, valamint az aláíró/bélyegző tanúsítvánnyal, illetve a benne feltüntetett nyilvános kulccsal végzett aláírás/bélyeg ellenőrzésével vagy annak magánkulcs párjával készített aláírással/bélyegzéssel kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi, valamint ugyanezen határidőig olyan eszközt biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.

5.5.3 Az archívum védelme

Az elektronikus dokumentumok és adatok védelmére Szolgáltató az 5.4.4 pontban meghatározott

előírásokat alkalmazza - az elektronikusan megkapott dokumentumokra és az általa készített elektronikus másolatokra egyaránt.

A papír alapon rendelkezésre álló dokumentumokat Szolgáltató az 5.1 fejezet szerinti biztonsági körleten belül tárolja, biztosítva, hogy azokba kizárólag a Regisztrációs ügyintézők, Hitelesítési ügyintézők és Regisztrációs felelősök nyerhessenek betekintést.

5.5.4 Az archívum mentési folyamatai

Az archívum mentésére az 5.4.5 pontban meghatározott naplófájl mentésére vonatkozó előírások alkalmazandók.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

A Szolgáltató az archiválandó adatokat az 5.4.1 pontban meghatározott módon időbélyeggel vagy időadattal látja el.

5.5.6 Az archívum gyűjtési rendszere

A Kihelyezett Regisztrációs Egységek által az Ügyfelektől bekért adatokat és dokumentumokat a Szolgáltatói Partner bizalmasan tárolja és szerződésben meghatározott időközönként és formában továbbítja azokat a Szolgáltatónak.

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

Az archívumhoz Szolgáltató ügyfélszolgálatán keresztül benyújtott kérelem alapján lehet kérni hozzáférést. A hozzáférés az Ügyfélnek a rá vonatkozó adatokhoz lehetséges, más feleknek a 2.4.1 pont szerint. Szolgáltató a jogosultságot minden esetben ellenőrzi, és a hozzáférést naplózza.

5.5.8 Egyéb archiválási rendelkezések

Az archiválásra vonatkozó részletes rendelkezéseket az Információbiztonsági Szabályzat tartalmazza.

5.6 Kulcscsere

Szolgáltató lecseréli az alkalmazott saját kulcsát, amennyiben szolgáltatói tanúsítványa lejár, illetve az általa alkalmazott kulcsok elavulnak. Mindezek mellett a Szolgáltató saját belátása szerint egyéb esetben is dönthet kulcscsere mellett.

A Szolgáltató az új kulccsal kiállított új tanúsítvány esetében annak profilját és adatait az aktuális előírásokhoz és legjobb gyakorlathoz igazítja.

5.7 Katasztrófaelhárítás és helyreállítás

A Szolgáltató a szolgáltatásokat érintő fenyegetettségek azonosítására és a lehetséges kockázatok kezelésére vonatkozóan kockázatkezelési értékelést alkalmaz, illetve a rendkívüli helyeztek kezelésére, a vészhelyzetek minél gyorsabb elhárítása valamint a folyamatos működés biztosítására vonatkozóan Üzletmenet Folytonossági és Katasztrófa-elhárítási Tervvel (ÜFKT) rendelkezik.

A Szolgáltató a szolgáltatói rendszerek biztonságának megsértéséről, illetve az adatok sértetlenségének megszűnésről, amennyiben az jelentős befolyást gyakorol a szolgáltatásra, vagy a tárolt személyes adatokra (incidens) haladéktalanul, de legkésőbb 24 (huszonnégy) órán belül

értesíti a Bizalmi Felügyeletet és adott esetben a Microsoft-ot vagy egyéb érintett szerveket, valamint a szolgáltatás azon Ügyfeleit, akiket ez hátrányosan érinthet.

5.7.1 Incidens- és kompromittálódás-kezelési eljárások

Az informatikai rendszerekbe való belépésekre, azok felhasználóira és a Szolgáltatási szerződésre vonatkozó rendszertevékenységeket a Szolgáltató folyamatosan ellenőrzi a vonatkozó előírásokban foglaltaknak megfelelően. Az ellenőrzés pontos szempontjait az Információbiztonsági Szabályzat tartalmazza.

Amennyiben Szolgáltató az informatikai rendszereiben kritikus sérülékenységet észlel, a sérülékenység felfedezésétől számított 48 órán belül az alábbi intézkedések egyikét hajtja végre.

1. Kijavítja a kritikus biztonsági rést.
2. Amennyiben egy kritikus biztonsági rés kijavítása nem lehetséges 48 órán belül, Szolgáltató a sérülékenység enyhítése érdekében egy intézkedési tervet készít és hajt végre, melyben elsődleges intézkedésként határozza meg az alábbiakat:
    a. az ún. CVSS specifikáció[12] szerinti legkritikusabb biztonsági rések javítása (a legmagasabb pontszámúval kezdve);
    b. azon rendszerek biztonsági réseinek javítása, melyek nem rendelkeznek kiegészítő védelmi mechanizmussal és melyek a sérülékenység csökkentése nélkül ki lennének téve az illetéktelen hozzáférés és kompromittálódás veszélyének.
3. Szolgáltató dokumentálja a tényeket, melyek alapján nem szükséges a sérülékenység kijavítása - ennek okai - többek között - az alábbiak lehetnek:
    a. Szolgáltató nem ért egyet a CVSS specifikáció szerinti sérülékenységi besorolással;
    b. a sérülékenység beazonosítása téves;
    c. a sérülékenység kihasználhatóságát a kiegészítő védelmi mechanizmus megakadályozta; *vagy*

A Szolgáltató által alkalmazott ÜFKT tartalmazza a katasztrófa helyreállítási tervet is. Az ÜFKT olyan eljárásokat tartalmaz, amelyek leírják a megbízható üzemmenet mielőbbi helyreállításának leggyorsabb módját. A Szolgáltató ellenőrzések végrehajtásával rendszeresen (minimum évente) teszteli a biztonsági előírások hiánytalan technikai és személyi végrehajtását.

A Szolgáltató mentésekkel biztosítja, hogy szükség esetén az informatikai rendszer egészét helyre tudja állítani. A mentéseket a Szolgáltató védi a módosítások és jogosulatlan személyek hozzáférhesse ellen.

Szolgáltató átfogó és végrehajtható tervet tart fenn a tömeges TLS tanúsítvány visszavonási események kezelésére, eljárásait évente teszteli és a tapasztalatokat beépíti a felkészültség folyamatos javítása érdekében.

5.7.2 IT erőforrások, szoftverek és/vagy adatok meghibásodása

Szolgáltató megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik a hardver- és szoftvermeghibásodások valamint az adatsérülések minimalizálása érdekében. A szolgáltatások helyreállíthatóságát Szolgáltató háttérszerződései és saját tartalékeszközei garantálják, amelyek az 5.7.4 pontban vállalt időn belül bármely kieső kritikus eszköz pótlására képesek. Szolgáltató rendszeres mentései (lásd 5.5 pont) és tranzakció naplózása (lásd 5.4 pont) biztosítja az adatok visszaállíthatóságát valamely adattároló eszköz kiesésének esetére. Ez a rendszer a legrosszabb esetben az előző napi adatok helyreállítására képes.

Az ÜFKT eseményjelentési előírásokkal rendelkezik valamennyi eszköze meghibásodása, illetve rendellenes működése tekintetében (ezek egy része automatizált, más része a kezelőszemélyzet felelőssége). A jelentéseket szakértő személyzet értékeli ki és válaszadás eljárásokat foganatosítva minimalizálja az esetleges károkat és szolgáltatás kieséseket.

[12] Common Vulnerability Scoring System v3.0 (https://www.first.org/cvss/specification-document)

A kritikus rendszerelemek meghibásodására vonatkozó részletes szabályokat az ÜFKT tartalmazza.

A helyreállítás során elsőbbséget élveznek a tanúsítványállapot-információkat szolgáltató rendszerelemek.

5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás

Végfelhasználói magánkulcs kompromittálódása

Végfelhasználói magánkulcs kompromittálódására vonatkozóan lásd a 4.9.12 pontban foglaltakat.

Szolgáltatói magánkulcs kompromittálódása

A szolgáltatói kulcs kompromittálódása esetén a Szolgáltató tájékoztatja Ügyfeleit, szerződéses partnereit, az Érintett Feleket és a Bizalmi Felügyeletet. A tájékoztatás tartalmazza, hogy az érintett szolgáltatói kulccsal kibocsátott tanúsítványok és a tanúsítványállapot-információ már nem érvényesek. A kompromittálódott magánkulcsot tartalmazó tanúsítványt a Szolgáltató visszavonja.

A szolgáltatói magánkulcs kompromittálódására vonatkozó további előírásokat és a követendő eljárást az ÜFKT tartalmazza. Katasztrófa bekövetkezése esetén a Szolgáltató megteszi a szükséges lépéseket a katasztrófa megismétlődésének elkerülése érdekében.

Algoritmus változása

Amennyiben a Szolgáltató által alkalmazott valamely algoritmus vagy ahhoz kapcsolóan valamely paraméter nem felel meg az elvárásoknak ill. nem alkalmas a rendeltetésszerű használatra a teljes tervezett felhasználási időtartamra (végfelhasználói és szolgáltatói tanúsítvány esetén egyaránt), akkor a Szolgáltató tájékoztatja Ügyfeleit, szerződéses partnereit, az Érintett Feleket és a Bizalmi Felügyeletet, valamint megteszi a szükséges lépéseket az érintett tanúsítványok visszavonása érdekében.

5.7.4 A működés folytonosságának fenntartása katasztrófaesemény után

Szolgáltató rendelkezik üzletfolytonossági tervvel, amit katasztrófa esetén életbe léptet. Katasztrófa bekövetkezte estén - beleértve valamely szolgáltatói magánkulcs vagy más hitelesítő adat kompromittálódását vagy a szolgáltatói rendszer kritikus elemeinek meghibásodását is - szolgáltató normál működése helyreállításra kerül, s egyúttal a hiba újbóli bekövetkeztének megelőzésére is sor kerül.

A Szolgáltató célja, hogy a hiba elhárítása és az integritás helyreállítása után a lehető leghamarabb újraindítsa valamennyi szolgáltatását. A visszavonási nyilvántartások megbízható üzemelésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását megelőzi.

Ha a rendkívüli üzemeltetési helyzet a BM rendelet 36. és 45. §-ban foglalt időtartamot meghaladja, a szolgáltató a bizalmi felügyeletet haladéktalanul értesíti a rendkívüli üzemeltetési helyzettel kapcsolatos alábbi információkról is:

- a rendkívüli üzemeltetési helyzet kezdetének, és ha eltér, észlelésének időpontja és a rendkívüli üzemeltetési helyzet leírása,
- a rendkívüli üzemeltetési helyzet hatása (ennek részeként biztonsági esemény esetén az érintett szolgáltatások, informatikai vagyonelemek és az érintett személyes adatok körének leírása, az érintett bizalmi szolgáltatási ügyfelek száma),
- a rendkívüli üzemeltetési helyzet várható időtartama,

- a rendkívüli üzemeltetési helyzet elhárítása és jövőbeli elkerülése érdekében tett és tervezett intézkedések, és
- a rendkívüli üzemeltetési helyzet megszűnése.

Természeti vagy más katasztrófát követően, illetve a Szolgáltató berendezéseinek meghibásodása esetén Szolgáltató a következő szolgáltatások legfeljebb 24 órán belüli elindítását vállalja:

- állapotváltoztatás-szolgáltatás,
- tanúsítványállapot-szolgáltatás.

Minden egyéb szolgáltatás elindítását Szolgáltató 5 munkanapon belül vállalja.

5.8 A hitelesítő vagy a központi regisztrációs egység megszűnése

Amennyiben a Szolgáltató tevékenységét tervezetten megszűnteti vagy tartósan szünetelteti, a tevékenység leállását megelőzően legalább az alábbi eljárásokat hajtja végre:

- Szolgáltatónak minden ésszerű erőfeszítést meg kell tennie annak érdekében, hogy egy erre alkalmas szolgáltató a nyilvántartásait és szolgáltatási kötelezettségeit legkésőbb a szolgáltatás leállításáig átvegye tőle.
- A szolgáltatás megszűnése előtt legalább 60 nappal értesítést tesz közzé weboldalán, e-mail címmel rendelkező ügyfelei számára a szolgáltatás befejezéséről elektronikus levélben értesítőt küld illetve tájékoztatja erről a Bizalmi felügyelet. Az értesítésekben megjelöli azt a - vele azonos besorolású – szervezetet, amely legkésőbb a tevékenység befejezésekor átveszi a tanúsítványállapot közlési nyilvántartásokat, valamint a regisztrációs információ és az eseménynapló archívumok fenntartására vonatkozó kötelezettségeket a Szolgáltató számára előírt vagy általa vállalt időtartamra.
- Saját magánkulcsait megsemmisíti, illetve a hozzájuk tartozó tanúsítványokat visszavonja, és erről weboldalán tájékoztatást tesz közzé.
- Amennyiben csak bizalmi szolgáltatás kerül megszüntetésre, akkor a szolgáltató lehetőség a visszavonási információkat továbbra is biztosítja.
- Amennyiben a bizalmi szolgáltatási tevékenységek teljes egészében megszüntetésre kerülnek:
  - Szolgáltató biztosítja, hogy az általa kezelt és közzétett (végfelhasználói és köztes kiadói) tanúsítványállapot-információk a tevékenység befejezéséig az eredeti URL-en elérhetők legyenek (ezt követően az átvevő szolgáltatónak kell biztosítania az állapotinformációk elérését); *valamint*
  - Szolgáltató a tevékenység beszüntetésének napján a szolgáltatói gyökértanúsítványt és kulcsát megsemmisíti, és melyről sajtóközleményt ad ki.

A Szolgáltató a tanúsítványok visszavonását követően a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének továbbra is eleget tesz.

- A Szolgáltató a tevékenység befejezését legalább 20 nappal megelőzően az általa kibocsátott, és még vissza nem vont tanúsítványokat visszavonja.
- Amennyiben a bizalmi szolgáltatási tevékenységek teljes egészében megszüntetésre kerülnek, a Gyökér Kiadó (rootCA) tanúsítványának tervezett megszüntetéséről legalább 20 nappal a tevékenység befejezése előtt értesítést küld azon szoftvergyártóknak, melyek ún. „root program”-jában a gyökértanúsítvány szerepel.
- A Szolgáltatóval szerződéses kapcsolatban álló, a tanúsítványkibocsátásban résztvevő, összes vállalkozással, Regisztrációs Egységgel korábban megkötött szerződés alapján fennálló kezelési jogokat, illetve felhatalmazást visszavonja, s valamennyi Regisztrációs Egységet felhívja a náluk tárolt adatok átadására.
- A regisztrációs információk és az eseménynapló archívumok megőrzése érdekében, időbélyegzővel ellátott teljes körű mentést hajt végre. A mentés tartalmazza a

tanúsítványokkal kapcsolatos korábbi változások adatait, a tanúsítványok helyzetére, esetleges felfüggesztésére, illetve visszavonására vonatkozó adatokat, valamint a tanúsítvány kibocsátásra vonatkozó Szolgáltatói szabályzatokat és az aláírás-ellenőrző adatokat, továbbá a visszavont tanúsítványok nyilvántartását. A mentett adatállományokat Szolgáltató védi a jogosulatlan módosítástól és biztosítja a jogosulatlan hozzáférés kizárását, valamint az adatoknak megőrzési időn belüli, hozzáférhetőségét és értelmezhetőségét a jogosult személyek számára.

- A Szolgáltató új tanúsítványokat a megszűnés bejelentése után nem bocsát ki.

Ha a Szolgáltató ellen a bíróság jogerős határozata alapján felszámolási vagy végelszámolási eljárás indult, haladéktalanul tájékoztatja a Bizalmi Felügyeletet e tényről, megnevezve az eljárást lefolytató szervezetet.

A Szolgáltató annak érdekében, hogy adatait átadhassa egy másik szolgáltatónak, azokat a szolgáltató által fogadóképes médián és formátumban helyezi el vagy biztosítja a másik szolgáltató számára az adatok eredeti formátumban történő feldolgozásának lehetőségét, melyekhez átadja a megfelelő eszközöket, dokumentációkat és ismereteket.

6. MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

A Szolgáltató megbízható, biztonságtechnikailag értékelt és ellenőrzött termékekből álló informatikai rendszert használ szolgáltatásai nyújtásához.

A kulcskezelési rendelkezések az alábbi kulcsokat különböztetik meg:

Szolgáltatói magánkulcsok:

- végfelhasználói tanúsítványokat, CRL és OCSP válaszokat aláíró magánkulcs,
- egyéb tanúsítványokat, CRL és OCSP válaszokat aláíró magánkulcs,
- infrastrukturális és kontrollkulcsok,
- viszontazonosítási válasz aláíró kulcs,
- egyéb szolgáltatói magánkulcsok (archiválást hitelesítő, időbélyegző)

Szolgáltatói nyilvános kulcsok:

- a szolgáltatói magánkulcsok nyilvános párjai.

Végfelhasználói magánkulcsok:

- végfelhasználó magánkulcsa, amelyet saját maga hozott létre,
- végfelhasználó magánkulcsa, amelyet számára a Szolgáltató hozott létre.

Végfelhasználói nyilvános kulcsok:

- a végfelhasználói magánkulcsok nyilvános párja.

6.1 Kulcspár generálás és telepítés

Amennyiben a tanúsítványban feltüntetésre kerülő másodlagos hitelesítési rend SCD alapú kulcstárolást jelöl (lásd a Szolgáltatási rend 1.2.1 Hitelesítési rendek fejezetet), a kulcs a 6.2.1 fejezetben megadott Ügyféleszközök valamelyikében kerül generálásra.

Ha a kriptográfiai eszközt, illetve az Ügyfél magánkulcsát egy harmadik fél kezeli, akkor szolgáltató a tanúsítvány teljes élettartama alatt meggyőződik arról, hogy e fél az ehhez szükséges feltételrendszernek (pl. felügyeleti nyilvántartás) megfelel.

Amennyiben az Ügyfél magánkulcsa mozgatásra kerül eszközök között, akkor Szolgáltató megfelelő intézkedésekkel kezeli az ebből fakadó biztonsági kockázatokat.

Amennyiben az eszköz a nem minősített szolgáltatás számára releváns tanúsítása érvényességét veszti, akkor szolgáltató az adott eszközre kiadott tanúsítványokat visszavonja.

6.1.1 Kulcspár előállítása

A Szolgáltató – attól függetlenül, hogy a kulcspárt ki generálta – ellenőrzi, hogy a nyilvános kulcs korábban nem került-e kiosztásra más Ügyfél számára.

Szolgáltatói kulcspár előállítása

A szolgáltatói kulcsok generálása (beleértve az időbélyegző kulcsokat is) a Szolgáltató fizikailag védett szervertermében két bizalmi munkakört betöltő személy együttes jelenlétében, más személy jelenlétének kizárásával jegyzőkönyvezetten történik. Azon bizalmi munkakört betöltő személyek listáját, akik jogosultak kulcsgenerálásra, a Szolgáltató Információbiztonsági Szabályzata tartalmazza.

A Szolgáltatói kulcsok generálására és tárolására (beleértve az időbélyegző kulcsokat is) a Szolgáltató a jelen Szabályzat 6.2.1 pontjában részletezett kriptográfiai hardvermodulokat használja. A Szolgáltató valamennyi szolgáltatói kulcspárt saját maga generálja. A generált magánkulcsok – a 6.2.4 fejezetben ismertetett mentés esetét leszámítva - teljes életciklusuk alatt a kriptográfiai hardverekben maradnak, megsemmisítésükig sehová nem kerülnek áthelyezésre. Amennyiben a szolgáltatói magánkulcs bármely okból történő megsemmisítése válik szükségessé, úgy az az eszköz tanúsítványában előírt módon két személyes kontroll mellett történik.

A Szolgáltatói kulcsok lejáratát megelőzően a Szolgáltató az új kiadói kulcsokat úgy generálja és adja ki az új szolgáltatói tanúsítványokat, hogy az átállás az Ügyfél részéről minél zökkenőmentesebb lehessen, és a tanúsítvány cseréje ne okozzon zavart az Ügyfelek és az Érintett Felek számára.

Szolgáltató új Gyökér Kiadójának kulcselőállítását egy minősített auditor is megfigyeli, ellenőrizve a fenti követelményeknek való megfelelést, illetve a kulcspár integritását és bizalmasságát. Az auditor egy igazolást állít ki, arról hogy a szolgáltató:

- A Gyökér Kiadó kulcselőállítási és védelmi eljárásait dokumentálta szabályzataiban;
- A kulcselőállító eljárás megfelelő részletezettségű;
- Hatékony kontrollokkal gondoskodott arról, hogy a kulcsgenerálás az előírásokkal összhangban megfelelő biztonsági szinten történjen meg;
- A kulcselőállító eljárás valamennyi eljárását végrehajtotta.

Amennyiben ugyanaz az időbélyegző kulcs több kriptográfiai modulban is alkalmazásra kerül, akkor Szolgáltató ugyanazt a tanúsítványt kapcsolja hozzá.

A Szolgáltatói kulcsok generálására vonatkozó részletszabályokat a kulcsgenerálási forgatókönyv tartalmazza.

Végfelhasználói kulcspár Szolgáltató által történő előállítása

A Szolgáltató a végfelhasználói aláíró és bélyegző tanúsítványokhoz tartozó kulcsok generálását vállalja, melynek során olyan algoritmusokat használ, amelyek megfelelnek a kibocsátáskor hatályos szabványokban, illetve a Bizalmi Felügyelet határozatban előírtaknak. Szolgáltató visszautasít minden olyan tanúsítványkibocsátásra vonatkozó igényt, amely nem felel meg e rendelkezéseknek.

A végfelhasználói kulcsok generálása automatizáltan vagy Szolgáltató védett szerverszobájában történik kizárólag bizalmi munkakört betöltő személyek által. Amennyiben a kulcspár Ügyféleszközön kerül alkalmazásra, akkor azt Szolgáltató közvetlenül az eszközben hozza létre, azt semmilyen más módon nem tárolja és menti, kivéve a 4.12 Kulcsletét és kulcshelyreállítás fejezetben ismertetett eseteket.

Az NL Sign szolgáltatás keretében igényelt végfelhasználói tanúsítványokhoz tartozó kulcspárt Szolgáltató saját kriptográfiai eszközén (HSM modulban) automatizáltan generálja. A kriptográfiai eszköz megfelel a szolgáltatói magánkulcs kriptográfiai eszközére vonatkozó elvárásoknak (lásd a 6.2.1 fejezetet).

Szolgáltató biztosítja, hogy végfelhasználó magánkulcsához és aktiváló adatához mások ne férhessenek hozzá.
Lásd még a 6.1.2 Magánkulcs eljuttatása a Végfelhasználóhoz fejezetet.

Weboldal-hitelesítő tanúsítványokhoz (DVCP) tartozó kulcsokat Szolgáltató nem generál.

Végfelhasználói kulcspár Végfelhasználó által történő előállítása

A nem-minősített végfelhasználói tanúsítványhoz tartozó kulcspárt előállíthatja a végfelhasználó maga is. . Végfelhasználói kulcsgenerálás esetén, amennyiben az igénylés olyan tanúsítványra vonatkozik, melynek másodlagos hitelesítési rendje SCD alapú kulcstárolást jelöl, Végfelhasználó köteles a kulcsgenerálást a 6.2.1 fejezetben megadott SCD vagy QSCD Ügyféleszköz valamelyikében végezni, továbbá köteles a kulcsot a teljes használati idő alatt ezen eszközön használni. A magánkulcs eszközről történő exportálása kizárólag biztonsági mentés készítése céljából megengedett. Lásd még a 6.1.3 Nyilvános kulcs eljuttatás a tanúsítvány kibocsátóhoz fejezetet.

6.1.2 Magánkulcs eljuttatása a Végfelhasználóhoz

Amennyiben a Szolgáltató generálta a végfelhasználói kulcspárt, akkor azt a hordozó Ügyféleszközzel egyetemben biztonságos módon Átvevőn keresztül juttatja el a Végfelhasználóhoz.

Menedzselt SCD esetén a szolgáltató nem juttat el kulcsot a felhasználóhoz, a felhasználó értesítést kap arról, hogy kulcsát a korábban megadott aktiváló adattal igénybe veheti.

6.1.3 Nyilvános kulcs eljuttatás a tanúsítvány kibocsátóhoz

Amennyiben a kulcsgenerálást a Végfelhasználó végzi, a nyilvános kulcsot a már sikeresen regisztrált Igénylő védett csatornán küldi meg a Regisztrációs Egységnek, amely – miután sikeresen ellenőrizte, hogy az Igénylő által megküldött nyilvános kulcsnak megfelelő magánkulccsal valóban rendelkezik az Igénylő – szintén védett csatornán továbbítja a Kiadónak.

Amennyiben a végfelhasználói tanúsítványhoz a kulcspárt a Szolgáltató generálja, úgy nincs szükség a nyilvános kulcs továbbítására.

Menedzselt SCD esetén Szolgáltató nem juttat el kulcsot a felhasználóhoz, a felhasználó értesítést kap arról, hogy kulcsát a korábban megadott aktiváló adattal igénybe veheti.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

Szolgáltató szolgáltatói tanúsítványai - beleértve az időbélyegző tanúsítványt - elérhetőek a Szolgáltató weboldalán (1.1.2 pont). A szolgáltatói tanúsítványok elérhetősége szabványos módon a végfelhasználói tanúsítvány AIA:CAIssuer mezőjében is megtalálható.

A szolgáltató nyilvános kulcsai a szolgáltatói tanúsítványai részeként elérhetőek.

6.1.5 Kulcsméretek

A Szolgáltató által alkalmazott kulcspárok (szolgáltatói és végfelhasználói tanúsítványok esetén egyaránt) megfelelnek a hatályos szabványokban, illetve a Bizalmi Felügyelet határozatban előírtaknak. A Szolgáltató által használt algoritmusok:

Lenyomatképző algoritmusok azonosítói:

- SHA-256 OID ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-256 (1) }
- SHA-384 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-384(2)}
- SHA-512 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-512(3)}

Kriptográfiai algoritmusok azonosítói és kulcsméretei:

- RSA OID ::= { iso(1) member-body (2) USA (840) RSADSI (113549) PKCS (1) PKCS-1 (1) RSA Encryption (1) } – Minimum 2048 bit kulcshossz
- DSA OID ::= { iso(1) member-body(2) us(840) X9-57 (10040) x9algorithm (4) id-dsa (1) }

A Szolgáltató az itt meghatározott algoritmusokat legfeljebb a Bizalmi Felügyelet Algoritmus Határozatában megjelölt időpontig használja.

6.1.6 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A kulcsgenerálás paramétereinek megfelelőségét a Szolgáltató által használt rendszer két szempontból ellenőrzi:

- a paraméterekhez felhasznált véletlenszám-generálás megfelelőségének ellenőrzése (statisztikailag kellőképpen véletlenszerű-e a generálás),

- a paraméterekre vonatkozó feltételek, összefüggések teljesülésének ellenőrzése.

A véletlenszám-generálás megfelelőség ellenőrzésének alapja, hogy a rendszerben használt valamennyi kriptográfiai hardver modul képes az általa generált bitsorozat egyenletességének és függetlenségének statisztikai tesztelésére. A modulok lehetővé teszik a tesztek meghívását egy szabványos interfészen keresztül.

A külső interfészen meghívható tesztelési utasításon kívül a hardver modulok is folyamatosan tesztelik saját véletlenszám-generálásukat, melyek hibás teszt esetén leállnak.

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

A Gyökér Kiadó kulcsa

A Gyökér Kiadó kulcsa kizárólag a következő célokra használható:

- A Gyökér Kiadó tanúsítványának aláírására (Önaláírt tanúsítvány)
- Alárendelt szolgáltatások hitelesítésére vonatkozó tanúsítványok aláírására
- Köztes Kiadó tanúsítványának aláírására és kereszthitelesítésre
- Belső szolgáltatói tanúsítványok aláírására (pl. OCSP)
- Tesztelési célra, amennyiben az éles célra a Gyökér Kiadó aláírása szükséges

A Köztes Kiadó kulcsa

A Köztes Kiadó kulcsa kizárólag a következő célokra használható:

- Végfelhasználói tanúsítványok aláírására
- Belső szolgáltatói tanúsítványok aláírására (pl. OCSP, CRL)
- Tesztelési célra, amennyiben az éles célra a Köztes Kiadó aláírása szükséges

A Végfelhasználói tanúsítványok kulcsa

A különböző típusú végfelhasználói tanúsítványok az alábbi célokra használhatók:

- Elektronikus aláírás létrehozására
- Elektronikus bélyegző létrehozására
- Weboldal-hitelesítésére és a titkosított kommunikáció felépítésére

a belefoglalt X509v3 biteknek megfelelően.

Lásd a 7.1.2 Tanúsítvány kiterjesztések fejezetben a kulcshasználat mezők ennek megfelelő értékeit.

6.2 Magánkulcs védelem és kriptográfiai modul előírások

Szolgáltató olyan fizikai és logikai védelmeket implementált, amelyek megakadályozzák a jogosulatlan tanúsítványkibocsátást.

Szolgáltató a magánkulcsát biztonságos módon tárolja, ami megakadályozza, hogy jogosulatlan személy hozzáférhessen és használhassa. Szolgáltató a tanúsítványok előállításához, a visszavonási nyilvántartások hitelesítéséhez és egyéb célra használt szolgáltatói magánkulcsait csak fizikailag védett környezetben, az adott kulcsra meghatározott rendeltetési célra használja fel.

6.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások

A szolgáltatói kulcsok - beleértve az időbélyegző kulcsokat is - létrehozása, mentése, tárolása és megsemmisítése kapcsán Szolgáltató az alábbiak szerint jár el:

- a kulcsok létrehozása, tárolása, mentése, helyreállítása, megsemmisítése fizikailag biztonságos környezetben, kettős személyi ellenőrzés mellett (két bizalmi munkakört

betöltő munkatárs együttes jelenlétében) valósul meg (lásd 6.1.1.1 pont),
- a Kiadók kulcsai a vonatkozó szabványoknak megfelelően legalább EAL4 tanúsítással rendelkező, az ISO/IEC 15408 vagy ezzel ekvivalens IT biztonsági elvárás szerint, vagy az ISO/IEC 19790 vagy FIP PUB 140-2 level 3 megfelelő hardver kriptográfiai eszközben kerülnek generálásra, tárolásra, illetve felhasználásra (lásd 6.1.1.2 és a 6.2.7 Magánkulcs tárolása kriptográfiai modulban fejezeteket),
- a kulcsokat kizárólag az arra felhatalmazottak használhatják, a létrehozás céljának megfelelő funkcióra,
- a Szolgáltató rendszerei saját szolgáltatói kulcsaik használata előtt meggyőződnek arról, hogy az e kulcsokhoz kapcsolódó tanúsítványok érvényesek,
- a Szolgáltató tanúsítvány-, CRL és OCSP aláíró kulcsai különböznek minden más funkcióra szolgáló kulcstól,
- a szolgáltatói kulcsfrissítés out-of-band cserével történik,
- biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálásakor a Szolgáltató gondoskodik a kulcs védelméről,
- azokat a rendszereket, melyek kriptográfiai hardver eszközön kívül dolgoznak fel kriptográfiai szempontból érzékeny információt (magán- vagy titkos kulcsokat) a Szolgáltató védi az elektromágneses kisugárzással történő kompromittálódás ellen (ld. 5.1.3 pont).

Szolgáltató elkülönítve kezeli és működteti a minősített szolgáltatásainak nyújtásához használt kriptográfiai eszközöket a nem minősített szolgáltatásokhoz és egyéb tevékenységeihez használt kriptográfiai eszközöktől, mely utóbbiak így nem befolyásolhatják a minősített szolgáltatást megvalósító termékek megbízható üzemeltetését.

Szolgáltató a bizalmi szolgáltatás nyújtását közvetlenül megvalósító termékeiről biztonsági osztályokba sorolt nyilvántartást vezet.

Mielőtt a szolgáltató a szolgáltatás nyújtásához használt bizalmi szolgáltatást megvalósító termékeit a saját maga által végzett szolgáltatásnyújtáson kívüli célokra használja fel, megbizonyosodik arról, hogy a termék nem tartalmaz olyan adatot, amely bizalmi szolgáltatáshoz fűződik, valamint arról, hogy az ilyen adatot nem lehet visszaállítani. E vizsgálatot és a vizsgálat eredménye alapján végrehajtott intézkedést a minősített szolgáltatónak naplózza.

A Szolgáltató által használt és biztosított kulcstároló, kulcsgeneráló és aláíró eszközök listája, valamint az eszközök megfelelőségi tanúsítványai letölthetők az alábbi linkről: https://netlock.hu/dokumentumtar/

Szolgáltató folyamatosan figyelemmel kíséri az általa alkalmazott eszközök tanúsításának érvényességét, illetve az alkalmazásukra vonatkozó esetleges újabb korlátozásokat. Ennek érdekében egyrészt belső adminisztrációs belső előírásokat hozott meg a tanúsítások érvényességének nyilvántartására, illetve az Európai Unión belül elvégzett tanúsítások érvényességei változásainak nyomon követésére, mely előírja ezen tanúsítások állapotának ellenőrzését legalább havonta. Továbbá a tanúsítással érintett eszközök gyártóival, forgalmazóval is kommunikál, hogy minél hamarabb értesülhessen a tanúsítások változásairól, teljesítse ehhez kapcsolódó Szolgáltatói teendőit.

Szolgáltató saját felhasználásra és ügyféleszközként egyaránt bevezethet további kulcskezelő és aláíró eszközöket, amennyiben azok rendelkeznek a felhasználási célnak megfelelő tanúsítással.

A végfelhasználói tanúsítványokhoz aktuálisan igényelhető Ügyféleszközökről Szolgáltató weboldalán (lásd 1.1.2) nyújt tájékoztatást.

6.2.2 Magánkulcs többszereplős (n-ből m) használata

A magánkulcs többszereplős használatára vonatkozó részletszabályokat a Szolgáltató Információbiztonsági Szabályzata tartalmazza.

6.2.3 Magánkulcs letétbe helyezése

Lásd a 4.12 pontban foglaltakat.

6.2.4 Magánkulcs mentése

A mentés rejtjeles formában hajtódik végre. A mentés során a magánkulcsot generáló kriptográfiai hardver modulból – a kriptográfiai hardver modul típusának megfelelően - intelligens kártyákra több darabban (lásd 6.2.2 pont), védetten másolódik át a magánkulcs vagy ún. backup HSM modulba kerül. A mentett példányok ugyanolyan jellegű és erősségű védelem alatt állnak, mint a kulcsgenerálást végző hardver modul eredeti példánya. A kulcs titkosítása során olyan algoritmus és kulcsméret került alkalmazásra, ami annak teljes hátralévő idejében biztosítja a védelmet. A szolgáltatói magánkulcs nem üzemben lévő másolatait legalább a produktív kulccsal azonos szintű biztonsági eljárások védik.

A Szolgáltatónál a következő szolgáltatói magánkulcsok kerülnek mentésre:

- a Gyökér Kiadó hitelesítő magánkulcsa,
- a Köztes Kiadók hitelesítő magánkulcsai.

A végfelhasználói magánkulcsok mentésével kapcsolatosan lásd a 4.12.1 pontot.

6.2.5 Magánkulcs archiválása

A Szolgáltató sem a szolgáltatói, sem a végfelhasználói magánkulcsokat nem archiválja.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba, vagy onnan történő exportja

A szolgáltatói magánkulcsok - beleértve az időbélyegző magánkulcsokat is - kriptográfiai modulba juttatását Szolgáltató fizikailag védett környezetben valósítja meg legalább két bizalmi munkakört betöltő személy együttes részvételével, más személy jelenlétének kizárásával.

Lásd a 6.2.4 pontban foglaltakat.

6.2.7 Magánkulcs tárolása kriptográfiai modulban

A kriptográfiai eszközön tárolt szolgáltatói magánkulcsok esetében Szolgáltató gondoskodik arról, hogy a kulcsok ne legyenek elérhetők az eszközön kívül (kivéve a 6.2.4 pontban foglalt mentés esetét). A kriptográfiai eszköz esetében Szolgáltató gondoskodik a hamisítás elleni védelemről a szállítás és a tárolás során is.

Lásd a 6.2.1 pontban foglaltakat.

6.2.8 A magánkulcs aktiválásának módja

A szolgáltatói magánkulcsok - beleértve az időbélyegző magánkulcsokat is - aktiválását Szolgáltató fizikailag védett környezetben valósítja meg legalább két bizalmi munkakört betöltő személy együttes részvételével, más személy jelenlétének kizárásával. A szolgáltatói kulcsok aktiválásának módját a Szolgáltató Információbiztonsági Szabályzata részletezi.

A szolgáltató által generált végfelhasználói magánkulcsok, illetve Ügyféleszközök kizárólag aktiváló adat segítségével aktiválhatók.

SCD kulcstárolással igényelt aláíró és bélyegző tanúsítványok (lásd 1.2.1) esetén a végfelhasználói magánkulcs az eszköz leírásának megfelelő módon aktiválandó.

Az NL Sign szolgáltatás keretében kiadott végfelhasználói tanúsítvány magánkulcsa minden egyedi vagy kötegelt aláírás/bélyegzési művelethez aktiválandó, az eszköz leírásának megfelelő módon.

6.2.9 A magánkulcs deaktiválásának módja

A szolgáltatói kulcsok deaktiválásának módját Szolgáltató Információbiztonsági Szabályzata részletezi.

NL Sign szolgáltatás keretében kiadott végfelhasználói tanúsítványok magánkulcsát Szolgáltató minden egyedi vagy kötegelt aláírás/bélyegzési műveletet követően azonnal és automatikusan deaktiválja.

6.2.10 A magánkulcs megsemmisítésének módja

A szolgáltatói kulcsokat a Szolgáltató olyan módon semmisíti meg, hogy az aláíró kulcsok ne legyenek visszanyerhetőek. A megsemmisítése során a Szolgáltató olyan biztonságos törlési folyamatokat alkalmaz, melyek ténylegesen felülírják a kulcsok összes előfordulását az összes olyan tárolóeszközön, melyen a kulcs példányai előfordulhattak.

Szolgáltatói eszköz megsemmisítése esetén Szolgáltató gondoskodik a rajta tárolt magánkulcsok megsemmisítéséről.

A végfelhasználói aláíró / bélyegző / weboldal-hitelesítő tanúsítványok magánkulcsait végfelhasználónak meg kell semmisítenie amennyiben a tanúsítvány visszavonásra kerül vagy érvényessége lejár és a magánkulcshoz tartozó nyilvános kulccsal újabb tanúsítvány nem kerül kiadásra.

Az NL Sign szolgáltatás keretében tárolt végfelhasználói magánkulcsokat Szolgáltató a fenti esetekben, valamint az aktiváló adat visszaállítása esetén visszaállíthatatlan módon megsemmisíti.

6.2.11 A kriptográfiai modulok értékelése

Lásd a 6.2.1 pontban foglaltakat.

6.3 A kulcspárkezelés további szempontjai

A Szolgáltató a szolgáltatói kulcsokat a tanúsítványban feltüntetett módon és érvényességi időtartam alatt használja.

6.3.1 Nyilvános kulcs archiválása

A Szolgáltató minden, általa előállított tanúsítványt archivál, az alábbi időszakra:

- Szolgáltatói tanúsítványok: az érvényesség lejártától számított 10 évig,
- végfelhasználói tanúsítványok: az érvényesség lejártától számított, jogszabályban meghatározott ideig (lásd 5.5.2 pont).

6.3.2 Tanúsítvány és kulcspár használati idő

Típus	Tanúsítvány élettartam	Kulcspár használati idő
Nem-minősített aláíró és bélyegzőtanúsítványok	legfeljebb 2 év (730 nap)	A Szolgáltató a kulcs élettartamára vonatkozóan korlátot nem állapít meg, de bármikor előírhatja az új kulcsgenerálás szükségességét.
Weboldal-hitelesítő tanúsítványok	legfeljebb 1 év (365 nap)	A Szolgáltató a kulcs élettartamára vonatkozóan korlátot nem állapít meg, de

		bármikor előírhatja az új kulcsgenerálás szükségességét.
Szolgáltatói tanúsítvány	legfeljebb 20 év (7300 nap)	A tanúsítvány érvényességi idejével megegyező.
Teszttanúsítvány	legfeljebb 2 év (730 nap)	A Szolgáltató a kulcs élettartamára vonatkozóan korlátot nem állapít meg, de bármikor előírhatja az új kulcsgenerálás szükségességét

Az tanúsítvány érvényességi időtartam a tanúsítványban feltüntetésre kerül. A tanúsítványok érvényességének kezdete a kibocsátás időpontjával megegyezik vagy azt követi.

A Szolgáltató nem állíthat ki olyan végfelhasználói tanúsítványt, melynek élettartama meghaladja a szolgáltatói tanúsítványok élettartamát.

6.4 Aktiváló adat

Az aktiváló adattal kapcsolatos kérdéseket az alábbi fejezetek írják le.

A Szolgáltatói kulcspár telepítése és helyreállítása a kriptográfiai eszközön kizárólag bizalmi munkakörben foglalkoztatott munkatársak legalább kettős kontrollja alatt valósulhat meg.

A Szolgáltatók biztosítja az Ügyféleszköz (SCD vagy menedzselt SCD) aktiváló adatának megváltoztatását az aktuális aktiváló adat ismeretében. A végfelhasználói aktiváló adatot a Szolgáltató semmilyen körülmények között nem tárolhatja, kivéve az aláírási munkafolyamat idejére a memóriában való tárolás esetét.

6.4.1 Aktiváló adat generálás és telepítés

A magánkulcsot aktiváló adatot Igénylő adja meg a kulcsgenerálás részeként vagy Szolgáltató által biztosított Ügyféleszköz alkalmazása esetén Szolgáltató generálja.

Szolgáltató az Ügyféleszközhöz tartozó aktiváló adatokat biztonságos módon, az eszközöktől elkülönítetten állítja elő. Szolgáltató az aktiváló adatot lezárt borítékban juttatja el Átvevőhöz. Az eszköz, és az aktiváló adatot tartalmazó boríték átvételét követően van lehetősége Végfelhasználónak Tanúsítványa aktiválására (lásd 4.9.3.2 pont, amennyiben azt Szolgáltató felfüggesztett állapotban feltöltötte Ügyféleszközre) vagy Ügyféleszközre történő feltöltésére (lásd 4.3 pont, amennyiben Szolgáltató csak a magánkulcs generálását végezte el Ügyféleszközre, a tanúsítványt pedig Ügyfélmenüből teszi elérhetővé). Az Ügyféleszköz első használatba vételekor javasolt az aktiváló adat cseréje.

Az NL Sign szolgáltatás keretében generált magánkulcs aktiváló adatát végfelhasználó hozza létre a kulcsgenerálás során Szolgáltató azt nem ismeri és nem tárolja, kivéve az aláírási munkafolyamat idejére a memóriában való tárolás esetét.
Az aktiváló adat az aktuális aktiváló adat ismeretében megváltoztatható.

6.4.2 Aktiváló adat védelme

Szolgáltató az Ügyféleszközhöz tartozó aktiváló adatokat csak abból a célból rögzíti, hogy azt a szolgáltatást igénybe vevő személy számára – másolat megőrzése nélkül – átadhassa.

Menedzselt SCD igénybevétele esetén (NL SIGN szolgáltatáson keresztül igényelt tanúsítvány) az aktiváló kód a szolgáltató által nem helyre állítható.

6.4.3 Egyéb aktiváló adattal kapcsolatos előírások

A Végfelhasználónak gondoskodnia kell arról, hogy a részére átadott magánkulcsok aktiválása és deaktiválása biztonságos módon történjen.

Menedzselt SCD igénybevétele esetén (NL SIGN szolgáltatáson keresztül igényelt tanúsítvány) az aktiváló kód a szolgáltató által nem helyre állítható.

6.5 Informatikai biztonsági előírások

A Szolgáltató rendszereit csak az arra jogosult személyek érhetik el. A Szolgáltató a belső zónák határait tűzfalakkal védi és megteszi a szükséges intézkedéseket arra vonatkozóan, hogy az érzékeny adatok az adathordozók újrafelhasználása során ne legyenek feltárhatók.

A Szolgáltató által alkalmazott Információbiztonsági Szabályzat biztosítja, hogy a tanúsítványtárhoz az adatok hozzáadása, illetve a tanúsítványállapot változásával kapcsolatos intézkedések (felfüggesztés, visszavonás, aktiválás) csak az arra jogosultak számára legyen elérhetők.

Szolgáltató a jogosulatlan hozzáférések kiszűrésére monitorozó és riasztó eszközöket alkalmaz.

6.5.1 Speciális informatikai biztonsági műszaki követelmények

A Szolgáltató az Információbiztonsági Szabályzatában részletezett módon multifaktoros azonosítást követel meg minden tanúsítványkibocsátásra jogosult felhasználó esetében.

6.5.2 Informatikai biztonság értékelése

Az ide vonatkozó rendelkezéseket a Szolgáltató belső használatú Kockázatkezelési Szabályzata tartalmazza.

6.6 Életciklusra vonatkozó biztonsági előírások

6.6.1 Rendszerfejlesztési óvintézkedések

A Szolgáltató által fejlesztett rendszerek esetében sor kerül a kockázatok biztonsági felmérésére és elemzésére.

A Szolgáltató a maga által fejlesztett szoftverek esetében változáskezelési eljárást alkalmaz a kibocsátásokra, a módosításokra, és a sürgős szoftverjavításokra. A változáskezelési eljárás lehetőség szerint az üzembe helyezés előtt lezajlik. Ez alól kivételt képezhetnek a sürgős javítások, melyek esetében a dokumentálás utólagos elvégzésére is van lehetőség, amennyiben a szoftverjavítás késedelmes üzembe helyezése a Szolgáltató működését érdemben veszélyezteti, illetve jelentős anyagi vagy erkölcsi kárt okozna.

Az ide vonatkozó rendelkezéseket részletesen a Szolgáltató belső használatú Szoftverfejlesztési Szabályzata és Informatikai Változáskezelési Szabályzata tartalmazza.

6.6.2 Biztonságkezelési előírások

A Szolgáltató olyan megbízható rendszereket és termékeket használ, amelyek védettek a módosítások ellen és biztosítják az ellátott műveletek műszaki biztonságát és megbízhatóságát. A Szolgáltató különös figyelmet fordít a biztonságra a beszerzések során is: a kulcsfontosságú rendszereinek szállítói a Beszerzési Szabályzat szabályai szerint értékelt beszállítók, illetőleg a beszerzett eszközök értékelt eszközök. Az eszközök gyártói számos referenciával és megbízható háttérrel rendelkező szervezetek. Ezen szabályok biztosítják, hogy Szolgáltató eszközeihez szükség esetén megkapja a szükséges támogatást, illetve meghibásodás esetén a szállítóval

szembeni jótállási, szavatossági igények érvényesíthetők legyenek. A felhasznált, beépített eszközök nagyrészt a kereskedelmi forgalomban könnyen beszerezhetők, így azok pótlása több forrásból, viszonylag gyorsan megoldható.

A Szolgáltató védi az informatikai rendszereit és információit a vírusoktól, a rosszindulatú és nem engedélyezett szoftverektől. A Szolgáltató olyan eljárásokat alkalmaz, amely biztosítják, hogy a biztonsági javítások ésszerű időn (6 hónapon) belül alkalmazásra kerüljenek. A Szolgáltató nem alkalmazza a biztonsági javításokat abban az esetben, ha azok további biztonsági réseket tartalmaznak, illetve ha azok instabilitást okoznak.

Szolgáltató adatain kizárólag arra feljogosított személyek végezhetnek bejegyzéseket és változtatásokat. Az adatok hitelessége ellenőrizhető. Az Ügyfelekre vonatkozó adatok kizárólag annak a személynek a hozzájárulásával kereshetők nyilvánosan, akire az adatok vonatkoznak.

6.6.3 Az életciklusra vonatkozó biztonsági előírások

A Szolgáltató folyamatosan monitorozza a kapacitáskihasználtságot és előrejelzéseket készít annak érdekében, hogy elegendő tárhely és feldolgozási kapacitás álljon rendelkezésre a jövőben is.

6.7 Hálózati biztonság

A Szolgáltató a szolgáltatások nyújtásához használt rendszereit különböző ún. biztonsági zónákba sorolja. A biztonsági zónákba sorolást követően a Szolgáltató gondoskodik arról, hogy az egyes zónák között a kommunikáció biztonságos módon történjen. A Szolgáltató a szolgáltatásnyújtás során minden olyan kapcsolatot, portot tilt vagy eltávolít, amelyek nem kapcsolódnak a szolgáltatásnyújtáshoz.

A Szolgáltató a szolgáltatói rendszerek számára külön hálózatot alakított ki. A produktív rendszerek elkülönülnek a fejlesztési, tesz és egyéb felhasználású rendszerektől. A Szolgáltató hálózati kapcsolatát redundáns módon alakította ki azokban az esetekben, ahol a szolgáltatáshoz nagy rendelkezésre állású külső elérés szükséges.

A biztonság folyamatos fenntartása érdekében a Szolgáltató rendszeresen (negyedévenkénti vagy szignifikáns hálózati változás esetén mihamarabbi) sebezhetőségi ellenőrzést végez.

A Szolgáltató a sebezhetőségi ellenőrzések mellett éves periódusban, vagy szignifikáns infrastrukturális változás esetén mihamarabb betörési ellenőrzést is végez.

A hálózati biztonsággal kapcsolatban további rendelkezéseket a Szolgáltató Információbiztonsági Szabályzata tartalmazza.

6.8 Időbélyegzés

Szolgáltató a tanúsítványkiadás szolgáltatás nyújtása keretében minősített bizalmi szolgáltató által kibocsátott időbélyegzőket használ, amennyiben szükség van időbélyegzésére.

A Szolgáltató a rendszerei időforrásait legalább naponta egyszer UTC időforráshoz szinkronizálja.

7. TANÚSÍTVÁNY, CRL, OCSP PROFILOK

A szolgáltató a tanúsítványok tartalmát és funkcióját elsősorban tanúsítvány profilokon keresztül szabályozza. A tanúsítvány Alanya, Alanyai meghatározzák a bele foglalandó alany adatokat, míg a felhasználás célja az X509 kiterjesztéseken keresztül meghatározza a tanúsítvány felhasználhatóságát.

7.1 Tanúsítványprofil

Szolgáltató különböző tanúsítványprofilokat alkalmaz a tanúsítvány Alanyának és a tanúsítvány felhasználásának megfelelően. Az egyes tanúsítványprofilok a MELASZ eIDAS kompatibilis profilajánlásának megfelelő adattartalommal bírnak, ami az alábbiak szerint értelmezendő.

A végfelhasználói tanúsítványokban az alábbi adatok találhatóak meg (profilfüggetlenül):

Név	Tartalom
Verzió (Version)	3 (0x2)
Sorszám (Serial Number)	sorszám, legalább 64 bit véletlen szám tartalommal
Kiadói aláírás algoritmusa (SignatureAlgorithm)	sha256withRSA
Kiadó (Issuer)	A tanúsítványt kiadó Kiadó adatai, a kiadó tanúsítványban található Subject adatokkal egyezően
Érvényesség (Validity)	Tanúsítvány érvényességi ideje (tól-ig)
A tanúsítvány aláírása	A tanúsítványt kiadó Kiadó kulcsával végzett aláírás eredménye
Hitelesítési Rend	Az adott végfelhasználói tanúsítványra vonatkozó szabályzat azonosító(k) Elsősorban szabványos, és ahol lehet másodlagos azonosítók is (lásd 1.2.1 Hitelesítési rendek).

ECDSA

Név	Tartalom
Verzió (Version)	3 (0x2)
Sorszám (Serial Number)	sorszám, legalább 64 bit véletlen szám tartalommal
Kiadói aláírás algoritmusa (SignatureAlgorithm)	ecdsa-with-SHA384
Kiadó (Issuer)	A tanúsítványt kiadó Kiadó adatai, a kiadó tanúsítványban található Subject adatokkal egyezően
Érvényesség (Validity)	Tanúsítvány érvényességi ideje (tól-ig)
A tanúsítvány aláírása	A tanúsítványt kiadó Kiadó kulcsával végzett aláírás eredménye
Hitelesítési Rend	Az adott végfelhasználói tanúsítványra vonatkozó szabályzat azonosító(k) Elsősorban szabványos, és ahol lehet másodlagos azonosítók is (lásd 1.2.1 Hitelesítési rendek)

RSA 4096

Név	Tartalom
Verzió (Version)	3 (0x2)
Sorszám (Serial Number)	sorszám, legalább 64 bit véletlen szám tartalommal
Kiadói aláírás algoritmusa (SignatureAlgorithm)	sha256WithRSAEncryption
Kiadó (Issuer)	A tanúsítványt kiadó Kiadó adatai, a kiadó tanúsítványban található Subject adatokkal egyezően
Érvényesség (Validity)	Tanúsítvány érvényességi ideje (tól-ig)
A tanúsítvány aláírása	A tanúsítványt kiadó Kiadó kulcsával végzett aláírás eredménye
Hitelesítési Rend	Az adott végfelhasználói tanúsítványra vonatkozó szabályzat azonosító(k) Elsősorban szabványos, és ahol lehet másodlagos azonosítók is (lásd 1.2.1 Hitelesítési rendek)

Személyes tanúsítványprofil Alany mezői:

A személyes tanúsítványok természetes személy Végfelhasználók részére kerülnek kibocsátásra, így a tanúsítványok alanyaként kizárólag egy természetes személy kerül megnevezésre, akit a valódi neve azonosít a tanúsítványban. Az alábbi profil az aláíró tanúsítványokra értelmezendő.

Mezőnév	Definíció
Subject mezők	
commonName (CN)	A Végfelhasználó közhiteles adatbázis szerinti teljes neve, ill. amennyiben ilyen nem elérhető, akkor az azonosításra szolgáló igazolvány szerinti név.
surname (SN)	A commonName mezőben szereplő név vezetéknév része, a MELASZ profilajánlás névfelbontási javaslata szerint.
givenName (G)	A commonName mezőben szereplő név keresztnév része, a MELASZ profilajánlás névfelbontási javaslata szerint.
emailAddress (E)	Végfelhasználó saját email címe.
serialNumber (CNSN) (1.)	Szolgáltató által képzett permanens azonosító (Szolgáltató + Ügyfél egyedi azonosítója).
serialNumber (2.) *Opcionális*	Egyedi személyazonosító az ügyfél vagy ügyfelek egy csoportja által kért tartalommal.
countryName (C)	Végfelhasználó lakóhelyének országa, ISO 3166-1 szerinti kétbetűs országkód.
localityName (L) *Opcionális*	Végfelhasználó lakhelyének helységneve.
Subject Alternative Name mezők	

email	Megegyezik az E mezővel.
othername	Szolgáltató OID alapú szolgáltatóazonosítója 1.3.6.1.5.5.7.8.3=1.3.6.1.4.1.3555.5

Megkötések / tiltott mezők:

- A mezőkből csak egy szerepelhet, kivéve a serialNumber mezőt.

Nem szereplő mezők:

- Pseudonym
- A személyes tanúsítványok Alanyaként nem szerepel szervezet, így az erre utaló mezők is hiányoznak (CN/organizationName, CN/organizationalUnitName, CN/ organizationIdentifier és CN/title).

Álneves tanúsítványprofil Alany mezői:

Az álneves tanúsítványok természetes személy Végfelhasználók részére kerülnek kibocsátásra. A természetes személyt egy általa választott név jelöli a tanúsítványban. A személy valódi neve (amit a Szolgáltató ismer) és hozzá kapcsolódó szervezet nem szerepel a tanúsítványban. Az alábbi profil kizárólag az aláíró tanúsítványokra értelmezendő.

Mezőnév	**Definíció**
Subject mezők	
commonName (CN)	Az Igénylő által választott álnév (szolgáltatón belül egyedi).
pseudonym (P)	Az Igénylő által választott álnév. Megegyezik a commonName tartalmával.
serialNumber (CNSN)	Szolgáltató által képzett permanens azonosító (Szolgáltató + Ügyfél álneves azonosítója – lásd 1.6.1). 1.3.6.1.4.1.3555. *ÜgyfélPseudID* Értéke az ÁLNÉV-re vonatkozóan egyedi, és nem egyezhet meg nem álneves tanúsítvány azonosítójával.
countryName (C)	Igénylő lakhelyének országa, ISO 3166-1 szerinti kétbetűs országkód.
Subject Alternative Name mezők	
othername	NetLock OID alapú szolgáltatóazonosítója 1.3.6.1.5.5.7.8.3=1.3.6.1.4.1.3555

Megkötések / tiltott mezők:

- A mezőkből csak egy szerepelhet.

Nem szereplő mezők:

- title, organizationName, organizationalUnitName, organizationIdentifier, localityName, surname, givenName, emailAddress, SAN/Email

Üzleti tanúsítványprofil Alany mezői:

Az üzleti tanúsítványok természetes személy Végfelhasználók részére kerülnek kibocsátásra, aki mellett a tanúsítványok alanyaként egy szervezet is megnevezésre kerül (aki a tanúsítvány Előfizetője). A természetes személy a szervezet hozzájárulásával igényli a tanúsítványt, amit így annak képviseletében (ami itt nem feltétlen jogi képviseletet jelent) használhat. A szervezet és a személy közti kapcsolat típusa bármilyen lehet (pl. munkatársi, tagi, szerződéses)[13], ez a tanúsítvány kiadása során nem kerül vizsgálatra, a szervezethez tartozás tényét azonban – és amennyiben Titulus megadásra kerül, ennek tartalmát – a szervezetnek igazolnia kell. Az alábbi profil az aláíró tanúsítványokra értelmezendő.

Mező neve	Definíció
Subject mezők	
commonName (CN)	Személyes profillal megegyezik.
surname (SN)	Személyes profillal megegyezik.
givenName (G)	Személyes profillal megegyezik.
serialNumber (1.) (CNSN)	Személyes profillal megegyezik.
serialNumber (2.) Opcionális	Személyes profillal megegyezik.
emailAddress (E)	Személyes profillal megegyezik.
organizationName (O)	Szervezeti profillal megegyezik.
organizationalUnitName (OU) Opcionális	Szervezeti profillal megegyezik.
organizationIdentifier Opcionális	Szervezeti profillal megegyezik.
title (T) Opcionális	A tanúsítványalany szervezetben viselt szerepe, munkaköre. Minden esetben csak igazolt adat kerülhet ebbe a mezőbe. Egyes titulusok csak kitüntetett esetekben adhatók ki: (pl. „ügyvéd”: csak ügyvédi tanúsítványra jogosultaknál, “cégvezető”, “ügyvezető” - a gazdasági társaság bejegyzési okirataiban ellenőrzött személy tanúsítványában).
countryName (C)	Szervezeti profillal megegyezik.
localityName (L)	Szervezeti profillal megegyezik.
Subject Alternative Name mezők	
email	Személyes profillal megegyezik.
othername	Személyes profillal megegyezik.
dirname Opcionális	Speciális esetekben a Végfelhasználó neve a CommonName-ben szereplőtől eltérő írásmóddal.

[13] A DÁP megfogalmazásában „természetes személy tanúsítvány alany: a tanúsítványban szereplő természetes személy, függetlenül attól, hogy a tanúsítványban egyúttal valamely nem természetes személy képviseletére való jogosultságát vagy azzal való kapcsolatát is igazolják;”

Megkötések / tiltott mezők:

- A mezőkből csak egy szerepelhet, kivéve a serialNumber és az organizationName mezőket.

Nem szereplő mezők:

- Pseudonym

Szervezeti tanúsítványprofil Alany mezői:

A szervezeti tanúsítványok jogi személy Előfizetők részére kerülnek kibocsátásra, így a tanúsítványok alanyaként kizárólag ez a jogi személy kerül megnevezésre. Az alábbi profil a bélyegző tanúsítványokra értelmezhető.

Mezőnév	Definíció
Subject mezők	
commonName (CN)	Az Előfizető teljes vagy rövid neve VAGY Igazolt DBA név / Trademark / Terméknév és kapcsolódó azonosítója, ami egyedi, és amelynek a jogi személy kizárólagosan birtokolja a használatát.
organizationName (O)	Az Előfizető teljes vagy rövid neve
organizationalUnitName (OU) Opcionális	Az Előfizető szervezeti egységének neve az organizationName mező által azonosított szervezeten belül.
countryName (C)	Előfizető székhelyének országa (ISO 3166-1 szerinti kétbetűs országkód).
localityName (L)	Az Előfizető székhelye szerinti helység neve.
serialNumber (CNSN) (1.)	Szolgáltató által képzett permanens azonosító (Szolgáltató + Ügyfél egyedi azonosítója). 1.3.6.1.4.1.3555.5.1.*ÜgyfélID*
organizationIdentifier	Előfizető nyilvántartott azonosítója (lásd a 3.1 Elnevezések fejezetet).
emailAddress (E)	Előfizető email címe.
Subject Alternative Name mezők	
email	Megegyezik az E mezővel.
othername	NetLock OID alapú szolgáltató azonosítója 1.3.6.1.5.5.7.8.3=1.3.6.1.4.1.3555.5
dirname Opcionális	A szervezet által használt, nyilatkozatban igazolt • DBA név • vagy Trademark • vagy Terméknév és kapcsolódó azonosítója.

Megkötések / tiltott mezők:

- A mezőkből csak egy szerepelhet, kivéve a serialNumber és az organizationName mezőket.
- Szervezeti tanúsítvány nem lehet álneves.

Nem szereplő mezők:

- Title, Pseudonym, surname, givenName

A tanúsítványba foglalt adattartalom értelmezése:

- A tanúsítvány a tanúsítványban található O nevű szervezethez tartozik (azon belül, ha megjelölt, az OU szervezeti egységhez).

OV weboldal hitelesítő tanúsítványprofil Alany mezői:

Az OV SSL tanúsítvány olyan weboldal hitelesítő tanúsítvány, amelynek Alanyaként egy vagy több domain név és az Előfizető szervezet kerül megnevezésre.

Mezőnév	Definíció
Subject mezők	
commonName (CN) Opcionális	Ha a mező jelen van, akkor egy domain nevet tartalmazhat a SAN/dNSName-ben szereplők közül.
organizationName (O)	Az Előfizető hiteles cégkivonatban (más szervezet esetén ennek megfelelő okiratban) szereplő teljes vagy rövid neve VAGY Igazolt DBA név / Trademark.
countryName (C)	Előfizető székhelye szerinti ország ISO 3166-1 szerinti kétbetűs országkódja.
localityName (L)	Előfizető székhelye szerinti helység neve.
stateOrProvinceName Opcionális	Előfizető székhelye szerinti állam neve (amennyiben értelmezhető).
organizationIdentifier Opcionális	Szervezeti profillal megegyezik.
Subject Alternative Name mezők	
DNSname	A tanúsítvány által hitelesített weboldalak domain neve. Csak létező és az igénylő által jogosan használt domain nevek tüntethetők fel. Tartalmazhat wildcard tagot.

Megkötések / tiltott mezők: UserNotice

Nem szereplő mezők:

- title, pseudonym, surname, givenName, organizationalUnitName.

Nem-minősített EV weboldal-hitelesítő tanúsítványprofilok Alany mezői:

Az EV SSL tanúsítvány olyan weboldal hitelesítő tanúsítvány, amelynek Alanyaként egy vagy több domain név és az Előfizető szervezet kerül megnevezésre.

Mezőnév	Definíció
Subject mezők	
commonName (CN) Opcionális	Ha a mező jelen van, akkor egy domain nevet tartalmazhat a SAN/dNSName-ben szereplők közül.
organizationName (O)	Az Előfizető teljes vagy rövid neve VAGY Igazolt DBA név, mögötte zárójelek között szerepeltetve a szervezet nevét.
countryName (C)	Előfizető székhelye szerinti ország ISO 3166-1 szerinti kétbetűs országkódja.
localityName (L)	Előfizető székhelye szerinti helység neve.
streetAddress Opcionális	Az Előfizető székhelye szerinti közterület neve, jellege és házszám.
postalCode Opcionális	Az Előfizető székhelye szerinti irányítószám.
stateOrProvinceName Opcionális	Előfizető székhelye szerinti állam neve (amennyiben értelmezhető).
organizationIdentifier	Szervezeti profillal megegyezik.
cabfOrganizationIdentifier	Adattartalma megegyezik az organizationIdentifier mezővel.
serialNumber (CNSN) (1.)	Szolgáltató által képzett permanens azonosító (Szolgáltató + Ügyfél egyedi azonosítója). 1.3.6.1.4.1.3555.5.1.*ÜgyfélID*
serialNumber (CNSN) (2.)	Megegyezik az organizationIdentifier mező értékével.
jurisdictionCountryName	Azon ország megnevezése, amely jogrendje szerint Előfizető működik. A jurisdictionLocalityName és jurisdictionStateOrProvinceName kitöltése egyúttal kötelező, amennyiben értelmezhetők ezek a mezők.
businessCategory	EV SSL üzleti kategória (Private Organization, Government Entity, Business Entity, Non-Commercial Entity).
Subject Alternative Name mezők	
DNSname	A tanúsítvány által hitelesített weboldalak domain neve. Csak létező és az igénylő által jogosan használt domain nevek tüntethetők fel. Nem tartalmazhat wildcard tagot.

Megkötések / tiltott mezők: UserNotice

Nem szereplő mezők:

- title, pseudonym, surname, givenName, organizationalUnitName.

Szolgáltatói Gyökér Kiadó tanúsítványprofilja:

Mező neve	Tartalom	
Certificate Serial Number	Tanúsítvány egyedi azonosítja (nem szekvenciális, legalább 64 bit entrópiával)	
public key	lásd minimum algoritmusok táblázat	
Érvényesség (Validity)	Tanúsítvány érvényességi ideje (tól-ig)	
subject:commonName (CN)	Gyökér Kiadó neve	
subject:countryName (C)	HU	
subject:localityName (L)	Budapest	
subject:organizationalUnitName	Tanúsítványkiadók (Certification Services)	
subject:organizationName (O)	NetLock Kft.	
Signature	Gyökér Kiadó saját aláírása	
Kiterjesztések		**Kritikus**
basicConstraints	CA:TRUE	Igen
keyusage	keyCertSign, cRLSign	Igen
Subject Key identifier	subject kulcs hash	Nem

Megkötések / tiltott mezők:

- a gyökérhitelesítő tanúsítvány self signed tanúsítvány subject és issuer része egyezik

Nem szereplő mezők:

- certificatePolicy, extendedKeyusage

ECDSA és RSA 4096

Mező neve	Tartalom
Certificate Serial Number	Tanúsítvány egyedi azonosítja (nem szekvenciális, legalább 64 bit entrópiával)
public key	lásd minimum algoritmusok táblázat
Érvényesség (Validity)	Tanúsítvány érvényességi ideje (tól-ig)
subject:commonName (CN)	Gyökér Kiadó neve
subject:countryName (C)	HU
subject:localityName (L)	Budapest
organizationIdentifier (OrdID)	VATHU-12201521
subject:organizationName (O)	NETLOCK Kft.

Signature	Gyökér Kiadó saját aláírása	
Kiterjesztések		**Kritikus**
basicConstraints	CA:TRUE	Igen
keyusage	keyCertSign, cRLSign	Igen
Subject Key identifier	subject kulcs hash	Nem
Authority Key Identifier	keyID	Nem

Megkötések / tiltott mezők:

- a gyökérhitelesítő tanúsítvány self signed tanúsítvány subject és issuer része egyezik

Nem szereplő mezők:

- certificatePolicy, extendedKeyusage

Szolgáltatói Köztes Kiadó tanúsítványprofilja

Mező neve	**Tartalom**	
Certificate Serial Number	Tanúsítvány egyedi azonosítja (nem szekvenciális, legalább 64 bit entrópiával)	
public key	lásd minimum algoritmusok táblázat	
Érvényesség (Validity)	Tanúsítvány érvényességi ideje (tól-ig)	
subject:commonName (CN)	Köztes Kiadó neve	
subject:countryName (C)	HU	
subject:localityName (L)	Budapest	
subject:organizationalUnitName	Tanúsítványkiadók (Certification Services) vagy nem szerepel	
subject:organizationName (O)	NetLock Kft. vagy NetLock Ltd.	
Signature	Gyökér Kiadó aláírása	
Kiterjesztések		**Kritikus**
basicConstraints	CA:TRUE	Igen
keyusage	keyCertSign, cRLSign	Igen
ExtendedKeyUsage	A kiadóra releváns EKU, mely nem lehet anyExtendedKeyUsage és nem veheti fel egyszerre az id-kp-serverAuth és id-kp-emailProtection értéket ugyanabban a tanúsítványban.	Nem
Subject Key identifier	subject kulcs hash	Nem
AIA:Ca issuers	A tanúsítványt kiadó gyökér Kiadó tanúsítványának elérhetősége http URL-en	Nem
AIA:OCSP	A tanúsítványt kiadó gyökér Kiadó OCSP szolgáltatásának elérhetősége http URL-en	Nem

CDP	A tanúsítványt kiadó gyökér Kiadó CRL szolgáltatásának elérhetősége http URL-en	Nem
Authority Key Identifier	Gyökér Kiadó kiadói kulcs lenyomata	Nem

Megkötések / tiltott mezők: -
Nem szereplő mezők:

- certificatePolicy, extendedKeyusage

ECDSA és RSA 4096

Mező neve	**Tartalom**	
Certificate Serial Number	Tanúsítvány egyedi azonosítja (nem szekvenciális, legalább 64 bit entrópiával)	
public key	lásd minimum algoritmusok táblázat	
Érvényesség (Validity)	Tanúsítvány érvényességi ideje (tól-ig)	
subject:commonName (CN)	Köztes Kiadó neve	
subject:countryName (C)	HU	
subject:localityName (L)	Budapest	
organizationIdentifier (OrgID)	VATHU-12201521	
subject:organizationName (O)	NETLOCK Kft.	
Signature	Gyökér Kiadó aláírása	
Kiterjesztések		**Kritikus**
basicConstraints	CA:TRUE	Igen
keyusage	keyCertSign, cRLSign	Igen
ExtendedKeyUsage	A kiadóra releváns EKU, mely nem lehet anyExtendedKeyUsage és nem veheti fel egyszerre az id-kp-serverAuth és id-kp-emailProtection értéket ugyanabban a tanúsítványban.	Nem
Subject Key identifier	subject kulcs hash	Nem
AIA:Ca issuers	A tanúsítványt kiadó gyökér Kiadó tanúsítványának elérhetősége http URL-en	Nem
AIA:OCSP	A tanúsítványt kiadó gyökér Kiadó OCSP szolgáltatásának elérhetősége http URL-en	Nem
CDP	A tanúsítványt kiadó gyökér Kiadó CRL szolgáltatásának elérhetősége http URL-en	Nem
Authority Key Identifier	Gyökér Kiadó kiadói kulcs lenyomata	Nem

Megkötések / tiltott mezők: -

Nem szereplő mezők:

- certificatePolicy, extendedKeyusage

Az egyes tanúsítványprofilok kapcsolata a hitelesítési rendekkel és tanúsítványtípusokkal:

A táblázat meghatározza, hogy az egyes tanúsítványtípusok milyen profillal és hitelesítési rendekkel érhetők el.

Profil	**Hitelesítési rendek**	**Tanúsítványtípusok**
Személyes	NCP, NCP+	Aláíró
Álneves	NCP, NCP+	Aláíró
Üzleti	NCP, NCP+	Aláíró
Szervezeti	NCP, NCP+	Bélyegző
Weboldal-hitelesítő	OVCP, EVCP	Weboldal-hitelesítő
Szolgáltatói	-	Szolgáltatói

Az itt felsorolt tanúsítványprofilokon belül, azoknak megfelelően Szolgáltató további speciális profilokat hozhat létre (pl. egyes szakmáknak megfelelő üzleti profilok).

7.1.1 Verzió szám(ok)

A Szolgáltató az X.509v3 specifikáció szerint bocsátja ki a tanúsítványokat.

7.1.2 Tanúsítványkiterjesztések

A Szolgáltató az X.509v3 specifikáció szerinti tanúsítványkiterjesztéseket használja a kritikus mezők jelzésével. Minden végfelhasználói tanúsítvány tartalmazza a következő tanúsítvány kiterjesztéseket:

Kiterjesztés	Kritikus	Tartalom
basicConstraints	igen	CA:FALSE
subjectKeyIdentifier	nem	Alany saját kulcsazonosítója
Subject Alternative Name	nem	Alany egyéb elnevezése. Kitöltését lásd az egyes tanúsítványprofilok Alany

		mezőinél.
authorityKeyIdentifier	nem	A tanúsítvány kiadó Kiadó kulcsazonosítója
crlDistributionPoints	nem	A visszavonási lista elérhetőségei
Authority Information Access:CAIssuers	nem	A kiadói tanúsítvány elérhetőségei
authorityInfoAccess:OCSP	nem	Az OCSP elérhetőségei
Hitelesítési Rendek Certificate Policies	nem	Azon Hitelesítési Rendek azonosítója, ami szerint a tanúsítvány kibocsátásra került (lásd Hitelesítési Rendek fejezet). Több HR azonosítása esetén a mező többször szerepel. Policy constrainst nem kerül alkalmazásra. A policyqualfierek közül csak a User Notice mező kerül kitöltésre, melynek tartalma ember által olvasható formában a tanúsítványra érvényes policy rövid szöveges leírása, megjelölése vagy kiegészítése korlátozó információkkal (kivéve weboldal-hitelesítő és OCSP tanúsítványok esetén). Expressz tanúsítványtípusok (LCP) esetén a Szolgáltató itt is jelzi az Érintett felek számára, hogy a kibocsátást megelőző azonosítási és hitelesítési eljáérásnak nem volt része Igénylő személyes megjelenésen alapuló vagy azzal egyenértékű azonosítása.
Keyusage	igen	A tanúsítványban szereplő nyilvános kulcs magánkulcs párjának engedélyezett felhasználási lehetőségei (kitöltést lásd alább).
extendedKey Usage	nem	Keyusage-ot kiterjesztő magánkulcs felhasználási lehetőségek (kitöltést lásd alább).
SCT	nem	X509 v3 extension a Google Certificate Transparency Policy[14]-jának megfelelően.

Végfelhasználói kulcshasználat kiterjesztések kitöltése tanúsítványtípusok szerint:

Tanúsítványtípus/ Kulcshasználat	Nem-minősített Aláíró és bélyegző tanúsítványok	Nem-minősített Aláíró és bélyegző tanúsítványok	Weboldal-hitelesítő tanúsítvány
Keyusage	nonRepudiation, digitalSignature	nonRepudiation, digitalSignature	keyAgreement, digitalSignature

[14] Lásd https://github.com/chromium/ct-policy

extendedKey Usage	documentSigning, emailProtection	clientAuth és opcionálisan emailProtection	serverAuth, clientAuth

Végfelhasználó csak az itt feltüntetett Felhasználási célokra használhatja a magánkulcsot (zárójelben a tanúsítvány ennek megfelelő alkalmazási lehetősége):

- nonRepudiation: Letagadhatatlanság biztosítása (Aláíró ellenőrzése)
- digitalSignature: Elektronikus aláírás (Sértetlenség és hitelesség ellenőrzése)
- KeyExchange: Kulcscsere
- keyAgreement: Kulcsmegegyezés
- KeyEncipherment: Kulcs titkosítása (Kulcs visszafejtése)
- clientAuth: Kliens azonosítás (Kliens hitelesítése)
- serverAuth: Szerver azonosítás (Szerver hitelesítése)
- documentSigning: Dokuemntum aláírása (Microsoft extension)
- emailProtection: Egyaránt használható titkosító és aláíró tanúsítvány esetében

7.1.3 Az algoritmus objektum azonosítója

A Szolgáltató a tanúsítványban jelzi azt az algoritmust és paramétereit, amellyel a tanúsítvány hitelesítésre került. A lehetséges értékeket lásd a 6.1.5 fejezetben.

7.1.4 Névformák

Az Alany névformái tekintetében a 3.1 pont rendelkezései az irányadóak.

A tanúsítvány Kiadó (Issuer) mezőjében szereplő érték megegyezik a kibocsátó Kiadó tanúsítványának "Subject" mezőjében szereplő értékkel.

7.1.5 Névhasználati megkötések

A Szolgáltató az alkalmazott névhasználati megkötéseket a "nameConstraints" mezőben tünteti fel.

7.1.6 Hitelesítési Rend azonosítója

A Szolgáltató a Hitelesítési Rend alapján kibocsátott tanúsítványokban jelzi a Hitelesítési Rend OID azonosítóját.

7.1.7 A szabályzati korlátozás kiterjesztés használata

A Szolgáltató nem alkalmaz erre vonatkozóan előírásokat.

7.1.8 Szabályzatminősítő szintaxis és szemantika

A Szolgáltató a Hitelesítési rendek (Certificate Policies) kiterjesztés Szabályzatminősítő (Policy Qualifier) mezejében rövid információt helyezhet el a tanúsítvány felhasználhatóságával kapcsolatban. A mező tartalmazza a Szolgáltatási szabályzat on-line elérhetőségét is (URL).

7.1.9 A kritikus Hitelesítési Rend kiterjesztés feldolgozása

A Szolgáltató nem alkalmaz specifikus szabályozást.

7.2 Tanúsítványvisszavonási profil

7.2.1 Verziószám(ok)

A Szolgáltató az X509 és az RFC5280 szabványnak megfelelő visszavonási listákat bocsát ki, a szabályzatban meghatározott sűrűséggel és tartalommal.

7.2.2 Tanúsítvány visszavonási lista kiterjesztések

A CRL tartalmában nincs kritikus jelzéssel ellátott mező. A Szolgáltató a visszavonási listákat egyesével növekvő sorozatszámmal látja el.

A tanúsítvány visszavonási lista (CRL) profilja:

Mező	Tartalom
Version	V2
Issuer	A CRL-t kiadó tanúsítványkiadó Issuer adata
Last update	Utolsó kibocsátás dátuma
Next update	Következő kibocsátás dátuma
Signature	Kibocsátó elektronikus aláírása
CRL entry	Az érvénytelenített tanúsítvány sorozatszáma, érvénytelenítés dátuma, időpontja, oka RFC 5280-nak megfelelő formában.
CRL entry extension	

7.3 Tanúsítványállapot-szolgáltatás profilok

7.3.1 Verziószám(ok)

Az OCSP szolgáltatás során a Szolgáltató az RFC 6960 szabvány V1 verziója alapján létrehozott tanúsítványállapot kérdéseket és válaszokat támogatja.

7.3.2 OCSP kiterjesztések

Az OCSP válaszadó tanúsítvány tartalmazza a NoCheck kiterjesztést, így az OCSP válaszadók ügyfél általi ellenőrzése nem szükséges.

Az OCSP válaszadó tanúsítványprofilja:

Mezőnév	Definíció
Subject mezők	
Certificate Serial Number	Tanúsítvány egyedi azonosítja (nem szekvenciális, legalább 64 bit entrópiával).
private and public key	Lásd minimum algoritmusok táblázat.

Érvényesség (Validity)	Tanúsítvány érvényességi ideje (tól-ig).
commonName (CN)	Kiadó egyedi elnevezése, ami tartalmazza a “minősített” és az “időbélyegző” vagy “időpecsét” szavakat, illetve ezek angol megfelelőjét.
organizationName (O)	NETLOCK Kft. vagy NETLOCK Ltd.
countryName (C)	A szolgáltató székhelyének országa (ISO 3166-1 szerinti kétbetűs országkód).
localityName (L)	Az szolgáltató hiteles cégkivonatban (más szervezet esetén ennek megfelelő okiratban) szereplő székhelye szerinti helység neve.
emailAddress (E) opcionális	Ha kitöltött, akkor a tartalma: info@netlock.hu

Kiterjesztések	**Tartalom**	**Kritikus**
basicConstraints	CA:FALSE	Igen
extendedKeyusage	OCSPSigning	Nem
keyusage	digitalSignature	Igen
Subject Key identifier	subject kulcs hash	Nem
Authority Key identifier	kiadói kulcs hash	Nem
OCSPNocheck	üres tartalom	Nem

Megkötések / Tiltott mezők: UserNotice
Nem szereplő mezők: certificatePolicy

ECDSA, RSA 4096

Az OCSP válaszadó tanúsítványprofilja:

Mezőnév	**Definíció**
Subject mezők	
Certificate Serial Number	Tanúsítvány egyedi azonosítja (nem szekvenciális, legalább 64 bit entrópiával).
private and public key	Lásd minimum algoritmusok táblázat.
Érvényesség (Validity)	Tanúsítvány érvényességi ideje (tól-ig).

commonName (CN)	Kiadó egyedi elnevezése, ami tartalmazza a “minősített” és az “időbélyegző” vagy “időpecsét” szavakat, illetve ezek angol megfelelőjét.
organizationName (O)	NETLOCK Kft. vagy NETLOCK Ltd.
organizationIdentifier	A Szolgáltató szervezet azonosítója.
countryName (C)	A szolgáltató székhelyének országa (ISO 3166-1 szerinti kétbetűs országkód).
localityName (L)	Az szolgáltató hiteles cégkivonatban (más szervezet esetén ennek megfelelő okiratban) szereplő székhelye szerinti helység neve.

Kiterjesztések	**Tartalom**	**Kritikus**
basicConstraints	CA:FALSE	Igen
extendedKeyusage	OCSPSigning	Nem
keyusage	digitalSignature	Igen
Subject Key identifier	subject kulcs hash	Nem
Authority Key identifier	kiadói kulcs hash	Nem
OCSPNocheck	üres tartalom	Nem

Megkötések / tiltott mezők: UserNotice
Nem szereplő mezők: certificatePolicy, emailAddress, organizationalUnitName

8. A MEGFELELŐSÉG VIZSGÁLATA

A Szolgáltató – összhangban az európai uniós és hazai szabályozással, valamint a Bizalmi Szolgáltatási Rendben meghatározott követelményekkel az alábbi szabványok szerint végzi szolgáltatási tevékenységét (a jogszabályi megfelelőséget lásd a 9.15 fejezetben).

Szabvány azonosító	Angol rövid elnevezés
ETSI EN 319 401	ESI; General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1	ESI; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
ETSI EN 319 412-1	ESI; Certificate Profiles; Part 1: Overview and common data structures
ETSI EN 319 412-2	ESI; Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI EN 319 412-3	ESI; Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
ETSI EN 319 412-4	ESI; Certificate Profiles; Part 4: Certificate profile for web site certificates

A Szolgáltató megfelelőségi vizsgálatokat és ellenőrzéseket végez, illetve végeztet annak érdekében, hogy a Szolgáltatásaival kapcsolatos folyamatai, személyzete, eszközei és környezete mindenkor megfeleljenek a vonatkozó jogszabályi és szakmai követelményeknek.

Szolgáltató tevékenységét annak megkezdése előtt a vonatkozó szabványok és jogszabályok előírásai alapján külső, független megfelelőségértékelő szervezettel értékeltette az alábbiak betartásával:

- az értékelés a jelen fejezetben közölt jogszabályok és szabványok alapján történik
- az értékelés figyelembe veszi a Szolgáltató összes értékelendő bizalmi szolgáltatásának sajátosságát;
- az értékelés a vizsgálat tárgyához tartozó minden szolgáltatói tevékenységet lefed.

8.1 Az ellenőrzések körülményei és gyakorisága

A Szolgáltató tevékenységének felügyeletét az európai uniós szabályozással összhangban a Bizalmi Felügyelet látja el. A Bizalmi Felügyelet legalább éves rendszerességgel helyszíni szemlét tart a Szolgáltató székhelyén, telephelyén.

Az ellenőrzések eredményei, valamint az azok alkalmával készült dokumentumok bizalmas jellegűek, hozzáférést csak a megfelelő jogosultsággal rendelkező személyek kapnak.

A Szolgáltató évente egy alkalommal saját belső önellenőrzéseket végez, amely segítségével rendszeresen felülvizsgálja a Szolgáltatási Rendnek és jelen szabályzatnak, valamint a korábbi auditoknak és értékeléseknek való megfelelőségét; eltérés esetén pedig megteszi a szükséges lépéseket.

Amennyiben a Kihelyezett Regisztrációs Egység(ek)et működtető Szolgáltatói Partner nem rendelkezik a vonatkozó előírásoknak való megfelelősséget igazoló éves külső audit jelentéssel, Szolgáltató a Kihelyezett Regisztrációs Egység(ek) működésének szabályosságát legalább évente, az éves ellenőrzések közti időszakokban pedig véletlenszerű mintavétel alapján eseti jelleggel is ellenőrzi.

Szolgáltató az éves önellenőrzések közti időszakban az előző önellenőrzés óta általa kibocsátott

weboldal-hitelesítő tanúsítványok (OVCP és EVCP) - véletlenszerű mintavétellel kiválasztott - legalább 3%-át negyedévente ellenőrizi.

A Szolgáltató legalább kétévente külső megfelelőségértékelő vizsgálatot hajtat végre független, akkreditált megfelelőségértékelő szervezettel.

A Szolgáltató a jelen Szabályzat 1.1.2 pontjában részletezett ISO 9001, valamint ISO 27001 szabvány megfelelőségét külső auditáló szervezet értékeli és vizsgálja felül folyamatosan, legalább évente egy alkalommal.

A NETLOCK Kft. a külső partnerek, szolgáltatók szabályozását, szerződéses kötelezettségeik ellenőrzését az ISO 27001 szabványban foglaltaknak megfelelően végzi.

8.2 Az értékelő és szükséges képesítése

A belső ellenőrzéseket megfelelő jogi és szakmai ismeretek birtokában lévő, olyan tapasztalt szakemberek végzik, akik rendelkeznek felsőfokú képesítéssel és legalább 5 éves szakmai gyakorlattal szabályozás, informatikai rendszeraudit vagy bizalmi szolgáltatás területén.

A külső megfelelőségértékeléseket olyan természetes vagy jogi személy végzi, aki rendelkezik egy EU tagállam nemzeti akkreditációs szervezetétől megfelelő felhatalmazással.]
A külső értékelések során a Szolgáltató olyan természetes vagy jogi személlyel, vagy természetes személyek csoportjával működik együtt, akik/amelyek

- képesek a 8. fejezetben megadott szabványokra vonatkozó audit elvégzésére;
- megfelelnek a 8.3 pontban foglalt követelménynek;
- megfelelő jártassággal bírnak a PKI, az IT illetve IT biztonsági megoldások, technológiák és auditok terén, valamint Kihelyezett Regisztrációs Egységnél végzett audit során annak funkcióival kapcsolatban;
- ETSI szabványok alapján végzett auditok/értékelések esetén rendelkezik vagy rendelkeznek
  - az ETSI EN 319 403 szerinti akkreditációval, *vagy*
  - egy ezzel egyenértékű nemzeti szabvány szerinti akkreditációval, *vagy*
  - a Nemzeti Akkreditációs Hatóság által ISO 17021 szabvány szerinti ISO 27006 módszertannal végrehajtott ISO 27001 vizsgálatra akkreditációval rendelkezik;
- WebTrust audit végzése esetén rendelkezik vagy rendelkeznek WebTrust audit elvégzéséhez szükséges engedéllyel;
- tevékenységét vagy tevékenységüket jogszabályok vagy szakmai etikai kódex szabályozza;
- rendelkezik az értékelő tevékenység végzéséből eredő mulasztások, hibák esetére szóló, legalább egymillió USD fedezetű biztosítással.

8.3 Az auditor és az auditált entitás kapcsolata

A Szolgáltató belső megfelelőségértékeléseit végző Független rendszervizsgáló szerepkörrel felruházott bizalmi munkatársak függetlenek a Szolgáltató szolgáltatásokért felelős szervezeti egységeitől.

A külső megfelelőségértékeléseket végző értékelők függetlenek az alábbiak tekintetében:

- a vizsgált szolgáltató tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- a vizsgált szervezettől, vagyis sem saját maga, sem közvetlen hozzátartozója nincs munkaviszonyban a Szolgáltatóval;
- díjazása nem függ az értékelés során végzett tevékenységének végkimenetelétől.

8.4 Az értékelés/audit által lefedett területek

Az auditok/értékelések során az alábbi területek kerülnek ellenőrzésre:

- a hatályos, vonatkozó jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;
- Bizalmi Szolgáltatási Rend(ek)nek és Szolgáltatási szabályzat(ok)nak való megfelelés;
- az alkalmazott folyamatok megfelelősége;
- a fizikai biztonság megfelelősége;
- a személyi állomány megfelelősége;
- az IT biztonság megfelelősége;
- az adatvédelmi szabályok betartása;
- a Bizalmi szolgáltatások konfigurációjának Információbiztonsági Szabályok szerinti ellenőrzése.

8.5 A hiányosságok kezelése

A külső és belső megfelelőségértékelések eredményét a Szolgáltató egy értékelési jelentésben foglalja össze, amely jelentés kitér a vizsgálat rendszerelemekre, folyamatokra. A dokumentum tartalmazza az ellenőrzés során felhasznált bizonyítékokat és értékelői megállapításokat. A jelentés tartalmazza továbbá az ellenőrzés során feltárt hiányosságokat, eltéréseket és a kijavításukra kitűzött határidőket. A feltárt hiányosságok súlyosságuknak megfelelően az alábbi kategóriába tartoznak:

- “Enyhe” eltérés, mely kapcsán a helyesbítő intézkedéseket igazoló dokumentumokat a következő értékelés alkalmával kell bemutatni.
- “Súlyos” eltérés, mely kapcsán a megvalósított helyesbítő intézkedést igazoló dokumentumokat az aktuális értékelés alkalmával kell bemutatni.

A Szolgáltató köteles a független értékelő által felvett eltérésekre írásában válaszolni, kijavításukra tett intézkedéséről a következő értékelés alkalmával beszámolni.

8.6 Az eredmények közzététele

A Szolgáltató nem hozza nyilvánosságra az ellenőrzésről, értékelésekről készült részletes vizsgálati jelentést. De az értékelést követő három hónapon belül nyilvánosságra hozza a kiállított tanúsítványt.

9. EGYÉB ÜZLETI ÉS JOGI TUDNIVALÓK

9.1 Díjak

Előfizető köteles az időszaki szolgáltatások és az ezek mellett vagy igénylésük során igénybevett egyéb szolgáltatások (pl. opcionális szolgáltatások) ellenértékét, illetve egyéb a Szolgáltató által megállapított díjakat (pl. adminisztrációs díj) előre, a Szolgáltató weboldalán közzétett mindenkori Árlista vagy egyedi ügyfélajánlatok szerint az ÁSZF-ben foglalt módon megfizetni.

A Szolgáltató a weboldalán közzétett árlistában és ajánlatokban különösen, de nem kizárólagosan az alábbi, jelen Szabályzat szerinti időszaki szolgáltatások és kapcsolódó opcionális szolgáltatások díjait határozza meg.

Időszaki szolgáltatások:

- Tanúsítványszolgáltatás (lásd 9.1.1 fejezet);
- NL Sign szolgáltatás (lásd 9.1.4.1 fejezet)
- Szolgáltatáscsomag (lásd 9.1.4.2 fejezet);
- jelen szabályzatban nem részletezett szolgáltatások (lásd 9.1.4.2 fejezet);

Tanúsítványkibocsátáshoz kapcsolódó opcionális szolgáltatások:

- Mobil regisztrációs szolgáltatás;
- Ügyféleszköz átadása kézbesítési megbízott által;
- Személyazonosítás regisztrációs megbízott által;
- Utólagos fizetés;
- Szolgáltatási szerződés módosításra vonatkozó ügyféligény kezelése;
- Blokkolt ügyféleszköz feloldása;
- Ügyféleszköz cseréje;
- Egyedi adminisztráció.

Az egyes opcionális szolgáltatások pontos leírását és feltételeit a Szolgáltató a weboldalán teszi közzé. Az opcionális szolgáltatások nyújtását Szolgáltató felfüggesztheti, illetve a fentiek mellett egyéb opcionális szolgáltatásokat is bevezethet, melyekről szintén weboldalán tesz közzé tájékoztatást.

A szolgáltatások igénylésével kapcsoltban, azzal együtt nyújtott opcionális szolgáltatások díjait az adott szolgáltatás díjával együtt kell Előfizetőnek megfizetni.

A szolgáltatásokat a Szolgáltató szolgáltatáscsomagok keretében is értékesítheti, ebben az esetben a szolgáltatás díját a szolgáltatáscsomag díja tartalmazza. Ennek feltételeit és a Szolgáltató díjaira vonatkozó egyéb szabályokat az ÁSZF tartalmazza.

9.1.1 Tanúsítványszolgáltatás díjai

A Tanúsítványszolgáltatás díja tartalmazza a tanúsítvány kibocsátását (kezdeti, megújítási, módosítási vagy kulcscsere eljárás keretében), a teljes érvényességi ideje alatt történő közzétételét (tanúsítványtárban vagy visszavonási listán), a kapcsolódó (pl. tanúsítványállapot) szolgáltatások nyújtását, valamint a teljes megőrzési időben való tárolását.

9.1.2 Tanúsítvány-hozzáférési díjak

A tanúsítványtár lekérdezéséért a Szolgáltató nem számít fel díjat, amennyiben az igénybevételre a 2.4 fejezet vonatkozó szabályai szerint valamint a Szolgáltató erre a célra fenntartott, a weboldalán elérhető lekérdező felületen kerül sor, és a tanúsítványok lekérdezése egyesével, az egyes tanúsítványok megtekintéséhez szükséges adatok manuális megadásával történik.

A tanúsítványtár egyéb módon történő igénybevételét (pl. tömeges automatikus lekérdezést) a Szolgáltató kizárólag külön megállapodás alapján, az abban foglalt feltételekkel és szolgáltatási díj

ellenében biztosítja.

9.1.3 A tanúsítványállapot-változtatás és a visszavonási nyilvántartások igénybevételének díjai

Szolgáltató a tanúsítványállapot-változtatásokért (lásd 9.1.3 fejezet) külön díjat nem számít fel.

A tanúsítványállapot-szolgáltatás 2.4 fejezet szabályaitól eltérő módon történő igénybevételét (pl. gyakori és tömeges OCSP lekérdezést) a Szolgáltató kizárólag külön megállapodás alapján, a megállapodás szerinti feltételekkel és szolgáltatási díj ellenében biztosítja.

9.1.4 Egyéb szolgáltatások díjai

NL Sign szolgáltatás díja

Az NL Sign szolgáltatás díja magában foglalja az adott időszakra vonatkozóan a kapcsolódó tanúsítvány- és opcionálisan időbélyegző szolgáltatások díját és adott számú aláírás/bélyegző létrehozását.

Szolgáltatáscsomagok díja

Az ÁSZF szerinti szolgáltatás csomagok díja magában foglalja a tanúsítvány érvényességi idején belül felhasználható időbélyegek és az ügyféleszközök díját is.

Jelen szabályzatban nem részletezett szolgáltatások díjai

A Szolgáltató jelen szabályzatban nem rendezett szolgáltatásokért is számíthat fel díjat, amennyiben azokat az ÁSZF-nek megfelelően közzéteszi weboldalán, vagy Előfizetővel ilyen szolgáltatás nyújtására előzetesen megállapodott.

9.1.5 Visszatérítési politika

Amennyiben a szolgáltatási szerződés Szolgáltató ÁSZF-ben meghatározott, bizonyított súlyos szerződésszegése vagy ÁSZF módosítása miatt kerül felmondásra vagy a vonatkozó szolgáltatást Szolgáltató megszünteti a szerződés ideje alatt (feltéve, hogy azt más szolgáltató nem veszi át) akkor Szolgáltató az igénybevétellel arányos szolgáltatási díjat térít az Ügyfél részére. A szolgáltatási szerződés megkötésétől számított 14 napon belüli felmondás vagy elállás esetén Szolgáltató a teljes szolgáltatási díjat visszatéríti.

Szolgáltató egyéb esetekben, pl. a szolgáltatási szerződés - adott esetben idő előtti - megszűnése, illetve a szolgáltatás igénybe nem vétele vagy Ügyféleszköz át nem vétele, vagy a szerződési időre vonatkozó díjcsomagok (pl. adott mennyiségű aláírás, vagy a tanúsítvány teljes érvényességi idejének) ki nem használása esetén, a kifizetett szolgáltatási díjakat sem egészben sem részben nem téríti vissza Előfizető részére. E szolgáltatások díjai kifejezetten azzal a feltételezéssel lettek megállapítva, hogy az Ügyfelek egy része e kvótákat csak részben veszi majd igénybe.

9.2 Pénzügyi felelősség

Szolgáltató a pénzügyi felelősségét az alábbiak szerint korlátozza:
Az egyes szolgáltatások és tanúsítványtípusok tekintetében különböző felelősségvállalási értéket határoz meg az Árlistájában, amely biztosítási eseményenként (egy vagy több azonos okból bekövetkezett, időben összefüggő káresemény) érvényesíthető. Amennyiben egy adott biztosítási eseményben több Ügyfél, illetve több különböző szerződés és azokhoz tartozó tanúsítványok is érintettek, akkor a kártérítés mértéke úgy kerül meghatározásra az egyes Ügyfelekkel és szerződésekkel (tanúsítványokkal) összefüggésben, hogy az összesen kártérítés a legmagasabb

felelősségvállalási értéket ne haladja meg és az adott szolgáltatáshoz, tanúsítványtípushoz tartozó felelősségvállalási érték is mindegyik esetben limitálásra kerüljön.
A végfelhasználói tanúsítványokhoz igényelhető felelősségvállalási értékekről Szolgáltató weboldalán nyújt tájékoztatást, mely végfelhasználói tanúsítványok esetén legalább 3 000 000 (hárommilió) forint (HUF).

Ezen értékek a Szolgáltatások árlista szerinti teljes díjára tekintettel lettek megállapítva. Amennyiben Ügyfél a szolgáltatást kedvezményes díjjal veszi igénybe, akkor a kártérítés mértéke a biztosított kedvezményekhez mérten, azzal arányos módon kerülhet megállapításra.

9.2.1 Biztosítási fedezet

Szolgáltató - az Ügyfelek és Érintett felek esetleges kártalanításhoz és egyéb rendkívüli költségek fedezésére - felelősségbiztosítással rendelkezik. A felelősségbiztosítás kiterjed minden jelen szabályzat szerinti szolgáltatás nyújtása során Szolgáltató kártérítési kötelezettségeire. Lásd a 9.6 fejezetet.

A felelősségbiztosítás továbbá kiterjed:

- a bizalmi szolgáltatási ügyfélnek a bizalmi szolgáltatási szerződés megszegésével összefüggésben okozott károkra,
- a bizalmi szolgáltatási ügyfélnek és harmadik személynek szerződésen kívüli okozott károkra,
- a DÁP-ban foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, a DÁP szerinti költségekre, és
- az eIDAS Rendelet vonatkozó rendelkezései alapján a bizalmi felügyelet által felkért megfelelőségértékelő szervek eljárásának költségeire, ha azt a bizalmi felügyelet eljárási költségként érvényesíti.

A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként nem alacsonyabb, mint 3 000 000 (hárommillió) forint (HUF).

Az EV weboldal-hitelesítő (EVCP) tanúsítványok esetére a felelősségbiztosítás kártérítésének felső határa 5 000 000 (ötmillió) USD-nak megfelelő forint ellenértéke, a kártérítés kifizetésekor aktuális banki árfolyam szerint.

9.2.2 Egyéb eszközök

Szolgáltató a szolgáltatás megszűntetési követelmények teljesítésével kapcsolatos költségek fedezetével rendelkezik. A kötelezettségek teljesítését 25.000.000 Ft-os bankgarancia szavatolja.

9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák

Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személynek okozott kárért a Polgári Törvénykönyv általános szabályai szerint felel.

9.3 Bizalmas üzleti információk kezelése

Szolgáltató a birtokába jutott bizalmas adatokat a hatályos jogszabályi rendelkezésekre figyelemmel és az 5. fejezet rendelkezéseinek és a Szolgáltató nem nyilvános Adatkezelési szabályzatának előírásai szerint tárolja és kezeli.

A megőrzési kötelezettség lejártával - amennyiben az Ügyfél erről másképpen nem rendelkezik -

Szolgáltató a bizalmas adatokat visszavonhatatlanul törli adatbázisából.

9.3.1 A bizalmas információk köre

A Szolgáltató bizalmas információnak tekint minden, az egyes Ügyfelekre vonatkozó adatot a 9.3.2 pontban foglaltak kivételével. Különösen és továbbá bizalmas adatok a következők:

- a tanúsítványba nem kerülő személyes adatok;
- regisztrációs adatok (pl. hang és videó felvételek, okmánymásolatok);
- az ügyfélszolgálaton rögzített hangfelvételek;
- magánkulcsok és azok aktiváló adatai;
- tanúsítványigénylések adatai;
- szolgáltatási szerződések;
- nem nyilvános szabályzatok;
- a szolgáltatásokkal kapcsolatban keletkezett naplóadatokat;
- minden olyan adat, melynek nyilvánosságra hozatala veszélyeztetné a szolgáltatások biztonságát;
- minden olyan adat, melynek nyilvánosságra hozatala a fenti adatok harmadik felek általi megismeréséhez vezethet.

A bizalmas információkat a Szolgáltató a 9.3.3 fejezet szerint kezeli.

9.3.2 A bizalmas információk körén kívül eső adatok

A Szolgáltató az alábbi adatokat nem tekinti bizalmas információnak:

- a visszavonási nyilvántartások biztosításához szükséges tanúsítványadatok;
- a tanúsítványba kerülő összes adat (lásd 7.1 fejezet), amennyiben Igénylő az igénylés során máshogy nem rendelkezett;
- egyéb személyes jellegüktől megfosztott adatokat úgy, hogy azok semmiképpen nem köthetők az információ birtokosához vagy ahhoz, akire vonatkozóan az információból következtetés vonható le.

A bizalmasnak nem tekintett adatokat a Szolgáltató nyilvánosságra hozhatja, megoszthatja partnereivel, illetve nyilvánosságra kerülésükért nem tartozik felelősséggel.

9.3.3 A bizalmas információk védelme

A Szolgáltató a törvényi előírásokon és jelen Szolgáltatási szabályzat követelményein túlmenően Adatkezelési szabályzatában is rögzített módon mindent megtesz a 9.3.1 fejezet szerinti bizalmas információk biztonságos kezelése érdekében.

Azon adatokat, melyekhez a Szolgáltató elektronikus formában jutott hozzá, elektronikus formában, amelyek pedig papír alapon jutottak a birtokába, azokat papír alapon és/vagy elektronikus formában is megőrizheti és kezelheti.

Szolgáltató a személyes adatok megőrzését azok biztonságát illetve az adatvesztés, -sérülés és az adatok helytelen vagy illetéktelen használata, megismerése elleni védelmét az 5.5. fejezet előírásai szerint végzi, a 6.5. fejezet szerinti informatikai biztonsági előírások figyelembe vételével.

A Szolgáltató a birtokába jutott bizalmas adatokhoz csak azon 5.2.1 pont szerinti munkatársai számára ad hozzáférést, akiknek munkájuk elvégzéséhez ez elengedhetetlen (pl. Regisztrációs ügyintézők).

Szolgáltató az Ügyféladatokat az adott feladat nyújtásához szükséges mértékben és céllal alvállalkozóinak, megbízottainak átadhatja a következő esetekben:

- Szolgáltatás igénybevételéhez szükséges eszközök előállítása;
- Számlázás;
- Ügyfél elleni követelés érvényesítése.

A Szolgáltató kizárólag a DÁP-ban meghatározott alábbi esetekben és módon fedheti fel a bizalmas adatokat:

- Amennyiben Szolgáltató valamennyi bizalmi szolgáltatását megszünteti, a DÁP vonatkozó rendelkezései értelmében a szolgáltatási tevékenység megszűnését követően biztosítja a törvényben meghatározott átvevő szolgáltatónak a szolgáltatásokkal kapcsolatos nyilvántartásokhoz való hozzáférést, valamint átadja a visszavont tanúsítványokkal kapcsolatos összes adatot (beleértve a személyes adatokat is).
- A DÁP vonatkozó rendelkezései értelmében Szolgáltató bizalmi szolgáltatásaival kapcsolatba hozható bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből a nyomozó hatóság és/vagy a nemzetbiztonsági szolgálatok megkeresésére – a külön törvényben meghatározott feltételek teljesülése esetén – Szolgáltató részükre a kért adatokat haladéktalanul átadja – beleértve az azonosítási-hitelesítési eljárások (lásd a 3. fejezetet) során a DÁP vonatkozó rendelkezései szerint ellenőrzött és rögzített személyes és egyéb adatokat is.. Az adatátadás tényét a Szolgáltató jegyzőkönyvben rögzíti, az adatátadásról a Szolgáltató a jogszabály értelmében érintett Ügyfelet vagy Ügyfeleket nem tájékoztathatja.
- A DÁP vonatkozó rendelkezései értelmében Szolgáltató az általa kibocsátott tanúsítvány érvényességét igazoltan érintő polgári peres, illetve nemperes eljárás esetén a tanúsítvány kibocsátását megelőző azonosítási-hitelesítési eljárások (lásd a 3. fejezetet) során a DÁP vonatkozó rendelkezései szerint ellenőrzött és rögzített személyazonosító és egyéb adatokat kérésre átadhatja az eljárásban részt vevő ellenérdekű félnek vagy képviselőjének, illetve közölheti azokat a megkereső bírósággal.
- Amennyiben a Bizalmi Felügyelet a DÁP vonatkozó rendelkezései alapján a hatáskörébe utalt feladatai ellátásával összefüggésben a Szolgáltatót adatszolgáltatásra szólítja fel, a kért adatokat Szolgáltató a Felügyelet által megjelölt határidőre és formában, hiánytalanul és a valóságnak megfelelően átadja a Bizalmi Felügyeletnek.

A fenti törvényileg szabályozott esetekben az adatszolgáltatást a Szolgáltatónak nem áll módjában megtagadni. A Szolgáltató az adatszolgáltatás során is biztosítja az adatok bizalmasságát, azok valódiságát és hiánytalanságát A kötelező adatszolgáltatások teljesítéséért és jegyzőkönyvezéséért felelős munkatársat Szolgáltató mindenkori ügyvezetése jelöli ki.

9.4 Személyes adatok kezelése

A Szolgáltató az Ügyfelek személyes adatait a 9.3.1 fejezet szerinti bizalmas információnak tekinti, a 9.3.2 fejezetben foglalt kivételekkel és ennek megfelelő védelem (9.3.3. fejezet) mellett a 9.4.1 fejezet szabályait betartva kezeli őket.

9.4.1 Adatkezelési szabályok

A Szolgáltató az Ügyfelek személyes adatait

- jelen Szabályzat és a Szolgáltatási Rend,
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,
- az Európai Parlament és a Tanács (EU) 2016/679 rendelete 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), és
- Szolgáltató Adatkezelési Szabályzatának

rendelkezéseit betartva kezeli.

A Szolgáltató biztosítja, hogy bármely adat rendelkezésére bocsátása esetén ezen adatokhoz illetéktelen személyek ne férhessenek hozzá.

Szolgáltató a hatályos jogszabályoknak megfelelően a tanúsítványokkal kapcsolatos információkat – beleértve az azok előállításával összefüggőket is – és az ahhoz kapcsolódó személyes adatokat a tanúsítvány érvényességének lejártától számított 10 évig, illetőleg az elektronikus aláírással/bélyegzővel, vagy az azzal ellátott elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrizi, valamint ugyanezen határidőig biztosít olyan eszközt, mellyel a kibocsátott tanúsítvány tartalma megállapítható.

Szolgáltató a tanúsítványok állapotinformációit minden esetben nyilvánosságra hozza illetve az Ügyfél írásbeli hozzájárulása/kérése esetén a tanúsítvány Alanyadatait és magát a tanúsítványt nyilvános tanúsítványtárában közzéteszi.

Szolgáltató rendelkezik adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a bizalmas és személyes információk kezelésére. Az adatkezelési szabályzat által lefektetett adatkezelési gyakorlatról Szolgáltató a weboldalán (lásd 1.1.2) közzétett Adatvédelmi Tájékozatóban tájékoztatja Ügyfeleit.

Szolgáltatót a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) nyilvántartásába vette, mint adatkezelőt; Szolgáltató adatkezelési nyilvántartási száma: NAIH-50145/2017.

9.4.2 Személyes adatok

A Szolgáltató minden olyan birtokába kerülő adatot személyes adatnak tekint,

- mely alapján természetes személy beazonosítható - különös tekintettel a természetes személy nevére vagy hatóság által nyilvántartott azonosítójára -, vagy
- ami természetes személlyel kapcsolatba hozható, vagy
- melyből a természetes személyre vonatkozó következtetés levonható,
- és amely nem sorolható egyúttal a 9.4.3 fejezet szerinti adatok közé.

A Szolgáltató csak az igényelt szolgáltatás nyújtásához elengedhetetlenül szükséges személyes adatokat kéri el az Ügyfelektől. Ez nem zárja ki, hogy a Szolgáltató a szolgáltatásnyújtáshoz kapcsolódóan olyan adatokat is elkérjen, amely birtokában a Szolgáltató hatékonyabban végezheti tevékenységét. Ezen adatok megadása nem kötelező, kezelésük pedig az érintett hozzájárulásán alapul.

9.4.3 Személyes adatnak nem minősülő információk

A 9.4.2 pontban meghatározott adatok körén kívül eső adatokat Szolgáltató nem tekinti személyes adatnak.

9.4.4 Személyes adatok védelme

Szolgáltató a tanúsítványkibocsátással kapcsolatos és a tanúsítványban nem szereplő személyes adatokat a vonatkozó előírásoknak megfelelően (lásd 9.4.1) biztonságosan tárolja és védi. Az adatokat megfelelő intézkedésekkel védi a jogosulatlan hozzáférés és a megváltoztatás ellen, különösen az Ügyfél és a Szolgáltató egyes egységei között történő továbbítás során. Továbbá védi őket, az adatvesztés, a károsodás és a nem engedélyezett feldolgozás ellen is. Lásd még az 5.3.1, 5.5.1, 5.7.1, 5.7.4 és 9.3.3 fejezeteket.

9.4.5 Személyes adatok felhasználása

A Szolgáltató csak a tanúsítványban szereplő személyes adatokat hozza nyilvánosságra, amennyiben ahhoz az Ügyfél előzetesen írásban hozzájárult.

A Szolgáltató a személyes adatokat csak az Info tv. előírásaira tekintettel illetve olyan módon és mértékben használja fel, amely a tanúsítvánnyal kapcsolatos (például: kiadási, állapotváltoztatási,

megújítási, módosítási vagy kulcscsere) műveletek elvégzéséhez szükséges.

9.4.6 Adatkezelés

Szolgáltató adatkezelésének jogalapja elsősorban az eIDAS és a DÁP tanúsítványkiadással kapcsolatos adatok megőrzésére vonatkozó előírásaiból fakadó jogszabályi kötelezettség teljesítése. A jogszabályi kötelezettség hatókörén kívül eső adatok esetében pedig az adatkezelés jogalapja a Szolgáltató és az érintett jogos érdekéből és az érintett előzetes – tájékoztatáson alapuló és konkrét – hozzájárulása.

A Szolgáltató a személyes adatokat a 9.4.1. pontban felsorolt hatályos jogszabályi rendelkezésekre figyelemmel és az 5. fejezet vonatkozó eljárási szabályainak megfelelően tárolja és kezeli; azokat csak a 9.3.3 pontban felsorolt, jogszabályok által meghatározott esetekben adhatja át a jogszabályok szerinti harmadik félnek.

9.4.7 Egyéb adatvédelmi követelmények

Szolgáltató az általa nyújtott bizalmi szolgáltatások felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából vagy nemzetbiztonsági érdekből - az érintett személyazonosságát igazoló, valamint egyeztetett adatok tekintetében - az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén díjmentesen adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét rögzíti, az adatátadásról az érintett feleket nem tájékoztatja (lásd 9.3.3).

9.5 Szellemi tulajdonhoz fűződő jogok

A szolgáltatási tevékenység során alkalmazott valamennyi

- név,
- termék,
- szoftver és hardver komponensek

a Szolgáltató tulajdonát képezik, vagy azokat jogszerűen használja.

A Szolgáltató tulajdonát képezik továbbá az általa közreadott / kibocsátott / létrehozott:

- szabályzatok,
- szerződési feltételek,
- általa készített egyéb dokumentumok és tájékoztatók,
- tanúsítványok,
- visszavonási nyilvántartások adatai,
- egyedi azonosítók

A Szolgáltató által kibocsátott magán- és nyilvános kulcs tulajdonosa az Előfizető.

Végfelhasználó teljes jogú felhasználója a végfelhasználói tanúsítványnak és az abban szereplő nyilvános kulcsnak és permanens azonosítónak.

A Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokat a benne szereplő nyilvános kulccsal és egyéb adatokkal együtt közzéteheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti (lásd 4. fejezet).

A Szolgáltató működése során ügyel arra, hogy harmadik személyek szellemi tulajdonjogait ne sértse.

9.6 Felelősség és garanciák

Szolgáltató felelős minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okozott kötelezettségeinek megszegésével.

Nem-minősített szolgáltatások esetén Szolgáltató szándékossága / gondatlansága vélelmezett

mindaddig, amíg Szolgáltató bizonyítja az ellenkezőjét.

Szolgáltató nem felelős a szolgáltatások igénybevételére vonatkozó korlátozásokat meghaladó károkért (a korlátozásokat lásd jelen szabályzatban, a Szolgáltatási Rendben, az ÁSZF-ben, és a Szolgáltatási szerződésben).

Szolgáltató felelős a szabályzatai keretei között végzett szolgáltatói tevékenységekért valamint Regisztrációs és Hitelesítő egységének működéséért akkor is, ha egyes funkciókat Szolgáltatói Partnerek végeznek.

9.6.1 A Hitelesítő Egység felelőssége

Lásd a Szolgáltatási Rend 9.6.1 fejezetét.

9.6.2 A Regisztrációs Egységek felelőssége

Lásd a Szolgáltatási Rend 9.6.2 fejezetét.

9.6.3 Ügyfelek felelőssége és kötelezettségei

Lásd a Szolgáltatási Rend 9.6.3 fejezetét.
Az Igénylő felelősséggel tartozik:

- az igénylések feldolgozásához szükséges adatok megadásáért és igazolásáért (lásd. 4. fejezet)
- a regisztráció és az igénylés során megadott adatok valódiságáért, pontosságáért és érvényességéért;
- a személyazonosságának és az igénylés során megadott adatok 3. fejezet szerinti ellenőrzésében való együttműködésért - minden tőle telhetőt megtéve azért, hogy a folyamat a lehető leggyorsabban befejeződhessen;
- kibocsátása után a tanúsítványban szereplő adatok ellenőrzéséért, eltérés észlelése esetén pedig a Szolgáltató értesítéséért az eltérésről;
- az adataiban bekövetkezett változások haladéktalan bejelentéséért és a tanúsítvány felfüggesztésének vagy visszavonásának igényléséért illetve a kulcsok használatának beszüntetéséért;
- a szolgáltatás igénybevétele előtt a Bizalmi Szolgáltatási Rend és jelen Szolgáltatási Szabályzat, illetve az ÁSZF és a Szolgáltatási szerződés tartalmának megismeréséért.

A Végfelhasználó az alábbiakért tartozik felelősséggel:

- Ügyféleszközének, kulcsának és tanúsítványának a szabályzatoknak megfelelő felhasználásáért;
- Ügyféleszközének, kulcsának és aktiváló adatának biztonságos kezeléséért;
- a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért a tanúsítványhoz vagy alkalmazásához köthető vitás ügyekben a vita jogi útra terelése előtt;
- a szolgáltatások jogszabályokban és jelen szabályzatban foglaltaknak megfelelő használatáért;
- a tanúsítványban feltüntetett felhasználási célokra, a benne jelzett korlátozásoknak megfelelő tanúsítványhasználatért;
- a teszttanúsítványokhoz tartozó magánkulcsok valódi kötelezettségvállalást nélkülöző, teszt jellegű alkalmazásáért;
- amennyiben az Végfelhasználó magánkulcsa, Ügyféleszköze vagy az aktiváló adatok illetéktelen kézbe kerültek, vagy ezek gyanúja merült fel, Végfelhasználó ezt köteles haladéktalanul jelezni a Szolgáltatónak és kezdeményeznie kell a tanúsítvány(ok) felfüggesztését vagy visszavonását valamint meg kell szüntetnie a tanúsítvány használatát.

Az Előfizető felelősséggel tartozik:

- a szolgáltatás igénybevétele előtt Szolgáltató szabályzatainak megismeréséért;
- az igénylés során megadott adatok valódiságáért, pontosságáért és érvényességéért;
- az igénylés során megadott adatok 3. fejezet szerinti ellenőrzésében való együttműködésért - minden tőle telhetőt megtéve azért, hogy a folyamat a lehető leggyorsabban befejeződhessen;
- a tanúsítvány módosítását, kulcscseréjét vagy visszavonását kezdeményezni a Szolgáltatási Rend 9.6.3 és 4.9.1 pontjai, illetve jelen szabályzat 4.7 és 4.8 pontja szerint;
- a Végfelhasználói kötelezettségek betartásáért, olyan mértékben, amennyiben azokra hatással van
- a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért a tanúsítványhoz vagy alkalmazásához köthető vitás ügyekben;
- köteles biztosítani, hogy a szolgáltatás igénybevételéhez szükséges adatokhoz és eszközökhöz illetéktelen személyek ne férhessenek hozzá;
- felelősséggel tartozik a Végfelhasználói kötelezettségek betartásáért, olyan mértékben, mennyiben azokra hatással van;
- díjfizetési kötelezettségének eleget tenni, kivéve, ha Előfizető és Díjfizető elkülönül, és a díj fizetés a Díjfizető kötelezettsége.

A Díjfizető felelősséggel tartozik:

- díjfizetési kötelezettségének eleget tenni.

9.6.4 Érintett felek felelőssége

Lásd a Szolgáltatási Rend 9.6.4 fejezetét.
Az Érintett Feleknek a Szolgáltató által garantált biztonsági szint megtartásához szükséges körültekintő eljárás érdekében továbbá javasolt:

- a Szolgáltatás elfogadottságának és nem-minősített voltának bizalmi listán való ellenőrzése;
- a Szolgáltató Bizalmi Szolgáltatási Rendjében és jelen Szabályzatban megfogalmazott követelmények, előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- a tanúsítvány állapotának ellenőrzése az aktuális CRL vagy OCSP válasz alapján (lásd 4.9.6 pont);
- a tanúsítvány felhasználására vonatkozó valamennyi (Szolgáltató szabályzataiban valamint a tanúsítványban feltüntetett) korlátozás figyelembe vétele.

Az Érintett Felek saját belátásuk és/vagy szabályzataik alapján jogosultak dönteni az egyes tanúsítványok elfogadásáról, illetve azok felhasználási módjáról.

9.6.5 Egyéb résztvevők felelőssége

Nincs előírás.

9.7 Szavatosság kizárása

A Szolgáltatóval szemben a szolgáltatásaival kapcsolatban támasztott jótállási, szavatossági vagy kártérítési igényeket Szolgáltató visszautasítja, amennyiben

- annak alapját képező eset Ügyfél mulasztására, kötelezettségeinek és felelősségeinek be nem tartására vagy külső, előre nem látható eseményekre vezethető vissza;
- az Érintett felek által alkalmazott eljárások nem felelnek meg a jelen Szolgáltatási szabályzatnak;

- Szolgáltató az internet, vagy egy részének működési hibájából adódóan nem tudja ellátni a tájékoztatási és egyéb kommunikációs kötelezettségeit;
- a károkozás a Felügyeleti szerv által jóváhagyott kriptográfai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8 Felelősség korlátozása

Szolgáltató a kártérítési felelősségét a 9.16.5 szerint és az alábbiak szerint korlátozza.

Szolgáltató nem felelős az olyan károkért, amelyeket a Szolgáltató szavatosságának 9.7 pont szerinti kizárásához vezető körülmények okoztak, továbbá abban az esetben, ha Ügyfél vagy az Érintett fél nem tanúsította a tőle elvárható gondosságot, nem a Szolgáltató Kikötései szerint vagy jogellenesen jártak el.

Szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag a saját hibájából, kötelezettségeinek megszegéséből, valamint a neki felróható okokból bekövetkező, bizonyítható károkért tartozik helyt állni.

A teszttanúsítványok nem tesztcélú felhasználásáért Szolgáltató nem vállal felelősséget.

A felelősség - és annak korlátozása - tekintetében lásd még a 9.2 és 9.6 pontban foglaltakat.

9.9 Kártérítés, kártalanítás

Szolgáltató kártérítési felelősségének fedezetéül felelősségbiztosítással rendelkezik (lásd. 9.2 pont).

Ügyfél kártérítési felelősséggel tartozik Szolgáltatónak azokért a bizonyított veszteségekért és károkért, amelyeket a rá vonatkozó kötelezettségek és ajánlások szándékos vagy gondatlan megszegésével okoz a Szolgáltató kárára.

A kártérítési és kártalanítási eljárásokra a Ptk. általános szabályai vonatkoznak, Szolgáltató az eljárást részletesen az ÁSZF-ben közli.

A felelősség bizonyítása tekintetében lásd a 9.6, a jótállási, szavatossági vagy kártérítési, kártalanítási igényekkel kapcsolatban lásd a 9.7, 9.8 pontban foglaltakat.

9.10 A szabályzat hatálya

9.10.1 Érvényesség

A Szabályzat időbeli hatálya a jelen verzió hatálybalépésének fedlapon jelzett dátumától (hatály kezdőnapja) kezdődik.

A Szabályzat személyi hatálya a Szolgáltató bizalmi munkatársaira, a szolgáltatói partnerekre, az Ügyfelekre és minden Érintett félre kiterjed.

A Szabályzat tárgyi hatálya a jelen Szolgáltatási szabályzat 1.1 pontja szerinti szolgáltatások nyújtását és igénybevételét foglalja magában.

9.10.2 Megszűnés

A Szabályzat érvényessége a szolgáltatási tevékenység beszüntetéséig, a szabályzat visszavonásáig vagy újabb szabályzatverzió hatályba lépéséig tart. A Szabályzat érvényessége alatt kibocsátott tanúsítványok tekintetében a Szabályzat 9. fejezetét a Szabályzat érvényességét követően is alkalmazni kell, függetlenül a Szabályzat érvényességének megszűnése módjától.

9.10.3 A megszűnés következményei

A Szabályzat visszavonása esetén a Szolgáltató weboldalán teszi közzé a visszavonás részletes

szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket. A Szolgáltató vállalja, hogy a Szolgáltatási Szabályzat visszavonása esetén is érvényben maradnak a mindenkor hatályos vonatkozó jogszabályokban meghatározott bizalmas adatok védelmére vonatkozó előírások.

9.11 Egyedi értesítések és a résztvevők közti kommunikáció

A Szolgáltató az Ügyfelekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát és telefonos ügyfélszolgálatot működtet az 1.1.2 pontban megadott elérhetőségekkel (lásd még 1.3.2 pont).

Az Ügyfélszolgálat a szolgáltatások igénybevételével és egyéb, a végfelhasználói tanúsítványokkal kapcsolatos ügyintézések és eljárások során elsősorban e-mailek útján kommunikál Ügyféllel. Emellett az Ügyfélszolgálat telefonon és személyesen is megkereshető.

Szolgáltató az ügyfelek felé küldött ügyfélszolgálati e-mailjeit egyedi azonosítóval látja el, mely alapján ügyfélmegkeresés esetén könnyen azonosítható az adott ügy vagy téma. Amennyiben Ügyfél egy ilyen levélre válaszol, az adott ügy minél gyorsabb előrehaladása érdekében, ügyelnie kell arra, hogy az üzenet tárgya változatlan maradjon.

Amennyiben Ügyfél nem ügyfélszolgálati levélre válaszol, tegyen meg mindent azért, hogy levele alapján a lehető legkönnyebben beazonosítható legyen, így például az e-mailt elektronikusan aláírva/bélyegezve és/vagy az e-mailt a kérdéses tanúsítványban szereplő email címről küldve.

Az e-mailes megkeresések során szükséges továbbá, hogy a levélben egyértelműen beazonosítható legyen a kérdéses szolgáltatás vagy tanúsítvány.

Amennyiben Ügyfél keresi fel a Szolgáltatót e-mailben a Regisztrációs ügyintéző felelőssége eldönteni, hogy az email alapján milyen lépések tehetők. Amennyiben Szolgáltatónak további információra van szüksége, arról válaszlevélben ad tájékoztatást. Amennyiben az Ügyfél beazonosíthatósága felől merülnek fel kétségek, Szolgáltató megkísérli telefonon felkeresi az Ügyfelet a személyes adatok egyeztetése céljából.

Az e-mailes kommunikáció mellett az alábbi kommunikációs lehetőségek állnak Ügyfelek rendelkezésére.

Telefon

Az ügyfélszolgálati telefonszámon ügyintéző kizárólag a weboldalon meghirdetett időpontokban érhető el, egyéb időszakokban üzenet hagyható (kivéve a visszavonási igények esetét, lásd 4.9.4).

Ügyfélszolgálati irodában, személyesen

Szolgáltató ügyfélszolgálati irodájában (lásd 1.1.2 pont) személyes egyeztetésre kizárólag előre egyeztetett kérdésekben fogadja az Ügyfeleket.

9.12 Módosítások

A Szolgáltató a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén megváltoztathatja Szolgáltatási szabályzatát.

A szabályzatok egymásnak, a vonatkozó jogszabályoknak és szabványoknak való megfelelés vizsgálata legalább évente történik. A szabályzatok rendkívüli felülvizsgálatára és módosítására a jogszabályi és/vagy a műszaki szabványkörnyezet változása esetén kerül sor. Szolgáltató a működése során szerzett gyakorlati tapasztalatok alapján is folyamatosan felülvizsgálja Szolgáltatási szabályzatát.

A módosított szabályzatot Szolgáltató legkorábban a közzététel és a bizalmi felügyelet értesítésének napján lépteti hatályba.

Szolgáltató a bizalmi felügyelet számára bejelenti, ha a korábbi bejelentések alapján nyilvántartásba vett adatokhoz képest működésében vagy a bizalmi szolgáltatás nyújtásában – így például a szolgáltatási rendben vagy szabályzatban – változás történik.

Lásd még az 1.5 és 2.1 fejezetet.

9.12.1 A módosítási eljárás

Szolgáltató a szabályzatváltoztatási igényeket gyűjti (lásd 1.5), a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz, s a változtatásokat életbe lépteti.

Szolgáltató a változtatási igényeket előzetesen megvizsgálja a Szolgáltatási Rendben meghatározott tartalmi követelményeknek valamint a jogszabályi és szabvány elvárásoknak való megfelelőség szempontjából. Amennyiben egyikkel kapcsolatban sem merül fel kifogás, a módosítási igényt elfogadja és megkezdi annak kidolgozását.

A változtatásokat gyűjtve a Szabályzatelfogadó Egység belső, nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. Szolgáltató a változásokat – lehetősége szerint – kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A kidolgozott módosításokat a Szabályzat jóváhagyója (lásd 1.5) fogadja el, melyet megelőzően szintén megvizsgálja a fenti tartalmi és formai követelményeket. Ezt követően kerül sor a Bizalmi Felügyelet, az Ügyfelek és az Érintett felek értesítésére (lásd 9.12.2). A Szabályzat jóváhagyására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik, majd bejelentés után a Szabályzatot a Bizalmi Felügyelet nyilvántartásba veszi.

A Szolgáltatási Szabályzat jóváhagyására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik.

A módosított szabályzatváltozatok – a nyilvános tervezetek is – mindig új verziószámmal kerülnek nyilvánosságra.

9.12.2 Az értesítések módja és határideje

Szolgáltató az új szabályzatváltozatok tervezett hatálybaléptetésének napján értesíti a bizalmi felügyeletet. Az értesítéssel egyidejűleg Szolgáltató változásokkal módosított és jóváhagyott új Szolgáltatási Rend és Szolgáltatási Szabályzat verziót is megküldi a Bizalmi felügyeletnek valamint – az Ügyfelek és Érintett felek tájékoztatására – közzéteszi azt a weboldalán (lásd 2.1.2).

Amennyiben a Szolgáltató a változás következtében, azzal egyidejűleg új szolgáltatás indítását is tervezi, az új szolgáltatás indítását legkésőbb annak indulásakor bejelenti azt a Bizalmi felügyeletnek.

A bejelentést Szolgáltató a bizalmi felügyelet weboldalán közzétett űrlapon, a 470/2017 Kormányrendeletben foglaltak szerint teszi meg. Az űrlaphoz a Szolgáltató csatolja

- a módosított és jóváhagyott új Szolgáltatási Rend verziót;
- a módosított és jóváhagyott új Szolgáltatási Szabályzat verziót;
- a módosított és jóváhagyott új Szabályzatkivonat verziót;
- valamint a 470/2017 Kormányrendeletben meghatározott egyéb iratokat és dokumentumokat.

9.12.3 A dokumentumazonosító változása

A Szolgáltatási Szabályzat újabb nyilvános változatai – a tervezetek is – mindig új verziószámmal kerülnek nyilvánosságra, vagyis a két eltérő tartalmú dokumentumnak nem lehet azonos OID azonosítója.

A dokumentum azonosítója a következő elemekből épül fel – az egyes elemeket pontok választják el egymástól:

- szolgáltatói OID (1.3.6.1.4.1.3555),
- nyilvános dokumentumok jelölése (1),
- a szabályzatok jelölése (1),
- a jelen dokumentum egyedi sorszáma a nyilvános szabályzatok között (15),

- annak jelölése, hogy a dokumentum nem melléklet (0),
- verzió (mely a hatálybalépés dátuma rövid formátummal),

azaz jelen szolgáltatási szabályzat esetén:
1.3.6.1.4.1.3555.1.1.15.0.ÉÉHHNN.

A módosított Szabályzat csak a hatálybalépését követően újonnan kibocsátásra kerülő tanúsítványokra vonatkozik, a már kibocsátottakra nem.

9.13 Vitás kérdések rendezése

A Szolgáltató (beleértve a szolgáltatói partnereket is) tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat e-mailben, telefonon vagy személyesen a Szolgáltató ügyfélszolgálati irodájában fogad (lásd 1.1.2. pont).

Bármely vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra terelése előtt az Ügyfélnek kötelessége, az Érintett Félnek vagy bármely harmadik félnek pedig ajánlott a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása az ügy minden vonatkozását érintően. A felek vitáikat mindenkor megkísérlik békés, tárgyalásos úton rendezni.

9.13.1 Panaszok kezelésének eljárása

Szolgáltató a panaszokat a bejelentésüktől számított 30 naptári napon belül kivizsgálja, a kivizsgálás eredményéről pedig - felek eltérő megállapodását kivéve - e-mailben tájékoztatja a panasz benyújtóját. Amennyiben a panasz jellege miatt a kivizsgálás előre láthatólag 30 naptári napnál hosszabb időt vesz igénybe, erről a Szolgáltató külön tájékoztatja a panaszbejelentő Ügyfelet.

A személyesen vagy telefonon tett panasz esetén a Szolgáltató jegyzőkönyvet vesz fel a panasz felvételéről.

A Szolgáltató a panasz kivizsgálását követően - amennyiben értelmezett - a felmerült hibát a műszakilag indokolt időn belül elhárítja, és mindezen tevékenységekről a bejelentőt írásban tájékoztatja.

Amennyiben a választ a bejelentő Ügyfél nem fogadja el, akkor egyeztetést kezdeményezhet a Szolgáltatóval. Amennyiben a Szolgáltató ezt megtagadja, vagy ha a felek közötti egyeztetés annak kezdeményezésétől számított 20 munkanapon belül nem vezet eredményre, akkor a vita rendezésére a 9.13.2 pont szerint kerülhet sor.

9.13.2 9.13.2 Vitás kérdések rendezése békés, tárgyalásos úton

Amennyiben Ügyfél és Szolgáltató közötti egyeztetés nem vezet eredményre, akkor az esetleges bírósági eljárást megelőzően javasolt Ügyfél számára a Budapesti Békéltető Testülethez fordulni.

Jelen szabályzat hatálybalépésekor az illetékes szervezetek elérhetőségei a következők:

Budapesti Békéltető Testület:

- Cím: 1016 Budapest, Krisztina krt. 99. III. em. 310.
- Levelezési cím: 1253 Budapest, Pf.: 10.
- E-mail cím: bekelteto.testulet@bkik.hu
- Weboldal: www.bekeltet.hu

Budapest Főváros Kormányhivatala Fogyasztóvédelmi Osztály:

- Cím: 1056 Budapest, Váci utca 62-64.
- Telefon: +36-1 328 5862
- Levelezési cím: 1364 Bp., Pf.: 234
- E-mail: budapest@bfkh.gov.hu

9.13.3 9.13.3 Vitás kérdések rendezése peres úton

Amennyiben a vitás kérdés rendezése a 9.13 pont szerinti tárgyalásos megoldások egyikével sem lehetséges, felek bírósági útra terelhetik az ügyet. Ebben az esetben a felek kölcsönösen alávetik magukat a Budapesti II. és III. Kerületi Bíróság kizárólagos illetékességének.

9.14 Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar és Európai Uniós jogszabályoknak megfelelően végzi. A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, és azok a magyar jog szerint értelmezendők (lásd a 9.15 fejezetet).

9.15 A hatályos jogszabályoknak és szabványoknak való megfelelés

A Szolgáltató a hatályos jogszabályoknak és szabványoknak megfelelően végzi tevékenységét. A hatályos jogszabályoknak megfelelő működést a Szolgáltató és a bizalmi szolgáltatások Bizalmi Felügyelet általi nyilvántartásba vétel is igazolja.

A Szolgáltató tevékenységét az alábbi jogszabályok, szabványok és egyéb előírások rá vonatkozó kötelező előírásainak megfelelően végzi:

- **eIDAS:** Az Európai Parlament és Tanács 910/2014/EU Rendelet (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről;
- **DÁP.:** A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény;
- **BM rendelet:** A bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016 (VI. 30.) BM rendelet;
- A bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről szóló25/2016. (VI. 30.) BM rendelet;
- A bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről szóló 470/2017 (XII. 28.) Korm. rendelet;
- **Közig. rendelet:** Az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről szóló 137/2016. (VI.13.) Korm. rendelet;
- A Bizottság (EU) 2015/1506 Végrehajtási határozata (2015. szeptember 8.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 27. cikkének (5) bekezdése és 37. cikkének (5) bekezdése szerint a közigazgatási szervek által elismert fokozott biztonságú elektronikus aláírások és fokozott biztonságú bélyegzők formátumaira vonatkozó specifikációk meghatározásáról;
- **Nytv.:** A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény;
- **Szmtv.:** A szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról szóló 2007. évi I. törvény;
- **Harmtv.:** A harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló 2007. évi II. törvény;
- **Ptk.:** a Polgári Törvénykönyvről szóló 2013. évi V. törvény;
- **Fgytv.:** A fogyasztóvédelemről szóló 1997. évi CLV. törvény;
- a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól szóló 45/2014 (II.

26.) Kormányrendelet;

- **GDPR:** az Európai Parlament és a Tanács (EU) 2016/679 rendelete 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;
- **Infotv.:** az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény;
- Közigazgatási Gyökér Hitelesítés-szolgáltató Hitelesítési Szabályzat;
- International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány-keretrendszer”;
- ISO 3166 English Country Names and Code Elements;
- FIPS PUB 140-2 (2001. május): "Kriptográfiai modulok biztonsági követelményei";
- RFC 5280 (korábban RFC 3280) és RFC 6818 Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány- és tanúsítvány visszavonási lista profil;
- RFC 3647 (korábban RFC 2527) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és Szolgáltatási Szabályzat keretrendszer - A szabályzatok szerkezete tekintetében;
- RFC 6960 Online Certificate Status Protocol (OCSP);
- RFC 6844 DNS Certification Authority Authorization (CAA) Resource Record;
- RFC 2616 Hypertext Transfer Protocol -- HTTP/1.1;
- RFC 6962 Certificate Transparency;
- **ETSI EN 319 401**; Electronic Signatures and Infrastructures (ESI) General Policy Requirements for Trust Service Providers;
- **ETSI EN 319 411-1** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- **ETSI EN 319 412-1** Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
- **ETSI EN 319 412-2** Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to natural persons;
- **ETSI EN 319 412-3** Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;
- **ETSI EN 319 412-4** Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;
- **ETSI TS 119 431-1** Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev;
- **ETSI TS 119 431-2** Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation;
- **ETSI TS 119 461** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- **ETSI TS 119 511** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- **ETSI EN 301 549** Accessibility requirements for ICT products and services;
- LCP: Lightweight Certificate Policy, Könnyített Hitelesítési Rend, OID: 0.4.0.2042.1.3;
- NCP: Normalized Certificate Policy, Normalizált Hitelesítési Rend, OID: 0.4.0.2042.1.1;
- NCP+: Extended Normalized Certificate Policy, Kiterjesztett (Kriptográfiai eszköz

használatát megkövetelő) Hitelesítési Rend, OID: 0.4.2042.1.2;

- EVCP: Extended Validation Certificate Policy: Kibővített ellenőrzésű weboldal-hitelesítő tanúsítványokra vonatkozó Hitelesítési Rend, 0.4.0.2042.1.4;
- CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates;
- CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Teljességi záradékot a Szolgáltató nem köt ki.

9.16.2 Átruházás

A szolgáltatások nyújtásába bevont Szolgáltatói partnerek csak a Szolgáltató előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és/vagy ruházhatják át kötelezettségeiket harmadik félnek.

9.16.3 Részleges érvénytelenség

Jelen Szabályzat egyes rendelkezéseinek bármilyen okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4 Igényérvényesítés

Szolgáltató kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei vagy ügyfelei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben a Szolgáltató egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben, vagy a Szolgáltatási szabályzat más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5 Vis maior

A Szolgáltató nem felelős a Szabályzatban megfogalmazott követelmények hibás vagy késedelmes teljesítéséért, ha a hiba vagy késedelem oka a Szolgáltató ellenőrzési körén kívül eső, előre nem látható körülmény volt.

9.17 Egyéb rendelkezések

Szolgáltató Regisztrációs és hitelesítő egységei a jelen szabályzat szerinti szolgáltatással kapcsolatos, saját felelősségi területükbe tartozó 3. és 4. fejezet szerinti tevékenységüket a Szolgáltató más szervezeti egységeitől függetlenül, saját hatáskörben végzik.

A Regisztrációs és Hitelesítő egység vezető munkatársa(i) független(ek) minden olyan üzleti, pénzügyi és más befolyástól, ami hátrányosan hathat a szolgáltatásokba vetett bizalomra.