Nem Minősített Nem Aláírás Célú Szolgáltatási Szabályzat



**NETLOCK Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság**

|  |  |
| --- | --- |
| *Azonosító szám (OID):* | **1.3.6.1.4.1.3555.1.49.20151014** |
| *Jóváhagyás időpontja:* | **2015.10.14** |
| *Hatály kezdőnapja:* | **2015.10.14** |
| *Oldalak száma:* | **102,** azaz százkettő |
| *Készítette:* | **Varga Viktor,** chief architect |
| *Ellenőrizte:*  | **dr. Lengyel Anett,** hatósági ügyintéző, belső ellenőr |
| *Jóváhagyta:* | **Dr. Szűcs Katalin,** cégvezető |
| ***COPYRIGHT, NETLOCK KFT. - MINDEN JOG FENNTARTVA*** |
| ***BELSŐ HASZNÁLATÚ*** |

|  |  |  |  |
| --- | --- | --- | --- |
| **OID** | **Változás leírása** | **Készítő** | **Ellenőrző** |
| 1.3.6.1.4.1.3555.1.49.20151014 | A korábbi DV SSL és általános fokozott tanúsítvány kiadást szabályozó szabályzatok helyett készült egyesített szabályzat.Első változat | NETLOCK Szabályzat Elfogadó Egység (SzEE) | NETLOCK Szabályzat Elfogadó Egység (SzEE) |

**TARTALOMJEGYZÉK**

## Tartalom

[1.1 Tartalom 3](#_Toc432709529)

[1. Bevezetés 11](#_Toc432709530)

[1.1. Áttekintés 11](#_Toc432709531)

[1.1.1 A Szabályzat 11](#_Toc432709532)

[1.1.2 A Szabályzat hatálya 11](#_Toc432709533)

[**1.1.3** **A** Szolgáltató 12](#_Toc432709534)

[1.1.4 Szolgáltatások 12](#_Toc432709535)

[1.1.5 Szabványok és előírások 12](#_Toc432709536)

[1.1.6 Hitelesítés-szolgáltatás és tanúsítványfajták 15](#_Toc432709537)

[1.1.7 Korlátozás 16](#_Toc432709538)

[1.1.8 Eszközszolgáltatás (autentikációs, titkosító és kódaláíró tanúsítványok esetében) 16](#_Toc432709539)

[1.1.9 Kulcsletét szolgáltatás (csak titkosító tanúsítványok esetében) 17](#_Toc432709540)

[1.2 Dokumentum neve és azonosítása 17](#_Toc432709541)

[1.3 PKI közösség 17](#_Toc432709542)

[1.3.1 Hitelesítő egységek 17](#_Toc432709543)

[1.3.2 Regisztrációs egységek 17](#_Toc432709544)

[1.3.3 Végfelhasználók 18](#_Toc432709545)

[1.4 Alkalmazhatóság 20](#_Toc432709546)

[1.4.1 Engedélyezett alkalmazási lehetőségek 20](#_Toc432709547)

[1.4.2 Korlátozott alkalmazási lehetőségek 20](#_Toc432709548)

[1.4.3 Tiltott alkalmazási lehetőségek 21](#_Toc432709549)

[1.5 Kapcsolattartás 22](#_Toc432709550)

[1.5.1 A Szolgáltató adatai 22](#_Toc432709551)

[1.5.2 Ügyfélszolgálat 22](#_Toc432709552)

[1.5.3 Szabályzattal kapcsolatos kérdések 22](#_Toc432709553)

[1.5.4 Szabályzat-jóváhagyási eljárás 22](#_Toc432709554)

[1.6 Fogalmak és rövidítések 23](#_Toc432709555)

[1.6.1 Fogalmak 23](#_Toc432709556)

[2 Közzététel és tanúsítványtár 27](#_Toc432709557)

[2.1 A Szolgáltatói információ közzététele 27](#_Toc432709558)

[2.1.1 Közzétételi és tájékoztatási elvek 27](#_Toc432709559)

[2.1.2 Kikötések és feltételek közzététele 27](#_Toc432709560)

[2.1.3 Rendkívüli információk közzététele 27](#_Toc432709561)

[2.1.4 CAA ellenőrzés 27](#_Toc432709562)

[2.1.5 Baseline előírásoknak megfelelés 27](#_Toc432709563)

[2.1.6 ETSI előírásoknak megfelelés 28](#_Toc432709564)

[2.2 Tanúsítványokkal kapcsolatos információk 29](#_Toc432709565)

[2.2.1 Tanúsítványok közzététele 29](#_Toc432709566)

[2.2.2 A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala 29](#_Toc432709567)

[2.2.3 Határidők meghatározása a tanúsítvány életciklusa kapcsán 29](#_Toc432709568)

[2.3 A közzététel gyakorisága 29](#_Toc432709569)

[2.3.1 Kikötések és feltételek közzétételi gyakorisága 29](#_Toc432709570)

[2.3.2 Rendkívüli információk közzétételi gyakorisága 29](#_Toc432709571)

[2.3.3 Tanúsítványok nyilvánosságra hozatalának gyakorisága 30](#_Toc432709572)

[2.3.4 A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága 30](#_Toc432709573)

[2.4 Hozzáférés ellenőrzések 30](#_Toc432709574)

[2.4.1 Tanúsítványtárak 30](#_Toc432709575)

[3 Azonosítás és hitelesítés 31](#_Toc432709576)

[3.1 Elnevezések 31](#_Toc432709577)

[3.1.1 Névtípusok 31](#_Toc432709578)

[3.1.2 Álnév/Márkanév használata 33](#_Toc432709579)

[3.1.3 Különböző elnevezési formák értelmezési szabályai 33](#_Toc432709580)

[3.1.4 A nevek egyedisége 35](#_Toc432709581)

[3.1.5 Védjegyek elismerése, hitelesítése és szerepe 35](#_Toc432709582)

[3.2 Kezdeti azonosítás 36](#_Toc432709583)

[3.2.1 A magánkulcs birtoklásának bizonyítási módszere 36](#_Toc432709584)

[3.2.2 Szervezeti azonosság hitelesítése 36](#_Toc432709585)

[3.2.3 Személyazonosság hitelesítése 36](#_Toc432709586)

[3.2.4 Domain birtokolásának hitelesítése 37](#_Toc432709587)

[3.3 Azonosítás tanúsítvány kulcscseréje esetén 37](#_Toc432709588)

[3.4 Visszavonási kérelem 37](#_Toc432709589)

[4 Működésre vonatkozó követelmények - tanúsítványok 38](#_Toc432709590)

[4.1 Tanúsítványigénylés 38](#_Toc432709591)

[4.1.1 Igénylés feltételei 38](#_Toc432709592)

[4.2 Tanúsítványkérelem feldolgozása 38](#_Toc432709593)

[4.2.1 Regisztrációs szabályok 39](#_Toc432709594)

[4.2.2 Ellenőrzésekre vonatkozó szabályok OV SSL tanúsítványok esetén 41](#_Toc432709595)

[4.2.3 Regisztrációs eljárások 43](#_Toc432709596)

[4.2.4 Szolgáltatási Szerződés 45](#_Toc432709597)

[4.2.5 Belépési nyilatkozat tartalma 46](#_Toc432709598)

[4.2.6 Tanúsítványkérelmek jóváhagyásának követelményei 46](#_Toc432709599)

[4.2.7 Tanúsítványok tartalma 47](#_Toc432709600)

[4.2.8 A tanúsítványok jellemzői 47](#_Toc432709601)

[4.2.9 Az Igénylő tájékoztatása a kibocsátást megelőzően 47](#_Toc432709602)

[4.2.10 Tanúsítványkérelmek elutasítása 48](#_Toc432709603)

[4.2.11 A tanúsítványokra vonatkozó további rendelkezések 48](#_Toc432709604)

[4.3 A tanúsítványok kibocsátása és hozzáférhetővé tétele 48](#_Toc432709605)

[4.3.1 DV tanúsítványok esetén 48](#_Toc432709606)

[4.3.2 Titkosító, összes típusú kódaláíró, autentikációs, OV SSL tanúsítványok esetén 49](#_Toc432709607)

[4.3.3 A tanúsítvány kibocsátásának időpontja 49](#_Toc432709608)

[4.3.4 A tanúsítvány érvényessége 49](#_Toc432709609)

[4.4 Tanúsítványelfogadás 49](#_Toc432709610)

[4.4.1 A tanúsítvány elfogadása 49](#_Toc432709611)

[4.4.2 A tanúsítványigénylő nyilatkozata 49](#_Toc432709612)

[4.4.3 Tanúsítvány közzététele 50](#_Toc432709613)

[4.5 A kulcspár és a tanúsítvány használata 50](#_Toc432709614)

[4.5.1 Az Igénylők számára szóló előírások 50](#_Toc432709615)

[4.5.2 Az Érintett Felek számára szóló ajánlások 51](#_Toc432709616)

[4.6 Tanúsítvány megújítása 51](#_Toc432709617)

[4.6.1 Végfelhasználói tanúsítványok 51](#_Toc432709618)

[4.6.2 Szolgáltatói tanúsítványok 52](#_Toc432709619)

[4.7 Kulcscsere 52](#_Toc432709620)

[4.8 Tanúsítvány módosítása 52](#_Toc432709621)

[4.9 Tanúsítvány felfüggesztése és visszavonása 53](#_Toc432709622)

[4.9.1 Általános rendelkezések 53](#_Toc432709623)

[4.9.2 A visszavonás körülményei 53](#_Toc432709624)

[4.9.3 Visszavonás kérelmezése 54](#_Toc432709625)

[4.9.4 Visszavonási kérelemre vonatkozó eljárás 54](#_Toc432709626)

[4.9.5 Visszavonási kérelemre vonatkozó türelmi idő 55](#_Toc432709627)

[4.9.6 Visszavonásra vonatkozó egyéb szabályok 56](#_Toc432709628)

[4.9.7 A felfüggesztés körülményei 56](#_Toc432709629)

[4.9.8 Felfüggesztés kérelmezése 56](#_Toc432709630)

[4.9.9 Felfüggesztési kérelemre vonatkozó eljárás 56](#_Toc432709631)

[4.9.10 A felfüggesztés időtartamára vonatkozó korlátozások 57](#_Toc432709632)

[4.9.11 Kulcskompromittálódás esetére vonatkozó speciális követelmények 57](#_Toc432709633)

[4.10 Tanúsítvány-állapot információk közzététele 57](#_Toc432709634)

[4.10.1 Tanúsítvány Visszavonási Lista (CRL) 57](#_Toc432709635)

[4.10.2 Az ajánlott CRL ellenőrzés az Érintett Fél számára 58](#_Toc432709636)

[4.10.3 Valós idejű visszavonási állapot ellenőrzés elérhetősége 58](#_Toc432709637)

[4.10.4 Valós idejű visszavonás ellenőrzési követelmények 58](#_Toc432709638)

[4.10.5 A visszavonási információ közzétételének egyéb formái 58](#_Toc432709639)

[4.11 Tanúsítvány-előfizetés vége 59](#_Toc432709640)

[4.12 Kulcs letétbe helyezése és visszaállítása 59](#_Toc432709641)

[5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések 60](#_Toc432709642)

[5.1 Fizikai óvintézkedések 60](#_Toc432709643)

[5.1.1 A telephely elhelyezése és szerkezeti felépítése 60](#_Toc432709644)

[5.1.2 A Second Site elhelyezése és szerkezeti felépítése 60](#_Toc432709645)

[5.1.3 Fizikai hozzáférés 61](#_Toc432709646)

[5.1.4 Áramellátás és légkondicionálás 61](#_Toc432709647)

[5.1.5 Beázás és elárasztódás veszélyeztetettsége 62](#_Toc432709648)

[5.1.6 Tűzmegelőzés és tűzvédelem 62](#_Toc432709649)

[5.1.7 Adathordozók tárolása 62](#_Toc432709650)

[5.1.8 Selejt kezelése, megsemmisítése 62](#_Toc432709651)

[5.1.9 Fizikailag elkülönítetten őrzött mentési példányok 62](#_Toc432709652)

[5.2 Eljárásbeli óvintézkedések 62](#_Toc432709653)

[5.2.1 Bizalmi munkakörök 62](#_Toc432709654)

[5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok 64](#_Toc432709655)

[5.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés 64](#_Toc432709656)

[5.2.4 Változáskezelés 64](#_Toc432709657)

[5.3 Személyzetre vonatkozó óvintézkedések 64](#_Toc432709658)

[5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények 65](#_Toc432709659)

[5.3.2 Biztonsági háttér ellenőrzésekre vonatkozó eljárások 65](#_Toc432709660)

[5.3.3 Képzési követelmények 65](#_Toc432709661)

[5.3.4 Továbbképzési gyakoriságok és követelmények 66](#_Toc432709662)

[5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje 66](#_Toc432709663)

[5.3.6 A felhatalmazás nélküli tevékenységek büntető következményei 66](#_Toc432709664)

[5.3.7 A szerződéses munkavállalókra vonatkozó követelmények 66](#_Toc432709665)

[5.3.8 A személyzet számára biztosított dokumentációk 66](#_Toc432709666)

[5.4 A biztonsági naplózás folyamatai 66](#_Toc432709667)

[5.4.1 A tárolt események típusai 66](#_Toc432709668)

[5.4.2 A napló állomány feldolgozásának gyakorisága 67](#_Toc432709669)

[5.4.3 A napló állomány megőrzési időtartama 67](#_Toc432709670)

[5.4.4 A napló állomány védelme 67](#_Toc432709671)

[5.4.5 A napló állomány mentési folyamatai 67](#_Toc432709672)

[5.4.6 A napló gyűjtési rendszere 67](#_Toc432709673)

[5.4.7 Az eseményeket kiváltó Igénylők értesítése 67](#_Toc432709674)

[5.4.8 Sebezhetőség felmérése 67](#_Toc432709675)

[5.5 Adatok archiválása 68](#_Toc432709676)

[5.5.1 A tárolt események típusai 68](#_Toc432709677)

[5.5.2 Az archívum megőrzési időtartama 68](#_Toc432709678)

[5.5.3 Az archívum védelme és hozzáférési szabályok 68](#_Toc432709679)

[5.5.4 Az archívum mentési folyamatai 68](#_Toc432709680)

[5.5.5 A rekordok időbélyegzésére vonatkozó követelmények 68](#_Toc432709681)

[5.5.6 Az archívum gyűjtési rendszere 68](#_Toc432709682)

[5.5.7 Archív információ hozzáférését és ellenőrzését végző eljárások 69](#_Toc432709683)

[5.5.8 Egyéb archiválási rendelkezések 69](#_Toc432709684)

[5.6 Biztonsági rendelkezések 69](#_Toc432709685)

[5.6.1 Biztonsági felülvizsgálati eljárások 69](#_Toc432709686)

[5.7 Helyreállítás kompromittálódás és katasztrófa esetén 69](#_Toc432709687)

[5.7.1 Incidens- és kompromittálódás-kezelési eljárások 69](#_Toc432709688)

[5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok 70](#_Toc432709689)

[5.7.3 Egy szolgáltatói egység kulcsának kompromittálódása 70](#_Toc432709690)

[5.7.4 Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően 70](#_Toc432709691)

[5.8 A Szolgáltató leállítása 70](#_Toc432709692)

[5.8.1 Szolgáltatás megszűntetése 70](#_Toc432709693)

[5.8.2 Regisztrációs pont megszűnése 71](#_Toc432709694)

[6 Műszaki biztonsági óvintézkedések 71](#_Toc432709695)

[6.1 Kulcspár előállítás és telepítés 72](#_Toc432709696)

[6.1.1 Kulcspár előállítás 72](#_Toc432709697)

[6.1.2 Magánkulcs eljuttatása az Igénylőhöz 73](#_Toc432709698)

[6.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz 73](#_Toc432709699)

[6.1.4 A szolgáltatói nyilvános kulcs közzététele 73](#_Toc432709700)

[6.1.5 Kulcsméretek 73](#_Toc432709701)

[6.1.6 A nyilvános kulcs paraméterek generálása és megfelelőségük ellenőrzése 74](#_Toc432709702)

[6.1.7 A kulcs használat célja (az X.509 v3 kulcshasználati mezők tartalmának megfelelően) 74](#_Toc432709703)

[6.2 A magánkulcsok védelme 74](#_Toc432709704)

[6.2.1 A szolgáltatói kulcsokra vonatkozó általános szabályok 74](#_Toc432709705)

[6.2.2 Magánkulcs letétbe helyezése 75](#_Toc432709706)

[6.2.3 Magánkulcs mentése 75](#_Toc432709707)

[6.2.4 Magánkulcs archiválása 75](#_Toc432709708)

[6.3 A kulcspár gondozásának egyéb szempontjai 75](#_Toc432709709)

[6.3.1 Egyéb kulcskezelési rendelkezések 75](#_Toc432709710)

[6.3.2 Nyilvános kulcs archiválása 75](#_Toc432709711)

[6.3.3 A nyilvános és magánkulcsok használatának periódusa 75](#_Toc432709712)

[6.4 Aktivizáló adatok 76](#_Toc432709713)

[6.4.1 Aktivizáló adatok előállítása és telepítése 76](#_Toc432709714)

[6.4.2 Az aktivizáló adatok védelme 76](#_Toc432709715)

[6.4.3 Az aktivizáló adatok egyéb szempontjai 76](#_Toc432709716)

[6.5 Számítógép-biztonsági óvintézkedések 76](#_Toc432709717)

[6.5.1 Speciális számítógép-biztonsági műszaki követelmények 77](#_Toc432709718)

[6.5.2 Informatikai biztonsági osztályozás 77](#_Toc432709719)

[6.6 Életciklusra vonatkozó műszaki óvintézkedések 77](#_Toc432709720)

[6.6.1 Rendszerfejlesztési óvintézkedések 77](#_Toc432709721)

[6.6.2 Biztonságkezelési óvintézkedések 78](#_Toc432709722)

[6.6.3 Az életciklusra vonatkozó biztonság osztályozása 78](#_Toc432709723)

[6.7 Hálózatbiztonsági óvintézkedések 78](#_Toc432709724)

[6.8 A kriptográfiai modul ellenőrzése 78](#_Toc432709725)

[6.8.1 Időforrás és időszinkronizáció 78](#_Toc432709726)

[6.8.2 Időforrások megnevezése 79](#_Toc432709727)

[6.8.3 Időforrás pontossága 79](#_Toc432709728)

[6.8.4 Alkalmazott eszközök 79](#_Toc432709729)

[7 Tanúsítvány, visszavonási lista, OCSP és időbélyeg profilok 80](#_Toc432709730)

[7.1 Végfelhasználói tanúsítványok profilja 80](#_Toc432709731)

[7.1.1 SSL profil DV 80](#_Toc432709732)

[7.1.2 SSL profil OV 81](#_Toc432709733)

[7.1.3 Személyes profil 82](#_Toc432709734)

[7.1.4 Munkatársi profil 83](#_Toc432709735)

[7.1.5 Szervezeti profil 84](#_Toc432709736)

[7.2 Szolgáltatói tanúsítványok 85](#_Toc432709737)

[7.2.1 Főtanúsítvány 85](#_Toc432709738)

[7.2.2 Kiadói (köztes) tanúsítvány 86](#_Toc432709739)

[7.2.3 OCSP válaszadó tanúsítvány 87](#_Toc432709740)

[7.2.4 Visszavonási lista aláírói tanúsítvány 88](#_Toc432709741)

[7.3 Tanúsítvány visszavonási lista profilok 89](#_Toc432709742)

[7.4 OCSP válasz profilok 89](#_Toc432709743)

[8 A megfelelőség vizsgálata 90](#_Toc432709744)

[8.1 A megfelelőség vizsgálatának gyakorisága 90](#_Toc432709745)

[8.2 Az átvizsgáló egységek megnevezése 90](#_Toc432709746)

[8.3 Az átvizsgáló egységek és a vizsgált fél kapcsolata 90](#_Toc432709747)

[8.4 A vizsgálat által érintett területek 91](#_Toc432709748)

[8.5 Hiányosságok esetén végrehajtandó tevékenységek 91](#_Toc432709749)

[9 Üzleti és jogi tudnivalók 92](#_Toc432709750)

[9.1 Díjak 92](#_Toc432709751)

[9.1.1 Egyéb szolgáltatásokra vonatkozó díjak 92](#_Toc432709752)

[9.1.2 Visszatérítési elvek 92](#_Toc432709753)

[9.2 Pénzügyi felelősség 93](#_Toc432709754)

[9.3 Bizalmasság, adatvédelem 93](#_Toc432709755)

[9.3.1 Bizalmasan kezelendő információ típusok 93](#_Toc432709756)

[9.3.2 Nem bizalmasnak tekintett információ típusok 94](#_Toc432709757)

[9.3.3 Tanúsítvány visszavonására / felfüggesztésére vonatkozó információ felfedése 94](#_Toc432709758)

[9.3.4 Szolgáltató leállása 94](#_Toc432709759)

[9.3.5 Az Igénylő kérésére történő felfedés 94](#_Toc432709760)

[9.3.6 Egyéb információ harmadik félnek történő átadása 94](#_Toc432709761)

[9.4 Szellemi alkotásokhoz fűződő jogok 94](#_Toc432709762)

[9.5 Jogok és kötelezettségek 94](#_Toc432709763)

[9.5.1 A hitelesítő egységek közös kötelezettségei 94](#_Toc432709764)

[9.5.2 A Regisztrációs Egységek közös kötelezettségei 95](#_Toc432709765)

[9.5.3 A végfelhasználó kötelezettségei 95](#_Toc432709766)

[9.5.4 Ajánlások az Érintett Fél részére 96](#_Toc432709767)

[9.5.5 Szolgáltató egyéb kötelezettségei 97](#_Toc432709768)

[9.5.6 A Szolgáltatói egységek közös kötelezettségei 97](#_Toc432709769)

[9.6 Felelősség 98](#_Toc432709770)

[9.6.1 A Szolgáltató általános felelőssége 98](#_Toc432709771)

[9.6.2 A végfelhasználó felelőssége 98](#_Toc432709772)

[9.6.3 Az Érintett Fél felelőssége 98](#_Toc432709773)

[9.7 Változtatási eljárás 99](#_Toc432709774)

[9.7.1 Szabályzat-változtatási eljárás 99](#_Toc432709775)

[9.7.2 Szabályzat Elfogadó Egység 99](#_Toc432709776)

[9.7.3 Értesítés nélkül változtatható elemek 100](#_Toc432709777)

[9.7.4 Értesítéssel változtatható elemek 100](#_Toc432709778)

[9.7.5 Szabályzati objektumazonosítót vagy mutatót változtató módosítások 100](#_Toc432709779)

[9.8 Panaszkezelési szabályok 100](#_Toc432709780)

[9.8.1 Panaszok benyújtásának helye 100](#_Toc432709781)

[9.8.2 Panaszok benyújtásának módja 100](#_Toc432709782)

[9.8.3 Panaszok kezelésének eljárása 100](#_Toc432709783)

[9.8.4 Illetékes fogyasztóvédelmi felügyelőség 100](#_Toc432709784)

[9.9 Hivatkozott jogszabályok, szabványok és egyéb dokumentumok 101](#_Toc432709785)

[9.10 Értelmezés és érvényesítés 101](#_Toc432709786)

[1.1.1 Irányadó jog 101](#_Toc432709787)

[1.1.2 A rendelkezések különválaszthatósága 101](#_Toc432709788)

[1.1.3 A rendelkezések jogfolytonossága 101](#_Toc432709789)

[1.1.4 A rendelkezések kiterjesztése 101](#_Toc432709790)

[9.10.1 Vitás kérdések megoldására vonatkozó eljárások 101](#_Toc432709791)

# Bevezetés

## Áttekintés

A jelen szabályzat a NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaságnak (a továbbiakban: Szolgáltató), nem minősített nem aláírás célú hitelesítés-szolgáltatásra vonatkozó Szolgáltatási Szabályzata (a továbbiakban: Nem Aláírás Célú Hitelesítés Szolgáltatási Szabályzat

**Jelen Szabályzat kizárólag nem minősített, nem aláírás célú tanúsítványokra (a továbbiakban: nem aláírás célú tanúsítványok) vonatkozó szabályokat tartalmazza.**

A Szolgáltató a folyamatos magas színvonalú szolgáltatás érdekében ISO 9001-es szabványnak megfelelő minőségbiztosítási rendszert üzemeltet, amelyet külső és belső, független szakértők évente több alkalommal is ellenőriznek. A Szolgáltató az általa kezelt információk, illetve általa nyújtott szolgáltatások bizalmasságának, integritásának és rendelkezésre állásának biztosítása érdekében ISO/IEC 27001 (korábban BS 7799-2:2002 elnevezésű) szabványnak megfelelő információbiztonsági irányítási rendszert is üzemeltet, amelynek megfelelőségét évente külső és belső, független ellenőrök és tanúsítók ellenőriznek.

A Szolgáltató legfelsőbb szintű hitelesítés-szolgáltatóként szerepel a legtöbb Microsoft termékben, Mozilla termékekben (Firefox), Mozilla Suite, számos egyéb szoftverben (Safari, Google Chrome, KDE Konqueror, Kmail, PGP, stb.), illetve Android és iPhone készülékek tanúsítvány-szolgáltatói listáján világszerte. Szolgáltatásaiért viszontbiztosítással rendelkező biztosító társaság vállal felelősséget.

### A Szabályzat

Jelen Szolgáltatási Szabályzat a Szolgáltató nem minősített, nem aláírás célú szolgáltatásokként nyújtott szolgáltatásaival kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazza.

A Szabályzat összefoglalóan tartalmazza mindazon szabályokat, információkat, melyek a Szolgáltató tevékenységével kapcsolatosak, és amelyeket a Szolgáltatóval valamilyen módon kapcsolatba kerülőknek (elsősorban a végfelhasználóknak és érintett feleknek) érdemes tudni. Mint ilyen, a Szolgáltató működésének átláthatóságát biztosítja, és lehetővé teszi a felhasználók számára, hogy megállapítsák, hogy a Szolgáltató gyakorlatai, illetve adott tanúsítványfajtája mennyiben felel meg elvárásaiknak. A Szabályzat ellenőrzésével a tanúsítvány elfogadói egyértelműen meg kell tudják állapítani a tanúsítvány kezelésének módját, az általa garantált biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügyi garanciákat, jogi felelősségvállalásokat.

A jelen Szabályzat tartalmára és felépítésére az RFC 3647 [8] dokumentum adott útmutatót.

### A Szabályzat hatálya

#### Tárgyi hatály

A Szabályzat tárgyi hatálya az 1.1.4 pontban ismertetett szolgáltatások nyújtását és igénybevételét foglalja magában.

#### Időbeli hatály

A Szabályzat időbeli hatálya a jelen verzió hatálybalépésének dátumától kezdődik, és a szolgáltatási tevékenység beszüntetéséig, illetve egy újabb szabályzat verzió hatályba lépéséig tart.

#### Személyi hatály

A Szabályzat személyi hatálya a Felhasználóra és a Szolgáltatóra terjed ki.

### **A** Szolgáltató

A jelen Szabályzatban Szolgáltatónak nevezett entitás a NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság. Cégjegyzékszáma: 01-09-563961.

Önkéntes akkreditáció, egyéb minősítések:

* ISO 9001 (2001. óta folyamatosan)
* BS 7799-2
* ISO/IEC 27001 (2005. óta folyamatosan)

### Szolgáltatások

A Szolgáltató jelen szabályzatot érintő tevékenységi köre: nem aláírás célú hitelesítés szolgáltatás.

### Szabványok és előírások

#### Szolgáltatási Szabályzat

A Szabályzat az RFC 3647 [4] szabványa alapján készült. A Szabályzat tartalmi vonatkozások kapcsán az x.509 [5] szabvány ajánlásait.

#### Lenyomatképző algoritmusok azonosítói

* RIPE-MD160OID ::= { iso(1) identified-organization(3) TeleTrusT(36) algorithm(3) hashAlgorithm(2) RIDEMD-160 (1) }
* 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)}

A Szolgáltató figyelemmel kíséri a kriptográfiai algoritmusok alkalmazhatóságára vonatkozó, irányadó nemzetközi dokumentumokat, és az itt meghatározott algoritmusokat az ezen dokumentumokban foglalt irányadó előírások szerint alkalmazza.

#### Kriptográfiai algoritmusok azonosítói

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

#### Tanúsítvány kiterjesztések azonosítói

* KeyUsage OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) certificateExtension (29) 15 }
* EnhancedKeyUsage OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) certificateExtension (29) 37 }
* BasicConstraints OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) certificateExtension (29) 19 }
* CertificatePolicies OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) certificateExtension (29) 32 }
* AIA:OCSP OID ::= {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) 1}
* AIA:CAIssuers OID ::= {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) 2}
* CRL Distribution Point OID ::= { Joint ISO/ITU-T assignment(2) X.500 Directory Services(5) objectClass(6) 19}

#### Szabályzat azonosítók

##### CAB fórum azonosítók

A CA az előírásoknak megfelelően a CAB fórum által fenntartott azonosítókat helyez el a tanúsítvány CertificatePolicies mezőjébe.

DV SSL tanúsítványok esetén - joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)

Az OID jelentése a tanúsítványban, hogy az ellenőrzés nem terjedt ki entitásra, a tanúsítvány nem tartalmazhat ez esetben organizationName, streetAddress, localityName, stateOrProvinceName, postalCode mezőket a tanúsítvány Subject szekciójában.

OV SSL tanúsítványok esetén - {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) subject-identity-validated(2)} (2.23.140.1.2.2)

Az OID jelentése a tanúsítványban, hogy az ellenőrzés nem kiterjedt entitásra, és a tanúsítvány tartalmazza az organizationName, localityName, stateOrProvinceName (ha értelmezhető) countryName in the Subject field. hat ez esetben organizationName, streetAddress, localityName, stateOrProvinceName (opcionálisan), postalCode mezőket a tanúsítvány Subject szekciójában.

##### ETSI 102042 azonosítók

Az ETSI 102042 által felsorol azonosítók a következők:

NCP: Normalized Certificate Policy

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)

NCP+: Normalized Certificate Policy biztonságos eszközön tárolással

itu-t(0) identified-organization(4) etsi(0)other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)

LCP: Lightweight Certificate Policy

itu-t(0) identified-organization(4) etsi(0)other-certificate-policies(2042) policy-identifiers(1) lcp (3)

EVCP: Extended Validation Certificate Policy

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcp (4)

EVCP+: Extended Validation Certificate Policy biztonságos eszközön tárolással

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcpplus (5)

Az alábbi ETSI azonosítók a teljesség kedvéért szereplnek, helyettük a CAB Fórum megfelelő OID-je kerül felhasználásra.

DVCP: Domain Validation Certificate Policy

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) dvcp (6)

OVCP: Organizational Validation Certificate Policy

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042)

policy-identifiers(1) ovcp (7)

#### Alkalmazott formátumok

|  |  |
| --- | --- |
| **Tétel** | **Alkalmazott / elfogadott formátum, szabvány** |
| Magánkulcs | PKCS12 PEM, PKCS12 DER |
| Kérelem | PKCS10 PEM  |
| Tanúsítvány | X509 PEM, X509 DER, X509 PKCS7 |
| CRL | X509 PEM, X509 DER, X509 PKCS7 |
| OCSP | RFC 2560 Online Certificate Status Protocol (OCSP) |

### Hitelesítés-szolgáltatás és tanúsítványfajták

A Szolgáltató előzetes entitásazonosítás után az Igénylők (későbbi Igénylőok) számára nem aláírás célú tanúsítványt bocsát ki.

A tanúsítvány a hitelesítés-szolgáltató által kibocsátott igazolás, amely a nyilvános kulcsot egy meghatározott személyhez, szervezethez vagy entitáshoz kapcsolja, és igazolja a személy személyazonosságát vagy valamely más tény fennállását, ideértve - amennyiben értelmezett - a hatósági (hivatali) jelleget.

A Szolgáltató jelen szabályzat szerint szabályozott végfelhasználói tanúsítványfajták összefoglaló táblázata az alábbi.

| **Fajta** | **Igénylő** | **Engedélyezett alkalmazási cél** | **Tiltott alkalmazások** | **Hitelesítés biztonságát védő joghatás** |
| --- | --- | --- | --- | --- |
| DV SSL tanúsítvány | Igénylő | Szerver(ek) azonosítása, titkosított kommunikáció | Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli, stb.) megszegése | Büntető és polgári jogi felelősség |
| OV SSL tanúsítvány | Szervezet vagy Magánszemély | Szerver(ek) azonosítása, titkosított kommunikáció | Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli, stb.) megszegése | Büntető és polgári jogi felelősség |
| Kliens oldali authentikációs tanúsítvány  | Természetes személyTermészetes személy, szervezet tagjakéntSzervezet, természetes személyhez nem kötött formában | Tanúsítvány Igénylő azonosítása, bejelentkezés | Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése | Büntető és polgári jogi felelősség |
| Kódaláíró (code signing) | Természetes személyTermészetes személy, szervezet tagjakéntSzervezet, természetes személyhez nem kötött formában | Futtatható kód aláírása fejlesztő vagy a terjesztő hitelesítéséhezFuttatható kód sértetlenségének védelme | Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése | Büntető és polgári jogi felelősség |
| Kernel Mode kódaláíró (Kernel mode code signing) | Szervezet | Futtatható kód aláírása fejlesztő vagy a terjesztő hitelesítéséhezFuttatható kód sértetlenségének védelme | Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése | Büntető és polgári jogi felelősség |
| Titkosító | Természetes személyTermészetes személy, szervezet tagjakéntSzervezet, természetes személyhez nem kötött formában | Kommunikáció, adatok titkosítása, illetve visszafejtése | Bármilyen korlátozás (földrajzi, tárgybeli, értékbeli, időbeli stb.) megszegése | Büntető és polgári jogi felelősség |

Az Igénylőnek egyéni mérlegelési joga és felelőssége, hogy a Szolgáltató szabályzatai alapján meghatározza, milyen tanúsítványt alkalmaz egy adott célra. Ugyanígy az Érintett Félnek is egyéni mérlegelési joga és felelőssége, hogy a Szolgáltató szabályzatai alapján meghatározza, milyen tanúsítványt fogad el egy adott célra.

### Korlátozás

Jelen szabályzat alapján kiadott tanúsítványok csak az engedélyezett alkalmazási célokra használhatók fel, minden egyéb mód tiltott.

Az SSL tanúsítvány szolgáltatáshoz joghatás nem kapcsolódik, használata kizárólag műszaki előnyöket biztosít. A tanúsítvány a szerver azonosítását végzi a felhasználó felé és biztosítja a titkosított kommunikációt.

A titkosító tanúsítványhoz joghatás nem kapcsolódik, használata kizárólag műszaki előnyöket biztosít. Lehetővé teszi, hogy a tanúsítvánnyal rendelkező fél titkosított emaileket és fájlokat fogadjon.

Az autentikációs tanúsítványhoz joghatás nem kapcsolódik, használata kizárólag műszaki előnyöket biztosít. Olyan tanúsítvány, mellyel különböző rendszerekbe authentikáció végezhető.

A kódaláíró tanúsítványhoz joghatás nem kapcsolódik, használata kizárólag műszaki előnyöket biztosít. A tanúsítvánnyal végzett aláírás kódok forrását azonosítja, illetve azok módosítását gátolja meg.

### Eszközszolgáltatás (autentikációs, titkosító és kódaláíró tanúsítványok esetében)

Eszközszolgáltatás csak autentikációs és titkosítási, kódaláíró szolgáltatásnál értelmezett.

Eszközszolgáltatás keretében a Szolgáltató kulcstároló eszközön kulcselhelyezési szolgáltatást végez, melynek során jelen Szabályzat rendelkezéseinek figyelembe vételével az Igénylő számára kulcspárt generál a kulcstároló eszközre vagy kulcsgenerálást végez a kulcstároló eszközön kívül, majd elvégzi annak eszközre töltését.

Kódaláíró tanúsítványok esetén, egyes előírások miatt kötelező lehet az eszközszolgáltatás igénybe vétele, melynek részleteiről a szolgáltatás használata során tájékozódhat.

Eszközszolgáltatás biztosítása során a Szolgáltató:

* a kulcspár generálását az irányadó nemzetközi előírások, szabványok által műszakilag alkalmasnak minősített kriptográfiai algoritmus felhasználásával végzi, illetve igénylés esetén külön díj fejében az eszközt megszemélyesíti;
* a kulcsok generálását és az Igénylőhöz történő továbbítását megelőző tárolását biztonságosan végzi;
* ha a kulcspár előállítása a kulcstároló eszközön kívül történik, a Szolgáltató a kulcspárt biztonságos módon juttatja a kulcstároló eszközbe. Ezt követően a magánkulcs kulcstároló eszközön kívüli másolatait megsemmisíti, kivéve, ha a tanúsítványtípus vonatkozásában a kulcsletét szolgáltatás igénybevétele biztosított, és ezen Szolgáltatást az Igénylő igénybe kívánja venni;
* gondoskodik arról, hogy - a kulcsletét szolgáltatás esetét kivéve - az Igénylő részére átadott kulcspár magánkulcsa az átadást követően semmilyen módon ne kerüljön tárolásra;
* gondoskodik az általa biztosított kulcstároló eszköz kibocsátásakor az eljárás biztonságosságáról;
* biztosítja, hogy a kulcsgenerálást követően, a kulcstároló eszköz a szándék szerinti, hitelesített Igénylőhoz kerül;
* gondoskodik róla, hogy a saját munkavállalói ne élhessenek vissza a kulcstároló eszközzel a következőképpen: aktivizáló adatok megismerése, magánkulcsok, tanúsítványok használata;
* a kulcstároló eszköz előkészítése és továbbítása során alkalmazza a biztonsági eljárásokat;
* a tanúsítvány csak az átadás után lesz érvényes.

### Kulcsletét szolgáltatás (csak titkosító tanúsítványok esetében)

A Szolgáltató a titkosító tanúsítványok kapcsán kulcsletét szolgáltatást nyújthat, melynek során a kibocsátott tanúsítványhoz tartozó kulcspárt a Szolgáltató az Igénylő további rendelkezéséig számára megőrzi. A Szolgáltató biztosítja, hogy a megőrzésében levő kulcspárhoz illetéktelenül sem saját munkavállalói, sem harmadik fél nem fér hozzá.

## Dokumentum neve és azonosítása

Jelen dokumentum:

* Jelen dokumentum teljes neve: NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság Nem Aláírás Célú Hitelesítés Szolgáltatás Szolgáltatási Szabályzata
* Rövid neve: Nem Aláírás Célú Hitelesítés Szolgáltatási Szabályzat
* Verziószáma: a fedlapon található egyedi azonosító (OID)

A Szabályzat hivatalos és aktuális verziója megtalálható és letölthető:

* Szolgáltató Internetes elérhetősége: [www.netlock.hu](http://www.netlock.hu)

## PKI közösség

A kibocsátott tanúsítványok és kulcstároló eszközök alkalmazó közössége a Szolgáltató, a vele szerződéses kapcsolatban álló regisztrációs és egyéb közreműködő szervezetek, a tanúsítványok végfelhasználói és az érintett felek.

### Hitelesítő egységek

A Szolgáltató saját szervezetén belül hitelesítő egységeket működtet, amelyek feladata a tanúsítványok központi létrehozása és kezelése a regisztrációs egységektől kapott kérelmeknek megfelelően.

A Hitelesítő Egység az előírt eljárási rend szerint a hozzá tartozó regisztrációs egységek kérelme alapján tanúsítványok kiadását, publikálását, visszavonását, felfüggesztését végzi. A Tanúsítvány Visszavonási Lista (a továbbiakban: CRL) publikálását automatizált szolgáltatói egység végzi.

|  |  |
| --- | --- |
| **Név:** | **Hitelesítő Egység** |
| Egység: | NETLOCK Kft.  |
| Cím: | 1101 Budapest, Expo tér 5-7.  |
| Telefon: | +36 40 22-55-22+36 (1) 437 6655 (külföldről) |
| Fax | +36 (1) 345-2250 |
| Internet cím: | [www.netlock.hu](http://www.netlock.hu) |
| E-mail: | info@netlock.hu |

### Regisztrációs egységek

A Szolgáltató Központi Regisztrációs Egységet, Mobil Regisztrációs Munkatársakat, Kihelyezett Regisztrációs Egységeket, valamint Regisztrációs- és Kézbesítési Megbízottakat alkalmaz, amelyek feladata a kezdeti regisztráció és a tanúsítvány kibocsátásával kapcsolatos egyéb tevékenységekben való részvétel.

Alapesetben a Központi Regisztrációs Egység feladata az Igénylő – ha van, akkor a másodlagos Alany is – kezdeti azonosítása (okmányok begyűjtése), adatainak ellenőrzése nyilvántartásban, kibocsátás során elektronikus kérelem-feldolgozási tevékenység, eljárási lépések koordinálása, dokumentálás, s további tanúsítványkezelési feladatok, többek között a felhasználókkal való kapcsolattartás. Egyes esetekben a kezdeti azonosításhoz szükséges okmányok begyűjtését a Központi Regisztrációs egység felügyelete és irányítása alatt álló Mobil Regisztrációs Munkatársak, valamint a Kihelyezett Regisztrációs Egység munkatársai végzik. Az ügyfélszolgálati teendőket, valamint a felhasználókkal való elsődleges kapcsolattartást a Szolgáltató külön erre a feladatra alkalmazott vevőszolgálati munkatársai végzik. Az ügyfélszolgálati munkatársak a Központi Regisztrációs Egységen belül alkotnak önálló csoportot.

A fentieken túl a Központi Regisztrációs Egység a regisztrációs eljárás egészének helyességét és szabályzatoknak való megfelelését ellenőrzi. A központi regisztrációs egység munkatársainak felelőssége a tanúsítvánnyal kapcsolatos végső döntések meghozatala is.

A Szolgáltatási Szerződés aláírására és/vagy az eszközátadásra a megrendelő vagy ügyfél választása valamint a választott terméknél elérhető lehetőségek alapján az alábbiak valamelyike szerint kerül sor:

* a Központi Regisztrációs Egység előtt, a Szolgáltató vagy megbízottja székhelyén, vagy
* a Mobil Regisztrációs Munkatárs előtt, Magyarország területén, vagy
* a Regisztrációs és Kézbesítési Megbízott előtt, Magyarország területén
* közjegyző előtt
* a szolgáltató által szabályozott egyéb módon

A regisztrációs munkatársak, valamint a Regisztrációs és Kézbesítési Megbízottak tanúsítvány-kibocsátás során, - amennyiben értelmezett - személyes megjelenés mellett, a felhasználói adatellenőrzést végzik, amely tevékenységüket az iparági szabványok követelményeinek megfelelően végzik. Az ügyfél választása szerint ők végzik az eszközátadást is, amennyiben ez értelmezhető és amennyiben az ügyfél nem jelent meg érte a Központi Regisztrációs Egység előtt.

A Szolgáltató a későbbiekben egyéb szervezetekkel is szerződést köthet regisztrációs szolgáltatások elvégzésére, illetve jogszabály megállapíthat egyéb regisztrációs egységként működő szervezeteket. Az így létrejövő regisztrációs pontok és közreműködők listáját a Szolgáltató honlapján publikálja.

DV SSL tanúsítvány szolgáltatásánál a regisztrációs egység nem értelmezett.

|  |  |
| --- | --- |
| **Név:** | **Hitelesítő Egység** |
| Egység: | NETLOCK Kft.  |
| Cím: | 1101 Budapest, Expo tér 5-7.  |
| Telefon: | +36 40 22-55-22+36 (1) 437 6655 (külföldről) |
| Fax | +36 (1) 345-2250 |
| Internet cím: | www.netlock.hu |
| E-mail: | info@netlock.hu |

### Végfelhasználók

A tanúsítványban annak Igénylője meg kerül nevezésre, a tanúsítvány típusától függő mezőben.

A Szolgáltató jelen szabályzat alapján a következő entitások részére bocsát ki különféle tanúsítványokat:

#### DV SSL tanúsítványok

Az Igénylő nem kerül megnevezésre, a tanúsítvány a technikai ellenőrzéssel sikeresen ellenőrzött domain nevet tartalmazza.

Igénylőnek a megrendelő minősül.

#### OV/IV SSL tanúsítványok

Az Igénylő megnevezésre kerül az O mezőben.

Az Igénylő lehet szervezet és magánszemély.

#### Titkosító tanúsítványok

A Szolgáltató jelen szabályzat alapján a következő entitások részére bocsát ki titkosító tanúsítványokat:

* természetes személyeknek – személyes tanúsítvány
* természetes személyeknek egy adott szervezethez tartozóként – munkatársi tanúsítvány
* nem természetes személyek részére – szervezeti tanúsítvány

#### Autentikációs tanúsítvány

A Szolgáltató jelen szabályzat alapján a következő entitások részére bocsát ki autentikációs tanúsítványokat:

* természetes személyeknek – személyes tanúsítvány
* természetes személyeknek egy adott szervezethez tartozóként – munkatársi tanúsítvány
* nem természetes személyek részére – szervezeti tanúsítvány

#### Kódaláíró tanúsítvány

A Szolgáltató jelen szabályzat alapján a következő entitások részére bocsát ki kódaláíró tanúsítványokat:

* természetes személyeknek – személyes tanúsítvány
* természetes személyeknek egy adott szervezethez tartozóként – munkatársi tanúsítvány
* nem természetes személyek részére – szervezeti tanúsítvány

#### Kernel módú kódaláíró tanúsítvány

A Szolgáltató jelen szabályzat alapján a következő entitások részére bocsát ki Kernel mód kódaláíró tanúsítványokat:

* nem természetes személyek részére – szervezeti tanúsítvány

## Alkalmazhatóság

### Engedélyezett alkalmazási lehetőségek

A kibocsátott végfelhasználói tanúsítványokba foglalt nyilvános kulcsok, illetve az ahhoz tartozó magánkulcsok az alábbi célokra használhatók fel:

#### DV, OV SSL tanúsítvány

A tanúsítványba foglalt kulcsok segítségével titkosított kapcsolat biztosítása szerver és kliens között.

A szerver pontos azonosítása a kliens szoftver felé, a tanúsítványban található szerverazonosító adat, és kliens szoftverben található elérési adat összehasonlításával.

#### Titkosító tanúsítvány

adatelkódolás (titkosítás) a tanúsítványba foglalt nyilvános kulccsal történő, illetve az adat dekódolása a magánkulccsal.

#### Authentikációs tanúsítvány

véletlen adaton történő hitelesítés végzése azonosítás céljából, a tanúsítványhoz tartozó magánkulccsal. A végzett művelet technikailag megegyezik az aláírással, de joghatás nem rendelődik hozzá.

#### Kódaláíró tanúsítvány

futtatható kód aláírása a tanúsítványban foglalt nyilvános kulcs magánkulcs-párjával, melynek ellenőrzése a tanúsítványban foglalt nyilvános kulccsal történik meg;

#### Kernel módú kódaláíró tanúsítvány

▪ Windows kernel és user szintű driver kód aláírása a tanúsítványban foglalt nyilvános kulcs magánkulcs-párjával, melynek ellenőrzése a tanúsítványban foglalt nyilvános kulccsal történik meg

#### Szolgáltatói kiadói tanúsítvány

A Szolgáltatói kiadói tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai tanúsítványhitelesítésre és CRL listák hitelesítésére, valamint a Szolgáltatói OCSP tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai az OCSP szolgáltatás hitelesítésére használhatók fel.

### Korlátozott alkalmazási lehetőségek

A Szolgáltató a jelen Szolgáltatási Szabályzatban leírt felhasználási feltételekkel korlátozza a kibocsátott tanúsítványok felhasználhatóságát (lásd 6.1.7 pont). A hatályos jogszabályok ugyancsak korlátozhatják a kibocsátott tanúsítványok felhasználhatóságát.

Az egyes tanúsítványfajtáknak megfelelő konkrét korlátozásokat lásd még a tanúsítványfajtáknál (1.1.6 pont), illetve a tanúsítványfajtákhoz tartozó profiloknál (7. fejezet).

### Tiltott alkalmazási lehetőségek

A tanúsítványok használatára vonatkozó bármely korlátozást (ld. előző pont) megszegő alkalmazása tilos.

A végfelhasználói tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai más nyilvános kulcsú tanúsítványok aláírására történő felhasználása, vagy bármilyen hitelesítés-szolgáltatás nyújtásához történő alkalmazása tilos.

A szolgáltatói kiadói tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai csak tanúsítványhitelesítésre és CRL listák hitelesítésére használhatók, egyéb más szolgáltatás nyújtásához történő alkalmazása tilos. A szolgáltatói OCSP tanúsítványokba foglalt nyilvános kulcsok magánkulcs párjai csak OCSP szolgáltatás során használhatók fel; egyéb más szolgáltatás nyújtásához történő alkalmazásuk tilos.

## Kapcsolattartás

### A Szolgáltató adatai

|  |  |
| --- | --- |
| **Név:** | **NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság** |
| **Egység:** | **NETLOCK Kft.**  |
| **Székhely:** | **1101 Budapest, Expo tér 5-7.** |
| **Telefon:** | **+36 (40) 22-55-22****+36 (1) 437 6655 (külföldről)** |
| **Fax:** | **+36 (1) 700-1101** |
| **Internet cím:** | [**www.netlock.hu**](http://www.netlock.hu) |
| **E-mail:** | **info@netlock.hu** |
| **Ügyfélfogadás/Nyitva tartás** | **Munkanapokon 9:00-17:00** |

### Ügyfélszolgálat

A szolgáltatással kapcsolatos kérdésekkel, problémákkal a végfelhasználók a Központi Regisztrációs Egység ügyfélszolgálati munkatársaihoz fordulhatnak szóban vagy írásban, az alábbiakban megadott módon. A Szolgáltató az Interneten információs szolgáltatást működtet.

A Szolgáltató internetes információs rendszere, telefonközpontja és e-mail fiókjai minden nap 0–24 óráig fogadják a bejelentéseket. A Szolgáltató legkésőbb a bejelentést követő 3. munkanapon felveszi a kapcsolatot a bejelentővel (válasz e-mail cím birtokában) és a bejelentőt a tartalmi válasz megérkezésének várható idejéről is tájékoztatja.

A Szolgáltató ügyfélszolgálati munkatársai 1.5.1 pontban meghatározott időpontban személyesen is fogadják az Ügyfeleket, Érintett Feleket, valamint az egyéb érdekelteket.

A szolgáltató az egyes szolgáltatási területeken eltérő kapcsolattartási lehetőségeket biztosít:

DV SSL tanúsítvány kiadás szolgáltatás esetén: interneten keresztül, online formában, 0-24 között; emailen keresztül munkanapokon 9-17 CET között

OV SSL tanúsítvány kiadás szolgáltatás esetén: interneten keresztül, online formában, 0-24 között; emailen és telefonon keresztül (magyar és angol nyelven) munkanapokon 9-17 CET között

Az összes típusú kódaláíró, titkosító és autetnikációs tanúsítvány kiadás szolgáltatás esetén: interneten keresztül, online formában, 0-24 között; emailen és telefonon keresztül (magyar és angol nyelven) munkanapokon 9-17 CET között

### Szabályzattal kapcsolatos kérdések

A Szolgáltató szabályzatainak karbantartását a Szabályzat Elfogadó Egység végzi. A szabályzatokkal és szerződésekkel kapcsolatos kérdésekkel és észrevételekkel a regisztrációs egységek, a Szolgáltató ügyfélszolgálata, vagy közvetlenül a Szabályzat Elfogadó Egység kereshető meg az info@NETLOCK.hu e-mail címen (ld. még 9.7.2 pont).

### Szabályzat-jóváhagyási eljárás

Lásd 9.7 pont.

## Fogalmak és rövidítések

### Fogalmak

**Igénylő:** A tanúsítvány Igénylő (Subject) mezőjében megadott adatokkal meghatározott természetes személy, aki a tanúsítványban szereplő nyilvános kulcs párját jelentő magánkulcs felett rendelkezik.

**(Papír alapú) Aláírás-hitelesítés**: Az az eljárás, melynek során az Igénylő a személyazonosságának igazolása után a Szolgáltatási Szerződést a regisztrációs feladatot ellátó munkatárs, megbízott vagy közreműködő előtt kézjegyével ellátja, vagy a dokumentumokon levő aláírást a sajátjának ismeri el (a továbbiakban: aláírja), a regisztrációs feladatot ellátó munkatárs, megbízott vagy közreműködő pedig írásban igazolja az aláírás tényét, feltüntetve az aláíró személy személyazonosító adatait.

**Aláíró:** a szerződést aláíró természetes személy.

**Alkalmazó Közösség**: A PKI rendszert alkalmazó, működtető entitások összessége.

**Általános Szerződési Feltételek (ÁSZF):** A Szolgáltató szolgáltatásainak, tanúsítványainak igénybevételéhez szükséges feltételeket, illetve egyéb szerződési feltételeket leíró dokumentum.

**Belépési Nyilatkozat:** Elsődlegesen az ÁSZF és a Szolgáltatási Szabályzat elfogadását jelző, aláírt dokumentum. A Belépési Nyilatkozat a Szolgáltató által meghatározott esetekben a Szolgáltatási Szerződéssel egyenértékűnek minősül (lásd: Szolgáltatási Szerződés).

**Common Name (CN):** Az Igénylő tanúsítványban szereplő, szokásos megnevezéséből képzett neve vagy az Igénylő által megjelölt álnévből képzett karaktersorozat. SSL tanúsítványok esetén az Igénylő által megadott 1 db domain nevet tartalmaz.

**CRL:** lásd: Tanúsítvány visszavonási lista

**Distinguished Name (DN):** A tanúsítványban szereplő, szokásos megnevezéséből, lakóhely vagy székhely szerinti város, ország megnevezéséből, valamint e-mail címéből képzett egyedi neve.

**DV (vagy automata) SSL:** olyan, szerverek számára kibocsátott SSL tanúsítvány, melynél kizárólag a domain feletti felügyeleti képesség kerül ellenőrzésre.

**Elektronikus aláírás:** Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.

**Ellenőrzési lépések:** A tanúsítványok használata során az Érintett Felek által kötelezően végrehajtandó lépések, melyeket a Szabályzat tartalmaz.

**Eredeti példány:** Magán- vagy jogi személyazonosító okmány eredeti aláírásokat és pecsétet tartalmazó példánya, vagy ezek hitelesített másolata.

**Érintett Fél:** Az a személy, aki elektronikus aláírás érvényességének ellenőrzése céljából a Szolgáltató által kibocsátott tanúsítványhoz fordul.

**Eszközszolgáltatás:** Az a szolgáltatás, melynek során a Szolgáltató a magánkulcsot, valamint a nyilvános kulcsot elhelyezi kulcshordozó eszközön.

**Felhasználó:** Szerződéses partner, aki közvetlenül vagy közvetett módon, az általa megbízott személyen keresztül igénybe veszi a Szolgáltató valamely szolgáltatását.

**Fizikailag biztosított terület:** Olyan helyiség, amely ésszerű határok mellett képes megvédeni a benne elhelyezett eszközöket az elemi károktól, illetve a szándékos, illetéktelen hozzáféréstől.

**Folyamatosan elérhető szolgáltatás:** Az év 365 napján a nap 24 órájában elérhető szolgáltatás, a Szolgáltató szabályzataiban meghatározott rendelkezésre állási időkkel.

**FQDN (Fully Qualified Domain Name):** Olyan domain név, amely a nevet DNS szerveren keresztül lekérdezve publikus, mindenki számára elérhető hálózati IP címre oldja fel.

**Hash:** Ld. Lenyomat.

**Hitelesítő Egységek:** A végfelhasználói tanúsítványokat létrehozó egységek a Szolgáltatónál.

**Hitelesítési rend:** szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely tanúsítvány felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.

**Hozzáférések:** Egy adott számítógépes hálózat vagy annak egyes elemei elérésére vonatkozó szabályok összessége.

**Igénylő:** Megegyezhet az Alannyal, vagy az Igénylő felkérésére tanúsítvány igénylést/rendelést hajthat végre.

**IV (individual/identity validation) SSL:** olyan SSL tanúsítvány, melynek kiadása során az igénylést végző személy kerül ellenőrzésre.

**Kihelyezett Regisztrációs Egység:** olyan, a Szolgáltatóval szerződéses jogviszonyban álló személy és/vagy szervezet, mely feladata, hogy a Szolgáltató munkáját segítse a tanúsítvány kibocsátásához szükséges dokumentumok összegyűjtésében, ellássa a tanúsítvány kibocsátásával kapcsolatos koordinációs feladatokat, valamint – adott esetben – részt vegyen az ügyféllel való kapcsolattartásban.

**Közhiteles nyilvántartás:** olyan, hatóság által vezetett nyilvántartás, melynek tartalmát, az abban szereplő adatok valódiságát az ellenkező bizonyításig mindenki köteles elfogadni.

 **(Kriptográfiai) Kulcs(pár)**: Kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete rejtjelezéshez és visszaállításhoz szükséges.

**Közjegyző:** Olyan személy, aki a vonatkozó jogrend alapján nem csak jogosult, hogy az aláírást hitelesítse, hanem a dokumentum tartalmáért és helyességéért is felelős.

**Lenyomat**: Olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti a következő feltételeket:

a képzett lenyomat egyértelműen származtatható az adott elektronikus dokumentumból,

a képzett lenyomatból az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés,

a képzett lenyomat alapján az elvárható biztonsági szinten belül nem lehetséges olyan elektronikus dokumentum utólagos létrehozatala, amelyre alkalmazva a lenyomatképző eljárás eredményeképp az adott lenyomat keletkezik.

**Magánkulcs:** A kulcspár azon, rejtjelezéshez, illetve visszaállításhoz használt része, mely az Igénylő kizárólagos birtokában van, és amelyet csak ő ismerhet.

**Magánkulcs védelme:** Mindazon tevékenységek összessége, melyek célja a magánkulcs megfelelő védelme, a magánkulcs teljes élettartama során annak generálásától, annak megsemmisítéséig, a hozzá tartozó tanúsítvány státuszától függetlenül.

**Másodlagos Alany: olyan** jogi személy vagy jogi személyiséggel nem rendelkező szervezet, amely a munkatársi tanúsítvány Igénylővel együttesen szerepel a tanúsítványban, valamint aki az Igénylőt saját magához tartozónak ismer el.

**Megerősítő személy:** Olyan személy az igénylő szervezetében, aki kérésre egy részlettényt megerősít.

**Munkatárs:** A természetes személyek azon köre, amelyeket egy adott szervezet saját magához tartozóként ismer el.

**Munkatársi tanúsítvány:** Olyan személyes tanúsítvány, melyben az abban szereplő természetes személyt a másodlagos Alany saját működési köre alá tartozónak ismeri el.

**NETLOCK Nem Minősített Hitelesítés-szolgáltatás:** Nem minősített tanúsítványok kibocsátása, hitelesítése, kezelése, megőrzése, egyéb a tanúsítványokkal kapcsolatos szolgáltatások nyújtása.

**Nyilvános kulcs:** A kulcspár azon, rejtjelezéshez, illetve visszaállításhoz használt, mindenki számára megismerhető része, amelynek az Igénylőhöz való tartozásáról a Szolgáltató tanúsítványt bocsát ki.

**Object Identifier (OID):** objektumok azonosítására használt, hierarchizált rendszer alapján definiált számsor.

**OCSP** **(Online Certificate Status Protokoll):** Valós idejű, online tanúsítvány állapot szolgáltatás. Az adott szolgáltatás keretében kibocsátott összes tanúsítvány aktuális visszavonási állapota (státusza) lekérdezhető. A lekérdezés azonnali, hiteles választ ad egy tanúsítvány állapotáról.

**OV (Organization validated) SSL:** olyan SSL tanúsítvány, melynek kiadása során az igénylő szervezet és az igénylést végző személy is ellenőrzésre kerül.

**Out-of-band:** Elektronikus információk szokásos használati környezeten kívül történő előállítási, továbbítási módja.

**Összesített felelősség:** Tanúsítványok és káresemények alapján történő, összesítés szerinti felelősség, a tranzakciók, elektronikus aláírások, és alkalmazások számától függetlenül.

**PEM formátumú kérelem:** Szöveges formátumú tanúsítványkérelem.

**Publikus (Nyilvános)** **Kulcsú Infrastruktúra:** A tanúsítványok kibocsátásában és kezelésében, valamint az időbélyegzésben részt vevő technikai eszközök, egységek, ezen tevékenységeket hivatalosan felügyelő és meghatározó intézmények, a felhasználók által alkalmazott kriptográfiai eszközök és tevékenységek összessége.

**Qualified Government Information Source (QGIS)**: Közigazgatási szerv által vezetett közhiteles nyilvántartás.

Olyan kormányzati adatbázis tekinthető QGIS-nek, amelyet egy hiteles kormányzati szerv tart fenn és amelynek adatközlési kötelezettsége törvényben előírt, illetve ahol a hamis adatközlést a törvény bünteti.(Közigazgatási szerv tanúsítványigénylése esetén nem tiltja a kormányzati források felhasználását az, hogy az adat forrása maga a kormányzat.)

**Qualified Tax Information Source (QTIS):** Olyan nyilvántartás, amit az állami Adóhatóság vezet, azaz egy olyan QGIS, amely kifejezetten az ügyfél vagy a megrendelő pénzügyi adatait, adózásával kapcsolatos információit tartalmazza.

**Qualified Independent Information Source (QIIS):** Olyan független, rendszeresen frissített, nyilvánosan elérhető információs adatbázis, amely megbízható forrásnak tekinthető.

Egy adatbázis akkor tekinthető független rendszernek, ha a CA ellenőrizte, hogy:

1) az adatbázist piaci szereplők használják, de nem a CA hozta létre

2) az adatbázis fenntartó legalább évente frissíti az adatot

A CA nem használhatja az adatbázist, ha ismert, hogy az adattartalma:

1. önbevallásos
2. nem kerül ellenőrzésre a QIIS által

 CA-k és kapcsolódó szervezetei által készített adatbázisok csak akkor használhatók, ha létrehozásukban a CA nem érintett.

**Regisztrációs Egység:** Az ügyfelek adatait összegyűjtő, ellenőrző, tanúsítvány kibocsátási, felfüggesztési, visszavonási kérelmeket összeállító, és azokat a Hitelesítő Egységhez továbbító egység.

**Subject Name (SN):** Az Igénylő megnevezése, egyedi neve (DN).

**Szabályzat Elfogadó Egység:** Jelen és más szabályzatok kialakításáért, elfogadásáért és adminisztrációjáért felelős szolgáltatói egység.

**Személyes tanúsítvány:** Természetes személyek számára kibocsátott tanúsítvány, melyekbe foglalt nyilvános kulcs magán párja kizárólag elektronikus aláírás előállítására használható.

**Szerződés aláíró (SZA):** Olyan természetes személy, aki maga az Igénylő, vagy az igénylő alkalmazottja vagy az igénylő jogosult képviselője (cégvezető, ügyvezető), és aki ezáltal jogosult az Igénylő szervezet nevében a Szolgáltatási szerződés aláírására.

**Szolgáltatási Szabályzat**: A Szolgáltató tanúsítvány-kibocsátási tevékenységével kapcsolatos, részletes eljárási és egyéb működési szabályokat tartalmazó nyilvános dokumentum.

**Szolgáltatási Szerződés:** a Szolgáltató által nyújtott szolgáltatások igénybevételéhez szükséges dokumentum, melynek elfogadása és aláírása a szolgáltatás igénybevételének előfeltétele. A Szolgáltató által nyújtott szolgáltatások igénybe vétele Szolgáltatási Szerződés megkötése helyett Belépési Nyilatkozat (lásd fentebb) elfogadásával, illetve DV SSL tanúsítvány szolgáltatásnál a rendelési folyamat sikeres megfizetésével is megtörténhet. Továbbá a Szolgáltató a Belépési Nyilatkozat elfogadását kötelezővé teheti.

**Szolgáltató:** A NETLOCK Kft, amely tevékenységi körében elektronikus aláírás hitelesítés-szolgáltatást, időbélyegzés illetve aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezés szolgáltatást végez.

**Tanúsítvány**: A Szolgáltató által kibocsátott elektronikus igazolás, amely a nyilvános kulcsot a tanúsítvány Igénylőához kapcsolja.

**Tanúsítvány fajta**: Jelen Szabályzat a tanúsítványok következő alapvető megjelenési formáiról rendelkezik: SSL, titkosító, kódaláíró és autentikációs.

**Tanúsítványtár:** A végfelhasználói és szolgáltatói tanúsítványok, felfüggesztett, visszavont tanúsítványadatok, Szolgáltatói Szabályzatok publikálásáért, tárolásáért felelős alegység.

**Tanúsítvány Visszavonási Lista (CRL – Certificate Revocation List)**: Valamely okból visszavont, azaz érvénytelenített, illetve felfüggesztett, azaz ideiglenesen érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet meghatározott időközökkel a Szolgáltató bocsát ki.

**Tanúsítvány-szolgáltatás**: azon eljárás, melynek során a Szolgáltató a Szolgáltatási Szabályzatokban meghatározott eljárásban új vagy – amennyiben értelmezett - megújított tanúsítványt bocsát ki a felhasználó részére. A tanúsítvány-szolgáltatáshoz kapcsolódóan a Szolgáltató tanúsítványállapot-szolgáltatást is nyújt, melynek keretében fogadja a tanúsítvány-visszavonási- és felfüggesztési kérelmeket és a Szolgáltatási Szabályzatokban meghatározott időközönként Tanúsítvány Visszavonási Listát bocsát ki.

**Tanúsítványállapot-nyilvántartás**: A legközelebb kibocsátásra kerülő Tanúsítvány Visszavonási Lista tartalmához kapcsolt online lekérdezhető információk.

**Ügyfélmenü:** A Szolgáltató Internetes oldalain online regisztrációt követően létrejövő, az adott felhasználó saját kérelmeit, tanúsítványait és egyéb egyedi információit tartalmazó felhasználói profil.

**Végfelhasználó:** Szerződéses partner, aki a Szolgáltató által kibocsátott végfelhasználói tanúsítvánnyal rendelkezik.

**Végfelhasználói tanúsítvány:** jelen szabályzat szerint a Szolgáltató által kibocsátott olyan tanúsítvány, amelyet az Igénylő kizárólag a benne megjelölt célra használhat, de más tanúsítvány hitelesítésére nem.

# Közzététel és tanúsítványtár

## A Szolgáltatói információ közzététele

### Közzétételi és tájékoztatási elvek

#### A szabályzatban nem tárgyalt elemek

Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyezteti. Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen Szabályzat több ilyet is megemlít).

#### A Szabályzat közzététele

Szolgáltató szabályzatainak a változásokkal egybeszerkesztett új verzióját annak elfogadását követően haladéktalanul, de minden esetben annak hatályba lépését megelőzően közzéteszi a weboldalán ezúton tájékoztatva a Közösséget a módosításokról. A jelen szabályzattal kapcsolatos közzéteendőket a 9.7.4 pont határozza meg.

#### Észrevételek kezelése

A közzétett szabályzatokkal kapcsolatos észrevételeket a Szolgáltató az info@NETLOCK.hu címen fogadja. A Szabályzat észrevételekkel módosított változatát Szolgáltató az előző pont alapján teszi ismételten közzé.

### Kikötések és feltételek közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait PDF formában hozza nyilvánosságra Internetes oldalain keresztül (ld. 1.5 alfejezet). Itt a dokumentumok aktuális verziója mellett megtalálhatóak azok korábban érvényben lévő változatai is, illetve rövid ismertető a változásokról.

### Rendkívüli információk közzététele

A Szolgáltató a következő eseményekről honlapján hirdetményt tesz közzé:

új szolgáltatás beindítása,

valamely szolgáltatás tervezett beszüntetése vagy tartós (7 naptári napot meghaladó) szüneteltetése, ( .Törvény 9. § 8. bek. alapján „A hitelesítés-szolgáltató tevékenységi köréből csak az új tanúsítvány kibocsátást szüneteltetheti.”),

tevékenységének befejezése (ld. bővebben 5.8 alfejezet),

rendkívüli üzemeltetési helyzetről tájékoztatás.

### CAA ellenőrzés

A hitelesítés szolgáltató jelen szabályzat alapján jelenleg CAA ellenőrzést nem végez.

### Baseline előírásoknak megfelelés

A Netlock Kft. megfelel az aktuális „Baseline Requirements for the Issuance and

Management of Publicly-Trusted Certificates” (BRG) előírásainak (elérhető: http:/

/www.cabforum.org oldalon található.

Ezen dokumentum és a BRG ütközése esetén a BRG-ben találhatókat kell figyelembe venni.

### ETSI előírásoknak megfelelés

Jelen szabályzat alapjának az ETSI 102042 V2.4.1-ben meghatározott normalizált tanúsítvány szabályzások (normalized certificate policies) közül az NCP certificate policy-t tekintjük.

Az egyes tanúsítvány fajtákra vonatkozó standardizált policy-k az alábbi felsorolásban olvashatók:

* DV SSL tanúsítványok – DVCP
* OV SLL tanúsítványok – OVCP
* Authentikációs tanúsítványok
	+ Alaphelyzetben – NCP
	+ Eszközös tárolás esetén – NCP+
* Titkosító tanúsítványok
	+ Alaphelyzetben – NCP
	+ Eszközös tárolás esetén – NCP+
* CodeSigning tanúsítványok
	+ Alaphelyzetben – NCP
	+ Eszközös tárolás esetén – NCP+
* Aláíró tanúsítványok
	+ Alaphelyzetben – NCP
	+ Eszközös tárolás esetén – NCP+
* Aláíró minősített tanúsítványok – NCP+

## Tanúsítványokkal kapcsolatos információk

### Tanúsítványok közzététele

A Szolgáltató az általa működtetett szolgáltatási egységek tanúsítványát a következő módszerekkel teszi közzé:

saját szolgáltatói tanúsítványát közzéteszi tanúsítványtárában (ld. 1.5.1 alfejezet),

minden hitelesítő egység tanúsítványát közzéteszi tanúsítványtárában, valamint Internetes honlapján keresztül.

A Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokat csak abban az esetben teszi közzé a nyilvános tanúsítványtárában, ha az Igénylő és a másodlagos Alany ehhez a regisztrációs eljárás során hozzájárult.

### A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala

A Szolgáltató az általa működtetett hitelesítő egységek tanúsítványával kapcsolatos állapotinformációkat a következő módszerekkel teszi közzé:

saját kiadói tanúsítványainak állapotváltozásáról sajtóközleményt jelentet meg, közzéteszi a weboldalán, illetve az állapotváltozást saját tanúsítványtárában is feltünteti,

egyéb szolgáltatói tanúsítványainak állapotváltozását a saját tanúsítványtárában tünteti fel,

A Szolgáltató a hitelesítő egységei által kiadott végfelhasználói tanúsítványával kapcsolatos állapotinformációkat a következő módszerekkel teszi közzé:

a végfelhasználói tanúsítványok állapotváltozását a tanúsítványtárában hozza nyilvánosságra,

végfelhasználói tanúsítvány visszavonását és felfüggesztését Szolgáltató akkor is nyilvánosságra hozza, ha a tanúsítvány közzétételéhez az Igénylő (Igénylő) nem járult hozzá.

### Határidők meghatározása a tanúsítvány életciklusa kapcsán

A Szolgáltató egyes eljárási részcselekmények elvégzésére (pl. tanúsítvány meghosszabbításának kezdeményezése; az aláírt Szolgáltatási Szerződés (Belépési Nyilatkozat) Szolgáltatóhoz történő eljuttatására, stb.) határidőket írhat elő az Igénylők részére, melyeket a Szolgáltató az internetes oldalán (ld. 1.5 pont), illetve az Igénylőnek a regisztráció során megadott elektronikus levelezési címére küldött tájékoztatóban tesz közzé. Amennyiben az Igénylő nem tartja be a Szolgáltató által megjelölt határidőket, a tanúsítvánnyal kapcsolatos eljárási cselekmények késedelmes elvégzésének következményeit maga viseli, továbbá a Szolgáltató fenntartja magának a jogot, hogy a késedelmes ügyintézésért a Szolgáltató internetes oldalán közzétett mértékű különeljárási díjat számoljon fel.

## A közzététel gyakorisága

### Kikötések és feltételek közzétételi gyakorisága

Jelen Szabályzattal kapcsolatos új verziók közzététele a 2.1 és 9.7 alfejezetben ismertetett eljárásoknak megfelelően történik.

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

### Rendkívüli információk közzétételi gyakorisága

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

### Tanúsítványok nyilvánosságra hozatalának gyakorisága

A Szolgáltató a tanúsítványok nyilvánosságra hozatala kapcsán a következő gyakorlatot követi:

saját szolgáltatói tanúsítványait a kibocsátást követő 10 munkanapon belül teszi közzé,

az általa működtetett szolgáltatási egységek tanúsítványa a tanúsítványtárában és az Internetes honlapján (ld. 1.5.1 alfejezet) 10 munkanapon belül jelenik meg,

a Szolgáltató a végfelhasználói tanúsítványokat a tanúsítványtárában az előállítást követően legkésőbb 10 munkanapon belül teszi közzé, illetve sűrűbben, ahol ezt vonatkozó szabályozás előírja.

Láncolt Hitelesítés Szolgáltatás esetén a vonatkozó Szolgáltatási Utasításban, illetőleg Szolgáltatási Szabályzat kiegészítésben a fentiektől el lehet térni.

### A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatali gyakorisága

A Szolgáltató az általa működtetett hitelesítő egységek és felhasználók tanúsítványával kapcsolatos állapotinformációkat a 4.10.1 pontban tárgyalt gyakorisággal teszi közzé.

## Hozzáférés ellenőrzések

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. A tanúsítványok és állapotinformációk elérése kapcsán az Érintett Felek részére a Szolgáltató által kibocsátott tanúsítványok, illetve időpont hitelesítésének ellenőrzésére jelen Szabályzat tartalmaz ajánlásokat (lásd 9.5.4 pont).

A Szolgáltató által közölt információkat kizárólag csak a Szolgáltató egészítheti ki, törölheti vagy módosíthatja. A Szolgáltató különböző védelmi mechanizmusokkal akadályozza meg az információkhoz való jogosulatlan hozzáféréseket.

### Tanúsítványtárak

A Szolgáltató az Érintett Felek számára a rendelkezésére álló legpontosabb adatokat biztosítja a lehetőségeknek, vállalásoknak megfelelően leghamarabb, és ennek érdekében – a DV SSL tanúsítványok kivételével - nyilvános Tanúsítványtárat üzemeltet az Internet címén (lásd 1.5 pont). A tanúsítványtárban a Szolgáltató által kiadott tanúsítványok, a visszavont tanúsítványok listái, eljárási rendek, szerződési feltételek és más dokumentációk találhatók.

A Szolgáltató tanúsítványtára szabványos HTTP, illetve HTTPS protokollokkal érhető el a Szolgáltató Internetes oldalain keresztül (ld. 1.5 alfejezet), az ott megvalósított lekérdezési műveletekkel. A tanúsítványtár többszintű keresési lehetőséget biztosít a tárolt adatok eléréséhez.

A tanúsítványtár elérhetőségét Szolgáltató folyamatosan (az év minden napján, 0–24h) biztosítja a karbantartáshoz szükséges idők kivételével. A Szolgáltató a tervezett karbantartásokat munkaidőn kívüli időszakokra ütemezi.

A Szolgáltató a kibocsátott tanúsítványok nyilvántartása, a visszavonási nyilvántartások, valamint visszavonási állapot-közzététel legalább 99%-os rendelkezésre állással elérhetők, egyúttal az eseti szolgáltatás kiesések nem haladják meg a 24 órás időtartamot.

# Azonosítás és hitelesítés

## Elnevezések

A nevek regisztrációjának szabályai valamennyi tanúsítványfajtára vonatkoznak.

### Névtípusok

#### Névszabályok személyhez köthető (autentikációs, titkosító és hagyományos kódaláíró) tanúsítványok esetében

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 elfogadott hatósági igazolványban (lásd 3.2.3 pont) foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve CN és opcionálisan SN mezőkkel (CN = Teljes név = Vezetéknév + Keresztnév, SN = Vezetéknév), általában az UTF-8 kódolást használva; a nevek egyes egységeit szóköz választja el. Ezen szabályoktól a Szolgáltató kivételesen, eltérhet, amennyiben a Common Name, Organization és Organization Unit mezőkre vonatkozó méretbeli korlátok nem teszik lehetővé az ilyen formában történő teljes adatrögzítést.

a tanúsítványban kivételesen, egyedileg meghatározott esetben, a vonatkozó szabványok szerinti meghatározott maximális karakterszámot meghaladó elnevezések esetén rövidítés használata lehetséges,

a tanúsítványban a „CN” mező nem üres,

a tanúsítvány SN mezőjének feltüntetése nem kötelező.

a „Title” mezőben az Igénylő beosztása szerepel, amennyiben lehetséges annak feltűntetése a hitelesítési rend esetében, egyéb esetben nem kerül feltüntetésre,

a „State” mezőben az ország, a megye, vagy megyei jogú város neve kerülhet feltüntetésre,

munkatársi tanúsítványokban az „Organization” mezőben szerepel a másodlagos Alany, valamint az „Organization-unit” mezőben szerepelhet a másodlagos Alany szervezeti egysége,

szervezeti tanúsítványokban az CN és az „Organization” mezőben szerepel a másodlagos Alany

a „Locality” mezőben feltüntethető az Igénylő lakcím szerinti vagy munkatársi tanúsítványokban a másodlagos Alany székhely, telephely szerinti városa,

a tanúsítvány Igénylő lakóhelyének, székhelyének ország megjelölésénél esetén a Szolgáltató az ISO 3166 [1] szabványban meghatározott kétkarakteres országkódot (Magyarország esetén „HU”) alkalmazza.

a tanúsítvány „SubjectAltname” mezőjében szereplő elektronikus levelezési cím struktúrája megfelel az RFC 822 előírásainak.

#### Névszabályok Kernel mode kódaláíró tanúsítványok esetében

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 a cégnévvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve CN és opcionálisan, általában az UTF-8 kódolást használva; a nevek egyes egységeit szóköz választja el. Ezen szabályoktól a Szolgáltató kivételesen, eltérhet, amennyiben a Common Name, Organization és Organization Unit mezőkre vonatkozó méretbeli korlátok nem teszik lehetővé az ilyen formában történő teljes adatrögzítést.

a tanúsítványban kivételesen, egyedileg meghatározott esetben, a vonatkozó szabványok szerinti meghatározott maximális karakterszámot meghaladó elnevezések esetén rövidítés használata lehetséges,

a tanúsítványban a „CN” mező nem üres,

a tanúsítvány SN mezőjének feltüntetése nem kötelező.

a „Title” mezőben az Igénylő beosztása szerepel, amennyiben lehetséges annak feltűntetése a hitelesítési rend esetében, egyéb esetben nem kerül feltüntetésre,

a „State” mezőben az ország, a megye, vagy megyei jogú város neve kerülhet feltüntetésre,

munkatársi tanúsítványokban az „Organization” mezőben szerepel a másodlagos Alany, valamint az „Organization-unit” mezőben szerepelhet a másodlagos Alany szervezeti egysége,

szervezeti tanúsítványokban az CN és az „Organization” mezőben szerepel a másodlagos Alany

a „Locality” mezőben feltüntethető az Igénylő lakcím szerinti vagy munkatársi tanúsítványokban a másodlagos Alany székhely, telephely szerinti városa,

a tanúsítvány Igénylő lakóhelyének, székhelyének ország megjelölésénél esetén a Szolgáltató az ISO 3166 [1] szabványban meghatározott kétkarakteres országkódot (Magyarország esetén „HU”) alkalmazza.

a tanúsítvány „SubjectAltname” mezőjében szereplő elektronikus levelezési cím struktúrája megfelel az RFC 822 előírásainak.

#### Névszabályok DV SSL tanúsítványok esetében

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 tanúsítványban csak a tanúsítvány kiadási folyamat során ellenőrzött adatok szerepelhetnek,
* a tanúsítványban a „CN” mező nem lehet üres: vagy legalább egy FQDN domain nevet tartalmaz, vagy nem szerepel a tanúsítványban
* A CN mező tartalmazhat \* tagot.
* a tanúsítvány „*SubjectAltname*” (SAN) mezője nem lehet üres: vagy ki van töltve, vagy nem szerepel a tanúsítványban. Ha kitöltött, akkor legalább egy FQDN domain nevet tartalmaz.
* A *SubjectAltname*” (SAN) mező tartalmazhat \* tagot.
* A *SubjectAltname*” (SAN) mezője a kérelmezett FQDN mellett tartalmazhat „[www](http://www.)” előtaggal kiegészített FQDN-t, amennyiben a kérelmezett FQDN nem tartalmazott „[www](http://www.)” előtagot.
* A CN mező és a *SubjectAltname*” (SAN) mező első FQDN tagjának egyeznie kell, amennyiben mindkettő megtalálható a tanúsítványban.
* A domain nevek dNSName formátumban kerülnek tárolásra.
* A tanúsítvány SN mezőjének feltüntetése nem kötelező.
* a tanúsítványban kivételesen, egyedileg meghatározott esetben, a vonatkozó szabványok szerinti meghatározott maximális karakterszámot meghaladó elnevezések esetén rövidítés használata lehetséges,
* a nevek alapértelmezetten tanúsítványban az alábbiak szerint kerülnek feltüntetésre:
* a szervezet neve a bejegyző okiratban foglaltaknak megfelelően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve általában az UTF-8 kódolást használva; a nevek egyes egységeit szóköz választja el. Ezen szabályoktól a Szolgáltató kivételesen, eltérhet, amennyiben a *Organization* és *Organization Unit* mezőkre vonatkozó méretbeli korlátok nem teszik lehetővé az ilyen formában történő teljes adatrögzítést.
* public suffix teljes tartományra nem adható ki \* tanúsítvány.

#### Névszabályok OV SSL tanúsítványok esetében

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 tanúsítványban csak a tanúsítvány kiadási folyamat során ellenőrzött adatok szerepelhetnek,
* a tanúsítványban a „CN” mező nem lehet üres: vagy legalább egy FQDN domain nevet tartalmaz, vagy nem szerepel a tanúsítványban
* A CN mező tartalmazhat \* tagot.
* a tanúsítvány „*SubjectAltname*” (SAN) mezője nem lehet üres: vagy ki van töltve, vagy nem szerepel a tanúsítványban. Ha kitöltött, akkor legalább egy FQDN domain nevet tartalmaz.
* A *SubjectAltname*” (SAN) mező tartalmazhat \* tagot.
* A *SubjectAltname*” (SAN) mezője a kérelmezett FQDN mellett tartalmazhat további FQDN tagokat.
* A CN mező és a *SubjectAltname*” (SAN) mező első FQDN tagjának egyeznie kell, amennyiben mindkettő megtalálható a tanúsítványban.
* A domain nevek dNSName formátumban kerülnek tárolásra.
* A tanúsítvány SN mezőjének feltüntetése nem kötelező.
* a tanúsítványban kivételesen, egyedileg meghatározott esetben, a vonatkozó szabványok szerinti meghatározott maximális karakterszámot meghaladó elnevezések esetén rövidítés használata lehetséges,
* a nevek alapértelmezetten tanúsítványban az alábbiak szerint kerülnek feltüntetésre:
* a szervezet neve a bejegyző okiratban foglaltaknak megfelelően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve általában az UTF-8 kódolást használva; a nevek egyes egységeit szóköz választja el. Ezen szabályoktól a Szolgáltató kivételesen, eltérhet, amennyiben a *Organization* és *Organization Unit* mezőkre vonatkozó méretbeli korlátok nem teszik lehetővé az ilyen formában történő teljes adatrögzítést.

### Álnév/Márkanév használata

#### Általános felhasználás esetén

A titkosító, autentikációs tanúsítványok esetén van lehetőség álnév, márkanév használatára a tanúsítványban.

SSL és kódaláíró tanúsítványok esetén lehetőség van márkanév használatára a tanúsítványban.

Az álnevet az Igénylő választja, a Szolgáltató az álnevet nem ellenőrzi, az Igénylő az esetleges álnévvel kapcsolatos problémákért (szerzői jogi, stb.) maga felel.

A tanúsítványban való feltüntetése kapcsán az ügyfél maga határozhatja meg, hogy a Szolgáltató az “ALNEV” előtét vagy a „(\*)” karakter alkalmazása mellett tünteti fel a tanúsítvány Subject mezőjében, vagy az álnevet a Pseudonym mezőben kéri feltüntetni; ez utóbbi esetben a CN mező „álneves tanúsítvány” elnevezést tartalmaz.

A Szolgáltató saját hatáskörében jogosult a jogi problémákba (akár valószínűsíthetően) ütköző álneves tanúsítvány kiadását megtagadni, a kiadott tanúsítványokat visszavonni.

### Különböző elnevezési formák értelmezési szabályai

A Szolgáltató által kibocsátott tanúsítványoknak nem célja, hogy az Igénylőként megjelölt természetes személyek számára digitális személyi igazolványként funkcionáljon, illetve hogy személyüket kizárólag a tanúsítványban feltüntetett adatok alapján azonosítani lehessen. A munkatársi tanúsítvány önmagában képviseleti jogosultságot nem igazol.

Az azonosítók értelmezése érdekében Érintett Feleknek a jelen Szabályzatban leírtak alapján kell eljárniuk. Amennyiben az azonosító, illetve a tanúsítványban foglalt adatok értelmezésével kapcsolatban az Érintett Félnek segítségre van szüksége, akkor a Szolgáltatóval közvetlenül is felveheti a kapcsolatot. A Szolgáltató az Igénylő, illetve a másodlagos Alany egyéb adatairól többlettájékoztatást – a tanúsítványban feltüntetett adatok értelmezését segítő információn kívül – csak az erre vonatkozó felhatalmazás alapján ad ki (ld. 9.3.5 pont).

#### Kibocsátó azonosító

A kibocsátó azonosítója úgy értelmezendő, hogy a tanúsítványt a Szolgáltató hitelesítő egysége adta ki (székhely, elérhetőség: ld. 1.5 alpont). A tanúsítványokhoz a hatályos magyar jogszabályok szerint semmilyen joghatás nem fűződik.

Az *Issuer* mező a tanúsítvány kibocsátójának székhely szerinti országkódját (*Country*) és városát (*Locality*), a szervezet nevét (*Organization*), szervezeti egységét (*Organization Unit*) és az adott tanúsítványkiadó megnevezését (*Common Name*) tartalmazza.

#### Igénylőazonosító

Az Igénylő azonosítója a *Common Name* mező alapján az alábbiak szerint értelmezhető:

Autentikációs, titkosító, kódaláíró tanúsítvány esetén:

természetes személy, amelynél munkatársi tanúsítvány esetében feltüntetésre kerül az Organization nevű szervezet Organization-unit szervezeti egysége, vagy

szervezet vagy szervezeti egység, amely az Organization nevű szervezet Organization-unit osztályához, illetve részlegéhez tartozik, vagy

DV SSL tanúsítványok esetén:

domain név, mely technikai ellenőrzés alapján került kibocsátásra. Amennyiben a szabvány előírja, a CN mező el is maradhat, ez esetben a SubjectAlternativeName tartalmazza a domain nevet.

OV SSL tanúsítványok esetén:

domain név, amelyet az Organization nevű szervezet Organization-unit szervezeti egysége, vagy az Organization mezőben feltüntetett magánszemély jogosult használni. Amennyiben a szabvány előírja, a CN mező el is maradhat, ez esetben a SubjectAlternativeName tartalmazza a domain nevet.

Kernel Mode Kódaláíró tanúsítvány

 szervezet vagy szervezeti egység, amely az Organization nevű szervezet Organization-unit osztályához, illetve részlegéhez tartozik, vagy

Az azonosításban egyéb mezők is értelmezettek lehetnek:

A természetes személy nevei (családi, elő- és utóneve) – UTF-8 kódolással - olyan sorrendben szerepelnek a Common Name mezőben, ahogyan azok a személyazonosságát igazoló okmányban.

Az Organization a szervezeti azonosság hitelesítésére szolgáló dokumentumban szereplő rövid név, vagy ha ilyen rövid név nem határozható meg, a Hitelesítő Egység saját hatáskörében a szervezet nevéből képzett olyan rövid elnevezés, amely beazonosíthatóvá teszi a szervezetet.

A természetes személy lakóhelye, illetve a szervezet székhelye vagy telephelye a Country ország, State ország/megye Locality településén található. Az Igénylő e-mail címe az Igénylő egységgel összefüggésben E-mail. Amennyiben feltüntetésre kerül, a Title mező tartalmazza az Igénylő beosztását.

Az Igénylőazonosító mezőnek célja, hogy a tanúsítvány Igénylőt (a felhasználó egységen belül) azonosítani lehessen. Az Igénylő és a másodlagos Alany egység(ek) együttes megjelenítése a tanúsítványban azt jelenti, hogy a másodlagos hozzájárult az Igénylő(ok) és az egység(ek) nevének együttes feltüntetéséhez.

### A nevek egyedisége

A Szolgáltató a kibocsátott összes tanúsítvány esetében a tanúsítványok Igénylőit egymástól egyértelműen megkülönbözteti a tanúsítványban rögzített összes személyes adatuk (név, lakóhely ország, lakóhely város, e-mail cím, ha van, sorszám) segítségével (egyedi név).

#### Eljárások a nevekre vonatkozó vitás kérdések megoldására

Szolgáltató fenntartja magának a jogot a név kiosztással kapcsolatos mindennemű döntés tekintetében. A tanúsítvány Igénylőnek bizonyítani kell a jogát egy adott név használatára. A nevek kiosztása érkezési sorrend alapján történik, azaz a később érkező nem kérheti egy már korábban kiosztott név újrakiosztását még akkor sem, ha a kívánt névvel kapcsolatos tanúsítvány már érvényét vesztette.

### Védjegyek elismerése, hitelesítése és szerepe

Szolgáltató nem garantálja az ügyfelek számára védjegyeik feltüntetését a tanúsítványban. Az ügyfél részéről egy védjegy megszerzése nem tekinthető olyan eseménynek, amely szükségszerűen a tanúsítvány megújítását eredményezi.

A tanúsítványkérelemmel és elfogadással az ügyfél kifejezi, hogy a benne foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik személy jogait. Szolgáltatónak nem kötelessége a védjegyek jogos használatának az ellenőrzése.

## Kezdeti azonosítás

### A magánkulcs birtoklásának bizonyítási módszere

Az eszközszolgáltatás esetében a Központi Regisztrációs Egység állítja elő az Igénylő számára a kulcspárt, így a Szolgáltató nem igényel bizonyítékot arra, hogy az Igénylő rendelkezik a hitelesítendő nyilvános kulcs magánkulcs párjával.

Amennyiben az ügyfél állítja elő a kulcspárt, úgy a Szolgáltató gondoskodik mindazon technikai és műszaki eljárás alkalmazásáról, melynek révén megbizonyosodhat arról, hogy az Igénylő ténylegesen birtokolja a nyilvános kulcshoz tartozó magánkulcsot.

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

### Szervezeti azonosság hitelesítése

A Szolgáltató által kibocsátott szervezeti tanúsítványban feltüntetésre kerül a felhasználó szervezet (másodlagos Alany). Opcionálisan egyéb adatok is feltüntetésre kerülhetnek.

A Szolgáltató a szervezetek azonosítását a 4.2.2 pont alatti táblázatban leírt módon végzi el.

Ha az ügyfél tanúsítványával kifejezetten jelezni kívánja, hogy ő egy adott szervezethez tartozik, és ez értelmezhető, akkor az azonosítás során fel kell mutatnia az adott szervezet nevében aláírásra jogosult személy által kiállított és aláírt, az adott szervezet nevét is tartalmazó meghatalmazást arra, hogy a szervezet képviseletében a tanúsítványt használja, az aláírásra jogosító aláírási címpéldányt, valamint a szervezet azonosságát is hitelesítő, közhiteles nyilvántartást vezető hatóság által kiadott igazolást.

A Szolgáltató weboldaláról (lásd 1.5.1 pont) letölthető az igényléshez szükséges meghatalmazás-minta.

Amennyiben az adott szervezet azonossága nem igazolható közhiteles nyilvántartást vezető hatóság által kiadott igazolással, úgy a szervezetet képviselő természetes személynek a személyazonosítás során fel kell mutatnia az adott szervezet által kiállított és közokiratba foglalt, a szervezet nevét is tartalmazó meghatalmazást arra, hogy a szervezet képviseletében a hitelesítés-szolgáltatónál előforduló ügyekben eljárjon, mely meghatalmazás egyúttal a szervezet azonosságát is hitelesíti.

Amennyiben az ügyfél rendelkezik a Netlock által kiadott aláíró tanúsítvánnyal, az azzal igényelt, azonos vagy magasabb ellenőrzési szinttel rendelkező kiadótól származó, egyező adattartalmú autentikációs vagy titkosító tanúsítványát egyszerűsítve igényelheti, az elektronikus megrendelés elektronikus aláírásával.

### Személyazonosság hitelesítése

A Szolgáltató a természetes személy azonosítását az egyes tanúsítványfajták esetében a 4.2.2 pont alatti táblázatban leírt módon végzi el.

A személyazonosításra alkalmas hivatalos igazolványban szereplő fénykép alapján az Igénylőnek egyértelműen felismerhetőnek kell lennie, a benne szereplő aláírásának meg kell egyeznie a Szolgáltatási Szerződésen tett aláírásával. Amennyiben kétség merül fel a fénykép vagy az aláírás megfeleltethetősége kapcsán, a Szolgáltató megtagadja a tanúsítványkiadási kérelem teljesítését.

A Szolgáltató továbbá megállapítja mindazon adatok hitelességét, melyeket a tanúsítványban feltüntet.

A regisztráció támogatására az Igénylő hozzájárulásával a személyazonosító dokumentumokról másolat készülhet, melyek archiválásra kerülnek. Amennyiben az Igénylő nem egyezik bele a másolat készítésébe, úgy a dokumentumokat személyesen is bemutathatja a Szolgáltató ügyfélszolgálatán a regisztrációs, vagy – amennyiben értelmezett - a mobil regisztrációt végző munkatársak előtt. A bemutatás megtagadása esetén a Szolgáltató a tanúsítványkiadási kérelmet elutasítja.

Amennyiben az Igénylő nem egyezik bele a másolat készítésébe, úgy az utóellenőrzésekhez kötött lehetőségek, funkciók (például – amennyiben értelmezett - meghosszabbítás) számára nem lesznek elérhetőek.

A személyazonosítás során a Szolgáltató regisztrációs munkatársai közhiteles nyilvántartásokban ellenőrzik a személyazonosság igazolására bemutatott dokumentumok azonosító adatait és a dokumentumok érvényességét, valamint hogy az ügyfél által megadott adatok megfelelnek-e a valóságnak.

### Domain birtokolásának hitelesítése

Amennyiben a tanúsítvány szerverek részére kerül kibocsátásra SSL célból, akkor a Szolgáltató a megfelelő technikai eljárással ellenőrzi, hogy az igényléssel érintett domain név ténylegesen az igénylő birtokában (vagy lányvállalat, anyavállalat, …) van-e, vagy – tanúsítvány típustól függően felette felügyeleti képességgel bír, illetve a tanúsítvány típusától függően felhívhatja az igénylőt annak igazolására, hogy a domain tulajdonosa engedélyezte az igénylő számára a domain név használatát.

## Azonosítás tanúsítvány kulcscseréje esetén

A tanúsítvány kulcscseréjét a Szolgáltató alapesetben nem támogatja. Amennyiben kulcscsere válna szükségessé, abban az esetben új tanúsítvány igénylést kell beadni, az ott meghatározott azonosítási szabályok szerint eljárva (lásd 4.2.2 pont).

## Visszavonási kérelem

Szolgáltató tanúsítvány visszavonási és -felfüggesztési szolgáltatásokat egyaránt nyújt. Az erre vonatkozó kérelmek azonosítási és hitelesítési vonatkozásait a 4.9.4 pont tárgyalja.

# Működésre vonatkozó követelmények - tanúsítványok

## Tanúsítványigénylés

### Igénylés feltételei

Tanúsítvány típustól függően tanúsítványt igényelhet:

* természetes személy, saját részére,
* természetes személy saját részére, feltüntetve a tanúsítványban, hogy meghatározott szervezethez tartozik,
* szervezet saját maga mint entitás részére,
* valamely szervezet a tulajdonában levő vagy a tulajdonos által használatra átengedett domain név alatt elérhető szerver számára.

Kizárólag a jelen Szabályzatban megadott fajtájú és profilú tanúsítványok igényelhetők, az alábbi módon:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **tanúsítvány típus** | **személy** | **munkatárs** | **szervezet** | **szerver** |
| titkosító | igen | igen | igen | - |
| autentikációs | igen | igen | igen | nem |
| kódaláíró | igen | igen | igen | nem |
| DV SSL | - | - | - | igen |
| OV SSL | nem | nem | nem | igen |

A regisztráció során szolgáltatott adatok ugyan önkéntesek, azonban a Szolgáltató megtagadhatja a tanúsítvány kibocsátását, amennyiben az igénylő által megadott igazolások alapján nem azonosítható be egyértelműen az a személy, szervezet vagy domain név, amely kapcsán a tanúsítvány kibocsátását kérik.

Az Igénylő köteles a tanúsítvány ellenértékét a mindenkori díjtáblázatban fogalt díjak alapján, a tanúsítvány kibocsátását megelőzően a Szolgáltató részére megfizetni. A díjfizetést megelőzően a tanúsítvány kibocsátásáról, annak egyéb feltételeiről (pl. külön eljárási díjáról) a Szolgáltató saját hatáskörén belül dönt. A tanúsítvány ellenértékének kiegyenlítésére vonatkozó szabályoktól a Szolgáltató egyedi esetekben, saját döntése alapján jogosult eltérni.

## Tanúsítványkérelem feldolgozása

Végfelhasználói tanúsítványok kibocsátására a tanúsítványigénylési eljárás lefolytatását követően kerül sor. A tanúsítvány elkészítésére az új tanúsítványigénylés során a kérelemben megadott, a Szolgáltatási Szerződésben megerősített, a tanúsítvány fajtájától függően ellenőrzött, illetve a Szolgáltató rendelkezésre álló és a tanúsítvány megújításának (amennyiben értelmezett) igénylése során (a megújítást Igénylő űrlapon) érvényesnek elismert adatok alapján kerül sor.

A tanúsítványigénylés feltételeinek teljesülése esetén a Szolgáltató feldolgozza a tanúsítványkérelmet a következőkben bemutatott eljárásrend szerint.

A Szolgáltató a megadott elektronikus levelezési címre utasításokat továbbít, és erről a levelezési címről várja a tanúsítvány kiadására vonatkozó kérelem megerősítését is.

### Regisztrációs szabályok

#### Regisztrációs szabályok DV SSL tanúsítványok esetén

##### A regisztrációs eljárás alapelvei DV SSL esetén

az eljárást a megrendelő végzi el

az eljárást minden új tanúsítványigénylés esetében teljes egészében le kell folytatni,

az eljárás teljesen automatizált, elektronikus rendszereken keresztül zajló folyamat,

DV SSL osztályban a regisztráció online módon, önállóan történik, a regisztrációs adatok nem feltétlenül kerülnek tanúsítványba foglalásra, így ellenőrzésre sem.

##### DV SSL regisztráció és kibocsátási lépések

az Igénylő regisztrálja magát a Szolgáltató Internetes oldalán és tanúsítványigénylést juttat el a Szolgáltatóhoz, melynek során elfogadja az Általános Szerződési Feltételeket (ld. 1.5 alfejezet);

az igénylő elhelyez egy szolgáltató által generált, technikai ellenőrzésre szolgáltató kódot a tanúsítani kívánt szerveren, vagy a domainhez tartozó DNS bejegyzésben,

a Szolgáltató fogadja a kérelmet, illetve ellenőrzi annak szabályosságát,

a Szolgáltató végrehajtja a technikai ellenőrzéseket és megfelelőség esetén kiadja a tanúsítványt,

a Szolgáltató dokumentálja a regisztrációs lépéseket.

##### DV SSL regisztráció során nyilvántartásba vett adatok köre

az ügyfél által megadott cím és/vagy más elérhetőség,

a kérelem elektronikus formában,

az Igénylő féllel kötött megállapodás esetleges specifikus választásai,

az ügyfélnek a rá vonatkozó kötelezettségekkel történő egyetértése,

a kérelmet elfogadó egység azonosítója,

a kérelem életciklusa során az igénylővel folytatott elektronikus és hagyományos levelezés, kommunikáció (pl. telefon) naplója,

minden, a tanúsítványok kiadásához kapcsolódó információ.

A Szolgáltató a nyilvántartásokat az ügyféllel közölt időpontig, illetve a jogszabályi előírásoknak megfelelően addig, ameddig a tanúsítványokra jogi eljárások során bizonyítási célból szükség lehet, megőrzi (ld. még 5.5 alfejezet).

#### Regisztrációs szabályok titkosító, autentikációs, kódaláíró, OV SSL esetén

##### A regisztrációs eljárásra alapelvei ezen tanúsítványokra

az eljárást a Regisztrációs- és Kézbesítési Megbízottak, Mobil Regisztrációs Munkatársak, a Kihelyezett Regisztrációs Egység és a Szolgáltató Központi Regisztrációs Egységének munkatársai végezhetik el,

a regisztrációs eljárás biztonságát további közreműködők is segítik,

az eljárást minden új tanúsítványigénylés esetében teljes egészében le kell folytatni,

az eljárás részben automatizált, elektronikus rendszereken keresztül zajló, részben humán beavatkozással végzett folyamat,

a megadott személyes és szervezeti adatok ellenőrzését a Központi Regisztrációs Egység munkatársai végzik. A tanúsítványkérelmet a Központi Regisztrációs Egység adminisztrátorai felelősek kezelni, miután azonosították az Igénylőt a kapcsolódó tanúsítványfajta által meghatározott követelményeknek megfelelően.

##### Regisztrációs és kiadási lépések ezen tanúsítványokra

az Igénylő regisztrálja magát a Szolgáltató Internetes oldalán vagy egyéb módon tanúsítványigénylést juttat el a Szolgáltatóhoz, melynek során elfogadja az Általános Szerződési Feltételeket (ld. 1.5 alfejezet); ehhez kapcsolódóan az előkészítéshez eljuttatja a személyazonosító dokumentumainak másolatát a Szolgáltatóhoz vagy személyesen bemutatja azokat a Szolgáltató regisztrációs munkatársai előtt,

 „A” és „B” osztályban a regisztráció eredeti dokumentumok alapján történik, a személyazonosítás és szolgáltatási szerződés megkötése pedig személyes találkozás mellett történik,

 „C” osztályban a regisztráció az eredeti dokumentumokról készült másolatok alapján történik,

a Szolgáltató fogadja a kérelmet, illetve ellenőrzi annak szabályosságát,

a Szolgáltató azonosítja az igénylő természetes személyt és szükség esetén közhiteles vagy QGIS nyilvántartásokban ellenőrzi a kérelmező által megadott személyes adatokat,

a Szolgáltató – amennyiben lehetséges és értelmezett – elektronikus úton ellenőrzi a kérelmező által megadott szervezeti adatokat,

az Igénylő vagy a Regisztrációs Egység munkatársa – amennyiben értelmezett - elkészíti szolgáltatási szerződését, előkészíti a további regisztrációhoz szükséges dokumentumokat,

a Szolgáltató - amennyiben a személy- és szervezetazonosítás rendben lezárult - átveszi az alannyal (és a másodlagos alannyal) kötött szolgáltatási szerződését -, és összeveti az abban foglalt adatokat a személy- és szervezetazonosítás során ellenőrzött adatokkal,

a Szolgáltató közhiteles vagy QGIS nyilvántartásokban – amennyiben lehetséges - elektronikus úton is ellenőrzi a kérelmező által megadott személyes és szervezeti adatokat A, B, C osztályú tanúsítványok esetében,

a Szolgáltató összeállítja a kibocsátandó tanúsítványt,

a Szolgáltató kibocsátja a tanúsítványt az összes ellenőrzés pozitív lezárása esetén,

a Szolgáltató dokumentálja a regisztrációs lépéseket.

##### Speciális lépesek eszközszolgáltatás esetén

A szolgáltató authetnikációs, titkosító, és kódaláíró tanúsítványok esetében biztosít eszközszolgáltatást, SSL tanúsítványok esetében nem

Az eszközszolgáltatás esetén:

a kulcspárt a Szolgáltató generálja az igénylő számára az „hitelesítés-létrehozó adat elhelyezése aláírás-létrehozó eszközön” szolgáltatás keretében,

A Szolgáltató biztonságos módon eljuttatja az Igénylőhöz a kulcspárt és a tanúsítványt tartalmazó aláírás-létrehozó eszközt.

##### Regisztráció során nyilvántartásba vett adatok köre ezen tanúsítványok esetén

az ügyfél által megadott cím és/vagy más elérhetőség,

az igénylő által a regisztráció támogatása céljából benyújtott dokumentum(ok) típusa és maguk a dokumentumok, másolataik,

az azonosítási dokumentumok egyedi azonosító adatai, és azonosító számai,

a kérelem és az azonosítási dokumentumok – beleértve az Aláíró féllel kötött megállapodást – másolatainak tárolási helyszíne,

az Aláíró féllel kötött megállapodás esetleges specifikus választásai,

az ügyfélnek a rá vonatkozó kötelezettségekkel történő egyetértése,

a kérelmet elfogadó egység azonosítója,

a kérelem életciklusa során az igénylővel folytatott elektronikus és hagyományos levelezés, kommunikáció (pl. telefon) naplója,

minden, a tanúsítványok kiadásához kapcsolódó információ.

A Szolgáltató a nyilvántartásokat az ügyféllel közölt időpontig, illetve a jogszabályi előírásoknak megfelelően addig, ameddig a tanúsítványokra jogi eljárások során bizonyítási célból szükség lehet, megőrzi (ld. még 5.5 alfejezet).

### Ellenőrzésekre vonatkozó szabályok OV SSL tanúsítványok esetén

Az alábbi fejezetek az OV SSL tanúsítványokra egyaránt vonatkozó ellenőrzéseket taglalják.

#### Domain név ellenőrzése

A domain név ellenőrzését minden egyes befoglalt domainre szükséges elvégezni, hogy a tanúsítvány kiadás pillanatában az Igénylő (vagy anya leányvállalat, affiliate) birtokolja a domaint, a következő módok egyikén:

1. A domain birtokosának ellenőrzése a domain regisztrátor cégen keresztül

2. Kommunikáció a domain birtokosával e-mailen telefonon, azon az elérhhetőségen, amit a regisztrátor adott meg

3. Direkt email vagy telefonos kommunikáció a domain birtokossal, amely adat a whois rekordok administrative, registrant technical, vagy administrative mezőjéből származik

4. Kommunikáció a domain administrátorával egy email címen keresztül, ami az ’admin administrator| webmaster hostmaster postmaster előtagú, és az igényelt fődomainre, vagy aldomainre szól.

5. Domain engedélyező dokumentumra hagyatkozva

6. Az igénylő olyan praktikus kontrollal történő ellenőrzésre, ahol egy olyan online információ megváltoztatása a kérés az igénylő felé, amely információ tartalmazza az igénylő által igénylőt FQDN-t.

Ennek megvalósítása történhet az igénylő weboldalán egyedi kód elhelyezésével, majd annak leolvasásával, illetve a DNS bejegyzések közé, TXT rekord felvételével, a kért domain alá, a megfelelő egyedi kóddal.

A domain nevek esetén kevert karakterkészlet esetében a High risk listán és homonym veszélyre az ellenőrzés szükséges.

A szolgáltató jelenleg kever karakterkészletű domain névhez tanúsítványt nem állít ki.

#### IP cím ellenőrzése

A szolgáltató nem ad IP címre tanúsítványt.

#### Wildcard Domain név ellenőrzése

Wildcard tanúsítvány kiadása előtt a CA-nak meg kell győződnie arról, hogy a wildcarddal lefedett teljes domain név tartomány kontrollja az igénylőnél van.

A wildcard segítségével nem fedhető le teljes TLD vagy ccTLD tartomány, a CA-nak ezt amíg nincs megfelelő RFC rá, publikus listák alapján ellenőriznie kell.

Ilyen ellenőrző lista található az alábbi oldalon: http://publicsuffix.org

#### Új gTLD domainek

A folyamatban lévő gTLD kérelmekre a CA NEM adhat tanúsítványt a Szolgálrató.

Adott gTLD bejegyzése után 30 nappal adott gTLD-re adható tanúsítvány.

#### Az Igénylő azonosságának ellenőrzése

Ha a tanúsítványba bekerül az igénylő neve vagy címe, akkor a CA-nak ellenőriznie kell, hogy a cím az igénylő működési címe, ennek ellenőrzése megtörténhet az alábbi forrásokból származó dokumentációk egyikével:

1. kormányzati forrás segítségével
2. harmadik fél rendszeresen frissített, megbízható adatforrásával
3. Helyszínre kiszállással, ahol a kiszálló személy a szolgáltató ügynökeként végez tevékenységet.

A CA a fenti adatforrásokat egyaránt használhatja azonosság és cím megállapítására.

#### DBA/ márkanév

Ha a tanúsítványba bekerül a DBA/márkanév, akkor a a CA-nak ellenőriznie kell a használat jogát a következő módok, hogy a cím az igénylő működési címe, ennek ellenőrzése megtörténhet az alábbi forrásokból származó dokumentációk egyikével:

1. kormányzati forrás segítségével
2. harmadik fél rendszeresen frissített, Megbízható adatforrásával

#### A tanúsítványkérelem forrása

A tanúsítvány kérelem forrása, abban az esetben, ha a tanúsítványba szervezet neve kerül, a CA-nak meg kell győződnie róla, megbízható kommunikációs módon, hogy a szervezet képviselőjétől érkezett.

A CA biztosíthat megbízható módot arra, hogy egy szervezet képviselője meghatalmazzon személyket az igénylés lebonyolítására.

#### Magánszemély igénylő ellenőrzése

A CA ellenőrizheti az igénylő nevét egy megfelelő másolat alapján, ami az igénylő képét mutatja, egy kormányzat által kibocsátott fényképes igazolvány alapján.

A másolatot a Ca-nak vizsgálnia kell hamisítás szempontjából

#### Az ország ellenőrzése

Az ország ellenőrzése történhet a következő módon:

1. ccTLD –je a kérd domain névnek
2. az Igénylő azonosságának ellenőrzése során beszerzett információk alapján

#### A tanúsítvány adatok kora

A beszerzett dokumentumok maximum 39 hónapig használhatók fel tanúsítványkiadásra.

#### ONION domain nevek

A hitelesítés szolgáltató jelen szabályzat alapján jelenleg NEM ad ki .onion TLD-re tanúsítványt.

### Regisztrációs eljárások

#### Regisztrációs eljárás DV tanúsítvány esetén

| **Eljárási lépés** | **Tevékenység** | **Végrehajtani jogosult** |
| --- | --- | --- |
| 1. Regisztráció | Ha az igénylőnek korábban nem volt rendelése, akkor az ügyfélmenü az első rendelés során jön létre. Ha volt, akkor az ügyfélnek be kell lépnie és a megrendelést a menüben kezdeményeznie.  | Igénylő  |
| 2. Rendeléshez szükséges lépések elvégzése | Szerveren történő kulcsgenerálás, CSR feltöltése a rendelési folyamatba, illetve az igényléshez szükséges adatok, paraméterek megadása. | Igénylő |
| 3. Automatizált hitelesítési eljárások elvégzése | A domain feletti felügyeleti képesség és a domaint kiszolgáló szerverhez, vagy a domain DNS TXT rekordjához való hozzáférés ellenőrzése. | Automatizált rendszer |
| 4. Fizetés | Elektronikus felületen történő fizetés. | Igénylő |
| 5. Kiadás | A tanúsítvány kiadása az igénylő kérésének megfelelő adatokkal és időpontban. | Automatizált rendszer |
| 6. Közzététel | Tanúsítvány közzététele a (nem nyilvános) tanúsítványtárban. | Automatizált rendszer |
| 7. Letöltés | A tanúsítvány letöltése. | Igénylő |

#### Regisztrációs eljárás titkosító, autentikációs, kódaláíró, OV tanúsítványok esetén

Ügyféllel kötött szerződés keretében egyedi eljárás is kiköthető, melynek során az alábbi folyamattól el lehet térni, de az eltérés nem érintheti az eljárás lényegi részét.

|  |  |
| --- | --- |
| **Eljárási lépés** | **Tanúsítványfajta** |
|  | Személyes | Munkatársi / Szervezeti | Szerver |
| 1. Regisztráció | Magánszemély adatainak (név, lakcím, telefon, fax, e-mail cím) elektronikus regisztrációja. A regisztráció támogatására az Igénylő a megküldött adatait alátámasztó dokumentumok másolatát megküldi vagy a Szolgáltató regisztrációs munkatársai előtt bemutatja.Végrehajtani jogosult: Igénylő, Központi Regisztrációs Egység, Kihelyezett Regisztrációs Egység, Mobil Regisztrációs Munkatársak | Szervezeti munkatárs adatainak (név, lakcím, telefon, fax, e-mail cím) elektronikus regisztrációja. A regisztráció támogatására az Igénylő a megküldött adatait alátámasztó dokumentumok másolatát eljuttatja a Szolgáltatóhoz vagy a Szolgáltató regisztrációs munkatársai előtt bemutatja.Végrehajtani jogosult: Igénylő, Központi Regisztrációs Egység, Kihelyezett Regisztrációs Egység, Mobil Regisztrációs Munkatársak. | Magánszemély vagy szervezeti munkatárs adatainak (név, lakcím, telefon, fax, e-mail cím) elektronikus regisztrációja. A regisztráció támogatására az Igénylő a megküldött adatait alátámasztó dokumentumok másolatát eljuttatja a Szolgáltatóhoz vagy a Szolgáltató regisztrációs munkatársai előtt bemutatja.Végrehajtani jogosult: Igénylő, Központi Regisztrációs Egység, Kihelyezett Regisztrációs Egység, Mobil Regisztrációs Munkatársak. |
| 2. Kapcsolt regisztráció | Nincs | Szervezet adatainak (név, székhely, telefon, fax, e-mail cím) elektronikus regisztrációja. A regisztráció támogatására az Igénylő a megküldött adatait alátámasztó dokumentumok másolatát eljuttatja a Szolgáltatóhoz vagy a Szolgáltató regisztrációs munkatársai előtt bemutatja.Végrehajtani jogosult: Igénylő munkatárs és Központi Regisztrációs Egység, Kihelyezett Regisztrációs Egység, Mobil Regisztrációs Munkatársak. | Szerver adatainak elektronikus regisztrációja (URL, székhely)Végrehajtani jogosult: Igénylő, Központi Regisztrációs Egység, Kihelyezett Regisztrációs Egység, Mobil Regisztrációs Munkatársak. |
| 3. Automatikus visszaigazolások, e-mail cím ellenőrzése, amennyiben az Igénylő rendelkezik e-mail címmel. | A Szolgáltató automatikus válaszlevélben igazolja vissza a tanúsítvány iránti kérelmet. Az Igénylőnek a visszaigazolásra válaszlevelet kell küldenie. Végrehajtani jogosult: Igénylő | A Szolgáltató automatikus válaszlevélben igazolja vissza a tanúsítvány iránti kérelmet. Az Igénylőnek a visszaigazolásra válaszlevelet kell küldenie.Végrehajtani jogosult: Igénylő | A Szolgáltató automatikus válaszlevélben igazolja vissza a tanúsítvány iránti kérelmet. Az Igénylőnek a visszaigazolásra válaszlevelet kell küldenie.Végrehajtani jogosult: Igénylő |
| 4. Természetes személy azonosítása, adatainak ellenőrzése közhiteles nyilvántartásban, ha szükséges | Végrehajtani jogosult: Központi Regisztrációs Egység munkatársa  | Végrehajtani jogosult: Központi Regisztrációs Egység munkatársa |
| 5. Szervezet azonosítása, adatainak ellenőrzése közhiteles nyilvántartásban | Nincs | Végrehajtani jogosult: Központi Regisztrációs Egység munkatársa  | Végrehajtani jogosult: Központi Regisztrációs Egység munkatársa  |
| 6. Kulcspár generálása eszközön és kérelem készítése (eszközszolgáltatás esetén) | Végrehajtani jogosult: Igénylő vagy Központi Regisztrációs Egység | Végrehajtani jogosult: Központi Regisztrációs Egység munkatársa  | Végrehajtani jogosult: Központi Regisztrációs Egység munkatársa  |
| 7. Ügyfélcsomag (PIN boríték, adatlap, számla, tájékoztató, hozzájáruló és elfogadó nyilatkozat, Szolgáltatási Szerződés) összeállítása és megküldése az Igénylőnek, amennyiben értelmezett | Végrehajtani jogosult: Központi Regisztrációs Egység | Végrehajtani jogosult: Központi Regisztrációs Egység |
| 8. Szolgáltatási Szerződés aláírás-hitelesített aláírása osztálytól függően személyesen a Központi, a Mobil Regisztrációs Egység, vagy közjegyző előtt, személyesen vagy másolatban beküldve | Végrehajtani jogosult: Igénylő  | Végrehajtani jogosult: Igénylő | Végrehajtani jogosult: Igénylő |
| 9. A Szolgáltatóhoz beérkezett, aláírás-hitelesített Szolgáltatási Szerződés, illetve annak kiállításának alapjául használt dokumentumok másolatának ellenőrzése | Végrehajtani jogosult: Központi Regisztrációs Egység | Végrehajtani jogosult: Központi Regisztrációs Egység |
| 10. Hordozóeszköz eljuttatása az aláíróhoz (eszközszolgáltatás esetén) | Végrehajtani jogosult: Igénylő választása szerint Központi Regisztrációs Egység, Mobil Regisztrációs Egység, Kihelyezett Regisztrációs Egység, Regisztrációs- és kézbesítési megbízott  | Nem értelmezett |
| 11. Személyazonosság ellenőrzése, a személyazonosító igazolványban szereplő fénykép megfeleltetése az Igénylőnek vagy Igénylőnek a személyazonosító igazolványban szereplő aláírás összevetése a Szolgáltatási Szerződésen levővel a Szolgáltató előtti személyes megjelenés során. | Végrehajtani jogosult: Igénylő választása szerint Központi Regisztrációs Egység, Mobil Regisztrációs Egység, Kihelyezett Regisztrációs Egység, Regisztrációs- és kézbesítési megbízott , közjegyző | Végrehajtani jogosult: Igénylő választása szerint Központi Regisztrációs Egység, Mobil Regisztrációs Egység, Kihelyezett Regisztrációs Egység, Regisztrációs- és kézbesítési megbízott, közjegyző |
| 12. Tanúsítvány előállítása  | Végrehajtani jogosult: Hitelesítő Egység | Végrehajtani jogosult: Hitelesítő Egység |
| 13. Tanúsítvány felfüggesztése | Végrehajtani jogosult: Automatikusan vagy a Központi Regisztrációs Egység által | Végrehajtani jogosult: Automatikusan vagy a Központi Regisztrációs Egység által |
| 14. Tanúsítvány tanúsítványtárban való közzététele | Végrehajtani jogosult: Automatikusan vagy a Központi Regisztrációs Egység által | Végrehajtani jogosult: Automatikusan vagy a Központi Regisztrációs Egység által |
| 15. Tanúsítvány hordozó eszközre való letöltése  | Végrehajtani jogosult: Igénylő vagy Igénylő vagy a Központi Regisztrációs Egység által | Nem értelmezett |
| 16. Tanúsítvány (re)aktiválása | Végrehajtani jogosult: Központi Regisztrációs Egység | Végrehajtani jogosult: Központi Regisztrációs Egység |
| 17. Dokumentáció | Tanúsítvány adatösszesítő lap, Igénylőlap vagy elektronikus aláírással hitelesített Szolgáltatási Szerződés, Személyes (és szervezeti) dokumentumösszesítő adatlap, Okmánymásolatok, E-mail cím ellenőrzés kinyomtatva, vagy egyéb megfelelő módon igazolva (Hozzájáruló és elfogadó nyilatkozat) | Tanúsítvány adatösszesítő lap, Igénylőlap vagy elektronikus aláírással hitelesített Szolgáltatási Szerződés, Személyes (és szervezeti) dokumentumösszesítő adatlap, Okmánymásolatok, E-mail cím ellenőrzés kinyomtatva, vagy egyéb megfelelő módon igazolva (Hozzájáruló és elfogadó nyilatkozat), Domain használati engedély, Domain ellenőrzési dokumentum |

### Szolgáltatási Szerződés

#### Szolgáltatási szerződés DV SSL tanúsítványok esetén

A szerződéskötés folyamata:

* A tanúsítvány igénylésével az Igénylő (későbbi Igénylő) és a Szolgáltató között Szerződés jön létre.
* A Szerződéskötésre az Igénylő (későbbi Igénylő) által a Szolgáltató részére eljuttatott és egyúttal ajánlatnak minősülő tanúsítványigénylése alapján kerül sor.
* Az igénylés véglegesítésével egyidejűleg az Igénylő kifejezetten elfogadja a jelen Szolgáltatási Szabályzatban foglaltakat és azt magára kötelezőnek ismeri el.

A tanúsítvány kibocsátásával a Szolgáltató magára nézve kötelezőnek ismeri el a jelen Szolgáltatási Szabályzatban foglaltakat

#### Szolgáltatási szerződés titkosító, kódaláíró és autentikációs és OV SSL típusú tanúsítványok esetén

A természetes személy és/vagy szervezet és a magánkulcs összetartozásának dokumentálására, illetve a kötelező tájékoztatásra a Szolgáltató Szolgáltatási Szerződést alkalmaz. A szerződés feltételeit az ÁSZF [13], jelen Szolgáltatási Szabályzat, illetve az Aláíró elfogadó nyilatkozata (Belépési Nyilatkozat) tartalmazza. A Szolgáltató ezen dokumentumokat az Aláíró számára történő elektronikus rendelkezésre bocsátásával az abban foglaltakat magára nézve kötelezőnek fogadja el. A Szolgáltatási Szerződést ezen dokumentumok együttese jelenti. Az Igénylő részéről feltételeket elfogadó nyilatkozat kapcsán a közjegyzők és Központi-, a Kihelyezett, vagy a Mobil Regisztrációs Egység munkatársai („A”, „B” és „C” osztályban), Regisztrációs- és Kézbesítési Megbízott („B” és „C” osztályban) aláírás-hitelesítést végeznek. A tanúsítvány kiadásának feltétele ezen szerződés létrejötte. A Szolgáltatási Szerződés akkor lép hatályba, ha az ügyfél a Szolgáltató, vagy annak egyéb regisztrációs egységei előtt személyesen megjelent és azonosítása Szolgáltató által megtörtént. „C” osztályban a fenti lehetőségeken kívül a 17/1999. (II. 5.) Korm. rendelet a távollévők között kötött szerződésről szóló jogszabály rendelkezései alapján is létrejöhet a szerződés.

A Szolgáltató előtti személyes megjelenés és ügyfél azonosítás („„A” és „B” osztály) kötelező, még a tanúsítvány kiadása előtt. Az ügyfél választása szerint ez teljesül:

a Központi Regisztrációs Egység előtt, a Szolgáltató vagy megbízottja székhelyén, vagy

a Mobil Regisztrációs Munkatárs előtt, Magyarország területén , vagy

a Regisztrációs és Kézbesítési Megbízott előtt, Magyarország területén

közjegyző előtt

a szolgáltató által szabályzott egyéb módon

A Szolgáltató az internetes oldalán, illetve az ügyfél-tájékoztató dokumentumokban közzéteszi, hogy az általa nyújtott szolgáltatások és szolgáltatáscsomagok során kiadott tanúsítványokat milyen módon lehet aláírás-hitelesítve aláírni. A Szolgáltató bizonyos feltételek esetében (pl. a tanúsítvánnyal az egy alkalommal, egyszerre vállalható kötelezettség meghatározott mértéke) kötelezően előírhatja, hogy a Központi vagy Mobil Regisztrációs Egység munkatársai vagy közjegyző előtt aláírás-hitelesített Szolgáltatási Szerződést fogad csak el; illetve meghatározott okirati formát követelhet meg.

### Belépési nyilatkozat tartalma

DV típusú tanúsítványok esetén Belépési nyilatkozat nincsen, az elfogadás az online felületen történő rendelés megtételével és a szerződéses feltételek elfogadásával történik.

Egyéb tanúsítványoknál a nyilatkozat, vagy melléklete legalább a következőket tartalmazza:

a nyilvános kulcs lenyomata (amennyiben lehetséges),

a kiadandó tanúsítvány „*Subject”* mezője (Igénylőazonosító),

az Igénylő azonosításához szükséges egyéb adatok,

a korlátozások, elfogadások,

a Szolgáltató által adatlapon közölt adatok.

A nyilvános kulcs lenyomat karaktereinek átírása:

0 – NULLA, 1 – EGY, 2 – KETTŐ, 3 – HÁROM, 4 – NÉGY, 5 – ÖT, 6 – HAT, 7 – HÉT, 8 – NYOLC, 9 – KILENC, A – ADÉL, B – BÉLA, C – CECIL, D – DÉNES, E – ELEMÉR és F – FERENC

Nem EV típusú tanúsítványok esetén a Belépési nyilatkozatot az Igénylő természetes személy vagy a szervezet törvényes, illetve meghatalmazott képviselője írja alá.

.

#### Belépési nyilatkozat minták

A Szolgáltató kérésre megküldi aláírás hitelesítésre előkészített belépési nyilatkozati mintákat.

### Tanúsítványkérelmek jóváhagyásának követelményei

#### DV SSL tanúsítványok esetén

A Szolgáltató csak akkor fogadja el a tanúsítványkérelmet, ha a következő feltételek teljesülnek:

* benyújtották a kérelmet a tanúsítvány kibocsátónak,
* a kérelemben szereplő adatok ellenőrizhetők és pontosak
* a regisztráció folyamán használt e-mail cím működőképes

#### Nem DV típusú tanúsítványok esetén

A Szolgáltató csak akkor fogadja el a tanúsítványkérelmet, ha a következő feltételek teljesülnek:

benyújtották a kérelmet a tanúsítvány kibocsátónak,

a természetes személy (akinek nevében az Igénylő eljár) azonos a kérelemben szereplő alannyal,

munkatársi tanúsítvány esetén a másodlagos Alany hozzájárult a kibocsátáshoz,

a kérelemben szereplő adatok ellenőrizhetők és pontosak.

az OV SSL tanúsítványok esetén a domain(ek) ellenőrzésre került(ek), valamint az Igénylő birtokában vannak a domainek vagy jogosult rendelkezni felettük

### Tanúsítványok tartalma

####  Nem DV típusú tanúsítványok esetén

A tanúsítványok tartalmazzák az alábbiakat:

a tanúsítvány azonosító kódját,

a Szolgáltató megnevezését, benne székhelyének ország-azonosítóját,

a tanúsítvány érvényességi idejének kezdetét és végét (amely nem lehet az érvényesség kezdete időpontnál korábbi),

az Igénylő nevét vagy amennyiben ilyen igénylést nyújtottak be, az álnevét (amennyiben értelmezett),

az Igénylőnek vagy Igénylőnek külön jogszabályban, illetve a Szabályzatban, illetőleg az Általános Szerződési Feltételekben meghatározott speciális jellemzőit, a tanúsítvány szándékolt felhasználásától függően,

azt a nyilvános kulcsot, amely az Igénylő által birtokolt magánkulcs párjának felel meg,

a tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat,

az adott tanúsítványt kibocsátó Hitelesítés-szolgáltató elektronikus aláírását.

### A tanúsítványok jellemzői

A Szolgáltató által kibocsátott tanúsítványok megfelelnek a következő követelményeknek:

a tanúsítványazonosító a kibocsátóra nézve egyedi,

a tanúsítványban foglalt megkülönböztetett név (DN, Distinguished Name) egyedi,

a kiadott tanúsítványokhoz tartozó kulcsok egyediek, ez alól természetesen kivételt jelent a megújított (amennyiben értelmezett) tanúsítványban szereplő kulcs,

a tanúsítványok a Szolgáltató megfelelő kiadó aláíró kulcsával vannak aláírva,

a tanúsítványok aláírása ellenőrizhető a tanúsítványban szereplő adatok és a Szolgáltató megfelelő nyilvános kulcsának felhasználásával.

### Az Igénylő tájékoztatása a kibocsátást megelőzően

A Szolgáltató a tanúsítvány Igénylőjét (vagy Igénylőt) magyar és/vagy angol nyelven, közérthetően és egyértelműen, írásban (a szabályzatok elektronikus publikálásával, és azok az ügyfélszolgálaton nyomtatott formában történő elhelyezésével) tájékoztatja a következőkről:

a tanúsítványok felhasználásával kapcsolatos alapvető előnyök,

a szolgáltatás igénybevételének feltételei,

a szolgáltatási díj,

az ügyfél jogai és kötelezettségei,

a magánkulcs felhasználásának és kezelésének gyakorlati módszere és szabályai,

a magánkulcs elvesztésének, kompromittálódásának veszélyei,

a tanúsítványok kibocsátásának körülményei,

a tanúsítvány használatának feltételei,

a tanúsítvánnyal kapcsolatos, a tanúsítványban meghatározott tárgybeli, időbeli, földrajzi vagy egyéb korlátozások,

a tanúsítvány érvényessége, érvényességi idejének lejárta,

a magánkulcs használatával kapcsolatosan szükséges biztonsági intézkedések,

a kulcshordozó eszköz használata, amennyiben a tanúsítvány kibocsátását kérő ezt a Szolgáltatótól szerzi be,

az irányadó szabályzatok tartalma, szerepe, elérésének módja,

a Szolgáltató minősítései,

a tanúsítványok visszavonásának, felfüggesztésének lehetősége,

a szolgáltatói nyilvános kulcs, valamint annak elérhetősége,

a panaszok benyújtására, a jogviták rendezésére vonatkozó szabályok,

Ezen adatoknak külön jogszabályban meghatározott körét az Alannyal jogviszonyban álló vagy jogviszonyt létesíteni kívánó harmadik személy számára kérésre is hozzáférhetővé teszi a Szolgáltató. Az Igénylő és Érintett Felek figyelmét a Szolgáltató külön felhívja az alábbiakra:

ha a hitelesítés-szolgáltatási rend nem nyilvános használatra szolgál,

ha a hitelesítési rend megköveteli aláírás-létrehozó eszköz használatát

ha a jelen követelményrendszer alapján meghatározott tanúsítvány alaptípusokat érintő előírások szűkítésére, illetve további követelmények támasztására kerül sor.

### Tanúsítványkérelmek elutasítása

A Szolgáltató elutasítja a tanúsítványkérelmeket, amennyiben

a tanúsítványigénylés nem teljes,

a tanúsítványigénylés nem helyes,

a jelen Szabályzatban felsorolt feltételek (ld. 4.2.4 pont) teljesülése nem bizonyítható az igényelt tanúsítvány fajtájának előírt módon,

a személy és/vagy szervezet kiléte nem állapítható meg minden kétséget kizáróan (amennyiben értelmezett), illetve a bemutatott iratok és okmányok eredetiségével, valódiságával vagy érvényességével kapcsolatban egyéb kétség merül fel,

a személy szervezethez tartozása nem egyértelmű (amennyiben értelmezett),

az Igénylő vagy TK, TJ, SZA (amennyiben értelmezett) felhatalmazása a tanúsítvány kibocsátásának kérésére nem egyértelmű,

az Igénylő vagy a másodlagos Alany nem járul hozzá másolat készítéséhez az okmányairól, és azokat nem mutatja be személyesen a Szolgáltató regisztrációs egységeinek munkatársai előtt sem (amennyiben a dokumentumok bemutatása értelmezett),

az igényléssel érintett domain név használatát nem tudja bizonyítani a Szolgáltató által meghatározott műszaki lépésekben,

az igényelt tanúsítvány típusától függően nem tudja hitelt érdemlően igazolni a domain név tulajdonosától származó engedéllyel, hogy jogosult használni az igényléssel érintett domain nevet.

Az elutasított kérelmekről az Igénylő értesítést kap, melyben szerepel az elutasítás indoka, illetve annak kódja. Amennyiben az elutasítás oka harmadik fél által szolgáltatott információ, az értesítés megnevezi az elutasítást eredményező információforrást is.

### A tanúsítványokra vonatkozó további rendelkezések

A tanúsítvány előállítás során a Szolgáltató biztosítja a tanúsítványt kérő üzenet sértetlenségét, az adatforrás hitelességét, és ahol szükséges, annak bizalmasságát, illetve a személyhez fűződő jogok védelmét.

## A tanúsítványok kibocsátása és hozzáférhetővé tétele

### DV tanúsítványok esetén

A kész tanúsítvány a Tanúsítványtárba kerül, ahonnan az interneten elérhető ügyfélmenün keresztül, böngésző szoftver segítségével letölthető.

### Titkosító, összes típusú kódaláíró, autentikációs, OV SSL tanúsítványok esetén

A Regisztrációs és Hitelesítő egységek a 4.2.2 pontban leírt módon feldolgozzák a kérelmet, illetve előállítják a tanúsítványt. Erről az ügyfél külön értesítést kap. A kész tanúsítvány a Tanúsítványtárba kerül, ahonnan Internetes felületen keresztül Internet böngésző szoftver segítségével is letölthető (ld. még 2.2 alfejezet).

A Szolgáltató regisztrációs egységei a nem teljesített tanúsítványigénylésekről értesítést kapnak a hiba okának megjelölésével hibaüzenet formájában.

### A tanúsítvány kibocsátásának időpontja

A tanúsítvány kibocsátásának időpontja az az időpont, amikor a Szolgáltató az aláírt tanúsítványt elérhetővé teszi a tanúsítványtárban (ld. 2.4.1 alfejezet).

### A tanúsítvány érvényessége

A tanúsítvány érvényességének időtartama feltüntetésre kerül a tanúsítványban. Ezen időtartamon belül használható fel az igénylés során meghatározott, jelen Szabályzat előírásaival összhangban levő célra.

 A tanúsítvány érvényességének ellenőrzése a tanúsítványt használó Igénylő, illetve Érintett Fél felelőssége.

## Tanúsítványelfogadás

### A tanúsítvány elfogadása

A magánkulcs használatba vétele előtt az Igénylőnek, illetve a másodlagos Alanynak (amennyiben értelmezett) kötelessége ellenőrizni a tanúsítványban feltüntetett adatainak helyességét. Amennyiben bármilyen rendellenességet talál, a magánkulcsot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonása érdekében.

A magánkulcs és a tanúsítvány elfogadottnak tekintendő, ha az Igénylő a hordozóeszközt (amennyiben értelmezett) és/vagy a magánkulcsot, illetve a tanúsítványt átvette vagy letöltötte.

### A tanúsítványigénylő nyilatkozata

A tanúsítvány elfogadásával együtt az Igénylő, illetve a másodlagos Alany (amennyiben értelmezett) kijelenti, hogy:

ismeri, érti és elfogadja jelen és kapcsolódó szabályzatokat,

a tanúsítványt kizárólag a jelen és kapcsolódó szabályzatoknak megfelelően használja,

minden adat, amit a Szolgáltatónak a tanúsítvány kiadásának céljából átadott, a valóságnak megfelel, és azok átadása önkéntes volt,

amennyiben ilyen adatot tartalmazó tanúsítványt igényelt, a választott álnév mások jogait nem sérti,

a tanúsítványban szereplő minden adat a tudomásával és egyetértésével került a tanúsítványba,

a tanúsítvány érvényességét befolyásoló tényekről, valamint az igénylés során megadott személyes és szervezeti adatok megváltozása esetén haladéktalanul értesíti a Szolgáltatót,

tisztában van azzal, hogy a magánkulcs védelme kizárólag a saját felelőssége, s ezzel kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,

jogosulatlan személy nem férhet hozzá magánkulcsához,

az Igénylő végfelhasználó, azaz nem hitelesítés-szolgáltató, és nem fogja a tanúsítványban megadott nyilvános kulcs párját újabb tanúsítványok vagy bármely más formátumú tanúsított nyilvános kulcs, visszavonási lista, időbélyeg, OCSP válasz, viszontazonosítási válasz hitelesítésére és egyéb, hitelesítés-szolgáltatói funkciókra használni; hacsak erről külön írásbeli szerződésben a Szolgáltatóval meg nem egyezett,

amennyiben az Igénylő beleegyezett a tanúsítvány nyilvánosságra hozatalába, felhatalmazza a Szolgáltatót a tanúsítvány közzétételével, és saját vagy más nyilvános tanúsítványgyűjtő helyeken történő elhelyezésével.

### Tanúsítvány közzététele

A Szolgáltató csak abban az esetben teszi közzé a kiadott tanúsítványt, ha a tanúsítvány előfizetője illetve Igénylő ehhez előzetesen hozzájárult.

## A kulcspár és a tanúsítvány használata

### Az Igénylők számára szóló előírások

Az autentikációs tanúsítványok online rendszerekbe történő tanúsítvány alapú bejelentkezésre használhatók. A kulcsbirtokos személyének ellenőrzése egy elektronikus aláírási művelet segítségével, az autentikációval történik. Az elektronikus aláírási művelet ellenőrzésével lehet meggyőződni arról, hogy az aláírás műveletet a tanúsítványban szereplő nyilvános kulcs titkos párjával hajtották végre.

A kódaláíró tanúsítványok futtatható állományok aláírására használhatók. A kódon található elektronikus aláírási ellenőrzésével lehet meggyőződni arról, hogy

az aláírás a tanúsítványban szereplő nyilvános kulcs titkos párjával készült,

az aláírt állomány nem változott meg az elektronikus aláírás elkészülte óta.

Az SSL tanúsítványok szerverek hitelesítésére és a kommunikáció titkosítására használhatók.

Az SSL tanúsítvány ellenőrzésével lehet meggyőződni arról, hogy a tanúsítványban szereplő domain név birtokosa ellenőrzötten rendelkezik a hozzá tartozó magánkulccsal, valamint a tanúsítvány lehetővé teszi a titkosított kommunikációt.

Az Igénylő és a nyilvános kulcsú kódolást használó felek a jelen és kapcsolódó szabályzatok, illetve törvényi előírások és nemzetközi szabványok, szabályozások szerint járnak el a tanúsítványok használatakor, valamint az Igénylő:

1. magánkulcsát és tanúsítványát csak a hitelesítés-szolgáltatóval szerződésben rögzített korlátozásnak megfelelően használhatja,
2. a megfelelő tanúsítvány lejárta után nem használhatja tovább magánkulcsát.

#### Autentikációs tanúsítvány használata

Az autentikációs tanúsítvány használatáért elsősorban az Igénylő a felelős. Az Igénylő birtokolja a magánkulcsot, ismeri az alkalmazást, amelybe bejelentkezni kíván, dönt a bejelentkezési szándékról és üzemelteti bejelentkezéshez szükséges technikai eszközt.

Amennyiben az Igénylő nem körültekintően jár el, úgy az ebből származó kárért ő, valamint ha a tanúsítványban feltüntetésre került, a másodlagos Alany felel.

#### Titkosító tanúsítvány használata

A titkosító tanúsítvány használatáért elsősorban az Igénylő a felelős. Az Igénylő birtokolja a magánkulcsot, dönt a dekódolási szándékról és üzemelteti a szükséges technikai eszközt.

Amennyiben az Igénylő nem körültekintően jár el, úgy az ebből származó kárért ő, valamint ha a tanúsítványban feltüntetésre került, a másodlagos Alany felel.

#### Kódaláírás készítése

Az elektronikusan aláírt kód előállításának folyamatáért elsősorban az Aláíró a felelős. Az Aláíró birtokolja a magánkulcsot, ismeri az aláírandó kód tartalmát, dönt az aláírási szándékról és üzemelteti az aláírást elvégző technikai eszközt.

Amennyiben az Igénylő nem körültekintően jár el, úgy az ebből származó kárért ő, valamint ha a tanúsítványban feltüntetésre került, a másodlagos Alany felel.

#### SSL tanúsítvány használata (DV, OV / IV, EV)

A tanúsítvány és kulcsai szerveren történő biztonságos elhelyezéséért elsősorban az Igénylő felelős. Az Igénylő birtokolja a magánkulcsot és üzemelteti az SSL használatához szükséges technikai eszközt.

Amennyiben az Igénylő nem körültekintően jár el, úgy az ebből származó kárért ő, valamint ha a tanúsítványban feltüntetésre került, a másodlagos Alany felel.

#### Magánkulcs megőrzése

A titkosítás, SSL, kódaláírás vagy authentikáció csak akkor biztonságos, ha a magánkulcs a jogos birtokosán kívül soha, senki más számára nem hozzáférhető. A kulcsot jelszóval kódoltan és egyes esetekben hardvervédelemmel javasolt ellátni. A kulcs elvesztéséből, véletlen vagy szándékos nyilvánosságra hozatalából eredő károkért az a kulcs jogos birtokosa felelős. A kulcs kompromittálódását az előírt módon a Szolgáltatónál be kell jelenteni. A szabályosan bejelentett letiltási kérelem után a jelen Szabályzat 4.9.1 pontjában meghatározott módon felel a felmerült károkért az Igénylő, a másodlagos Alany (amennyiben értelmezett), illetve a Szolgáltató.

### Az Érintett Felek számára szóló ajánlások

Nem érvényes tanúsítvány esetén az elfogadásból eredő minden kár és kockázat az Érintett Felet terheli (lásd még 9.5.4 és 9.6.3 pont).

## Tanúsítvány megújítása

### Végfelhasználói tanúsítványok

#### Egyszerűsített megújítás (DV SSL)

DV SSL típusnál a megújítás nem értelmezett, helyette új tanúsítvány igénylése szükséges.

#### Egyszerűsített megújítás (autentikációs, titkosító, kódaláíró, OV/IV SSL)

A végfelhasználói tanúsítványok megújítására a kezdeti ellenőrzési lépések ismételt lefolytatása nélkül kizárólag a jelen pontban leírt módon van lehetőség, egy alkalommal, a megújítást megelőzően alkalmazott érvényességi idő megadásával.

Az alábbi eljárás alkalmazása a feltételek teljesítése esetén sem jelent kötelezettséget az Igénylő számára, csupán lehetőséget.

A Szolgáltató saját hatáskörben az okmányok ellenőrzésénél eltekinthet a személyes megjelenéstől.

##### Tanúsítvány megújítás általános feltételei

A tanúsítvány-megújítás általános feltételei:

* a tanúsítvány korábban nem volt megújítva,
* az Igénylő korábbiakban tanúsított nyilvános kulcsának kriptográfiai biztonsága még megfelelő az új tanúsítvány tervezett élettartamára, és nincs utalás arra vonatkozóan, hogy az Igénylő magánkulcsa kompromittálódott,
* az Igénylő, illetve a másodlagos Alany tanúsítványba foglalt adatai, valamint az ezeket igazoló azonosító dokumentumai érvényesek és az abban foglalt adatok nem változtak a tanúsítvány-igénylés óta,
* a tanúsítvány érvényessége még nem járt le,
* a tanúsítvány nem szerepel a visszavonási listán.

##### Rendkívüli tanúsítvány-megújítási eljárás

A fentieken túl a Szolgáltató – fenntartva a jogot a Szolgáltató internetes oldalán feltüntetett mindenkori külön eljárási díj kivetésére – biztosíthatja a korábban még meg nem újított tanúsítvány egyszerűsített módon történő megújítását abban az esetben, ha az Igénylő, illetve a másodlagos Alany kiléte változatlan marad és az Igénylő/másodlagos Alany azonosító adataiból legfeljebb egy, tanúsítványban szereplő adat változott meg.

##### A tanúsítvány-megújítási eljárás (autentikációs, titkosító, kódaláíró, OV SSL)

Amennyiben a szerződés megkötése óta az Igénylő, illetve a másodlagos Alany adataiban nem következett be változás, a megújítás során az Igénylő az Ügyfélmenüből letölthető, az adatait tartalmazó Szolgáltatási Szerződést (Belépési Nyilatkozatot) egy még érvényes aláíró kulcspárja segítségével érvényesen, elektronikusan aláírja és ezeket elektronikus úton eljuttatja a Szolgáltatónak. Ha az Igénylő, illetve a másodlagos Alany adataiban változás következett be, akkor az elektronikusan aláírt Szolgáltatási Szerződés mellé csatolni kell mellékletként a változott adatok igazolását.

A Szolgáltatási Szerződést (Belépési Nyilatkozatot) kinyomtatva és a tanúsítványosztályra vonatkozó előírásnak (lásd 4.2.3 pont) megfelelő módon aláírás-hitelesítve kell visszajuttatni a Szolgálathoz, ha az Igénylő nem rendelkezik érvényes aláíró tanúsítvánnyal, vagy nem áll módjában elektronikusan aláírással ellátni az Ügyfélmenüből letölthető, az Igénylő adatait tartalmazó Szolgáltatási Szerződést (Belépési Nyilatkozatot).

A Szolgáltató a beérkezett dokumentumok alapján (szükség esetén) közhiteles vagy QGIS elektronikus nyilvántartásokban ellenőrzi, hogy az Igénylő és a másodlagos Alany azonosságának igazolására használt információ még mindig érvényes. Amennyiben a Szolgáltató a nyilvántartásokban történő ellenőrzés során a kibocsátáskor megadott adatok változását észleli, az egyszerűsített tanúsítvány-megújítási kérelmet elutasítja, illetve fenntartja a jogot az újbóli, ezennel már a valóságnak megfelelő adatokat tartalmazó megújítási kérelem teljesítése esetén az internetes oldalán feltüntetett mindenkori különeljárási díj felszámítására.

Amennyiben a Szolgáltató bármely feltétele, illetve kikötése megváltozott, a változásról a Szolgáltató a tanúsítvány megújítása során tájékoztatja az Igénylőt, illetve a másodlagos Alanyt.

A tanúsítvány-megújítás során a Szolgáltató garantálja a feldolgozás biztonságát a tanúsítvány-helyettesítési támadás ellen.

### Szolgáltatói tanúsítványok

A Szolgáltató saját tanúsítványait legfeljebb egy alkalommal, alkalmanként a megújítást megelőzően alkalmazott érvényességi idő megadásával újítja meg.

## Kulcscsere

A kulcscsere az a folyamat, amelynek során a Szolgáltató úgy bocsát ki egy megújított tanúsítványt, hogy abban az eredeti tanúsítvány Igénylőre vonatkozó adatai közül csak a nyilvános kulcs kerül lecserélésre.

Kulcscsere esetére a Szolgáltató nem állapít meg külön eljárási szabályokat. (lásd. 3.33.3 pont) Amennyiben a tanúsítványban szereplő nyilvános kulcsot le kell cserélni, azt a Szolgáltató új tanúsítvány-igénylési kérelemként kezeli.

## Tanúsítvány módosítása

A tanúsítvány-módosítás az a folyamat, amelynek során a hitelesítés-szolgáltató úgy bocsát ki egy módosított tanúsítványt, hogy abban az eredeti tanúsítvány Igénylőre vonatkozó adatai – a nyilvános kulcs kivételével – változnak, és a tanúsítvány az új adatokkal, valamint a régi nyilvános kulccsal kerül kiadásra.

Tanúsítvány módosítására a Szolgáltató nem állapít meg külön eljárási szabályokat. Amennyiben a tanúsítványban szereplő adatok – a nyilvános kulcs kivételével – lecserélése szükségessé válik, azt a Szolgáltató új tanúsítvány-igénylési kérelemként kezeli.

## Tanúsítvány felfüggesztése és visszavonása

### Általános rendelkezések

Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatásokat nyújt.

A felfüggesztett és visszavont tanúsítványok érvénytelenek. A felfüggesztett tanúsítvány azonban csak a felfüggesztés időtartama alatt érvénytelen. A felfüggesztés meghatározott időtartamra szól, annak letelte után a Szolgáltató végleges döntést hoz (ld. még 4.9.10 pont).

A visszavont, illetve felfüggesztett tanúsítványhoz tartozó magánkulcs használatát azonnal meg kell szüntetni, illetve fel kell függeszteni. Amennyiben van rá lehetőség, a visszavont tanúsítványhoz tartozó magánkulcsot a visszavonást követően azonnal meg kell semmisíteni (ld. még 4.11 pont).

A visszavont, visszavonandó és felfüggesztett, felfüggesztendő tanúsítvány elfogadásából eredő károkra a következő felelősségi szabályok vonatkoznak:

a visszavonási/felfüggesztési kérelem Szolgáltatóhoz történő megérkezéséig az Általános Szerződési Feltételeknek és jelen szabályzatnak megfelelően az Igénylő, illetve a másodlagos Alany felelős a felmerülő károkért,

a visszavonási és felfüggesztési kérelem, Szolgáltató általi befogadását követően a nyilvánosságra hozatalig a Szolgáltató felelős a felmerülő károkért,

az érvénytelen állapot tanúsítványtárban való megjelenése után az Érintett Fél felelős a felmerülő károkért.

#### DV SSL –re vonatkozó speciális rendelkezések

Felfüggesztés művelete DV SSL tanúsítványok esetén nem értelmezett, csak visszavonásra van lehetőség.

#### OV SSL –re vonatkozó speciális rendelkezések

Felfüggesztés művelete OV SSL tanúsítványok csak visszavonási kérelem elbírálásának idejére van szükség, egyébként csak visszavonásra van lehetőség.

### A visszavonás körülményei

Végfelhasználói tanúsítvány visszavonásához a következő körülmények vezetnek:

végfelhasználói vagy szolgáltatói magánkulcs kompromittálódása, vagy a kompromittálódás gyanúja,

a tanúsítvány Igénylőainak (Igénylő vagy másodlagos Alany) kérelme,

a tanúsítvány használatának visszautasítása hibás tanúsítvány miatt,

a Szolgáltató tudomására jutott tény, vagy megalapozott vélelem a regisztrációs adatok valótlanságáról,

a tanúsítványban foglalt adatok megváltozása,

a tanúsítvány felfüggesztési idejének lejárata,

az Igénylő és a másodlagos Alany kötelezettségeinek be nem tartása,

rosszhiszemű felhasználás,

a bíróság erre vonatkozó jogerős és végrehajtható határozata,

a felhasználói szerződés megszűnése,

a hitelesítési szolgáltatás megszűnése,

visszavonást jogszabály teszi kötelezővé,

a tanúsítványba foglalt domain név tulajdonosának a domain név használatának visszavonására vonatkozó nyilatkozata.

Kompromittálódott magánkulcs soha többet nem használható, és megsemmisítéséig ugyanolyan felügyeletben részesítendő, mint egy érvényes magánkulcs.

### Visszavonás kérelmezése

A visszavonást az alábbi entitások kérelmezhetik:

|  |  |
| --- | --- |
| **Tanúsítványok** | **Visszavonást és felfüggesztést kérheti** |
| Végfelhasználói személyes tanúsítvány | Igénylő, Szolgáltató |
| Végfelhasználói munkatársi tanúsítvány | Igénylő, Másodlagos Alany, Szolgáltató |
| Végfelhasználói szervezeti tanúsítvány | Igénylő képviselője, Szolgáltató |
| SSL tanúsítványok | Domain név használója, domain név tulajdonosa, Másodlagos Alany, Szolgáltató |
| Minden végfelhasználói tanúsítvány | Harmadik fél, visszaélés gyanújával a szolgáltatónál |
| Szolgáltatói tanúsítványok | Szolgáltató, Felügyelet |

### Visszavonási kérelemre vonatkozó eljárás

Végfelhasználói tanúsítvány visszavonása egy visszavonási kérelem Szolgáltató számára történő benyújtásával kezdeményezhető. A visszavonási kérelem benyújtható:

Ügyfélszolgálati időben:

személyesen, a Szolgáltató székhelyén, a Központi Regisztrációs Egységnél,

Ügyfélszolgálati időben és azon kívül:

telefonon, a Szolgáltató ügyeleti rendszerén keresztül, folyamatosan, 0-24 órában,

a Szolgáltatónak küldött e-mailben, illetve faxon,

a Szolgáltató székhelyére küldött levélben.

Az egyes kérések feldolgozása az alábbiak szerint kerül végrehajtásra:

|  |  |  |  |
| --- | --- | --- | --- |
| tanúsítvány típus | kezdeményező | kezdeményezés módja | elérhetőség |
| DV SSL | Igénylő | online | 0-24 |
| OV SSL | Igénylő | telefon (Magyarország)email | 9-17 (CET)0-24 (feldolgozás a következő munkanapon) |
| kódaláíró tanúsítvány | Igénylő,Harmadik Fél | telefon (Magyarország)email | 9-17 (CET)0-24 (a feldolgozás következő munkanapon) |
| titkosító tanúsítvány | Igénylő | telefon (Magyarországon)email | 9-17 (CET)0-24 (de feldolgozás következő munkanapon) |
| autentikációs tanúsítvány | Igénylő | telefon (Magyarországon)email | 9-17 (CET)0-24 (de feldolgozás következő munkanapon) |

A visszavonási kérelemnek legalább a következő adatokat kell tartalmaznia:

a tanúsítvány sorszáma vagy egyedi neve,

a visszavonást kérő megnevezése,

a visszavonást kérő elérhetősége,

a visszavonást kérő kapcsolata a tanúsítvány Igénylőval,

a visszavonás oka.

A visszavonásra irányuló kérelmeket a Szolgáltató más kérelmeket megelőzően, soron kívül bírálja el.

A visszavonási eljárás során a Szolgáltató Központi Regisztrációs Egysége ellenőrzi a visszavonási kérelemben szereplő adatokat, a kérelmező személyazonosságát, a kérelem előterjesztésére való jogosultságát, a kérelemben foglalt indokok (ld. 4.9.2 pont) valóságalapját, illetve visszavonásra való alkalmasságát. A kérelemre vonatkozó fenti adatokat a Szolgáltató lehetőleg független, illetve az Igénylő által megadott forrásból ellenőrzi. A visszavonási kérelem hitelességének megállapításának alapjául a tanúsítvány kibocsátásakor alkalmazott ellenőrzési rend szolgál kiindulásként vagy az Igénylő egy aláíró magánkulcsának felhasználásával aláírt dokumentum vagy a személyes megjelenés esetén történő személyazonosság megállapítás. Ha az adatok helytelenek, az Igénylő kiléte vagy a visszavonásra való jogosultság nem állapítható meg, akkor Szolgáltató a tanúsítvány visszavonását megtagadja.

### Visszavonási kérelemre vonatkozó türelmi idő

A visszavonási lépések – figyelemmel az alábbiakban foglaltakra - a lehetséges legkisebb késlekedéssel követik egymást.

* A faxon, e-mailben, illetve postai úton érkezett visszavonási kérelmeket a Szolgáltató folyamatosan fogadja, feldolgozásukat azonban munkaidőben végzi, a munkaidőn túl érkezett kérelmeket a következő munkanapon bírálja el.
* A telefonon keresztül érkezett visszavonási kérelmeket a Szolgáltató folyamatosan fogadja és haladéktalanul megkezdi azok feldolgozását, a feldolgozás nem függ a Szolgáltató ügyfélszolgálati idejétől.
* A feldolgozás megkezdése és a tanúsítvány státuszváltásról való döntést követően Szolgáltató a tanúsítványállapot-adatbázist szükség esetén késedelem nélkül frissíti.

Az emberi beavatkozást Igénylő visszavonási kérelmek feldolgozásának ideje 24 óra. Amennyiben ezen időszak alatt a Szolgáltató önhibáján kívül nem képes a visszavonási vagy felfüggesztési kérelem jogszerűségéről – a benyújtó személy jogosultságáról vagy a visszavonást indokoló tény valóságalapjáról - megbizonyosodni, úgy a továbbiakban – ellenkező tény tudomására jutásáig – a visszavonási kérelmet illetéktelen személytől származónak tekinti, és a visszavonási vagy felfüggesztési folyamatot eredménytelenként lezárja.

A visszavont tanúsítvány státusza azonnal bekerül a tanúsítványtárba (ún. tanúsítványállapot-adatbázisba), ezzel lehetővé téve a valós idejű visszavonási állapot ellenőrzést. A tanúsítványállapot-változást követő legkésőbb 1 órán belül új visszavonási lista kiadására is sor kerül, mely ugyancsak tartalmazza a tanúsítvány megváltozott státuszát.

### Visszavonásra vonatkozó egyéb szabályok

A visszavonási kérés és válasz üzeneteket a Szolgáltató védi a visszajátszáson alapuló támadások ellen.

A Szolgáltató rendszerei ésszerű határokon belül képesek üzemzavar vagy katasztrófa esetén is minden kibocsátott tanúsítvány visszavonására.

A végfelhasználói tanúsítványokat aláíró, az infrastrukturális és az időbélyegzéshez használt kulcsokhoz tartozó tanúsítványok visszavonása kettős ellenőrzés mellett történik.

Amennyiben egy tanúsítvány visszavonásra került, azt nem lehet újra használatba venni.

Visszavont tanúsítvánnyal végzett művelet érvénytelennek tekintendő.

### A felfüggesztés körülményei

A tanúsítvány felfüggesztéséhez a visszavonáshoz vezető körülmények fennállására vonatkozó alapos gyanú vezethet.

Szolgáltató saját belátása szerint, a visszavonási kérelmeket ideiglenesen kielégítheti felfüggesztéssel is, amennyiben a bejelentett körülmények kivizsgálását szükségesnek tartja.

### Felfüggesztés kérelmezése

A felfüggesztést ugyanazok kérelmezhetik, akik a visszavonást (ld. 4.9.3 pont), kiegészítve olyan harmadik felekkel, akik hitelt érdemlő módon bizonyítani tudják a visszavonáshoz vagy felfüggesztéshez vezető körülmények alapos gyanújának a fennállását.

Egyes tanúsítványtípusok esetén a felfüggesztés nem, csak visszavonás kérhetó.

### Felfüggesztési kérelemre vonatkozó eljárás

A felfüggesztési kérelem a visszavonási kérelemhez hasonlóan (lásd előzőekben) nyújtható be Szolgáltatóhoz, továbbá – amennyiben elérhető - a felfüggesztés esetében lehetőség van automata felfüggesztési rendszer igénybe vételére is. Harmadik fél által történő beadás esetén Szolgáltató a rendelkezésére álló eszközökkel meggyőződik a személy kilétéről, a felfüggesztési kérelem jogosságáról. A felfüggesztési kérelmet a visszavonási kérelemmel megegyező módon dolgozza fel Szolgáltató, ha azonban az automata felfüggesztési rendszer útján történik a felfüggesztés akkor, annak jogosult használata esetén a kérelemre vonatkozó 4.9.4. pontban részletezett adatokat a Szolgáltató egyéb módon nem vizsgálja.

Automatikus felfüggesztés esetén a felfüggesztés automatikusan, Szolgáltatói humán közreműködés nélkül hajtódik végre. Az automata felfüggesztési rendszer használatával beadott kérelmeket azonnal teljesíti.

Az automatikus, humán beavatkozást nem igénylő felfüggesztési kérelem feldolgozása nem függ a Szolgáltató ügyfélszolgálati idejétől, a rendszer jogosult használatával történt bejelentéseket a Szolgáltató azonnal, mérlegelés nélkül végrehajtja. Az automatikus rendszerben indított kérelmek bejelentése és a valamint a tanúsítvány státuszának tanúsítványállapot-adatbázisba való bekerülése között normál üzemmenet esetén nem telik el több, mint 30 perc; rendkívüli üzemeltetési helyzet esetére az 5.7.4. pontban vállalt határidő az irányadó.

### A felfüggesztés időtartamára vonatkozó korlátozások

Érvényes tanúsítvány felfüggesztett állapotban addig lehet, míg a visszavonáshoz vezető körülmények fennállásának gyanúja bizonyítást vagy cáfolatot nem nyer, de legfeljebb 30 munkanapig. Ez alól a kibocsátás során a Szolgáltató általi technikai felfüggesztés időtartama jelent kivételt, mely során a tanúsítvány legfeljebb 30 naptári napig lehet felfüggesztett állapotban. Ezen technikai felfüggesztésre csak egy alkalommal kerülhet sor és a tanúsítvány kibocsátásától annak aktiválásáig tart. Minden egyéb esetben a felfüggesztés ideje legfeljebb 30 munkanap lehet. A tanúsítvány visszavonásáról, illetve újbóli érvényesre állításáról Szolgáltatónak a lehető leghamarabb intézkednie kell. A felfüggesztett állapot kezdő időpontja a felfüggesztési kérelem elfogadásától számítandó. Ha ez idő alatt a visszavonáshoz vezető körülmények gyanúja cáfolatot nem nyer, Szolgáltató a tanúsítványt visszavonja.

A Szolgáltató honlapján keresztül kezdeményezett automatikus tanúsítvány felfüggesztés – amennyiben elérhető - annak sikeres kezdeményezése időpontjától számított 30 munkanapig lehet ebben az állapotban, ezen idő elteltét követően a tanúsítvány automatikusan visszavonásra kerül.

Felfüggesztett tanúsítvánnyal végzett művelet érvénytelennek tekintendő.

#### Újraérvényesítés módja

A tanúsítvány újbóli érvénybe helyezését az Igénylő és – adott esetben - a másodlagos Alany kérelmezheti a visszavonásra vonatkozó eljárási rend szerinti módon és az ott minimálisan előírt adatok megküldése révén. A kérelem során a honlapon feltüntetett mindenkori különeljárási díjat számíthatja fel a Szolgáltató.

### Kulcskompromittálódás esetére vonatkozó speciális követelmények

Magánkulcs kompromittálódása vagy vélelmezett kompromittálódása esetén a visszavonási eljárásban leírt lépések végrehajtandóak. Kompromittálódott magánkulcs soha többet nem használható, és megsemmisítéséig ugyanolyan felügyeletben részesítendő, mint egy érvényes magánkulcs. Az Igénylő, illetve a másodlagos Alany kötelessége a kompromittálódott magánkulcs által esetlegesen érintett felek értesítése, és minden intézkedés megtétele az esetleges károk megelőzése vagy enyhítése érdekében.

## Tanúsítvány-állapot információk közzététele

### Tanúsítvány Visszavonási Lista (CRL)

A Szolgáltató X.509 V2 típusú tanúsítvány visszavonási listák kibocsátását és tanúsítvány visszavonási kiterjesztések alkalmazását támogatja.

A Szolgáltató a CRL listán jelöli annak érvényességi idejét. CRL egy előző CRL érvényességi ideje alatt is kibocsátható. Amennyiben egy időben több érvényes CRL is létezik, a legutolsó az irányadó.

A CRL tartalmazhatja a tanúsítvány visszavonásának okát.

A Szolgáltató a visszavont tanúsítványok listáját a crl1.NETLOCK.hu, crl2.NETLOCK.hu és crl3.NETLOCK.hu internet címeken (URL) publikálja.

A Szolgáltató feltüntetheti a tanúsítványokban az internet címeket (URL) is, amelyeken keresztül elérhető a visszavont tanúsítványok listája (a feltüntetés a CDP mezőben történik), egyes címek elérhetetlensége esetén a soron következő elérhetőt kell használni.

A CRL ellenőrzése ajánlott minden Érintett Fél részére az elektronikus aláírás ellenőrzési eljárásának részeként, az elvárható gondosság követelményének megfelelően. A CRL-en szereplő, - azaz érvénytelen tanúsítvány – elfogadása az Érintett Fél önhibájának minősül, így az ebből adódó kárért felel..

A Szolgáltató az egyes CRL-eket a kapcsolódó egyéb adatok megőrzési idejével megegyező ideig őrzi meg (ld. 5.5.2 pont).

A visszavonási listán azon visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre, amelyek érvényességi ideje még nem járt le. Ezen kívül Szolgáltató kibocsáthat olyan visszavonási listákat, melyeken az összes visszavont tanúsítvány (érvényességi idejüktől függetlenül), illetve a kibocsátás pillanatában felfüggesztett tanúsítványok kerülnek feltüntetésre.

A visszavonási lista kibocsátása a Szolgáltató tanúsítványtárába történik. A listák kibocsátása közt legfeljebb 24 óra telik el. Ezen időközönként CRL akkor is kibocsátásra kerül, ha a legutóbbi kibocsátás óta nem történt tanúsítvány visszavonás vagy felfüggesztés.

Tanúsítvány visszavonása vagy felfüggesztése esetén a tanúsítványállapot-változásnak a Szolgáltató nyilvántartásában való átvezetést követő 1 órán belül a Szolgáltatónak a kérelem szerint módosított visszavonási állapotot közzéteszi.

A visszavonási listák mindig tartalmazzák a következő lista kibocsátásnak idejét, melyet megelőzve is kibocsáthat Szolgáltató új listát. A listák érvényességi ideje legfeljebb 24 óra.

A felfüggesztett tanúsítványok az újbóli érvényesítés hatására kerülhetnek ki a listából.

Szolgáltató gyökértanúsítványait biztonsági okokból off-line módon tárolja, biztonságos - zárt – zónában. Gyökértanúsítványok esetén ezért a CRL kiadás sűrűsége és a lista érvényessége a többi rendszertől eltér. Ezen CRL listák kibocsátása között sem telhet el több mint 90 nap. Mivel azonban az automata rendszerek által vizsgált tanúsítványok esetén az aláírást hitelesítő teljes tanúsítványláncolat ellenőrzése így hosszabb időt vehet igénybe, ezért Szolgáltató fenntartja magának a lehetőséget arra, hogy - a gyökértanúsítvány által kibocsátott tanúsítványokra - delegált CRL aláíró tanúsítványt bocsásson ki, illetve azonnali OCSP válasszal tegye lehetővé a tanúsítványláncolat ellenőrzését.

### Az ajánlott CRL ellenőrzés az Érintett Fél számára

A visszavonási lista ellenőrzése érintett felek részére ajánlott a tanúsítványok elfogadását megelőzően tekintettel a 4.5.2 pontban foglaltakra. A lista ellenőrzésének arra kell vonatkozni, hogy a kérdéses tanúsítványt a lista tartalmazza-e, a lista hiteles és sértetlen-e, és a kérdéses tranzakció szempontjából időben releváns-e.

Szolgáltatót nem terheli felelősség a visszavonási listában közzétett tanúsítványok elfogadásából keletkező esetleges károkért.

### Valós idejű visszavonási állapot ellenőrzés elérhetősége

A Szolgáltató valós idejű visszavonási állapot-szolgáltatásokat is nyújt, melyet egyrészt a tanúsítványállapot-nyilvántartáson keresztül, másrészt az OCSP szolgáltatás segítségével érhető el.

A tanúsítványállapot-nyilvántartás a Szolgáltató tanúsítványtárán keresztül érhető el.

A Szolgáltató a tanúsítványállapot-adatbázisa lekérdezéséhez támogatja az OCSP (Online Certificate Status Protocol) protokollt. Az OCSP szolgáltatás elérhető a kiadóhoz tartozó válaszadó internet címén, valamint a tanúsítványtárban közzétett egyéb címeken. Az aktuális OCSP válaszadótanúsítványok és a rájuk vonatkozó visszavonási listák a Szolgáltató tanúsítványtárában érhetőek el.

A Szolgáltató feltüntetheti a tanúsítványokban az internet címeket (URL) is, amelyeken keresztül elérhető a valós idejű visszavonási állapot ellenőrzés (a tanúsítvány AIA:OCSP mezőjében kerül feltüntetésre), a címek közül egyik elérhetetlensége esetén a következő elérhetőt kell használni.

### Valós idejű visszavonás ellenőrzési követelmények

A tanúsítványállapot-adatbázis bárki számára hozzáférhető, kereshető a Szolgáltató tanúsítványtárán keresztül. Ez alól kivételt képez a DV SSL tanúsítvány típus. Az adatbázisban mindig a keresett tanúsítvány aktuális állapota található.

Az OCSP válaszokat aláíró tanúsítványok profilját a 7.1 pont tartalmazza. Az OCSP szolgáltatás által kiadott, elektronikusan aláírt válaszokat az Érintett Félnek ellenőriznie kell, melynek lépéseit a 9.5.4 pont tartalmazza. Az érvénytelennek bizonyult OCSP válaszokat elfogadni nem szabad, ez esetben a tanúsítványállapot-adatbázis adataira, illetve a visszavonási listákra kell támaszkodni.

A valós idejű visszavonás szolgáltatások hozzáférési díjait az árlistában elérhető.

### A visszavonási információ közzétételének egyéb formái

A visszavonási hirdetmények csak a Szolgáltató tanúsítványtárában és annak biztonsági másolatában, illetve két másik tárban érhetők el. A Szolgáltató saját szolgáltatói tanúsítványának állapotváltozásait, sajtóközleményt jelentet meg, illetve közzéteszi saját weboldalán.

## Tanúsítvány-előfizetés vége

A Szolgáltató által kiadott tanúsítványok érvényességi ideje és az adott tanúsítvány előfizetési ideje összekapcsolódik, vagyis az előfizetési idő megegyezik a tanúsítványban feltüntetett érvényességgel. Mindez nem zárja ki természetesen, hogy a Szolgáltató – kivételesen, egyedileg meghatározott esetben – a tanúsítványok díjaira vonatkozóan különböző fizetési kedvezményeket határozzon meg (pl. részletfizetés, kedvezmény, stb.).

Amennyiben az Igénylő még a tanúsítványban feltüntetett érvényességi idő lejárta előtt kívánja lemondani az előfizetést, úgy a tanúsítvány visszavonására vonatkozó szabályok az irányadóak (lásd 4.9 pont). A visszavonással egy időben a szolgáltatási szerződés megszűnik.

Ha az tanúsítvány érvényességének lejártakor az Igénylő a Szolgáltató előírásai szerint (lásd 4.6.1 pont) nem újítja meg a tanúsítványt, a Szolgáltatási Szerződés automatikusan megszűnik.

## Kulcs letétbe helyezése és visszaállítása

Szolgáltató nem nyújt magánkulcs letéti szolgáltatást, illetve az Igénylő magánkulcsát semmilyen más módon nem tárolja el vagy menti. Ez alól kivételt képez a titkosító tanúsítvány típus.

A Szolgáltató a saját, szolgáltatói magánkulcsait elmentve is tárolja.

# 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 (second site) tárolja. A két helyszín biztonsági előírására vonatkozó szabályok egyenszilárdságúak, az esetleges eltérések a megfelelő pontoknál feltüntetésre kerültek. Ezen túlmenően a Szolgáltató több helyszínen alárendelt elektronikus aláírással kapcsolatos szolgáltatást nyújt – ezen szolgáltatások pontos helyszínei, illetve a szolgáltatásokra vonatkozó nyilvános szabályzatok megtalálhatóak a Szolgáltató honlapján.

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

Az egységek megfelelő működésének biztosítása érdekében a rendszer szoftver és hardver elemein az operációs dokumentumokban meghatározott módon és rendszerességgel, az arra kijelölt személyek belső karbantartást végeznek, a munka naplózásával.

Az egységek adatállományairól biztonsági mentések készülnek (ld. 5.5 alfejezet). A mentéseket a Szolgáltató a 5.5.2 pontban meghatározott ideig megőrzi.

Az alábbi szolgáltatásokat biztosító rendszerek ellenállnak az egyszeres meghibásodásnak: tanúsítvány kibocsátás, visszavonás-kezelés, visszavonási állapot-közzététel. E szolgáltatások a nem minősített tanúsítványok esetén legalább 99%-os rendelkezésre állással elérhetők, egyúttal az eseti szolgáltatás kiesések nem haladják meg a 24 órás időtartamot (lásd még 5.7.4 pont).

A biztonsági szabályokra vonatkozó rendelkezéseket a nem nyilvános Biztonsági Szabályzat tartalmazza.

A folyamatos, magas színvonalú biztonságos szolgáltatás fenntartására a Szolgáltató ISO 27001 (korábban BS 7799-2: elnevezésű) szabványnak megfelelő információbiztonsági irányítási rendszert alkalmaz, amelyet független külső és belső auditorok vizsgálnak folyamatosan, továbbá ISO 9001 szabvány szerinti minőségirányítási rendszert üzemeltet.

## Fizikai óvintézkedések

A fizikai óvintézkedések célja a Szolgáltató bizalmas információira és fizikai körleteire irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken valósítják meg a Szolgáltató rendszerében. A biztosított védelem arányban áll a Szolgáltató által végzett kockázatelemzésben megállapított kockázatokkal.

### A telephely elhelyezése és szerkezeti felépítése

A Szolgáltató védett számítógép termében valósítják meg a leginkább veszélyeztetett szolgáltatásokat. Ezt a számítógéptermet speciálisan erre a célra tervezték és alakították ki, és tervezésénél sok különböző védelmi szempont (a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés, beléptetés ellenőrzése és felügyelete, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása, stb.) egységes érvényesítésére került sor. Illetéktelen személyek 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 Second Site elhelyezése és szerkezeti felépítése

A Szolgáltató másodlagos helyszíne egy védett számítógép teremben található szerver széfben található. Ezt a másodlagos helyszínt speciálisan erre a célra tervezték és alakították ki, és tervezésénél sok különböző védelmi szempont (a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés, beléptetés ellenőrzése és felügyelete, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása, stb.) egységes érvényesítésére került sor. Illetéktelen személyek nehezen juthatnak be, a biztonsági őrség viszont rövid idő alatt meg tudja közelíteni riasztás esetén. A biztonsági körletnek (szerverszéf) nincs ablaka, az ajtókon kívül csak az erős fal bontásával lehetne behatolni ide.

### Fizikai hozzáférés

A területek pontos paramétereit, illetve a belépni jogosultak listáját a mindenkori belső operációs dokumentumok tartalmazzák. A bizalmi munkakört betöltő munkatársakon kívül más személyek (pl. karbantartók, takarítók) csak külön felhatalmazással és kísérettel léphetnek be. A belépések biometrikus azonosításra épülő beléptető rendszeren (kivéve másodlagos helyszín) keresztül történnek a belépések naplózásával. A helyiség kétszerezett (redundáns) klíma-, automata tűzoltó, továbbá illetéktelen behatolást jelző (riasztó) berendezéssel van ellátva. Az eszközök többszörösen túlbiztosított elektromos energiaellátással rendelkeznek. A biztonsági körletet beléptető zsilipét 24 órás videó kamerás megfigyelő rendszer is védi.

A másodlagos helyszín beléptetési rendszere biometrikus beléptető automatizmussal nem rendelkezik, de az egyenszilárdság megőrzésére, a másodlagos helyszínt biztonságát állandó élőerős védelem biztosítja.

### Áramellátás és légkondicionálás

#### Áramellátás

A Szolgáltató védett számítógép termének zavartalan áramellátása kiemelten fontos a folyamatos üzemeltetés biztosítása érdekében. Ez a következő – egységes tervezéssel megalapozott, a vonatkozó szabványoknak megfelelő – védelmi megoldások együttműködésével biztosított:

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.

#### EMC védelem

A villamos zavar, villám és túlfeszültség védelem szempontjából a gépterem nagy értékű, kritikus szolgáltatásokat biztosító berendezései védve vannak a különböző vezetett és sugárzott villamos zavarok, villámok miatt bekövetkező túlfeszültség hatásai ellen. A rendszert külön mechanizmusok védik a villámok által keltett elektromágneses impulzusok (EMI) hatása ellen. A védelem alapfogalmait az MSZ IEC 1312-1, nem kötelező szabvány írja le.

Az üzemeltetett berendezések a sugárzott elektromágneses zavarás elleni védelem (ezt az elektromágneses összeférhetőségnek (EMC) nevezett tulajdonságot az MSZ IEC 1000-1-1 szabvány tárgyalja részletesen) mindkét elvárását teljesítik:

egyrészt védettek az üzemelési környezetükben jelen levő hatások ellen,

másrészt nem bocsátanak ki olyan zavaró elektromágneses jeleket, amely a környezetükben üzemelő többi berendezés működését zavarhatná.

Az üzemeltetett berendezéseket a gépterem elektromágneses zavarvédelme továbbá védi az elektromágneses kisugárzással történő kompromittálódás (lehallgatás) ellen.

#### Légkondicionálás

A Szolgáltató biztosítja a géptermek épülettől független légkondicionálását. A védett számítógéptermek üzemi hűtésigényének kiszolgálását ipari klímaberendezések biztosítják. 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.

### Beázás és elárasztódás veszélyeztetettsége

A biztonsági körletek kialakítása során külön szempont volt az elárasztódás veszélyének minimalizálása. A védett számítógép teremben a fenti biztonságot tovább növeli az álpadló alkalmazása.

### Tűzmegelőzés és tűzvédelem

A géptermet befogadó épületben központilag kiépített tűzvédelmi rendszer működik. Az egész épület építési engedélyének tűzvédelmi fejezetét az illetékes tűzoltó parancsnokság jóváhagyta.

A biztonsági körlet utólagos kialakítása során, járulékos tűzvédelmi rendszert építettek ki (melynek fő elemei: füstérzékelő- és tűzjelző rendszer, tűzeseti vezérlések, automatikus oltórendszer), melyet az illetékes tűzoltó parancsnokság engedélyezett.

### Adathordozók tárolása

Az adathordozók biztonságos tárolására biztonsági körlet, illetve egy bérelt banki széf szolgál.

### Selejt kezelése, megsemmisítése

A biztonsági körletben a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat, csak tartalmuk többszörös visszaállíthatatlan törlése után használják fel nem minősített adatok tárolására (a folyamat pontos leírását a Biztonsági Szabályzat tartalmazza). A feleslegessé vált, bizalmas minősítésű adatokat tartalmazott és megfelelően nem törölhető adathordozókat fizikailag megsemmisítik:

a papíralapú dokumentumokat zúzógéppel felaprítják,

a hajlékony lemezeket (házából való kibontás után) zúzógéppel felaprítják,

egyéb más mágneses adathordozókat, demagnetizálás után összetörik,

egyéb más adathordozókat összetörik.

### Fizikailag elkülönítetten őrzött mentési példányok

A szolgáltatásra nagy hatással lévő úgynevezett kritikus adatokat két helyen (bérelt banki széfben is) tárolják.

## Eljárásbeli óvintézkedések

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

A Szolgáltató azon egységei, amelyek tanúsítvány előállítással és visszavonás kezeléssel foglalkoznak, olyan dokumentált szervezeti struktúrával rendelkeznek, amely védi a műveletek semlegességét.

### Bizalmi munkakörök

A Szolgáltató biztonság politikája a következő bizalmi munkaköröket határozza meg az alábbi felelősségkörökkel:

|  |  |
| --- | --- |
| **Megnevezés** | **Rövid leírás** |
| Biztonsági Tisztviselő | A szolgáltatás biztonságáért általánosan felelős személy, aki tanúsítványok előállítását, kibocsátását, felfüggesztését és visszavonását nem végzi. |
| Rendszeradminisztrátor | Az informatikai rendszer telepítését, konfigurálását, karbantartását a regisztráció, a tanúsítványok előállítása, az aláírás-létrehozó eszközök szolgáltatása és a tanúsítványok visszavonása, felfüggesztése céljából végző személy. |
| Rendszerüzemeltető | Az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy. |
| Rendszervizsgáló | A szolgáltató naplózott, illetve archivált adatállományát kezelővizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy |
| Informatikai vezető | Szolgáltató informatikai rendszeréért általánosan felelős vezető |
| Regisztrációs adminisztrátor | A végfelhasználói tanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy. |

A Szolgáltató **informatikai vezetője**:

felügyeli a Szolgáltató informatikai rendszert érintő folyamatait,

koordinálja a rendszer üzemeltetésével foglalkozó munkatársak tevékenységét,

koordinálja Szolgáltató szoftverfejlesztési tevékenységét,

a Változáskezelési Szabályzat rendelkezéseinek megfelelően elbírálja a hatáskörébe sorolt változási kérelmeket,

a MIBF ülésein történő részvételen keresztül közreműködik a Szolgáltató biztonsági megoldások kidolgozásában és felügyeli a biztonsági szempontok érvényesülését,

A Szolgáltatóval munkaviszonyban álló, változó helyszínen dolgozó **biztonsági tisztviselő** általánosan (a hitelesítő egységekre, a regisztrációs egységre, valamint az összes külső regisztrációs munkatársra nézve egyaránt)felel:

a különböző biztonsági óvintézkedések kidolgozásáért,

a különböző biztonsági óvintézkedések rendszeres felülvizsgálatáért, a szükségessé váló módosítások kezdeményezéséért,

a biztonsági óvintézkedések érvényre jutásáért, betartatásáért,

az informatikai rendszerek biztonsági szintjének megőrzéséért (rendszeres auditok szervezésével, támogatásával).

Ők hajtják végre a rendszeradminisztrátorok rendszerhez való hozzáférésének kezelését is, ami magában foglalja az alábbiakat:

profil felvétele,

jogosultságok beállítása,

kezdeti jelszó meghatározása,

a távozó, illetve munkakört váltó rendszeradminisztrátorok hozzáférési jogainak azonnali megszüntetése.

A Szolgáltatóval munkaviszonyban álló **rendszeradminisztrátorok**:

telepítik, konfigurálják és karbantartják a hitelesítő egység védett számítógép termében üzemeltetett megbízható rendszert,

beállítják a fenti megbízható rendszer kezdeti hálózati konfigurációját,

kezelik a hitelesítő egység állományába tartozó rendszerüzemeltetők vonatkozásában a rendszerhez való hozzáféréseket (profil felvétele, jogosultságok beállítása, módosítása, kezdeti jelszó meghatározása, a távozó, illetve munkakört váltó rendszerüzemeltetők hozzáférési jogainak azonnali megszüntetése),

letöltik és installálják a felügyeletük alatt üzemeltetett operációs rendszerre és adatbázisra kiadott biztonsági javítócsomagokat, ezen keresztül gondoskodnak az informatika biztonsági szint folyamatos megőrzéséről,

rendszeres időnként ellenőrzik (víruskereső programok futtatásával, az engedélyezett és a ténylegesen telepített szoftverek egybevetésével) a hitelesítő egység védett géptermében üzemeltetett informatikai rendszerének és információinak a sértetlenségét,

gondoskodnak a rendszerüzemeltetők által végzett rendszermentések, illetve a regisztrációs egység rendszermentés másolatainak biztonságos tárolásáról,

gondoskodnak a rendszermentésekről készített, elkülönítetten őrzendő másolati példányok szállításáról.

A Szolgáltatóval munkaviszonyban álló **rendszerüzemeltetők** folyamatosan üzemeltetik a védett számítógépteremben működő megbízható rendszert, melynek során:

időszakosan rendszermentéseket végeznek,

naponta egyszer archiválják az előállított tanúsítványokat és visszavonási listákat,

szükség esetén (a rendszermentések alapján) helyreállításokat hajtanak végre.

A Szolgáltatóval munkaviszonyban álló **rendszervizsgáló**:

ellenőrzi (áttekinti) és karbantartja (archiválja és törli) a Szolgáltató védett számítógép termében működő megbízható rendszer biztonsági naplóit,

szükség esetén az általa készített archívumokban keresést végez.

A Szolgáltatóval munkaviszonyban álló **regisztrációs felelős**:

a regisztrációs adminisztrátorok tevékenységét irányító személy,

a végfelhasználói tanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.

A bizalmi munkakörök között a biztonságos feladatvégzést akadályozó, illetve a jogszabályokban tiltott személyi átfedések nincsenek. Valamennyi fent megnevezett bizalmi munkakört részletes munkaköri leírások dokumentálják. A Szolgáltatónál a bizalmi munkakört betöltő személyek szakirányú felsőfokú végzettséggel és gyakorlattal rendelkeznek. A bizalmi munkakörökbe az ügyvezető nevezi ki a Szolgáltató munkatársait, a biztonsági alapellenőrzés sikeres befejezése után.

### Az egyes feladatokhoz szükséges személyzeti létszámok

A Szolgáltatónál az alábbi kettős felügyeletet Igénylő munkafolyamatok vannak:

Két bizalmi munkakört betöltő személy együttes jelenléte (és előzetes, sikeres hitelesítése) szükséges az alábbi funkciók kiváltásához:

a Szolgáltató első saját kulcsának generálása (ld. 6.1 pont),

a Szolgáltató későbbi saját kulcsgenerálása,

a Szolgáltató magán aláíró kulcsának biztonsági mentése (klónozása) (ld. 6.2.3 pont),

a Szolgáltató magán aláíró kulcsának visszaállítása,

a Szolgáltató magán aláíró kulcsának (és annak összes másodpéldányának) megsemmisítése,

minden tanúsítvány-kibocsátást megelőző regisztrációs feladatok (ld. 4.2.2 pont).

### Az egyes munkakörökben elvárt azonosítás és hitelesítés

A Szolgáltató valamennyi, bizalmi munkakört betöltő munkatársának a zárt körletbe való belépéskor az azonosítását és hitelesítését biometrikus azonosító rendszer végzi (kivéve másodlagos helyszín, ahol biometrikus azonosítás nincs, bővebben lásd a 5.1.3 pontban foglaltakat), amely a rendszerekhez való hozzáférésnél egyéb, rendszerenként különböző védelemmel egészül ki. Sikeres hitelesítés nélkül a zárt körletbe való bejutás, illetve rendszerhozzáférés nem lehetséges, így egyetlen biztonság szempontjából kritikus tevékenység sem végezhető el.

### Változáskezelés

A Szolgáltató a szolgáltatási folyamatokban és az azt kiszolgáló informatikai szolgáltatásokban bekövetkező módosítások, változások biztonságos végrehajtása érdekében szabályozott és dokumentált változáskezelési eljárást alkalmaz.

## Személyzetre vonatkozó óvintézkedések

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

Ennek érdekében a Szolgáltató a személyi biztonsággal már a felvételi szakaszban foglakozik, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését. Ennek érdekében a Szolgáltató a Biztonsági Szabályzatának részeként pontosan és részletesen kidolgozott, folyamatosan karbantartott Személyzeti Politikával rendelkezik. A Szolgáltató személyzeti politikájában meghatározott ideiglenes és állandó szerepköröket és felelősségeket a megfelelő 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 (felelős munkatársak) függetlenek minden olyan kereskedelmi, pénzügyi és egyéb hatástól, ami hátrányosan befolyásolhatja a Szolgáltató által nyújtott szolgáltatások iránti bizalmat.

### Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

A hitelesítő egység, a regisztrációs egység minden bizalmi munkakörére jelölt személynek (emberi megbízhatósága és szakmai alkalmassága ellenőrzése céljából) kezdeti ellenőrzésen (biztonsági alapellenőrzésen) kell keresztülmennie.

A 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.

Az ügyfél regisztráció területén dolgozó munkatársak ismerik a forgalomban lévő hatósági, illetve azonos funkciójú dokumentumokat, azok fajtáit, ismertetőjegyeit, képesek az átadott iratok valódiságának, érvényességének megállapítására.

### Biztonsági háttér ellenőrzésekre vonatkozó eljárások

Valamennyi bizalmi munkakört betöltő munkatársnak a biztonsági alapellenőrzésen túl időszakos biztonsági ellenőrzéseken 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.

Az időszakos biztonsági ellenőrzésre évente kerül sor

az informatikai vezető,

a biztonsági tisztviselők,

a rendszeradminisztrátorok,

a rendszerüzemeltetők,

regisztrációs felelősök

rendszervizsgáló

esetében egyaránt.

Az ellenőrzés során vizsgálják a munkatárs erkölcsi bizonyítványát és olyan körülményeket, melyek kockázati tényezőt jelentenek. E mellett figyelembe veszik a közvetlen vezetők véleményét is.

### Képzési követelmények

A hitelesítő egység, a Központi Regisztrációs Egység területén dolgozó valamennyi munkatárs felvételét követően, a saját munkakörének betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt. Ennek keretében minden munkatárs egy egységes informatika biztonsági alapkiképzésben is részesül. Ennek a képzési formának a fő célja az egész hitelesítés-szolgáltatásra vonatkozó egységes biztonságpolitika megismerése, megértése, az ezen alapuló aktuális eljárások és követelmények megismerése és a későbbi helyes alkalmazása érdekében. További részletek a személyzeti politikában találhatók.

### Továbbképzési gyakoriságok és követelmények

Abban az esetben, amikor a hitelesítés-szolgáltatásban jelentős változás következik be, valamennyi munkatárs a szükséges felépítésű és szintű moduláris továbbképzésben részesül, illetve megkapja a szükséges dokumentációkat. További részletek a személyzeti politikában találhatók.

### Munkabeosztás körforgásának gyakorisága és sorrendje

Körforgás az egyes munkabeosztások között nem valósul meg.

### A felhatalmazás nélküli tevékenységek büntető következményei

Az ide vonatkozó szabályokat a személyzeti politika szabályzata tartalmazza.

### A szerződéses munkavállalókra vonatkozó követelmények

Az ide vonatkozó szabályokat a személyzeti politika szabályzata tartalmazza.

### A személyzet számára biztosított dokumentációk

Az ide vonatkozó szabályokat a személyzeti politika szabályzata tartalmazza.

## A biztonsági naplózás folyamatai

Szolgáltató hitelesítési rendszere a jogszabályi követelményeknek megfelelő, széleskörű naplózási tevékenységet folytat a tanúsítványokra 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 követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét. A Szolgáltató a naplókban feltüntetett időt olyan gyakorisággal szinkronizálja a Szabályzatban megjelölt referencia időforráshoz (ld. 6.9.1 pont), 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.

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

### A tárolt események típusai

Az alkalmazott PKI rendszer minden jogszabályban előírt eseményt és hibát regisztrál, amely a rendszer üzemeltetése, visszakereshetősége és adminisztrációja szempontjából kritikus.

Különösen az alábbi fő eseménytípus csoportok kerülnek naplózásra:

rendszertevékenységek (indítás, leállítás, verziófrissítés, újraindexelés, újrakulcsolás, saját kulcsok és tanúsítványok kezelése, stb.),

mentési tevékenységek (teljes mentés, különbségi mentés, mentés ellenőrzés, stb.),

naplózási tevékenységek (naplózási funkció elindítása és leállítása, naplózási paraméterek megváltoztatása, a naplózás tárolási hibája miatt végzett tevékenységek, stb.)

CRL tevékenységek (kiadás, ko mbinált kiadás, visszavonás, felfüggesztés, stb.),

felhasználói események (tanúsítványkiadás, regisztráció, visszavonás, kulcsvisszaállítás, a biztonságos aláírás-létrehozó eszközök készítésével és átadásával kapcsolatos események, stb.),

adminisztratív események (adminisztrátor ki-, belépés, felhasználó visszaállítás, stb.),

adatbázis események,

címtár események,

operációs rendszer események,

hibák.

A naplózott események időbélyegzővel 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 a Szolgáltató biztosítja a naplóbeli események között az esemény típusa és/vagy a felhasználó személye szerinti keresést. A naplóbejegyzések szöveges formátumban jelenítődnek meg.

### A napló állomány feldolgozásának gyakorisága

Szolgáltató naplóbejegyzéseinek átvizsgálása napi rendszerességgel megtörténik. Szolgáltató hálózati védelmi rendszerei 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.

### A napló állomány megőrzési időtartama

A napló állományok keletkezésük helyén tárolódnak, illetve archiválásra kerülnek (ld. 5.5.4 pont), és a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg a velük kapcsolatban felmerült és bejelentett jogvita jogerős lezárásáig megőrződnek.

### A napló állomány 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. Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi.

### A napló állomány mentési folyamatai

A naplóállományok rendszeresen mentésre kerülnek (ld. 5.5.4 pont) rejtjelezett és aláírt formában.

### A napló gyűjtési 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.

### Az eseményeket kiváltó Igénylők 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.

### 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.

## Adatok archiválása

Szolgáltató informatikai rendszerének biztonsági és egyéb általános naplózási folyamatait ugyanazon rendszerek végzik, ugyanazon módszerek segítségével. Jelen fejezetben csak a Szolgáltató ettől eltérő papír alapú és egyéb speciális archiválási rendszerét ismertetjük.

### A tárolt események típusai

A Szolgáltató regisztrációs egységei valamennyi regisztrációs eljárás során keletkező iratot tárolják. Így tárolásra kerül:

a Szolgáltatóhoz benyújtott valamennyi elektronikus, illetve papír alapú kérelem (tanúsítvány kibocsátás, megújítás, visszavonás, stb.);

az Igénylő hozzájárulása esetén a személyes és szervezeti identitásának igazolására bemutatott valamennyi dokumentum másolata;

a Szolgáltató és az Igénylő, illetve a másodlagos Alany között megkötött valamennyi vonatkozó megállapodás (ideértve a tanúsítvány közzétételéhez történő hozzájárulást is);

a kérelmet elfogadó regisztrációs ügyintéző azonosítója;

a küldő regisztrációs szervezet neve.

A Szolgáltató továbbá megőrzi a tanúsítványokkal kapcsolatos elektronikus információkat – beleértve az, azok előállításával összefüggőket is – és az ahhoz kapcsolódó személyes adatokat.

### Az archívum megőrzési időtartama

Szolgáltató a tanúsítványokkal kapcsolatos elektronikus információkat és az ahhoz kapcsolódó személyes adatokat – amennyiben a Törvény  **.** szigorúbb követelményt nem támaszt - legalább a tanúsítvány érvényességének lejártától számított tíz évig, illetőleg az elektronikus aláírással, illetve az azzal aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi, valamint ugyanezen határidőig olyan eszközt biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható. E megőrzési kötelezettségnek Szolgáltató minősített elektronikus archiválási szolgáltató igénybevételével is eleget tehet.

### Az archívum védelme és hozzáférési szabályok

A Szolgáltató az archivált adatállományt legalább fokozott biztonságú elektronikus aláírás és időbélyeg elhelyezésével hitelesíti, védi a módosítástól, illetve biztosítja azt, hogy az adatállomány tartalmához jogosulatlan személyek ne férhessenek hozzá. Az archívum nem tartalmaz védelem nélkül kritikus biztonsági paramétereket. A Szolgáltató a tanúsítványokra vonatkozó archivált adatok titkosságát és integritását fenntartja.

Az archivált adatokhoz a Szolgáltató vezető tisztségviselői és a Szolgáltató auditorai férnek hozzá. A Szolgáltató biztosítja, hogy az adatok az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.

### Az archívum mentési folyamatai

Az adatok mentése naponta – legalább 1 példányban - történik. Ezen kívül heti, havi mentésekre és hosszú távú archiválásokra kerül sor. A mentést hordozó médiát a Szolgáltató biztonságos környezetben tárolja.

### A rekordok időbélyegzésére vonatkozó követelmények

Lásd a 5.4.1 pontot.

### Az archívum gyűjtési rendszere

A külső regisztráció során keletkezett iratokat a regisztrációt végző szervezetek bizalmasan tárolják és őrzik. Az elektronikus másolati példányban is létező iratok elektronikus üzenet formájában kerülnek a Szolgáltató központi adattárba.

### Archív információ hozzáférését és ellenőrzését végző eljárások

Az archívumhoz Szolgáltató ügyfélszolgálatán keresztül biztosít hozzáférést. A hozzáférés az Igénylőnek, illetve a másodlagos Alanynek a rá vonatkozó adatokhoz lehetséges, más feleknek a 2.4 pont szerint. Szolgáltató a jogosultságot minden esetben ellenőrzi, és a hozzáférést naplózza.

### Egyéb archiválási rendelkezések

Az archívumban esemény típus szerinti keresést lehet végrehajtani.

Az archiválásra vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat tartalmazza.

## Biztonsági rendelkezések

A Szolgáltató biztonsági műveleteit az üzemi műveletektől elkülöníti. A Szolgáltató biztonsági műveleteivel kapcsolatos felelősségek:

üzemeltetési eljárások és felelősségek,

biztonsági rendszerek tervezése és elfogadása,

káros szoftver elleni védelem,

rendszeradminisztráció,

hálózatkezelés,

audit napló, eseményelemzések és nyomon követések,

adathordozók kezelése és biztonsága,

adat és szoftver javítása, cseréje.

A Szolgáltató elvégzi a biztonsági követelmények elemzését, minden egyes rendszerfejlesztési vagy bővítési folyamat tervezési és követelmény specifikálási eljárás során.

A Szolgáltató rendszeres ellenőrzésekkel biztosítja, hogy a személyi azonosító eszközök (chipkártyák stb.) elvesztését, esetleges sérülését, kompromittálódását minél hamarabb felfedezze (nyilvántartások vezetése).

### Biztonsági felülvizsgálati eljárások

A Szolgáltató a tanúsítványok kiadásával, megújításával, felfüggesztésével, továbbá visszavonásával kapcsolatos összes eseményt felülvizsgáltatja. A felülvizsgált események tételes felsorolását a Biztonsági Szabályzat tartalmazza.

A Szolgáltató szúrópróbaszerű esemény felülvizsgálatot havonta többször, általános felülvizsgálatot félévente, illetve rendkívüli üzemeltetési helyzetet követően hajt végre.

Szolgáltató a felülvizsgálatról készült feljegyzéseket a felülvizsgálattól számított 10 évig megőrzi.

A felülvizsgálati naplókhoz a Szolgáltató vezető tisztségviselői férhetnek hozzá, a hozzáférés naplózásával. Az elektronikus feljegyzéseket a Szolgáltató elektronikusan aláírja.

A feljegyzésekre vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat tartalmazza.

## Helyreállítás kompromittálódás és katasztrófa esetén

### Incidens- és kompromittálódás-kezelési eljárások

A Szolgáltató a folyamatos működés biztosítása, illetve a vészhelyzetek minél gyorsabb elhárítása érdekében Üzleti Folytonossági Tervvel (ÜFT) rendelkezik, amely tartalmaz katasztrófa helyreállítási tervet is. Az ÜFT olyan eljárásokat tartalmaz, amelyek leírják a megbízható üzemmenet mielőbbi helyreállításának leggyorsabb módját. A Szolgáltató ellenőrzések végrehajtásával rendszeresen 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, illetve az ellen, hogy jogosulatlan személyek a mentett adatállományhoz hozzáférhessenek.

A rendkívüli üzemeltetési helyzet bekövetkezése esetén a visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását megelőzi.

Rendkívüli üzemeltetési helyzet bekövetkezése esetén a Szolgáltató haladéktalanul értesíti a Felügyeletet a rendkívüli üzemelési helyzet bekövetkezéséről, annak hatásáról, várható időtartamáról, a rendkívüli üzemeltetési helyzet elhárítása érdekében tett és tervezett intézkedésekről, valamint a rendkívüli üzemeltetési helyzet megszűnéséről. Ezenfelül közvetlenül értesíti mindazon személyeket, akiket a rendkívüli üzemeltetési helyzet érint, illetve tájékoztatást tesz közzé az interneten (lásd 2.3.2 pont).

### Sérült számítási erőforrások, szoftverek és/vagy adatok

Szolgáltató megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik, a hardver- és szoftver meghibásodások 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 és tranzakció naplózása biztosítja az adatok visszaállíthatóságát valamely adattároló eszköz kiesésének esetére. Ez a rendszer a legrosszabb esetben az előző napi adatok helyreállítására képes.

Szolgáltató katasztrófa elhárítási terve 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.

### Egy szolgáltatói egység kulcsának kompromittálódása

Szolgáltató katasztrófa elhárítási terve a szolgáltatói magánkulcsok kompromittálódása esetére akciótervvel rendelkezik (ld. Üzleti Folytonossági Terv). Az akcióterv a szolgáltatói nyilvános kulcs visszavonása mellett feltárja a kompromittálódás körülményeit, intézkedik az ez által érintett valamennyi fél értesítéséről (a 2.1 ponttól függetlenül, de arra tekintettel), megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen és szükség esetén új kulccsal látja el a szolgáltatói egységet, valamint a kompromittálódott kulccsal kiadott tanúsítványokat visszavonja.

### Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően

Természeti vagy más katasztrófát követően, illetve a Szolgáltató berendezéseinek meghibásodása esetén Szolgáltató a következő szolgáltatások legfeljebb 3 órán belüli elindítását vállalja:

visszavonáskezelés-szolgáltatás,

visszavonási állapot közzététele szolgáltatás.

Minden egyéb szolgáltatás elindítását Szolgáltató 5 munkanapon belül vállalja.

## A Szolgáltató leállítása

### Szolgáltatás megszűntetése

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

A tevékenység befejezését legalább 60 nappal megelőzően értesíti az általa kibocsátott és még vissza nem vont tanúsítványokban Aláíróként megjelölt személyeket, a Felügyeletet, megjelölve azt a - vele azonos besorolású – szervezetet, amely legkésőbb a tevékenység befejezésekor átveszi a visszavonási állapot közlési nyilvántartásokat, valamint a regisztrációs információ és az eseménynapló archívumok fenntartására vonatkozó kötelezettségeket a Szolgáltató számára előírt vagy általa vállalt időtartamra (lásd 9.3 pont).

A szolgáltatás megszűnése előtt 30 nappal értesítést tesz közzé Internetes oldalain (ld. 1.5 alfejezet), e-mail címmel rendelkező ügyfelei számára a szolgáltatás befejezéséről elektronikus levélben értesítőt küld.

A Szolgáltató a tevékenység befejezését legalább 20 nappal megelőzően az általa kibocsátott, és még vissza nem vont tanúsítványokat visszavonja.

A Szolgáltatóval szerződéses kapcsolatban álló, a tanúsítvány kibocsátásban résztvevő, összes vállalkozással, regisztrációs szervezettel korábban megkötött szerződés alapján fennálló kezelési jogokat, illetve felhatalmazást visszavonja, valamennyi regisztrációs szervezetet felhívja a náluk tárolt adatok átadására.

A regisztrációs információk, és az eseménynapló archívumok megőrzése érdekében, időbélyegzővel ellátott teljes körű mentést hajt végre. A mentésnek tartalmaznia kell 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 a Szolgáltató védi jogosulatlan módosítástól és biztosítja a jogosulatlan hozzáférés kizárását, valamint az adatoknak megőrzési időn belüli, jogosultak számára való hozzáférhetőségét és értelmezhetőségét.

Saját magánkulcsait megsemmisíti, illetve a hozzájuk tartozó tanúsítványokat visszavonja, és erről egy országos terjesztésű napilapban hirdetést tesz közzé.

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

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

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

A Szolgáltató rendelkezik a leállási követelmények teljesítésével kapcsolatos költségek fedezetével. A leálláshoz kapcsolódó kötelezettségek teljesítését 25.000.000 Ft-os bankgarancia szavatolja.

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

### Regisztrációs pont megszűnése

A Szolgáltató a lehetőségeknek megfelelően folyamatosan törekszik arra, hogy az esetlegesen kieső Regisztrációs Pontokat újakkal pótolja, s regisztrációs szolgáltatásának személyes elérhetőségét országosan fenntartsa. Valamely regisztrációs pont megszűnése esetén a Szolgáltató biztosítja a regisztrációs ponton tárolt adatok begyűjtését, illetve a vele kötött szerződéstől és az adatkezelés céljától függően felhívja a Regisztrációs Pontot az adatkezelés megszüntetésére.

# 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,

időbélyegző magánkulcs,

infrastrukturális és kontrollkulcsok,

viszontazonosítási válasz aláíró kulcs.

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.

## Kulcspár előállítás és telepítés

### Kulcspár előállítás

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Végfelhasználói kulcspár** | **Szolgáltatói kulcspárok** |
| Kulcsgenerá-lás és installáció | Kulcsgenerálás, tárolás | A kulcsgenerálást a végfelhasználó saját maga vagy aláíró eszköz szolgáltatás keretében a Szolgáltató végzi.Szolgáltató aláíró eszközszolgáltatás keretében csak megfelelően tanúsított kriptográfiai hardvereszközt használ. | Szolgáltató a saját tanúsítvány aláíró és egyéb infrastrukturális kulcspárjait biztonságos módon generálja és tárolja. A kulcsgenerálás a Szolgáltató kizárólagos feladata és felelőssége.A magánkulcsokat a Szolgáltató nem bocsátja ki nyíltan. |
| Kulcs méretek | A végfelhasználóknak legalább 2048 bites hosszúságú kulcsok kerülnek generálásra kivéve, ha a végfelhasználó műszaki okból kifejezetten kéri az ennél kisebb kulcshosszúság alkalmazását, azonban ilyenkor a Szolgáltató tájékoztatja a kockázatokról. | A Szolgáltató legalább 2048 bites kulcshosszúságú kulcsokat generál. |
| Kulcs felhasználási célok | A Szolgáltató vagy végfelhasználó kulcspárt generál jelent szabályzat szerinti célokra. | - végfelhasználói tanúsítvány, CRL és OCSP válaszok aláírása;- egyéb tanúsítvány, CRL és OCSP válaszok aláírása,- időbélyegző aláírása,- infrastrukturális és kontrollkulcsok,- viszontazonosítási válasz aláírására használt kulcsok. |
| Magánkulcs védelme | Magánkulcs több-személyes kontrollja | A Szolgáltató eszközszolgáltatás esetén többszemélyes kontrollt vagy ennek megfelelő technikai védelmet biztosít a magánkulcsok generálásakor és kezelésekor. | A Szolgáltató legalább kétszemélyes kontrollt alkalmaz a magánkulcsok esetében. |
| Magánkulcs mentése | Magánkulcsot a Szolgáltató nem ment. | Magánkulcsait a Szolgáltató menti. |
| Magánkulcs aktiválása | A magánkulcsok aktiválását az Igénylő kezdeményezi. | A Szolgáltató magánkulcsainak aktiválását a Szolgáltató végzi. |
| Magánkulcs deaktiválása | A magánkulcsok deaktiválását a felhasználó alkalmazás végzi működésének befejezésekor. | A magánkulcsok deaktiválását a Szolgáltató végzi. |
| Magánkulcs megsemmisítése | Végfelhasználó köteles a magánkulcsát az érvényességi idő lejárta után megsemmisíteni. | A Szolgáltató magánkulcsait és azok minden előfordulását az érvényesség lejáratakor a Szolgáltató megsemmisíti. |
| Egyéb tevékenységek | Nyilvános kulcs archiválása | A végfelhasználói nyilvános kulcsokat a Szolgáltató a jogszabályokban meghatározott ideig archív formában megőrzi (ld. 5.5.2 pont). | A szolgáltatói nyilvános kulcsokat a Szolgáltató a jogszabályokban meghatározott ideig archív formában megőrzi (ld.. pont). |
| Kulcsok felhasználási ideje | A végfelhasználói magánkulcs felhasználási ideje megegyezik a hozzá tartozó tanúsítvány(ok) érvényességi idejével, de maximálisan 2, a tanúsítványok meghosszabbítása esetén 4 év. A nyilvános kulcs a kriptográfiai biztonságáig érvényes. | A szolgáltatói magánkulcs felhasználási ideje megegyezik a hozzá tartozó tanúsítvány(ok) érvényességi idejével. A nyilvános kulcs a kriptográfiai biztonságáig érvényes. |

A Szolgáltató valamennyi szolgáltatói kulcspárát saját maga generálja, védett kriptográfiai hardver modulban. A generált magánkulcsok mentést (klónozást) leszámítva, teljes életciklusuk alatt a kriptográfiai hardverekben marad, megsemmisítéséig azt sehová nem kell továbbítani. Amennyiben a szolgáltatói kulcspár, bármely okból történő megsemmisítése válik szükségessé, úgy az az eszköz tanúsítványában előírt módon két személyes kontroll mellett történik.

#### Alkalmazott eszközök

|  |  |  |
| --- | --- | --- |
| **Aláíró eszközök** | **Hardware és firmware specifikáció** | **Kulcskezeléshez közvetlenül használt szoftverek specifikációja** |
| Hitelesítő Egység | ProtectServer Gold (hardware verzió: B2, firmware verzió: 2.03.00)Luna PCI 3000 V3.0 /Hardver verzió: VBD-03-0100, förmver verzió: 4.7.1(3000)/ kriptográfiai modulLuna PCI-e 3000 SFF V3.0 /Hardver verzió: VBD-04-0102, förmver verzió: 4.7.1(3000)/ kriptográfiai modul | ProtectServer Gold (hardver verzió: B2, firmware verzió: 2.03.00) drivere, , PKCS11 interfész, tanúsított NCA NETLOCK tanúsítványkiadó rendszer.Luna kriptogáfiai modulok driverei |
| Végfelhasználói eszköz | IDOneClassIC Card: ID-One Cosmo 64 RSA v5.4, applet IDOneClassIC v1.0 embedded, P5CT072VOP-en,ID-One Cosmo v7.0.1-n kártya IAS ECC 1.0.1 alkalmazással (applet version 1121), NXP P5CC081 V1A (Standard) komponensselGemalto MultiApp ID Citizen 72k intelligens kártya: S3CC91C mikrochip, MultiApp v1.1 Java Card platform és IAS Classic v.3.0 elektronikus aláíró alkalmazásSafeNet eToken (Smartcard or USB token), 9.1-es Verzió, Athena IDProtect/OS755 Java Card kártya, Atmel AT90SC25672RCT-USB Microcontrolleren, IDSign applet beágyazássalIAS Classic v3 alkalmazás Java Card platformon P5CC081V1A chippel, MultiApp ID V2.1 nyílt szabvány szerint, szűrővel ellátott MPH117 v2.2ProtectServer Orange (korábbi nevén CSA 8000 Adapter), hardver verzió: G verzió, Cprov förmver verzió: 1.10  | ProtectServer Orange (korábbi nevén CSA 8000 Adapter), hardver verzió: G verzió, Cprov förmver verzió: 1.10 Oberthur eszközök drivereiGemalto eszközökhöz driverekSafeNet eszközök driverei |

A Szolgáltató által alkalmazott eszközökhöz közvetetten felhasználásra kerülhetnek más, tanúsított szoftverekben is, mint a Mokka, az NCA rendszer, az Archer és az e-Szigno termékek.

### Magánkulcs eljuttatása az Igénylőhöz

Mivel a Szolgáltató valamennyi kulcspárja helyben generálódik (ld. 6.1.1 pont), azokat nem kell sehová továbbítani.

A végfelhasználók aláíró magánkulcsát nem kell továbbítani, ha azt az Igénylő saját maga állítja elő. Amennyiben a Szolgáltató aláíró eszköz-szolgáltatás keretében generálta a végfelhasználói kulcspárt, akkor az eszközt biztonságos módon közvetlenül juttatja el az Igénylőhoz és adja át annak.

### A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A Szolgáltató valamennyi nyilvános kulcsáról saját maga készít tanúsítványt.

A végfelhasználók nyilvános kulcsát a már sikeresen regisztrált Igénylő (ld. 4.2.2 pont) védett csatornán küldi meg a regisztrációs egységnek, amely – miután sikeresen ellenőrizte, hogy az Igénylő által megküldött nyilvános kulcsnak megfelelő magánkulccsal valóban rendelkezik-e az Igénylő – szintén védett csatornán továbbítja a hitelesítő egységnek.

Eszközszolgáltatás esetén a kulcspárt a Szolgáltató helyben generálja, így nincs szükség a nyilvános kulcs továbbítására.

### A szolgáltatói nyilvános kulcs közzététele

A Szolgáltató a hitelesítő egység által aláírt tanúsítványait saját tanúsítványtárában, illetve ügyfélszolgálatán teszi mindenki számára elérhetővé.

### Kulcsméretek

Lásd 6.1.1 pont.

### A nyilvános kulcs paraméterek generálása és megfelelőségük ellenőrzése

A nyilvános kulcs paraméterek megfelelnek az előírásoknak (ld. **.**Irányelv melléklete), és előállításuk során a megfelelő szabványok, algoritmusok kerültek alkalmazásra.

#### A paraméterek megfelelőségének ellenőrzése

A kulcsgenerálás paramétereinek megfelelőségét két szempontból ellenőrzi a rendszer:

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

a paraméterekre vonatkozó feltételek, összefüggések teljesülésének ellenőrzése.

A véletlenszám-generálás megfelelőségének 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.

Ezeken felül a tanúsító szervezetek évente felülvizsgálják, 3 évente újra tanúsítják az eszközöket.

### A kulcs használat célja (az X.509 v3 kulcshasználati mezők tartalmának megfelelően)

A Szolgáltatónak a tanúsítványok aláírásához használt magánkulcsát, ezeken kívül csak a tanúsítvány visszavonási lista (CRL) aláírására szabad felhasználnia.

A Szolgáltató csak olyan, az elektronikus aláírás hitelesítés-szolgáltatás során kibocsátott, aláírásra használható aláíró tanúsítványt bocsáthat ki, melyekre teljesül, hogy az aláíró tanúsítvány kulcshasználati mezője kritikus, és a mezőben a "NonRepudiation", és a DigitalSignature bit van „true” értékre beállítva.

## A magánkulcsok védelme

### A szolgáltatói kulcsokra vonatkozó általános szabályok

A szolgáltatói kulcsokra az alábbi szabályok vonatkoznak:

a kulcsok létrehozása, tárolása, mentése, helyreállítása, megsemmisítése fizikailag biztonságos környezetben, kettős személyi ellenőrzés mellett valósul meg,

a hitelesítő egységek kulcsai FIPS 140 vagy FIPS140-2 Level 3 tanúsítvánnyal rendelkező kriptográfiai modulban kerülnek előállításra, tárolásra,

eszközszolgáltatásnál, ha a kulcspár előállítása az aláírás-létrehozó eszközön kívül történik, a kulcspárt előállító kriptográfiai eszköz tanúsítvánnyal igazoltan megfelel az alábbi szabványok, szabványjellegű dokumentumok legalább egyikének: a) FIPS 140, 3-as szint, b) CEN HSM – PP.

a kulcsokat kizárólag az arra felhatalmazottak használhatják, a létrehozás céljának megfelelő funkcióra,

a Szolgáltató rendszerei saját szolgáltatói kulcsaik használata előtt meggyőződnek arról, hogy az ezen kulcsokhoz kapcsolódó tanúsítványok érvényesek,

a Szolgáltató tanúsítvány- és CRL aláíró kulcsai különböznek minden más funkcióra szolgáló kulcstól,

a szolgáltatói kulcsfrissítés out-of-band cserével történik,

a szolgáltatói kulcsok megsemmisítése során olyan biztonságos törlési folyamatokat alkalmaz a Szolgáltató, melyek ténylegesen felülírják a kulcsok összes előfordulását az összes olyan tárolóeszközön, melyen a kulcs példányai előfordulhattak,

 biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálásakor a Szolgáltató gondoskodik a kulcs védelméről,

élettartamuk végén a kulcsokat a Szolgáltató olyan módon semmisíti meg, hogy az aláíró kulcsok ne legyenek visszanyerhetőek,

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. 5.1.4.2 pont).

### Magánkulcs letétbe helyezése

A szolgáltatói és végfelhasználói magánkulcsot nem lehet letétbe helyeztetni, kivéve a titkosítói magánkulcsok.

A Szolgáltató biztosíthat olyan eszközt, amely lehetővé teszi a kulcsok távoli, biztonságos tárolását és használatát.

### Magánkulcs mentése

A Szolgáltatónál a következő magánkulcsok kerülnek mentésre (illetve duplikálásra, klónozásra).

a hitelesítő egység aláíró magánkulcsa,

A mentés során a magánkulcsot generáló kriptográfiai hardver modulból intelligens kártyákra több darabban, védetten másolódik át a magánkulcs.

A mentés funkció kiváltásához speciális eszközök kellenek.

A mentési funkció első lépéseként a kettős ellenőrzés mellett működő végrehajtók hitelesítik magukat.

Sikeres hitelesítés esetén a mentés rejtjeles formában hajtódik végre.

A mentett példányok a továbbiakban ugyanolyan jellegű és erősségű védelem alatt állnak, mint a kulcsgenerálást végző hardver modul eredeti példánya.

Amennyiben a Szolgáltató által biztosít távoli tárolásra eszközt a Végfelhasználói magánkulcsot, tárolására úgy a Szolgáltató mentheti azt, jellemzően olyan formában, hogy a kulcsokhoz nem fér hozzá.

### Magánkulcs archiválása

A Szolgáltató sem az aláíró magánkulcsát, sem a végfelhasználói magánkulcsokat nem archiválja.

## A kulcspár gondozásának egyéb szempontjai

### Egyéb kulcskezelési rendelkezések

A Szolgáltató a szolgáltatások nyújtásához használt termékeit elkülönítetten kezeli és működteti az egyéb tevékenységeihez használt termékektől. A Szolgáltató a szolgáltatások nyújtásához használt valamennyi elektronikus terméket kockázatelemzések alapján biztonsági osztályokba sorolja, és ezekről nyilvántartást vezet.

A még tanúsítvánnyal el nem látott nyilvános kulcsokat a Szolgáltató fizikailag biztosított környezetben tárolja.

### Nyilvános kulcs archiválása

A regisztrációs egység minden a Szolgáltató által előállított tanúsítványt archivál az érvényesség lejártától számított 10 évig.

Szolgáltatói kulcs használati idejének végén archiválható, hogy esetleg később (nem meghatározott idő múlva) újra használatba vehető legyen. Ez különösen az elektronikus aláírás ellenőrzésére szolgáló nyilvános kulcsokra vonatkozik.

A Szolgáltató az Aláíró magánkulcsát nem archiválja. (Lásd 6.2.4 pont.)

### A nyilvános és magánkulcsok használatának periódusa

Szolgáltatói tanúsítványok és a bennük foglalt nyilvános kulcsok magán párjai:

nem minősített tanúsítvány- és CRL aláíró magánkulcs: legfeljebb 20 év

A végfelhasználói aláíró kulcsokhoz tartozó tanúsítványoknak és a bennük foglalt nyilvános kulcsok magán párjainak érvényességi ideje maximálisan 2, a tanúsítvány meghosszabbítása esetén 4 év. Az érvényességi periódus a tanúsítványban feltüntetésre kerül. A tanúsítványok érvényességének kezdete a kibocsátás időpontjával egyezik meg.

|  |  |  |  |
| --- | --- | --- | --- |
| tanúsítvány típus | maximum érvényességi idő hosszabbítás nélkül | maximum érvényességi idő hosszabbítással | Megújíthatóság |
| titkosító | 2 | 4 | igen |
| autentikációs | 2 | 4 | igen |
| kódaláíró | 2 | 4 | igen |
| DV SSL | 2 | - | nem |
| OV SSL | 2 | 4 | igen |

A magánkulcs érvényességi ideje megegyezik a tanúsítvány érvényességi idejével. Valamennyi fenti tanúsítványban szereplő nyilvános kulcs érvényességi ideje annak kriptográfiai biztonságnak megfelelő voltáig tart.

## Aktivizáló adatok

Az aktivizáló adatokkal kapcsolatos előírások kizárólag az eszközszolgáltatás keretében kibocsátott tanúsítványokra vonatkoznak, mivel ezeknél szükséges kriptográfiai hardvereszköz alkalmazása.

### Aktivizáló adatok előállítása és telepítése

A Szolgáltató az aláírás-létrehozó eszközhöz tartozó aktivizáló adatokat (PIN kód) biztonságos módon, az eszközöktől elkülönítetten állítja elő. A PIN kód beállítása az aláírás-létrehozó eszköz tanúsítója által előírt módon történik. A további pontos szabályok az Igénylő érdekében nem nyilvánosak.

### Az aktivizáló adatok védelme

A Szolgáltató az aláírás-létrehozó eszközhöz tartozó aktivizáló adatokat (PIN kód) csak abból a célból rögzíti, hogy azt a szolgáltatást igénybe vevő személy számára – másolat megőrzése nélkül – átadhassa.

### Az aktivizáló adatok egyéb szempontjai

A Szolgáltató az aláírás-létrehozó eszközhöz tartozó aktivizáló adatot (PIN kód) az aláírás-létrehozó eszköztől elkülönítve juttatja el az Igénylőhöz. Kivételt jelent ez alól a személyes átadás, ahol az aláírás létrehozó eszköz és az azt aktivizáló adat egyszerre is átadásra kerülhet, a bizalmassági követelményeknek való megfelelés fenntartása mellett.

## Számítógép-biztonsági óvintézkedések

A Szolgáltató a következő számítógép-biztonsági óvintézkedéseket alkalmazza:

megköveteli, hogy az informatikai rendszerek és alkatrészek szállítói olyan dokumentációkat biztosítsanak, melyek érthetővé teszik a megbízható rendszerek helyes és biztonságos működtetését, a rendszerhibák kockázatának minimalizálását biztosító telepítését, a vírusokkal és kártékony szoftverekkel szembeni védelmet a rendszerek és az általuk feldolgozott információk sértetlenségének fenntartása érdekében,

megköveteli a szolgáltatási rendszerek szállítóitól a következők átadását: telepítési útmutató, rendszeradminisztrációs útmutató, üzemeltetési útmutató,

az egyes rendszerek kezelése során hozzáférési szinteket, hozzáférési jelszavakat alkalmaz,

az audit napló állományokat napi, heti és havi, valamint éves gyakorisággal ellenőrzi.

Az ide vonatkozó részletes rendelkezéseket az 5.6 5.4 és az 5.1 alfejezet, valamint a Szolgáltató belső szabályzatai tartalmazzák.

### Speciális számítógép-biztonsági műszaki követelmények

Az **alkalmazások** által megvalósított biztonsági funkciók az alábbiak:

biztonsági naplózás (a rendszerüzemeltetői hozzáférések és tevékenységek rögzítése),

kommunikáció (a hitelesítő egység és a Központi Regisztrációs Egység közötti kommunikáció bizalmasságának, sértetlenségének és hitelességének biztosítása a kriptográfiai hardver modulok megfelelő funkcióinak aktivizálásával),

a felhasználói adatok védelme (a hozzáférés ellenőrzési szabályok érvényre juttatása az elindított alkalmazások csak a jogosultságnak megfelelő funkciók elérhetőségét biztosítják, a maradvány információ védelmének támogatása),

azonosítás és hitelesítés (a rendszerüzemeltetők azonosítása, hitelesítése, az alkalmazások által biztosított funkciók elérésének sikeres hitelesítéshez kötése).

A **kriptográfiai hardver modulok** által megvalósított biztonsági funkciók az alábbiak:

kriptográfiai támogatás (kriptográfiai kulcsok generálása, védelme és megsemmisítése; bizalmasságot, sértetlenséget, hitelességet és letagadhatatlanságot biztosító kriptográfiai eljárások megvalósítása),

a felhasználói adatok védelme (a saját hozzáférés ellenőrzési szabályok érvényre juttatása),

azonosítás és hitelesítés (a saját felhasználók /biztonsági tisztviselők vagy rendszerüzemeltetők azonosítása, hitelesítése, a saját funkciók elérésének sikeres hitelesítéshez kötése),

biztonságkezelés (saját biztonsági szerepkörök kezelése, a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),

a biztonsági funkciók megbízható védelme (saját működés biztonsági tesztelése, biztonságos állapot megőrzése hiba esetén, a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása),

megbízható út/csatorna (megbízható útvonal kiépítése a magát hitelesítő felhasználóval, mely alkalmas az átvitt adatok illetéktelen felfedésének és módosításának megakadályozására).

Az informatikai biztonsági intézkedéseket részletesen a Szolgáltató Biztonsági Szabályzata tartalmazza.

### Informatikai biztonsági osztályozás

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

## Életciklusra vonatkozó műszaki óvintézkedések

### Rendszerfejlesztési óvintézkedések

A Szolgáltató által fejlesztett rendszerek esetében sor kerül az esetleges kockázatok felmérésére és elemzésére.

A Szolgáltató a maga által fejlesztett szoftverek esetében változáskezelési eljárást alkalmaz a kibocsátásokra, a módosításokra, és a sürgős szoftver javításokra. 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.

### Biztonságkezelési óvintézkedések

A Szolgáltató kockázatelemzést végez az üzleti kockázatainak felmérésére, széleskörűen figyelembe véve a szolgáltatásokat, adatokat, eszközöket, információkat fenyegető veszélyforrásokat. A kockázatelemzés eredménye alapján határozza meg a szükséges biztonsági követelményeket és a működési eljárásokat.

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. Kiválasztásuk gondos mérlegelés alapján történt, a beruházás megtörténte után a kapcsolat hosszabb távú. 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 számos forrásból, viszonylag gyorsan megoldható.

### Az életciklusra vonatkozó biztonság osztályozása

Az alkalmazott biztonsági eljárások, módszerek értékelését független szakértő vizsgálja. A folyamatos, magas színvonalú biztonságos szolgáltatás fenntartására a Szolgáltató ISO 27001 (korábban BS 7799-2:2002 elnevezésű) szabványnak megfelelő információbiztonsági irányítási rendszert is alkalmaz, amelyet ugyancsak független külső és belső auditorok vizsgálnak.

A szükséges biztonsági értékelést független auditor vizsgálja.

## Hálózatbiztonsági óvintézkedések

A Szolgáltató saját hálózatát a nyílt hálózatokról tűzfal szerverekkel választja le. Az ide vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat és az Üzleti Folytonossági Terv tartalmazza.

A **tűzfal** és a **behatolás detektáló** által megvalósított biztonsági funkciók az alábbiak:

biztonsági naplózás (a hálózati kommunikáció naplózása, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása, a napló folyamatos elemzése: biztonsági riasztások és automatikus válaszok megvalósítása),

a felhasználói adatok védelme (az információ áramlás ellenőrzési szabályok érvényre juttatása /szűrés, a tiltott információ áramlás megakadályozása, megfigyelése),

azonosítás és hitelesítés (a saját felhasználók /hálózati adminisztrátorok/ azonosítása, hitelesítése, a saját funkciók elérésének sikeres hitelesítéshez kötése),

a biztonsági funkciók megbízható védelme (az információ áramlás ellenőrzés megkerülhetetlenségének biztosítása).

## A kriptográfiai modul ellenőrzése

Szolgáltató a jelen Szabályzat vonatkozó részében megadott szintű minősítéssel rendelkező kriptográfiai modulokat alkalmaz. Az ide vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat és az Üzleti Folytonossági Terv tartalmazza.

### Időforrás és időszinkronizáció

A Szolgáltató megbízható rendszereinek belső órája szabványos időforráshoz van szinkronizálva.

A Szolgáltató a csatlakoztatott időforrást szolgáltató berendezések esetében a beérkező időadatok sérthetetlenségét, illetve módosíthatatlanságát biztosítja.

A rendszeridő szinkronitásának kiesését a Szolgáltató a szinkron eltérés észlelésének időpontjában az eltérés mértékének megjelölésével naplózza, illetve időszinkron kieséskor OCSP válaszadás-, CRL- és tanúsítvány kibocsátás, valamint időbélyegzés-szolgáltatást nem végez.

### Időforrások megnevezése

A Szolgáltató több független UTC forrási rendszert és azok jeleit venni képes eszközöket alkalmaz az időforrás üzembiztonsága érdekében:

időforrás GPS: GPS műholdas navigációs rendszer által szolgáltatott referenciaidő,

időforrás DCF: németországi referenciaidő,

időforrás PRS: ACTS kompatibilis nemzeti időszolgáltatókhoz szinkronizált, nagy pontosságú, rubídium oszcillátor alapú, független helyi időforrás,

időforrás NTP: minimum 4 stratum 1 szintű, interneten elérhető NTP szerver.

### Időforrás pontossága

A megbízható rendszerek minden időponttal kapcsolatos szolgáltatáshoz használt óráját a Szolgáltató szinkronizálja az ún. koordinált, egységes időforrással (UTC - Universal Time Co-ordinated) minősített időbélyegzés esetén legalább 0,1 másodperces, egyéb hitelesítés-szolgáltatáshoz kapcsolódó tevékenység esetén legalább egy másodperces pontossággal. A Szolgáltató által alkalmazott időforrás pontossága maximum néhány ezred másodperc eltérés az UTC-hez képest.

Szolgáltató biztosítja az egyedi külső időforrások szinkronból kiesése, vagy elérhetetlensége esetére a rendszereinek megbízható időforrással való kapcsolatát.

Az időszinkronizációt a Szolgáltató az elfogadott referencia időhöz képest minimum naponta 64 alkalommal elvégzi, amennyiben a szinkronitási követelmény teljesítéséhez ez szükséges, a napi időszinkronizációk számát növeli.

### Alkalmazott eszközök

|  |  |
| --- | --- |
| **Időszinkronizációs eszközök** | **Időszinkronizációs forrás** |
| HOPF 6039 GPS típusú vevő | GPS műholdas navigációs rendszer (időforrás GPS)  |
| HOPF 6039 DCF típusú vevő | németországi referenciaidő (időforrás DCF) |
| PRS10 rubídium oszcillátor | ACTS kompatibilis nemzeti időszolgáltatók (időforrás PRS) |
| NTP szerver | 4 külső időforrás (időforrás NTP) |

# Tanúsítvány, visszavonási lista, OCSP és időbélyeg profilok

## Végfelhasználói tanúsítványok profilja

A Szolgáltató az X.509 [5] ajánlásnak megfelelő tanúsítványokat bocsát ki.

### SSL profil DV

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mező neve** | **Tartalom** | **Kritikus** | **Feltüntetés** | **forrás dokumentum** |
| AIA:Caissuers | A tanúsítványt kiadó CA tanúsítványának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 3 C |
| AIA:OCSP | A tanúsítványt kiadó CA OCSP szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 3 C |
| basicConstraints | CA:FALSE | Igen | Kötelező | *BL 1.1.6* | A 3 D |
| CDP | A tanúsítványt kiadó CA CRL szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | EV 1.4.5 | 9.7 |
| Certificate Serial Number | Nem szekvenciális sorozatszám legalább 20 bit entrópiával | Nem | Kötelező | BL 1.1.6 | 9.6 |
| CertificatePolicy | A kiadott tanúsítványhoz tartozó policy azonosítója, ami bizonyítja, hogy 1) Melyik cp tartozik a tanúsítványhoz | Nem | Kötelező | EV 1.4.5 | 9.3.2 |
| ExtendedKeyusage | id-kp-serverAuth | Nem | Ajánlott | BL 1.1.6 | A 3 F |
| KeyUsage | Digital Signature, KeyEncypherment, KeyAgreement | Igen | Kötelező | BL 1.1.6 R5280 | A 3 E |
| Private and public key | lásd minimum algoritmusok táblázat | Nem | Kötelező | BL 1.1.6 | 9.5 -> App A 1,2,3 |
| subject:commonName (CN) | Ha a mező jelen van, akkor egy domain nevet tartalmaz az igényeltek közül. | Nem  | már nem ajánlott | EV 1.4.5 | 9.2.3 |
| subject:countryName (C ) | A mező nincs jelen | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subject:localityName (L) | A mező nincs jelen | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subject:organizationalUnitName  | A mező nincs jelen | Nem | Opcionális | BL 1.1.6 | 9.2.6 |
| subject:organizationName (O) | A mező nincs jelen | Nem  | kötelező | EV 1.4.5 | 9.2.1 |
| subject:stateOrProvinceName (ST) | A mező nincs jelen | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subjectAltName (SAN) | Egy vagy több domain nevet tartalmazhat.Az első domain névnek egyeznie kell a CN mezőben találhatóval, ha az jelen van. | Nem  | kötelező | EV 1.4.5 | 9.2.2 |
| Validity  | Az érvényesség ajánlott hossza 12 hónap, maximum hossza 36 hónap | Nem | Kötelező |   |   |
| Subject Key identifier | Alany kulcs hash | Nem | Kötelező | R 5280 |   |
| Authority Key dentifier | Kiadói kulcs hashe | Nem | Kötelező | R 5280 |   |
| Signature | Kiadó aláírása SHA256 algoritmussal | Nem | Kötelező | R 5280 |   |

### SSL profil OV

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mező neve** | **Tartalom** | **Kritikus** | **Feltüntetés** | **forrás dokumentum** |
| AIA:Caissuers | A tanúsítványt kiadó CA tanúsítványának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 3 C |
| AIA:OCSP | A tanúsítványt kiadó CA OCSP szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 3 C |
| basicConstraints | CA:FALSE | Igen | Kötelező | *BL 1.1.6* | A 3 D |
| CDP | A tanúsítványt kiadó CA CRL szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | EV 1.4.5 | 9.7 |
| Certificate Serial Number | Nem szekvenciális sorozatszám legalább 20 bit entrópiával | Nem | Kötelező | BL 1.1.6 | 9.6 |
| CertificatePolicy | A kiadott tanúsítványhoz tartozó policy azonosítója, ami bizonyítja, hogy 1) Melyik cp tartozik a tanúsítványhoz | Nem | Kötelező | EV 1.4.5 | 9.3.2 |
| ExtendedKeyusage | id-kp-serverAuth | Nem | Ajánlott | BL 1.1.6 | A 3 F |
| KeyUsage | Digital Signature, KeyEncypherment, KeyAgreement | Igen | Kötelező | BL 1.1.6 R5280 | A 3 E |
| Private and public key | lásd minimum algoritmusok táblázat | Nem | Kötelező | BL 1.1.6 | 9.5 -> App A 1,2,3 |
| subject:commonName (CN) | Ha a mező jelen van, akkor egy domain nevet tartalmaz az igényeltek közül. | Nem  | már nem ajánlott | EV 1.4.5 | 9.2.3 |
| subject:countryName (C ) | A mező a szervezet/személy székhely szerinti országát tartalmazza. | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subject:localityName (L) | A mező a szervezet/személy székhely szerinti városát tartalmazza | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subject:organizationalUnitName  | A mező a szervezeti egység nevét tartalmazza. | Nem | Opcionális | BL 1.1.6 | 9.2.6 |
| subject:organizationName (O) | A mező a szervezet nevét tartalmazza. | Nem  | kötelező | EV 1.4.5 | 9.2.1 |
| subject:stateOrProvinceName (ST) | A mező nincs jelen | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subjectAltName (SAN) | Egy vagy több domain nevet tartalmazhat.Az első domain névnek egyeznie kell a CN mezőben találhatóval, ha az jelen van. | Nem  | kötelező | EV 1.4.5 | 9.2.2 |
| Validity  | Az érvényesség ajánlott hossza 12 hónap, maximum hossza 36 hónap | Nem | Kötelező |   |   |
| Subject Key identifier | Alany kulcs hash | Nem | Kötelező | R 5280 |   |
| Authority Key dentifier | Kiadói kulcs hashe | Nem | Kötelező | R 5280 |   |
| Signature | Kiadó aláírása SHA256 algoritmussal | Nem | Kötelező | R 5280 |   |

### Személyes profil

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mező neve** | **Tartalom** | **Kritikus** | **Feltüntetés** | **forrás dokumentum** |
| AIA:Caissuers | A tanúsítványt kiadó CA tanúsítványának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 3 C |
| AIA:OCSP | A tanúsítványt kiadó CA OCSP szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 3 C |
| basicConstraints | CA:FALSE | Igen | Kötelező | *BL 1.1.6* | A 3 D |
| CDP | A tanúsítványt kiadó CA CRL szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | EV 1.4.5 | 9.7 |
| Certificate Serial Number | Nem szekvenciális sorozatszám legalább 20 bit entrópiával | Nem | Kötelező | BL 1.1.6 | 9.6 |
| CertificatePolicy | A kiadott tanúsítványhoz tartozó policy azonosítója, ami bizonyítja, hogy 1) Melyik cp tartozik a tanúsítványhoz | Nem | Kötelező | EV 1.4.5 | 9.3.2 |
| ExtendedKeyusage | Tanúsítvány felhasználásnak megfelelő biteket tartalmaz. | Nem | Ajánlott | BL 1.1.6 | A 3 F |
| KeyUsage | Tanúsítvány felhasználásnak megfelelő biteket tartalmaz. | Igen | Kötelező | BL 1.1.6 R5280 | A 3 E |
| Private and public key | lásd minimum algoritmusok táblázat | Nem | Kötelező | BL 1.1.6 | 9.5 -> App A 1,2,3 |
| subject:commonName (CN) | A mező a személy nevét tartalmazza. | Nem  | már nem ajánlott | EV 1.4.5 | 9.2.3 |
| subject:countryName (C ) | A mező a személy lakhely szerinti országát tartalmazza. | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subject:localityName (L) | A mező a személy lakhely szerinti városát tartalmazza | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subject:organizationalUnitName  | A mező nincs jelen | Nem | Opcionális | BL 1.1.6 | 9.2.6 |
| subject:organizationName (O) | A mező nincs jelen | Nem  | kötelező | EV 1.4.5 | 9.2.1 |
| subject:stateOrProvinceName (ST) | A mező nincs jelen | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subjectAltName (SAN) | a személy email címét tartalmazza. | Nem  | kötelező | EV 1.4.5 | 9.2.2 |
| Validity  | Az érvényesség ajánlott hossza 12 hónap, maximum hossza 36 hónap | Nem | Kötelező |   |   |
| Subject Key identifier | Alany kulcs hash | Nem | Kötelező | R 5280 |   |
| Authority Key dentifier | Kiadói kulcs hashe | Nem | Kötelező | R 5280 |   |
| Signature | Kiadó aláírása SHA256 algoritmussal | Nem | Kötelező | R 5280 |   |

### Munkatársi profil

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mező neve** | **Tartalom** | **Kritikus** | **Feltüntetés** | **forrás dokumentum** |
| AIA:Caissuers | A tanúsítványt kiadó CA tanúsítványának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 3 C |
| AIA:OCSP | A tanúsítványt kiadó CA OCSP szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 3 C |
| basicConstraints | CA:FALSE | Igen | Kötelező | *BL 1.1.6* | A 3 D |
| CDP | A tanúsítványt kiadó CA CRL szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | EV 1.4.5 | 9.7 |
| Certificate Serial Number | Nem szekvenciális sorozatszám legalább 20 bit entrópiával | Nem | Kötelező | BL 1.1.6 | 9.6 |
| CertificatePolicy | A kiadott tanúsítványhoz tartozó policy azonosítója, ami bizonyítja, hogy 1) Melyik cp tartozik a tanúsítványhoz | Nem | Kötelező | EV 1.4.5 | 9.3.2 |
| ExtendedKeyusage | Tanúsítvány felhasználásnak megfelelő biteket tartalmaz. | Nem | Ajánlott | BL 1.1.6 | A 3 F |
| KeyUsage | Tanúsítvány felhasználásnak megfelelő biteket tartalmaz. | Igen | Kötelező | BL 1.1.6 R5280 | A 3 E |
| Private and public key | lásd minimum algoritmusok táblázat | Nem | Kötelező | BL 1.1.6 | 9.5 -> App A 1,2,3 |
| subject:commonName (CN) | A mező a személy nevét tartalmazza. | Nem  | már nem ajánlott | EV 1.4.5 | 9.2.3 |
| subject:countryName (C ) | A mező a szervezet székhely szerinti országát tartalmazza. | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subject:localityName (L) | A mező a szervezet székhely szerinti városát tartalmazza | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subject:organizationalUnitName  | A mező a szervezeti egység nevét tartalmazza. | Nem | Opcionális | BL 1.1.6 | 9.2.6 |
| subject:organizationName (O) | A mező a szervezet nevét tartalmazza. | Nem  | kötelező | EV 1.4.5 | 9.2.1 |
| subject:stateOrProvinceName (ST) | A mező nincs jelen | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subjectAltName (SAN) | a személy email címét tartalmazza. | Nem  | kötelező | EV 1.4.5 | 9.2.2 |
| Validity  | Az érvényesség ajánlott hossza 12 hónap, maximum hossza 36 hónap | Nem | Kötelező |   |   |
| Subject Key identifier | Alany kulcs hash | Nem | Kötelező | R 5280 |   |
| Authority Key dentifier | Kiadói kulcs hashe | Nem | Kötelező | R 5280 |   |
| Signature | Kiadó aláírása SHA256 algoritmussal | Nem | Kötelező | R 5280 |   |

### Szervezeti profil

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mező neve** | **Tartalom** | **Kritikus** | **Feltüntetés** | **forrás dokumentum** |
| AIA:Caissuers | A tanúsítványt kiadó CA tanúsítványának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 3 C |
| AIA:OCSP | A tanúsítványt kiadó CA OCSP szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 3 C |
| basicConstraints | CA:FALSE | Igen | Kötelező | *BL 1.1.6* | A 3 D |
| CDP | A tanúsítványt kiadó CA CRL szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | EV 1.4.5 | 9.7 |
| Certificate Serial Number | Nem szekvenciális sorozatszám legalább 20 bit entrópiával | Nem | Kötelező | BL 1.1.6 | 9.6 |
| CertificatePolicy | A kiadott tanúsítványhoz tartozó policy azonosítója, ami bizonyítja, hogy 1) Melyik cp tartozik a tanúsítványhoz | Nem | Kötelező | EV 1.4.5 | 9.3.2 |
| ExtendedKeyusage | Tanúsítvány felhasználásnak megfelelő biteket tartalmaz. | Nem | Ajánlott | BL 1.1.6 | A 3 F |
| KeyUsage | Tanúsítvány felhasználásnak megfelelő biteket tartalmaz. | Igen | Kötelező | BL 1.1.6 R5280 | A 3 E |
| Private and public key | lásd minimum algoritmusok táblázat | Nem | Kötelező | BL 1.1.6 | 9.5 -> App A 1,2,3 |
| subject:commonName (CN) | A mező a szervezet nevét tartalmazza.. | Nem  | már nem ajánlott | EV 1.4.5 | 9.2.3 |
| subject:countryName (C ) | A mező a szervezet székhely szerinti országát tartalmazza. | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subject:localityName (L) | A mező a szervezet székhely szerinti városát tartalmazza | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subject:organizationalUnitName  | A mező a szervezeti egység nevét tartalmazza. | Nem | Opcionális | BL 1.1.6 | 9.2.6 |
| subject:organizationName (O) | A mező a szervezet nevét tartalmazza. | Nem  | kötelező | EV 1.4.5 | 9.2.1 |
| subject:stateOrProvinceName (ST) | A mező nincs jelen | Nem  | kötelező | EV 1.4.5 | 9.2.7 |
| subjectAltName (SAN) | A szervezet email címét tartalmazza. | Nem  | kötelező | EV 1.4.5 | 9.2.2 |
| Validity  | Az érvényesség ajánlott hossza 12 hónap, maximum hossza 36 hónap | Nem | Kötelező |   |   |
| Subject Key identifier | Alany kulcs hash | Nem | Kötelező | R 5280 |   |
| Authority Key dentifier | Kiadói kulcs hashe | Nem | Kötelező | R 5280 |   |
| Signature | Kiadó aláírása SHA256 algoritmussal | Nem | Kötelező | R 5280 |   |

#### Felhasználás függő mezők, személyes, munkatársi, szervezeti tanúsítványoknál, felhasználások szerint

**Authetnikációs**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ExtendedKeyusage | clientAuth, emailProtection | Nem | Ajánlott | BL 1.1.6 | A 3 F |
| KeyUsage | digitalSignature, keyAgreement | Igen | Kötelező | BL 1.1.6 R5280 | A 3 E |

**Titkosító**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ExtendedKeyusage | emailProtection | Nem | Ajánlott | BL 1.1.6 | A 3 F |
| KeyUsage | dataEncipherment, keyEncipherment | Igen | Kötelező | BL 1.1.6 R5280 | A 3 E |

**Kódaláíró**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ExtendedKeyusage | CodeSigning | Nem | Ajánlott | BL 1.1.6 | A 3 F |
| KeyUsage | digitalSignature | Igen | Kötelező | BL 1.1.6 R5280 | A 3 E |

## Szolgáltatói tanúsítványok

### Főtanúsítvány

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Mező neve** | **Tartalom** | **Kritikus (critical)?** | **Feltüntetése** | **forrás dokumentum** | **dokumentum fejezet** |
| basicConstraints | CA:TRUE | Igen | Kötelező | *BL 1.1.6* | *A 1 A* |
| Certificate Serial Number | nem szekvenciális minimum 20 bit entrópiával | Nem | Kötelező | BL 1.1.6 | 9.6 |
| Certificatepolicy |   | Tiltott | Tiltott | *BL 1.1.6* | A 1 C |
| extendedKeyusage |   | Tiltott | Tiltott | *BL 1.1.6* | A 1 D |
| *keyusage* | *keyCertSing, cRLSign* | *Igen* | *Kötelező* | *BL 1.1.6* | *A 1 B* |
| private and public key | lásd minimum algoritmusok táblázat | Nem | Kötelező | BL 1.1.6 | 9.5 -> App A 1,2,3 (root, sub, ee) |
| **Validity**  | tanúsítványban szereplő notbefore-notafter érték | **Nem** | **-** |  |  |
| Subject Key identifier | subject kulcs hash | Nem | Kötelező | RFC 5280 |   |
| **subject:commonName (CN)** | **tanúsítvány kiadó neve** | **Nem**  | **-** | **EV 1.4.5** | **9.2.3** |
| **subject:countryName (C )** | **HU** | **Nem**  | **-** | **EV 1.4.5** | **9.2.7** |
| **subject:localityName (L)** | **Budapest** | **Nem**  | **-** | **EV 1.4.5** | **9.2.7** |
| **subject:organizationalUnitName**  | **Tanúsítványkiadók (Certification Services)** | **Nem** | **-** | **BL 1.1.6** | **9.2.6** |
| **subject:organizationName (O)** | **NetLock Kft.** | **Nem**  | **-** | **EV 1.4.5** | **9.2.1** |
| **Signature** | **Kiadó aláírása SHA256 algoritmussal** | **Nem** | **Kötelező** | **R 5280** |  |

### Kiadói (köztes) tanúsítvány

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Mező neve** | **Tartalom** | **Kritikus (critical)?** | **Feltüntetése** | **forrás dokumentum** | **dokumentum fejezet** |
| AIA:Caissuers | A tanúsítványt kiadó CA tanúsítványának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 2 C |
| AIA:OCSP | A tanúsítványt kiadó CA OCSP szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 2 C |
| basicConstraints | CA:TRUE | Igen | Kötelező | *BL 1.1.6* | A 2 D |
| CDP | A tanúsítványt kiadó CA CRL szolgáltatásának elérhetősége http URL-en | Nem | Kötelező | *BL 1.1.6* | A 2 B |
| Certificate Serial Number | Nem szekvenciális sorozatszám legalább 20 bit entrópiával | Nem | Kötelező | BL 1.1.6 | 9.6 |
| Certificatepolicy  | nincs feltüntetve | Nem | Kötelező | BL 1.1.6 | B2A |
| *keyusage* | *keyCertSing, cRLSign* | *Igen* | *Kötelező* | *BL 1.1.6* | A 2 E |
| private and public key | lásd minimum algoritmusok táblázat | Nem | Kötelező | BL 1.1.6 | 9.5 -> App A 1,2,3 (root, sub, ee) |
| Validity  | tanúsítványban szereplő notbefore-notafter érték | Nem | Kötelező |   |   |
| Subject Key identifier | Köztes kiadó kulcs hash | Nem | Kötelező | RFC 5280 |   |
| Authority Key dentifier | Legfelsőbb kiadó kiadói kulcs hashe | Nem | Kötelező | RFC 5280 |   |
| Signature | Kiadó aláírása SHA256 algoritmussal | Nem | Kötelező | R 5280 |   |

### OCSP válaszadó tanúsítvány

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Mező neve** | **Tartalom** | **Kritikus (critical)?** | **Feltüntetése** | **forrás dokumentum** | **dokumentum fejezet** |
| basicConstraints | CA:FALSE | Igen | Kötelező | *BL 1.1.6* | A 2 D |
| Certificate Serial Number | nem szekvenciális minimum 20 bit entrópiával | Nem | Kötelező | BL 1.1.6 | 9.6 |
| extendedKeyusage | OCSPSigning | Nem | Kötelező | *RFC 5280* |   |
| *keyusage* | *digital signature* | *Igen* | *Kötelező* | *BL 1.1.6* | A 2 E |
| private and public key | lásd minimum algoritmusok táblázat | Nem | Kötelező | BL 1.1.6 | 9.5 -> App A 1,2,3 (root, sub, ee) |
| Validity  |  tanúsítványban szereplő notbefore-notafter érték | Nem | Kötelező |   |   |
| Subject Key identifier | subject kulcs hash | Nem | Kötelező | RFC 5280 |   |
| Authority Key dentifier | kiadói kulcs hashe | Nem | Kötelező | RFC 5280 |   |
| OCSPNocheck | üres tartalom | Nem | Kötelező | RFC 5280 |   |

### Visszavonási lista aláírói tanúsítvány

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Mező neve** | **Tartalom** | **Kritikus (critical)?** | **Feltüntetése** | **forrás dokumentum** | **dokumentum fejezet** |
| basicConstraints | CA:TRUE | Igen | Kötelező | *BL 1.1.6* | *A 1 A* |
| Certificate Serial Number | nem szekvenciális minimum 20 bit entrópiával | Nem | Kötelező | BL 1.1.6 | 9.6 |
| Certificatepolicy |   | Tiltott | Tiltott | *BL 1.1.6* | A 1 C |
| extendedKeyusage |   | Tiltott | Tiltott | *BL 1.1.6* | A 1 D |
| *keyusage* | *cRLSign* | *Igen* | *Kötelező* | *BL 1.1.6* | *A 1 B* |
| private and public key | lásd minimum algoritmusok táblázat | Nem | Kötelező | BL 1.1.6 | 9.5 -> App A 1,2,3 (root, sub, ee) |
| **Validity**  | tanúsítványban szereplő notbefore-notafter érték | **Nem** | **-** |  |  |
| Subject Key identifier | subject kulcs hash | Nem | Kötelező | RFC 5280 |   |
| subject:commonName (CN) | Hozzárendelt kiadóra utaló név | Nem  | - | EV 1.4.5 | 9.2.3 |
| subject:countryName (C ) | HU | Nem  | - | EV 1.4.5 | 9.2.7 |
| subject:localityName (L) | Budapest | Nem  | - | EV 1.4.5 | 9.2.7 |
| subject:organizationalUnitName  | Tanúsítványkiadók (Certification Services) | Nem | - | BL 1.1.6 | 9.2.6 |
| subject:organizationName (O) | NetLock Kft. | Nem  | - | EV 1.4.5 | 9.2.1 |

## Tanúsítvány visszavonási lista profilok

A Szolgáltató az x.509 [9] megfelelő visszavonási listákat (CRL) bocsát ki. A Szolgáltató által aktuálisan kibocsátott tanúsítvány visszavonási lista profilokat a Nem minősített tanúsítvány, visszavonási lista, OCSP és időbélyeg profildefiníciók [12] dokumentum tartalmazza és azt a Szolgáltató saját Internetes oldalán (ld. 1.5 alfejezet), a Tanúsítványtárnál megadott publikálási szabályoknak megfelelően közzéteszi.

|  |  |
| --- | --- |
| **Mező** | **Tartalom** |
| Version | V2 |
| Issuer | Kiadónként eltérő, lásd profildefiníciók [12]  |
| Last update | Utolsó kibocsátás dátuma |
| Next update | Következő kibocsátás dátuma |
| Signature | Kibocsátó elektronikus aláírása |
| CRL entry | Az érvénytelenített tanúsítvány sorozatszáma, érvénytelenítés dátuma, időpontja |
| CRL entry extension | Profildefiníciók [12] dokumentum tartalmazza |

## OCSP válasz profilok

A Szolgáltató által nyújtott OCSP szolgáltatás az RFC 2560 [9] ajánlás figyelembevételével működik. A Szolgáltató által aktuálisan kibocsátott OCSP válasz profilokat a Nem minősített tanúsítvány, visszavonási lista, OCSP és időbélyeg profildefiníciók [12] dokumentum tartalmazza és azt a Szolgáltató saját Internetes oldalán (ld. 1.5 alfejezet), a Tanúsítványtárnál megadott publikálási szabályoknak megfelelően közzéteszi. A Szolgáltató által kiadott tanúsítványok általában az általa kibocsátott OCSP válasz profilok alapján ellenőrizhetőek.

# A megfelelőség vizsgálata

Szolgáltató szolgáltatásának következő elemeinek megfelelőségét vizsgálja, vizsgáltatja:

a végfelhasználói tanúsítványok aláírására használt biztonságos eszközeit;

a saját magánkulcsainak tárolására használt kriptográfiai hardver modult;

az Igénylőok számára biztosított aláírás-létrehozó eszközöket (pl. intelligens kártyákat);

a végfelhasználói és szolgáltatói tanúsítványok kezeléshez használt módszereit, eljárásait;

a közigazgatásban felhasználható tanúsítványokra vonatkozó előírások teljesülését

az ISO 9001 minőségbiztosítási rendszer előírásai szerinti működést;

az ISO 27001 információbiztonsági irányítási rendszer előírásainak megfelelő működést,

## A megfelelőség vizsgálatának gyakorisága

A különböző vizsgálatokra a jogszabályoknak megfelelően az alábbi gyakorisággal kerül sor:

az eszközök vizsgálatára a használatba vételt megelőzően egyszer, majd a folyamatos megfelelés ellenőrzéseképpen legalább évente;

 a magas színvonalú szolgáltatást biztosító ISO 9001 minőségbiztosítási rendszer ellenőrzésére évente legalább 1 alkalommal, a teljes rendszerre vonatkozóan;

az információbiztonsági irányítási rendszer ISO 27001 (korábban BS 7799-2:2002 elnevezésű) szabványnak való megfelelés ellenőrzése évente legalább 1 alkalommal a teljes rendszerre vonatkozóan;

## Az átvizsgáló egységek megnevezése

A megfelelőségi vizsgálatokat külső szervezetek végzik/végezték:

a biztonságos aláírás létrehozó eszközök tanúsítását a jogszabályi előírásoknak megfelelő tanúsító szervezet (ld. **.** Törvény 24. §), amelynek kijelölésére a  **.** Rendelet előírásainak megfelelően kerül sor;

a közigazgatásban használható tanúsítványok kezeléshez használt módszerek, eljárások ellenőrzését hatósági eljárás keretében a Felügyelet;

a közigazgatásban használható tanúsítványokra vonatkozó előírásoknak ( **.**, **.**, **.**) való megfelelést a Közigazgatási Gyökér Hitelesítés-szolgáltató;

a szolgáltatási rendszer jogszabályi követelményeknek való megfelelését, illetve biztonságát legalább évente független szakértő felülvizsgálja. A vizsgálat kiterjed a kontroll rendszerre, a szabályozásra, a szabályok implementációjára és azok monitorozására;

az ISO 9001 minőségbiztosítási rendszer működtetését legalább évente akkreditált ISO tanúsító szervezet;

az ISO 27001 (korábban BS 7799-2:2002 elnevezésű) információbiztonsági irányítási rendszer működtetését legalább évente akkreditált, külső, független tanúsító szervezet.

A Szolgáltató e külső vizsgálatokon túl saját belső ellenőrzési rendszerrel is rendelkezik, mely rendszeresen vizsgálja a korábbi tanúsításoknak való megfelelőséget, és eltérés esetén megteszi a szükséges lépéseket. Az egyes szolgáltatói tevékenységek a jogszabályoknak és kapcsolódó szabályzatoknak való megfelelését a Szabályzat Elfogadó Egység vizsgálja saját munkarendje szerint.

## Az átvizsgáló egységek és a vizsgált fél kapcsolata

A Szolgáltatóval kapcsolatban vizsgálatot végző külső szervezetek a Szolgáltatótól függetlenek, és befolyástól mentesen végzik tevékenységüket. A vizsgálatot végző szervezetek nem rendelkeznek tulajdonrésszel vagy érdekeltséggel a Szolgáltatóban, és a Szolgáltató nem tulajdonosa közvetlenül vagy közvetve a vizsgálatot végző szervezeteknek. A szervezetek díjazása nem függ a tanúsítás során végzett tevékenységük megállapításaitól.

A belső függetlenséget a munkatársak esetében a Szolgáltató Függetlenségi Nyilatkozat aláíratásával, valamint a tevékenységi körök elválasztásával biztosítja. A Nyilatkozatot a Szolgáltató Személyzeti Politikája tartalmazza.

## A vizsgálat által érintett területek

A vizsgálatok vizsgáló szervezetenként más és más területekre terjednek ki. A vizsgálatok keretében sor kerül valamennyi a Szolgáltató működésére vonatkozó jogszabályi feltétel teljesítésének ellenőrzésére. A vizsgálatok kiterjednek továbbá a Szolgáltató saját hitelesítés-szolgáltatási rendjeinek és egyéb szabályzatainak való megfelelőség ellenőrzésére is.

A szabályzatoknak való megfelelés vizsgálata során a Szolgáltató teljes tevékenységi köre, illetőleg annak összes belső szabályzata vizsgálatra kerül (így például a Regisztrációs és Hitelesítő Egységek szabályzatai).

## Hiányosságok esetén végrehajtandó tevékenységek

A Szabályzat Elfogadó Egység a jogszabályok, illetve szabványok, szokványok és ajánlások előírásainak ellentmondó működés esetén a szolgáltatói tevékenységeket szabályozó belső eljárásrendek és szabályzatok megváltoztatásával, illetőleg a változás végrehajtásához szükséges rendszer implementáció végrehajtatásával intézkedik.

.

# Üzleti és jogi tudnivalók

## Díjak

A mindenkor érvényes szolgáltatások díjait a Szolgáltató saját Internetes oldalán (ld. 1.5 alfejezet), a Tanúsítványtárnál megadott publikálási szabályoknak megfelelően közzéteszi.

A közzétett adatok:

tanúsítvány kibocsátásának és megújításának díja,

tanúsítvány hozzáférési, tárolási díj,

visszavonási adatok hozzáférési díja,

időbélyegzés díja,

egyéb, a hitelesítés-szolgáltatáshoz kapcsolódó, különleges díjtételek (pl.: különeljárási díj, stb.).

A tanúsítvány kibocsátásának és megújításának a Szolgáltató mindenkor érvényes díjszabásában közzétett díja abban az esetben érvényes, ha a regisztráció Igénylő, illetve Másodlagos Alany eleget tud tenni a Szolgáltató regisztrációs eljárásrendjében meghatározott feltételeknek. A regisztrációs eljárásrendről tájékoztatás a Szolgáltató tanúsítványtárában található, a Központi Regisztrációs Egységtől és ügyfélszolgálattól kérhető (lásd 1.5 pont), valamint a tanúsítványkérés megkezdésekor automatikus tájékoztató is továbbításra kerül. A regisztrációs eljárásrendben meghatározott eseteken kívül (tipikusan külföldi személyazonosítók, elektronikusan nem lekérdezhető szervezeti nyilvántartások ellenőrzésének szükségessége) a Szolgáltató egyedi díjszabást alkalmaz.

A Szolgáltató díjaira vonatkozó egyéb szabályokat az ÁSZF tartalmazza.

### Egyéb szolgáltatásokra vonatkozó díjak

A Szolgáltató a kibocsátott tanúsítványok visszavonásáért, felfüggesztéséért és újraérvényesítéséért eljárási díjat számolhat fel az Igénylő felé, mely tartalmazza a tanúsítvány megváltozott állapotának a tanúsítványtárban visszavonási lista formájában történő közzétételének költségét.

A Szolgáltató az ezt igénylő ügyfeleinek emelt szintű szolgáltatásokért (pl. közvetlen bérelt vonali hozzáférés, gyorsított kibocsátás) egyedi díjszabást alkalmazhat.

A Szolgáltató díjaira vonatkozó egyéb szabályokat az ÁSZF tartalmazza.

### Visszatérítési elvek

Indokolt esetben a Szolgáltató a tanúsítványok kibocsátásához kapcsolódó, meghatározott időszakra vonatkozó egyes díjakat (pl.: tanúsítványtárolási díj) egyedi elbírálás alapján, időarányosan téríti vissza. Az egyszeri díjak visszatérítése teljes összegben történik.

Az Igénylő, illetve másodlagos Alany a számára kibocsátott tanúsítvány kibocsátási és teljes fenntartási díjának visszatérítésére tipikusan a következő esetekben jogosult:

a kibocsátott tanúsítvány valamely adata a Szolgáltató hibájából fakadóan nem megfelelő,

a Szolgáltató egyéb hibát követ el a tanúsítvány kibocsátásakor,

a Szolgáltató bizonyítottan nem tartja be valamely kötelezettségét az Igénylő tanúsítványának kezelésekor.

A díj visszatérítésére az Igénylőnek, illetve másodlagos Alanynek a tanúsítvány kibocsátását vagy megújítását követő 30 naptári napon belül a regisztrációs egység központi egységénél kérvényben kell beadnia a Szolgáltató részére. A kérvény pozitív elbírálása esetén a Szolgáltató a tanúsítványt díjmentesen visszavonja és a kibocsátási és teljes fenntartási díjat az Igénylő számára a kérelemben megjelölt bankszámlaszámra 20 naptári napon belül visszautalja.

A tanúsítvány kibocsátása, illetve megújítása a Szolgáltató általi teljesítésnek tekintendő, így ezt követően az Igénylő kizárólag csak a Szolgáltató bizonyított szerződés- vagy kötelezettségszegése esetén jogosult díjvisszatérítésre. Nem tartozik a visszatérítési okok közé a különösen a kibocsátott tanúsítványhoz tartozó magánkulcs bármely okból történő megsemmisülése.

A Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

## Pénzügyi felelősség

A Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személynek okozott kárért a Polgári Törvénykönyv általános szabályai szerint felel, az Igénylővel szemben pedig a szerződésszegésért való felelősség szabályai szerint felelős mindazon kárért, melyet saját felelősségi körében eljárva saját hibájából vagy mulasztásából erednek, így különösen:

az Igénylő alapos és mindenre kiterjedő mulasztása

a tanúsítvány felfüggesztéssel és visszavonással kapcsolatos kötelezettségek.

A Szolgáltató az alábbiakban meghatározza azt az egy alkalommal vállalható legmagasabb kötelezettség értéket, ameddig a Szolgáltató helytáll az okozott kárért.

Az egy alkalommal vállalható legmagasabb kötelezettség értéke a nem minősített tanúsítványoknál a tanúsítványban feltüntetett összeg, amennyiben ilyen korlát nem szerepel benne, akkor az „A” osztály esetében 5,000,000 magyar forint, azaz ötmillió magyar forint, míg a „B” osztály esetén 500,000 magyar forint, azaz ötszázezer magyar forint, „C” osztályú tanúsítvány esetén 50,000 magyar forint, azaz ötvenezer magyar forint.

A Szolgáltató biztosítója azon bizonyított károkért, amelyek a Szolgáltató felelősségi körében annak saját hibájából vagy mulasztásából keletkeztek, kártérítést fizet a fenti, káreseményenkénti felső határral.

Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.

## Bizalmasság, adatvédelem

A Szolgáltató a birtokába jutott adatokat a hatályos jogszabályi rendelkezésekre figyelemmel tárolja és kezeli. A Szolgáltató a törvényi előírásokon túlmenően saját belső szabályozási rendszerében is rögzített módon mindent megtesz az ügyfelek adatainak biztonságos kezelése érdekében.

Az adatgyűjtések célja a hitelesítés-szolgáltatási tevékenység regisztrációs feladatainak ellátása. A Szolgáltató az adatokat a törvények által előírt eseteken kívül kizárólag a főtevékenység hatékonyságának funkcionális támogatásához (lásd 9.3.6 pont), illetve megfelelő módon anonimizálva a belső statisztikáihoz használja fel.

Szolgáltató a regisztráció során kitöltött regisztrációs adatlap adatait elektronikus formában, a jelen Szabályzatban meghatározott azonosítási eljárások végrehajtása során fénymásolat formájában birtokába jutott adatokat papír alapon, illetve elektronikus formában tárolja. Biztonságos fizikai tárolással, illetve logikai védelmi rendszerrel biztosítja az adatok biztonságát, lehetővé téve az adatvesztés, adatsérülés, az adatok helytelen vagy illetéktelen használatának elkerülését.

A Szolgáltató a hatályos jogszabályoknak megfelelően a tanúsítványokkal kapcsolatos elektronikus információkat – beleértve az azok előállításával összefüggőket is – és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejártától számított 10 évig, illetőleg az elektronikus aláírással, illetve az azzal aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi (amennyiben annak kezdetéről és végéről a 9.5.3.1 pontban megfogalmazott kötelezettségek szerint értesítik), valamint ugyanezen határidőig olyan eszközt biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható.

A Szolgáltató biztosítja, hogy honlapján történő információkeresés, illetve az ún. ügyfélmenü használatán kívül eső oldalak tallózása során az ügyfelek névtelenek maradjanak.

A Szolgáltató biztosítja, hogy bármely adat rendelkezésre bocsátása esetén ezen adatokhoz illetéktelen személyek ne férhessenek hozzá.

### Bizalmasan kezelendő információ típusok

Alapértelmezésben a felhasználók azon adatai, amelyek a tanúsítványban nem szerepelnek. Bizalmas adatnak számítanak továbbá a Szolgáltató belső eljárásrendjei és a magánkulcsok.

### Nem bizalmasnak tekintett információ típusok

Azon regisztrációs adatok, amelyeket a felhasználó engedélye alapján a Szolgáltató nyilvánosként kezel. Nyilvánosak továbbá a tanúsítványtárban elhelyezett tanúsítványok, a szabályzatok, a CRL.

### Tanúsítvány visszavonására / felfüggesztésére vonatkozó információ felfedése

A Szolgáltató az általa kibocsátott tanúsítványok visszavonását és felfüggesztését a Tanúsítvány Visszavonási Listában teszi közzé, a tanúsítvány sorszámának és opcionálisan a visszavonás okának a jelölésével. A Szolgáltató a Tanúsítvány Visszavonási Listában a tanúsítvány azonosítója szerint is keresési lehetőséget biztosít (ld. még 4.6 alfejezet).

### Szolgáltató leállása

A Szolgáltató tevékenységének befejezésekor a tanúsítványokkal kapcsolatos adatokat (így különösen tanúsítványokkal kapcsolatos változások adatai, a tanúsítványok aktuális helyzetéről, visszavonásáról, felfüggesztéséről vezetett nyilvántartásokat) más, vele a befejezett szolgáltatás vonatkozásában azonos besorolású hitelesítés-szolgáltatónak adja át.

### Az Igénylő kérésére történő felfedés

A Szolgáltató az Igénylő, illetve másodlagos Alany meghatalmazása alapján tár fel bizalmas felhasználói információkat harmadik fél részére, melyért a Szolgáltató az internetes oldalán (lásd 1.5 pont) feltüntetett, mindenkor érvényes különeljárási díjat számol fel.

### Egyéb információ harmadik félnek történő átadása

Egyéb információ harmadik félnek történő átadására sor kerülhet 30 napja lejárt díjtartozás esetén, annak érvényesítése céljából.

A Szolgáltató átadhat egyéb információt vele szerződéses kapcsolatban álló olyan szervezeteknek, amelyek a Szolgáltató szolgáltatásai kapcsán kibocsátott elektronikus dokumentumok vagy az azokkal hitelesített más elektronikus dokumentumok érvényességének, hatályosságának, alkalmazhatóságának megállapításával kapcsolatos szolgáltatást nyújtanak.

## Szellemi alkotásokhoz fűződő jogok

A szolgáltatási tevékenység során alkalmazott összes név, termék, szabályzat, CRL a Szolgáltató tulajdonát képezi, a szoftver és hardver komponensek a Szolgáltató tulajdonát képezik vagy azokat jogszerűen használja.

## Jogok és kötelezettségek

### A hitelesítő egységek közös kötelezettségei

1. szabványos X509 tanúsítvány kibocsátása, megújítása, felfüggesztése, reaktiválása, visszavonása a Központi Regisztrációs Egység által küldött erre vonatkozó kérelem esetén,
2. tanúsítvány felfüggesztésének vagy visszavonásának publikálása CRL-en,
3. saját tanúsítványának nyilvánosságra hozatala,
4. saját magánkulcsának teljes körű védelme, a kulcs dedikált kriptográfiai hardver modulban történő tárolásával,
5. a hitelesítő kulcspár kompromittálódásának feltételezése, a kulcspár sérülése, megsemmisülése esetén az alkalmazó Közösség tagjainak késedelem nélküli értesítése elektronikusan (pl. elektronikus levélben, Internet oldalon közzététellel), illetve out-of-band módon (pl. postai úton, napilapban közzététellel) továbbá a Szabályzat Elfogadó Egység bármely tagjának írásban vagy személyesen történő megkeresésével.

### A Regisztrációs Egységek közös kötelezettségei

1. úgy működni, hogy semmilyen módon ne sértsék a szolgáltatás biztonságát,
2. tevékenységüket saját maguk ellátni,
3. az Igénylő (Igénylő) tanúsítványra vonatkozó kérelmeinek (kibocsátás, megújítás, felfüggesztés, visszavonás) kezelése,
4. az ügyféladatok összegyűjtése, közhiteles nyilvántartásban való ellenőrzése és döntés meghozatala azok valódiságára vonatkozóan,
5. a nem nyilvános ügyféladatok megfelelő szintű védelme,
6. az Igénylő (és az Igénylő) és a Közösség többi tagjának értesítése a tanúsítvány kibocsátásáról és a tanúsítvánnyal végzett műveletekről,
7. a tanúsítványnak az Igénylő számára elérhetővé tétele,
8. a belépés lehetővé tétele a Szabályzat Elfogadó Egység számára a szolgáltatás területére.

#### Külső regisztrációs munkatársak

1. a személyazonosságot és az egyéb adatok valódiságát igazoló okmányoknak ellenőrzése és az ügyfél Szolgáltatási Szerződésének – az igényelt felelősségvállalás mértékétől, illetve egyéb feltételektől függően - aláírás hitelesítése,
2. az ellenőrzésére használt eredeti iratok másolatának a Szolgáltatónál működő központi egységhez való eljuttatása,

#### „A” osztályú külső regisztrációs munkatársak

1. a személyazonosságot és az egyéb adatok valódiságát igazoló okmányoknak ellenőrzése és a szolgáltatási szerződésen aláírás hitelesítése,
2. az ellenőrzésére használt eredeti iratok másolatának a Szolgáltatónál működő központi egységhez való eljuttatása,

#### Központi Regisztrációs Egység

1. A külső regisztrációs munkatársak hitelesítésének ellenőrzése
2. a hitelesítés ellenőrzése, melynek alapját a hozzá eljutatott másolati dokumentumok képezik; és az adatok valós idejű, elektronikus közhiteles nyilvántartásban való ellenőrzése.
3. a tanúsítvány- és visszavonási kérelem nyilvántartásba vétele és a kérelem elbírálása, továbbítása.

### A végfelhasználó kötelezettségei

#### A végfelhasználó általános kötelessége:

1. megismerni és betartani az Általános Szerződési Feltételeket és a jelen Szabályzatot,
2. igényeinek és a kiválasztott hitelesítési rendnek megfelelő tanúsítványfajtát kiválasztani,
3. jelezni a Szolgáltatónak, ha a tanúsítványt jogszabályban meghatározott ügyintézésre is fel kívánja használni,
4. álnevet tartalmazó tanúsítvány esetén olyan álnevet választani, amely mások jogait nem sérti,
5. a feltételeknek és szabályzatoknak megfelelően eljárni a szolgáltatások felhasználása során, beleértve a tanúsítvány és magánkulcs igénylését és alkalmazását,
6. hozzájárulni a szolgáltatás biztonságához, elsősorban korrekt adatszolgáltatáson keresztül, valamint a nyilvános kulcsú infrastruktúra tudatos és felelősségteljes alkalmazásával,
7. esetleges jogvita kezdetéről és jogerős lezárásáról haladéktalanul tájékoztatni a Szolgáltatót,
8. a tanúsítvánnyal kapcsolatban észlelt – külön jogszabályban, illetve a Szabályzatban meghatározott – rendellenességről tájékoztatni a Szolgáltatót,
9. betartani a tanúsítványban jelzett esetleges korlátozásokat.

#### A végfelhasználó kötelessége saját kulcs kezelése során:

1. a magánkulcsát biztonságos módon tárolni, kezelni,
2. a kulcspárt és tanúsítványát rendeltetésszerűen használni,
3. magánkulcsát a hozzá tartozó tanúsítvány lejárta után megsemmisíteni,
4. amennyiben magánkulcsa kompromittálódásának lehetősége fennáll, a lehető leghamarabb tanúsítványának visszavonását, illetve felfüggesztését kérni a Szolgáltatótól.

#### A végfelhasználó kötelessége a tanúsítványának kezelése során:

1. a tanúsítványkiadáshoz előírt regisztrációs eljárásrend alapján felvett adatainak valódiságát a jelen Szabályzat vonatkozó pontjaiban (ld. 3. fejezet) található eljárások alapján a szükséges okmányok eredetijének, hiteles másolatának továbbá másolatának bemutatásával alátámasztani,
2. az azonosításához szükséges személyazonosító adatokról, munkatársi tanúsítvány esetén a szervezet nevében aláírásra jogosult személy személyazonosító adatairól, valamint a cégadatokról és mindezek változásáról tájékoztatni a Szolgáltatót,
3. a regisztrált adatainak a kibocsátott tanúsítványának érvényességi ideje alatt történő megváltozásáról késedelem nélkül a Szolgáltatót tájékoztatni,
4. olyan eljárásokat követni és alkalmazásokat használni, amelyek támogatják a Szolgáltató által kibocsátott tanúsítványok helyes kezelését,
5. a tanúsítvány első felhasználása előtt ellenőrizni a tanúsítványban feltüntetett adatainak helyességét és amennyiben azok nem felelnek meg a valóságnak, akkor a tanúsítvány visszavonását kérni.
6. A kötelezettségek értelemszerűen alkalmazandók a tanúsítvány és kulcs érvényességi időszaka alatt, és ha szükséges, akkor azt követően is.

**Figyelem!**

**Nem valós, hamis vagy hamisított adatok közlésével az Igénylő, illetve a másodlagos Alany egyes esetekben okirat-hamisítás bűntettét valósítja meg, amelyért büntető jogi felelősséggel tartozik.**

### Ajánlások az Érintett Fél részére

Jelen Szabályzatban az Érintett Fél számára meghatározott tevékenységek ajánlást jelentenek a Szolgáltató részéről, amelyek szükségesek az elektronikus aláírás elfogadása biztonságos végrehajtásához.

A Szolgáltató kizárja a felelősségét, ha az érintett fél az aláírás, tanúsítvány vagy időbélyeg érvényességének és hatályosságának ellenőrzése során - a Szolgáltató hitelesítési rendjében, szolgáltatási szabályzatában lévő ajánlások ellenére - a tőle az adott helyzetben általában elvárható magatartást nem tanúsítja, illetve ha nem a hatályos jogszabályok szerint jár el.

#### Az Érintett Fél számára az alábbi előírások betartása ajánlott:

1. Meghatározott célokra korlátozva és csak olyan alkalmazásokkal fogad el nyilvános kulcsokat, melyek összhangban vannak a megfelelő tanúsítványok „kulcshasználat” és „kiterjesztett kulcshasználat” mezőinek tartalmával.
2. Olyan eljárásokat, alkalmazásokat használni, amelyek támogatják a Szolgáltató által kibocsátott tanúsítványok helyes kezelését,

**Figyelem!**

**Az Érintett Félnek ajánlott visszautasítania minden olyan tanúsítvány elfogadását, ha bármely ellenőrzési lépés eredményéből a tanúsítvány vagy annak alkalmazásának érvénytelenségére, jogszerűtlenségére, jelen és kapcsolódó szabályzatokba ütköző voltára utaló következtetés vonható le.**

**Amennyiben ezt nem teszi meg, az érvénytelen, jogszerűtlen, vagy jelen és kapcsolódó Szabályzatba ütköző tanúsítványalkalmazás elfogadásából eredő károkért maga felel.**

### Szolgáltató egyéb kötelezettségei

A Szolgáltató általános kötelessége:

1. a hitelesítő és regisztrációs egységek és a tanúsítványtár felügyelete, üzemeltetése;
2. a szolgáltatásainak az irányadó nemzetközi előírásokkal, jelen szabályzattal és egyéb nyilvánosságra hozott szabályzataival, szerződéses feltételeivel összhangban való nyújtása;
3. a magas színvonalú és biztonságos szolgáltatások folyamatos biztosítása;
4. az alvállalkozók feladatainak egyértelműen meghatározása, működésük rendszeres ellenőrzése, a Szolgáltató által előírt eljárások betartásának biztosítása, és az esetlegesen szabályzattól eltérő működés esetén a helytelen működés megszüntetésének előírása és ellenőrzése;

### A Szolgáltatói egységek közös kötelezettségei

A Szolgáltatóhoz tartozó szervezetek, regisztrációs és hitelesítő egységek kötelessége:

1. a Közösség elektronikus hitelesítéssel kapcsolatos tevékenységeinek, alapelveinek meghatározása, ezek alapján a működést részletesen tárgyaló szabályzatok készítése és rendszeres felülvizsgálata,
2. megfelelő szakmai végzettséggel rendelkező, a folyamatos, szabályzatokban előírt működés biztosításához elégséges számú kezelőszemélyzet biztosítása,
3. a szabályzatokban előírt PKI folyamatok elvégzésére alkalmas, megfelelően beállított szoftver és hardver infrastruktúra biztosítása, a szükséges változtatások megtétele,
4. az infrastruktúra működtetéséért, javításáért és karbantartásáért felelős személyzet munkájának és szakmai felkészültségének folyamatos ellenőrzése, a szükséges változtatások megtétele,
5. az előző pontokban előírt infrastruktúra folyamatos, biztonságos üzemeltetése, hibajavítása és az infrastruktúrába tartozó eszközökre előírt szabványos karbantartás elvégzése,
6. Üzleti Folytonossági Terv készítése, alkalmazása,
7. a szabályzatokban előírt módon folytatott tevékenység során keletkező adatok jelen és kapcsolódó szabályzatokban meghatározott kezelésére, tárolására, archiválására alkalmas szoftver és hardver eszközök biztosítása, működtetése, karbantartása,
8. a PKI folyamatokat végző és az azok során keletkező adatokat tároló szoftver és hardver rendszer jelen és kapcsolódó szabályzatokban előírt logikai és fizikai védelmét biztosító szoftver és hardver eszközök biztosítása,
9. a logikai és fizikai védelmet megteremtő eszközök megfelelő üzemeltetése, az informatikai, fizikai, adminisztrációs és üzleti biztonság megteremtése és fenntartása.
10. szabad hozzáférés biztosítása a Szabályzat Adminisztrátor részére a felügyelendő dokumentumokhoz, továbbá a megfelelő körülmények biztosítása számára a belső ügyviteli folyamatok azok helyszínén való ellenőrzéséhez.

#### A Szabályzat Elfogadó Egység kötelezettségei

1. a felügyelendő dokumentumok, továbbá a belső ügyviteli folyamatok azok helyszínén való ellenőrzése és a Szolgáltató vezetésének tájékoztatása a megfigyelésekről,
2. a Szolgáltatóhoz érkező szabályzatokkal kapcsolatos észrevételek és javaslatok fogadása,
3. a szabályzatok aktualizálásának előkészítése, egyeztetése és végrehajtása,
4. a különböző hitelesítés-szolgáltatási rendek specifikálása, jóváhagyása és karbantartása.

#### A tanúsítványtár kötelezettségei és vele kapcsolatos tevékenységek

A Tanúsítványtár kötelessége az üzemeltetés során:

1. a Tanúsítványtár nyilvános, minden Érintett Fél számára elérhető módon való üzemeltetése a Szolgáltató Internetes oldalán (ld. 1.5 alfejezet),
2. a Szolgáltató saját tanúsítványainak, a Szolgáltató által kibocsátott tanúsítványok, CRL listák, aktuális és korábbi szabályzatok (NETLOCK ÁSZF, Szolgáltatási Szabályzat és Hitelesítési Rend) késedelem nélküli közzététele,
3. a szabályzatok során minimum Adobe Acrobat és Microsoft Word dokumentum formátumban közzétenni,
4. bizalmas információkat, nem nyilvános adatokat a Tanúsítványtárban meg nem jeleníteni,
5. a Tanúsítványtárat minimum 99 %-os rendelkezésre állással működtetni, ezt a mutatót is figyelembe véve elérhetővé tenni az év valamennyi napján, 0–24 óráig; a leállások nem haladhatják meg a 24 órát,
6. a rendelkezésre állást a Szolgáltató az Üzleti Folytonossági Tervben rögzített, a szokásostól eltérő üzletmenet elhárítására kidolgozott eljárások végrehajtásával biztosítani,
7. a Tanúsítványtárhoz írási jogosultságot csak a Szolgáltatónak biztosítani.

## Felelősség

### A Szolgáltató általános felelőssége

A Szolgáltató felelős:

a Szabályzat keretei között végzett szolgáltatói tevékenységekért,

a szolgáltatásai ellátásához szükséges regisztrációs és hitelesítő egységek működéséért akkor is, ha egyes funkciókat alvállalkozók végeznek.

#### A felelősség korlátai

Szolgáltató nem felelős az olyan károkért, amelyek abból adódtak, hogy az Aláíró vagy az Érintett Fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályoknak, illetve szolgáltatói szabályzatoknak megfelelően járt el, illetve nem tanúsította a tőle elvárható gondosságot.

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 (lásd 9.2 pont).

### A végfelhasználó felelőssége

Ha végfelhasználó a jelen szabályzat szerinti kötelezettségét megszegte, felel az ebből fakadó károkért.

### Az Érintett Fél felelőssége

A Szolgáltató kizárja a felelősségét, ha az érintett fél az aláírás, tanúsítvány vagy időbélyeg érvényességének és hatályosságának ellenőrzése során - a Szolgáltató hitelesítési rendjében, szolgáltatási szabályzatában lévő ajánlások ellenére- a tőle az adott helyzetben általában elvárható magatartást nem tanúsítja, illetve ha nem a hatályos jogszabályok szerint jár el.

## Változtatási eljárás

### Szabályzat-változtatási eljárás

A Szolgáltatón belül Szabályzat Elfogadó Egység működik, amely a Szabályzat karbantartásáért felelős. A változtatási igényeket ezen egység gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz, s a változtatásokat életbe lépteti.

A változtatásokat gyűjtve az egység belső nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. Szolgáltató a változásokat kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A Szolgáltató elfogadás előtt megvizsgálja a hitelesítés-szolgáltatási rendek meghatározott követelményeknek való megfelelőségét:

* tartalmi megfelelés az Ajánlás által támasztott minimális követelményeknek,
* formai megfelelés a RFC 3647 [4] szabványnak.

A hitelesítés-szolgáltatási rendek elfogadására vagy esetlegesen a Felügyelet által már nyilvántartásba vett hitelesítés-szolgáltatási rendek közül történő kiválasztására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik, majd egyetértés esetén a Felügyelet nyilvántartásba veszi a Szolgáltató által jóváhagyott és bejelentett hitelesítés-szolgáltatási rendet.

A Szolgáltató jóváhagyás előtt megvizsgálja a Szabályzatot a szolgáltatási szabályzat megfelelőség szempontjából, hogy a Szabályzat tartalmilag és formailag megfelel-e a hitelesítés-szolgáltatási rendeknek.

A Szabályzat jóváhagyására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik, majd bejelentés után a Szabályzatot a Felügyelet nyilvántartásba veszi.

A Szolgáltatási Szabályzat módosított változatai mindig új verziószámmal kerülnek nyilvánosságra. A szabályzatok egymásnak, a vonatkozó jogszabályoknak és szabványoknak való megfelelés vizsgálata legalább évente kétszer történik. A szabályzatok rendkívüli felülvizsgálatára és módosítására a jogszabályi változások esetén kerül sor. A szabályzatok felülvizsgálatát a Szolgáltató a működése során szerzett gyakorlati tapasztalatok alapján is elvégzi.

### Szabályzat Elfogadó Egység

#### A Szabályzat Elfogadó Egység összetétele

A Szabályzat Elfogadó Egység a következő összetételű munkacsoportként működik:

Szabályzat Vezető: a Szabályzat Elfogadó Egység vezetője, feladata az Egység munkájának koordinálása, illetve határozatainak jóváhagyása.

Szabályzat Adminisztrátor: a Szabályzat Elfogadó Egység által felügyelt szabályzatokat alkalmazó Közösség felől a szabályzatok módosítása tekintetében érkező igények feldolgozására, illetve a szabályzatok módosításának kidolgozására és javaslat formában történő előterjesztésére kijelölt személy. Az adminisztrátor hatásköre és felelőssége továbbá a hitelesítés-szolgáltatási rendek specifikálása, jóváhagyatása és karbantartása.

#### A Szabályzat Elfogadó Egység működése

A Szabályzat Elfogadó Egységet a Szabályzat Vezető hívja össze. A Szabályzat Elfogadó Egység évente legalább kétszer a felügyelt szabályzatok rendelkezéseinek átfogó felülvizsgálata miatt kerül összehívásra.

Az Egység határozatait a szükséges változtatások előterjesztése és megvitatása után a Szabályzat Vezető hozza meg, melyeknek a szabályzatokba történő bevezetéséért a Szabályzat Adminisztrátor felelős.

A Szabályzat Elfogadó Egység tagjainak mindenkor érvényes névsorát a Szabályzat Elfogadó Egység tagjegyzéke tartalmazza. A Szabályzat Elfogadó Egység üléseiről jegyzőkönyv készül.

### Értesítés nélkül változtatható elemek

A Szolgáltató jelen Szabályzat módosítását a jogszabályokban erre előírt módosítási eljárás nélkül nem lépteti hatályba.

### Értesítéssel változtatható elemek

A Szolgáltató jelen Szabályzat, valamennyi módosítását kizárólag az erre a vonatkozó jogszabályokban előírt eljárásban meghatározott feltételek teljesülése esetén lépteti hatályba. Azon módosítások, melyek a szolgáltatások biztonsági szintjét, felhasználhatóságát nem módosítják (ilyenek tipikusan a helyesírási hibák, formai változtatások, különböző kontaktadatok, Internet címek, telefonszámok) összevontan kerülnek módosításra és ezzel együtt értesítésre. A szolgáltatások biztonsági szintjét, felhasználhatóságát módosító változtatásokra pedig a Szolgáltató a weboldalán közzétett tájékoztatással hívja fel a Közösség figyelmét (lásd 2.1.2 pont).

### Szabályzati objektumazonosítót vagy mutatót változtató módosítások

Minden módosítás megváltoztatja a Szabályzat verziószámát és objektumazonosítóját. Azt a módosított szabályzatot, amely csak az újonnan kibocsátásra kerülő tanúsítványokra vonatkozik (de a már kibocsátottakra nem), a Szolgáltató az előző főbb verziótól eltérő Internet címen teszi közzé, így csak az újonnan kibocsátott tanúsítványok mutatói fognak rá hivatkozni, amennyiben a tanúsítványban van ilyen mutató.

## Panaszkezelési szabályok

### Panaszok benyújtásának helye

A Szolgáltató (beleértve a regisztrációs egységeket is) tevékenységével kapcsolatos kérdések, kifogások és panaszok benyújtásának helye a Szolgáltató ügyfélszolgálati irodája (ld. 1.5 alfejezet).

### Panaszok benyújtásának módja

A panaszokat a Szolgáltató levélben, e-mailben az info@NETLOCK.hu címen, faxon, telefonon és személyesen fogadja.

### Panaszok kezelésének eljárása

A panasz kézhezvételéről a Szolgáltató az érkeztetést követően 3 munkanapon belül értesíti a beadó felet a megjelölt címen, az ügy kivizsgálásához szükséges idő megjelölésével. A jelzett időn belül, amely lehetőség szerint nem több, mint 10 munkanap, a Szolgáltató a panaszt kivizsgálja, a felmerült hibát a műszakilag indokolt időn belül elhárítja, és mindezen tevékenységekről a bejelentőt írásban tájékoztatja. Ha a választ bejelentő nem fogadja el, egyeztetést kell kezdeményeznie a Szolgáltatóval. Ha a Szolgáltató ezt megtagadja, vagy ha a felek közötti egyeztetés annak megkezdésétől számított 20 munkanapon belül nem vezetne eredményre, akkor a bejelentő jogi útra terelheti az ügyet. A panaszkezelés véghatárideje a fentiek a bejelentéstől számított figyelembevételével 30 nap.

### Illetékes fogyasztóvédelmi felügyelőség

**NFH Közép-magyarországi Regionális Felügyelősége,** elérhetőségei:

* + - **Regionális Igazgatóság:** Cím: 1052 Budapest, V. ker. Városház u. 7. Levelezési cím:  1364 Budapest, Pf. 144. Telefon: +36 1 328-0185 Fax: +36 1 411-0116 E-mail: fogyved\_kmf\_budapest@nfh.hu
		- **Fogyasztókapcsolati Iroda:** Cím: 1088 Budapest, VIII. ker. József krt. 6. Telefon: + 36 1 459 4999, +36 1 459 4836, +36 1 459 4833, +36 1 459 4832

##  Hivatkozott jogszabályok, szabványok és egyéb dokumentumok

Jelen dokumentum az alábbi dokumentumokra hivatkozik:

1. ISO 3166 English Country Names and Code Elements
2. FIPS PUB 140-2 (2001. május): "Kriptográfiai modulok biztonsági követelményei"
3. RFC 5280 (korábban RFC 3280) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány- és tanúsítvány visszavonási lista profil
4. RFC 3647 (korábban RFC 2527) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és Szolgáltatási Szabályzat keretrendszer
5. International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány-keretrendszer”
6. 9/2005. IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról
7. RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
8. ETSI 102 042 v2.1.1 (2009-05) Policy requirements for certification authorities issuing public key certificates
9. RFC 2560 Online Certificate Status Protocol (OCSP)
10. Általános Időbélyegzési Rend – NETLOCK Kft.
11. 1992 évi XLIII. törvény a személyes adatok védelméről és a közhasznú adatok nyilvánosságáról
12. Nem minősített tanúsítvány, visszavonási lista, OCSP és időbélyeg profildefiníciók mindenkor hatályos változata
13. Általános Szerződési Feltételek (ÁSZF) – NETLOCK Kft.

## Értelmezés és érvényesítés

### Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi (ld.  **.**Törvény, **.** Irányelv,  **.**Rendelet). A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, és azok a magyar jog szerint értelmezendők.

### A rendelkezések különválaszthatósága

Bármely rendelkezés hatályon kívül kerülése vagy bíróság általi semmissé nyilvánítása nem befolyásolja a többi rendelkezés hatályát, érvényességét.

### A rendelkezések jogfolytonossága

A visszavonásra és a visszavonási információ kezelésére vonatkozó szabályok abban az esetben is érvényben maradnak (és az archivált adatok megőrződnek), ha a szolgáltatás és ezáltal a Szabályzat megszűnik.

### A rendelkezések kiterjesztése

A szolgáltatási tevékenységhez kapcsolódó egyéb szerződések figyelemmel vannak jelen Szabályzat rendelkezéseire is.

### Vitás kérdések megoldására vonatkozó eljárások

A Szolgáltató (beleértve a regisztrációs egységeket is) tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az info@NETLOCK.hu e-mail címen, valamint a Szolgáltató központi fax számán lehet írott formában bejelenteni (ld. 9.8 pont), illetve telefonon vagy személyesen a Szolgáltató ügyfélszolgálati irodájában (lásd:1.5. ).

Bármely vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra terelése előtt a felhasználónak kötelessége, az Érintett Félnek vagy bármely harmadik félnek ajánlott a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása az ügy minden vonatkozását érintően. A felek vitáikat mindenkor megkísérlik békés, tárgyalásos úton rendezni.

Amennyiben a Felek közötti egyeztetés - mely a Szolgáltató a panasz kivizsgálásának eredményeként adott válaszát követi- valamelyik fél által kezdeményezetett egyeztetés napjától számított 20 napon belül nem vezet eredményre, arra az esetre a Felek kölcsönösen alávetik magukat a Kereskedelmi és Iparkamara mellett szervezett Állandó Választottbíróság kizárólagos illetékességének. A Választottbírósági eljárás nyelve a magyar, az eljárásban irányadó jog a mindenkor hatályos magyar anyagi és eljárásjog. Az eljáró bírók száma: 3.