MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó Kft.

Trust&Sign

Hitelesítés Szolgáltatási Szabályzat
Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatáshoz

Verziószám	**1.3**
Hatálybalépés dátuma	**2004. március 1.**

MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Kft.
1012 Budapest, Krisztina krt. 37/a., 1253 Budapest Pf. 28, Tel.: 457-9300, fax: 457-9500,
e-mail: mavinformatika@mavinformatika.hu

A dokumentum neve	Hitelesítés Szolgáltatási Szabályzat Fokozott Biztonságú Elektronikus Aláírás-hitelesítés Szolgáltatáshoz (HSzSz)*
HSzSz verziószám	1.3
Üzemelő PKI szoftver verziószám (Technikai azonosító)	trust-sign ACA v1.0
NHH regisztrációs szám	MH-13181-1/2002
HSzSz objektum azonosító (OID)	1.3.6.1.4.1.14868.1.1
Első hatálybalépés időpontja	2002. november 5.
Aktuális változat hatálybaléptetés időpontja	2004. március 1.
Következő felülvizsgálat időpontja:	2005. január 31.

* A MÁV INFORMATIKA Kft. Hitelesítés Szolgáltatási Szabályzata az elektronikus aláírásról szóló 2001. évi XXXV. törvény szerint előírt Szolgáltatási Szabályzat, amely a hazai gyakorlatnak megfelelően az Internet Közösség RFC 2527 ajánlásában és az EU ETSI TS 101 456 szabványában javasolt Certificate Practice Statement (CPS) szerkezetet követi.

TARTALOMJEGYZÉK

1. Bevezetés 9

1.1. Alapok 9
1.1.1. Szabályzat célja 9
1.1.2. Szabályzat tartalma 10
1.1.3. Jogszabályok, szabványok 13

1.2. HSzSz Azonosítás 15

1.3. Hitelesítés szolgáltató és felhasználó közösség, alkalmazhatóság 16
1.3.1. Hitelesítési Politika és Szabályozási Csoport 16
1.3.2. Hitelesítő Központ ("CA") 16
1.3.3. Regisztrációs Iroda ("RA") 17
1.3.4. Ügyfélkapcsolati Irodák ("ÜKI") 17
1.3.5. Felhasználók 18
1.3.5.1. Előfizető 18
1.3.5.2. Érintett fél 19
1.3.6. Alkalmazhatóság 19
1.3.6.1. Szabályzat hatálya 19
1.3.6.2. Szolgáltatás szintje 19
1.3.6.3. Tanúsítványok alkalmazhatósága 20

1.4. Tanúsítványok típus, tanúsítvány osztály és tanúsítvány fajta 21
1.4.1. Tanúsítványok osztályai, fajtái és tulajdonságaik 23
1.4.1.1. Nem minősített Tanúsítvány 23
1.4.1.2. Teszt Tanúsítvány 24
1.4.1.3. Előfizetői Tanúsítvány 24
1.4.1.4. Szolgáltatói Tanúsítvány 26
1.4.2. Tanúsítvány fajták és tulajdonságaik 26
1.4.2.1. „Személyes” típusú tanúsítvány 26
1.4.2.2. „Szervezeti személy” típusú tanúsítvány 27
1.4.2.3. Eszköz tanúsítvány 28

1.5. Szolgáltató adatai 28
1.5.1. Cím, cégjegyzékszám, kontakt információk 28
1.5.2. Hitelesítési Politika és Szabályozási Csoport adatai 30

2. Általános rendelkezések 31

2.1. Feladatok és hatáskörök 31
2.1.1. A MÁV INFORMATIKA Kft. feladatai és hatásköre 31
2.1.2. A Hitelesítő Központok („CA”-k) feladatai és hatásköre 36
2.1.3. A Hitelesítési Politika és Szabályozási Csoport feladatai és hatásköre 38
2.1.4. A Regisztrációs Iroda ("RA") feladatai és hatásköre 39
2.1.5. Az Ügyfélkapcsolati Iroda feladatai és hatásköre 42
2.1.6. A Címtárral (Tanúsítványtárral) kapcsolatos feladatok és kötelezettségek 44
2.1.7. Az Igénylő, az Előfizető és Aláíró feladatai és hatásköre 45
2.1.8. Érintett fél feladatai és hatásköre 48

2.2. A hitelesítés szolgáltató és felhasználó közösség tagjainak felelőssége 49
2.2.1. A MÁV INFORMATIKA Kft. felelőssége 49
2.2.2. A Hitelesítő Központok felelőssége 50
2.2.3. Hitelesítési Politika és Szabályozási Csoport felelőssége 51
2.2.4. A Regisztrációs Iroda felelőssége 51
2.2.5. Az Ügyfélkapcsolati Iroda felelőssége 51
2.2.6. Előfizető és az Aláíró felelőssége 51
2.2.7. Érintett fél felelőssége 52
2.3. A pénzügyi felelősség korlátjai 53
2.3.1. Kártérítés 53
2.3.2. Megbízotti kapcsolatok 54
2.3.3. Adminisztratív eljárások 54
2.4. Értelmezés és alkalmazás 55
2.4.1. Alkalmazott jogszabályok 55
2.4.2. Érvénytelenség, hatályosság, megszűnés, értesítések 56
2.4.2.1. Érvénytelenség 56
2.4.2.2. Hatályosság 56
2.4.2.3. Megszűnés 57
2.4.2.4. Értesítések 57
2.4.3. Vitás kérdések kezelése 57
2.5. Díjak 58
2.5.1. Tanúsítvány kibocsátás és megújítás 58
2.5.2. Tanúsítvány hozzáférés 59
2.5.3. Visszavonás és állapot információ hozzáférés 59
2.5.4. Egyéb szolgáltatásokra vonatkozó díjak 59
2.5.5. Visszatérítési elvek 59
2.6. Közzététel 60
2.6.1. Szolgáltatói információk közzététele 60
2.6.2. A közzététel gyakorisága 63
2.6.3. Elérési szabályok 64
2.6.4. Címtár 64
2.7. A megfelelőség vizsgálata 65
2.7.1. Vizsgálatok gyakorisága 66
2.7.2. Az átvizsgáló szervezet megnevezése/jellemzői 66
2.7.3. Az átvizsgáló szervezet és a vizsgált fél kapcsolata 66
2.7.4. A vizsgálatok kiterjedése 66
2.7.5. Hiányosságok kezelése 67
2.7.6. Eredmény kommunikációja 68
2.8. Bizalmasság – Adatkezelési szabályzat 68
2.8.1. Bizalmas információk 68
2.8.2. Nem bizalmas információk 70
2.8.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése 71
2.8.4. Feltárás törvényi meghatalmazással rendelkezők részére 71
2.8.5. Feltárás törvényi meghatalmazással rendelkezők részére 71
2.8.6. Feltárás tulajdonos kérésére 72

2.8.7. Feltárás más esetekben 72
2.9. Szellemi tulajdonhoz fűződő jogok 72
3. Azonosítás és hitelesítés 73
3.1. Kezdeti regisztráció 73
3.1.1. Nevek típusa 73
3.1.2. Név jelentése, szemantikája 73
3.1.3. Különböző névmegadási formák értelmezési szabályai 74
3.1.4. Nevek egyedisége 74
3.1.5. Név igénylési viták feloldása 74
3.1.6. Védjegyek elismerésének és hitelesítésének módszere 75
3.1.7. Az Aláírás létrehozó adat birtoklás ellenőrzésének módszere 75
3.1.8. Személyes azonosság hitelesítése „Személyes" tanúsítvány igénylése esetén 76
3.1.9. Szervezeti identitás hitelesítése „Szervezeti személy" tanúsítvány igénylése esetén 76
3.1.10. Eszköz identitás hitelesítése 79
3.2. Érvényes tanúsítvány megújítása (tanúsítvány frissítése) 80
3.3. Érvénytelen tanúsítvány megújítása 81
3.4. Felfüggesztés és visszavonási kérés 81
4. A működésre vonatkozó követelmények 83
4.1. Tanúsítványigénylés 83
4.2. Tanúsítvány kibocsátás 86
4.3. Tanúsítvány elfogadás 87
4.4. Tanúsítvány visszavonás és felfüggesztés 89
4.4.1. Visszavonáshoz vezető körülmények 90
4.4.2. Visszavonás kérelmezése 91
4.4.3. Visszavonási eljárás 92
4.4.4. Visszavonási kérelemre vonatkozó türelmi idő 93
4.4.5. Felfüggesztéshez vezető körülmények 93
4.4.6. Felfüggesztés kérelmezése 94
4.4.7. Felfüggesztési eljárás 95
4.4.8. Felfüggesztett állapotra vonatkozó korlátozások 95
4.4.9. CRL kibocsátás gyakorisága 96
4.4.10. CRL ellenőrzési követelmények 96
4.4.11. On-line visszavonási státusz-szolgáltatás 97
4.4.12. On-line visszavonás ellenőrzési követelmények 97
4.4.13. Visszavonási állapot közlés más formái 97
4.4.14. Visszavonási állapot közlés más formáinak ellenőrzési követelményei 97
4.4.15. Magánkulcs kompromittálódás speciális követelményei 97
4.5. Biztonsági audit eljárások 98
4.5.1. Naplózott esemény típusok 98
4.5.2. Napló adatok feldolgozásának gyakorisága 99
4.5.3. Napló adatok tárolási ideje 99
4.5.4. Napló adatok védelme 99

4.5.5. Napló adatok mentési eljárásai 100
4.5.6. Napló adatok gyűjtési rendszere 100
4.5.7. Rendkívüli eseményekről történő értesítés 100
4.5.8. Sebezhetőség kiértékelése 101
4.6. Adatarchiválás 101
4.6.1. A tárolt események típusai 101
4.6.2. Az archívum megőrzési időtartama 102
4.6.3. Az archívum védelme 102
4.6.4. Az archívum mentési folyamatai 103
4.6.5. A rekordok időbélyegzésére vonatkozó követelmények 103
4.6.6. Az archívum gyűjtési rendszere 103
4.6.7. Archív információ hozzáférését és ellenőrzését végző eljárások 103
4.7. Kulcs csere 103
4.8. Katasztrófa elhárítás, Aláírás létrehozó adat kompromittálódás 104
4.8.1. Hardver, szoftver, vagy adatsérülés esete 104
4.8.2. Egy szolgáltatói egység nyilvános kulcsának visszavonása 105
4.8.3. Egy szolgáltatói egység kulcsának kompromittálódása 105
4.8.4. Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően 106
4.8.5. Üzletmenet-folytonossági Terv 106
4.9. A hitelesítés-szolgáltatási tevékenység megszüntetése 106
5. Fizikai, eljárásrendi, és humán biztonsági szabályozások 108
5.1. Fizikai biztonsági szabályozások 110
5.1.1. Hitelesítő Központok 110
5.1.2. Regisztrációs Iroda 111
5.2. Eljárásrendi szabályozások 111
5.3. Humán szabályozások 113
5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények 114
5.3.2. Biztonsági háttér ellenőrzésekre vonatkozó eljárások 114
5.3.3. A felhatalmazás nélküli tevékenységek büntető következményei 116
5.3.4. A szerződéses alkalmazottakra vonatkozó követelmények 116
5.3.5. A személyzet számára biztosított dokumentációk 117
6. Műszaki biztonsági óvintézkedések 118
6.1. Kulcs-pár előállítás és telepítés 118
6.1.1. Kulcs-pár előállítás 118
6.1.2. Az Aláírás létrehozó adat felhasználóhoz történő eljuttatása 120
6.1.3. Aláírás ellenőrző adat eljuttatása a tanúsítvány kibocsátóhoz 121
6.1.4. Hitelesítő Szervezet Aláírás ellenőrző adatának eljuttatása a felhasználókhoz 121
6.1.5. Kulcs méretek 122
6.1.6. Előfizetői Aláírás ellenőrző adat előállításához használt paraméterek előállítása 122
6.1.7. Előfizetői Aláírás ellenőrző adat előállításához használt paraméterek előállítása 123
6.1.8. Szoftveres / hardveres kulcsgenerálás 123

6.1.9. Kulcs felhasználási célok 123
6.2. Aláírás létrehozó adat védelme 124
6.2.1. Kriptográfiai modulra vonatkozó szabványok 124
6.2.2. A több- szereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése 124
6.2.3. Aláírás létrehozó adat letét 124
6.2.4. Aláírás létrehozó adat mentése 124
6.2.5. Aláírás létrehozó adat archiválása 124
6.2.6. Aláírás létrehozó adat kriptográfiai modulba helyezése 124
6.2.7. Aláírás létrehozó adat aktiválása 125
6.2.8. Aláírás létrehozó adat deaktiválása 125
6.2.9. Aláírás létrehozó adat megsemmisítése 125
6.3. Kulcs-pár kezelés egyéb aspektusai 125
6.3.1. Aláírás ellenőrző adat archiválása 125
6.3.2. Aláírás létrehozó és ellenőrző adatok felhasználási ideje 125
6.4. Aktiválási adatok 126
6.4.1. Aktiválási adatok generálása és installációja 126
6.4.2. Aktiválási adatok védelme 126
6.4.3. Aktiválási adatok egyéb aspektusai 127
6.5. Számítógép biztonsági szabályok 127
6.5.1. Számítógép biztonság technikai követelményei 127
6.5.2. Számítógép biztonsági értékelések 129
6.6. Életciklus technikai szabályok 130
6.6.1. Rendszerfejlesztési szabályok 130
6.6.2. Biztonságkezelési szabályok 130
6.6.3. Életciklus biztonsági értékelések 130
6.7. Hálózati biztonsági szabályok 131
6.8. Kriptográfiai modul ellenőrzése 131
7. Tanúsítvány és kulcs-visszavonási profil 132
7.1. Tanúsítvány profil 132
7.1.1. Alap mezők 132
7.1.2. Tanúsítvány kiterjesztések 133
7.2. Kulcs-visszavonási profil 134
7.2.1. Verzió szám(ok) 135
7.2.2. „Tanúsítvány visszavonási lista” és „Tanúsítvány visszavonási lista bejegyzési” kiterjesztések 135
8. HSzSz adminisztráció 136
8.1. A HSzSz változáskezelés 136
8.1.1. HSzSz változtatási eljárások 136
8.1.2. Értesítés nélkül változtatható elemek 136
8.1.3. Értesítéssel változtatható elemek 136
8.1.4. Észrevételek kezelése 136
8.1.5. Szabályzati objektumazonosítót vagy mutatót változtató módosítások 137

8.2. Közzétételi és tájékoztatási elvek 137
8.2.1. A HSzSz-ben nem tárgyalt elemek 137
8.2.2. A HSzSz közzététele 137
8.3. HSzSz elfogadási eljárások 137
9. Hivatkozások és Meghatározások 139
9.1. Hivatkozások 139
9.2. Meghatározások 140

1. Bevezetés

E dokumentum a MÁV INFORMATIKA Kft. (továbbiakban Szolgáltató) fokozott biztonságú elektronikus aláírás hitelesítés szolgáltatására vonatkozó eljárásrendet és az egyéb működési szabályokat tartalmazza.

A Szolgáltató a fokozott biztonságú elektronikus aláírás hitelesítés szolgáltatást a vele előfizetői szerződéses viszonyban álló igénybevevők részére szolgáltatja.

Az elektronikus aláírás hitelesítés szolgáltatások keretében a Szolgáltató a vele szerződéses kapcsolatban álló Aláírók részére a 2001. évi XXXV. törvényben meghatározott szolgáltatások közül a következőket nyújtja:

- elektronikus aláírás hitelesítés szolgáltatás (továbbiakban: hitelesítés szolgáltatás),
- aláírás-létrehozó eszközön az Aláírás létrehozó adat elhelyezése.

A HSzSz további fejezeteiben a „*szolgáltatások*” kifejezés alatt a fenti részszolgáltatások bármelyike értendő.

A szolgáltatások részletezése az 1.3.6.2 pontban olvasható.

Ezen szolgáltatásokat a Szolgáltató fokozott biztonságú szinten szolgáltatja.

A Hitelesítés Szolgáltatási Szabályzat (továbbiakban: HSzSz) jelen aktuális verziója a PKI alkalmazás mindenkori technikai azonosítójával van összerendelve, azaz a HSzSz-ben foglaltak a technikai azonosítóval azonosított PKI alkalmazásra vonatkoznak.
Az aktuális PKI alkalmazás technikai azonosító*:* **trust-sign ACA v1.0**

A szolgáltatások védett márkaneve: **Trust&Sign**

1.1. Alapok

1.1.1. Szabályzat célja

Jelen HSzSz célja, hogy összefogja azokat az előírásokat, adatokat és információkat, melyeket a Szolgáltató elektronikus aláírás szolgáltatásával valamilyen módon kapcsolatba kerülő feleknek tudni kell vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát, s lehetővé teszi a felhasználók számára, hogy megállapítsák azt, hogy az ismertetett szolgáltatási gyakorlat,

valamint a kibocsátott tanúsítványok mennyiben felelnek meg az elvárásaiknak. A HSzSz és egyéb, a HSzSz-ben hivatkozott dokumentumok, ajánlások, szabványok tartalmának megismerése után, a tanúsítvány elfogadóinak egyértelműen meg kell tudni állapítani a tanúsítvány kezelésének módját, az általa garantált hitelesség és biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügy garanciákat, jogi felelősség vállalásokat.

A tanúsítványok végfelhasználóinak tevékenységére vonatkozóan jelen HSzSz-től és Szolgáltatótól független egyéb szabályzatok is élhetnek előírásokkal. Amennyiben e szabályzatok bármely vonatkozásban ellentmondást vagy eltérő kikötést tartalmaznának, jelen HSzSz előírásai tekinthetők magasabb szintűnek, s ezek alkalmazandók.

1.1.2. Szabályzat tartalma

A HSzSz 1. fejezet (Bevezetés):

- ismerteti a Szolgáltatóval kapcsolatos adminisztratív adatokat,
- eligazítást ad a dokumentum szerepét és a szolgáltatás mibenlétét illetően,
- megnevezi azon szabványokat, ajánlásokat és előírásokat, melyeket a szabályzat formai megjelenésében és tartalmilag követ,
- felsorolja a szabályzat alapján kibocsátható tanúsítvány osztályokat és típusokat,
- ismerteti a szabályzat egyéb dokumentumokhoz való viszonyát, tájékoztatást ad a Szolgáltató által nyújtott szolgáltatásokról, és ezek alkalmazói közösségéről.

A 2. fejezet (Általános rendelkezések) tájékoztat:

- a Szolgáltató és annak egységeinek, valamint a szolgáltatásokkal kapcsolatba kerülő szereplőknek a kötelezettségeiről, jogairól, felelősségéről és ennek korlátozásáról,
- felsorolja a Szolgáltató által publikált információkat, dokumentumokat és adatokat a publikálás helyével, gyakoriságával és elérhetőségével, s az esetleges korlátozásokkal, valamint az információk használatára vonatkozó követelményekkel,
- összefoglaló jellegű felvilágosítást ad a Szolgáltató által kezelt adatokról, az adatkezelés céljáról, a közzétett adatokról és azok jogalapjáról, az egyes adatok törlési határidejéről,
- ismerteti a Szolgáltató önkéntes tanúsításával kapcsolatos információkat.

A 3. fejezet (Azonosítás és hitelesítés) leírja

- a tanúsítványok igényléséhez kapcsolódó előfizetői regisztráció menetét ismerteti, a regisztrációval kapcsolatos tájékoztatással, a regisztrációs adatok összegyűjtésével, és egyéb részletekkel,
- a kezdeti regisztráció kapcsán felsorolja
  - az elnevezés során követett szabványokat és szabályokat,

- a különböző név formátumok értelmezését,
- a nevek egyediségének biztosítását,

♦ ismerteti a név igénylési viták feloldását,

♦ leírja a tanúsítvány megújításának kérelmezését, hitelesítését, és elbírálását, valamint a megújítás menetét;

♦ kifejti a tanúsítvány visszavonásának kérelmezését, hitelesítését, elbírálását, és végrehajtását.

A 4. fejezet (A működésre vonatkozó követelmények) leírja

♦ a Szolgáltató által követett gyakorlatot és a támasztott követelményeket a tanúsítványok igénylése, kibocsátása, elfogadása, felfüggesztése és visszavonása, és kezelése kapcsán,

♦ tájékoztat a szolgáltatás megszűnésének körülményeiről, a felek ez esetre vonatkozó jogairól és kötelességeiről, a tanúsítványok kezeléséről, az előfizetők értesítéséről, és az archív adatok kezelésére vonatkozó eljárásokról; valamint ismerteti Szolgáltató naplózási, archiválási és katasztrófa elhárítási eljárásait.

Az 5. fejezet (Fizikai, eljárásrendi, és humán biztonsági szabályozások) leírja azokat a szabályokat, melyek a szolgáltatás környezetének, a bizalmi tevékenységek végzésének és a megfelelő munkatársak rendelkezésre állásának biztonsági előírásait határozzák meg.

A 6. fejezet (Fizikai, eljárásrendi, és humán biztonsági szabályozások) ismerteti:

♦ a kulcs-párok generálásának, a magánkulcs címzetthez juttatásának, a 1.3.2 pontban definiált Hitelesítő Szervezet (amely lehet a Szolgáltató maga vagy egy fölé rendelt Hitelesítő Szervezet) nyilvános kulcsának a felhasználókhoz való eljuttatásának szabályait, s a kulcsokkal kapcsolatos technikai követelményeket,

♦ megadja a Szolgáltató és az előfizetők magánkulcsának védelmére vonatkozó előírásokat, a magánkulcs kriptográfiai modulba helyezésének módját, aktiválását, deaktiválását és megsemmisítését,

♦ tájékoztatást ad a kulcs-párok kezelésének egyéb aspektusairól, mint például a nyilvános kulcs archiválására vonatkozó előírásokról, vagy a nyilvános és magánkulcs felhasználási idejéről,

♦ leírja a magánkulcsok védelmére szolgáló aktiválási adatok generálását, installációját, s védelmét; valamint számítógépes és hálózati biztonsági, életciklus technikai eljárásokat ismertet.

A 7. (Tanúsítvány és kulcs-visszavonási profil) fejezet ismerteti

- a kiadott tanúsítványok alap és opcionális mezőit,
- a tanúsítvány felépítését,
- az egyes mezők tartalmát,
- a tanúsítványban alkalmazott névformátumokat,
- az ezekre vonatkozó kötöttségeket.

A 8. (HSzSz adminisztráció) fejezet ismerteti a szolgáltatást meghatározó kapcsolódó dokumentumok változatásának, elfogadtatásának és publikálásának szabályait.

A 9. (Hivatkozások és Meghatározások) fejezet a jelen szabályzatban hivatkozott jogszabályok, belső szabályzatok, szabványok és ajánlások, valamint a használt kifejezések értelmezését, magyarázatát tartalmazza.

1.1.3. Jogszabályok, szabványok

A jelen HSzSz a következő jogszabályokat, szabványokat, és ajánlásokat vesz figyelembe:

- a HSzSz teljes tartalmára vonatkozóan:
  - 2001. évi XXXV. törvény az elektronikus aláírásról,
  - 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,
  - ISO/IEC 15408 1999: Információ technológia - Biztonsági módszerek - Informatikai biztonság értékelési kritériumai (1-3 részek)
- A HSzSz szerkezetére és tartalmára vonatkozóan:
  - RFC 2527 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer)
  - Európai Unió ETSI TS 101 456 szabvány,
  - American Bar Association (ABA),
  - PKI Assessment Guidelines (PAG),
- Tanúsítványok, visszavonási listák szerkezete, tartalma:
  - ITU-T X.509 “Information technology - Open Systems Interconnection - The Directory: Public -key and attribute certificate frameworks” ajánlás 3. verziója,
  - RFC 2459 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány és tanúsítvány visszavonási lista profil)

- Fokozott biztonságú szolgáltatók:
  - 2001. évi XXXV. törvény az elektronikus aláírásról, 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,
  - 151/2001. (IX. 1.) Korm. rendelet a Hírközlési Felügyeletnek az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól,
  - 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről
  - ETSI TS 101 456 (Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények).
- Minősített tanúsítványok:
  - RFC 3039 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil),
  - ETSI TS 101 862 (Minősített tanúsítvány profil).
- Informatikai biztonsági követelmények:
  - MeH 12. ajánlás, ITSEC[1], CC[2]
- Aláírás létrehozó eszköz:
  - NIST FIPS PUB 140-1 (1994. január 11.) (Kriptográfiai modulok biztonsági követelményei),
  - CEN 14167-2 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató aláíró műveleteit megvalósító kriptográfiai modulra” (MCSO-PP, HSM-PP),
  - CEN 14167-3 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató kulcs előállítási szolgáltatásait megvalósító kriptográfiai modulra” (CMCKG-PP, HSM-PP)
- CWA 14167-1, és a CWA 14172-1,-2,-3,-4 CEN Workshop Agreement-ek

[1] ITSEC = Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritériumok) az Európai Közösség ajánlása az IT termékek és rendszerek biztonságának funkcionális és minősítési követelményeire.

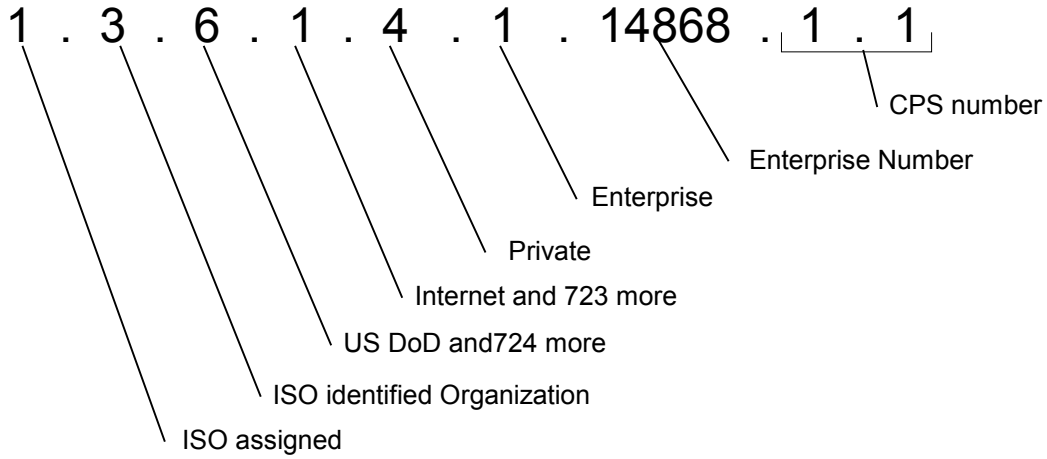
[2] CC = Common Criteria (Közös /Informatikai Biztonsági/ Követelmények) az Európai Közösség, az Egyesült Államok és Kanada közös ajánlása az IT termékek biztonsági minősítésének követelményeire.

1.2. HSzSz Azonosítás

Az elektronikus aláírásról szóló évi XXXV. törvény 7. § 1. bek. értelmében a Szolgáltató tevékenységének megkezdése előtt 30 nappal bejelentette szolgáltatási szándékát a Nemzeti Hírközlési Hatóságnak a törvény által előírt dokumentumok kíséretében. A Hatóság a fokozott biztonságú elektronikus aláírás hitelesítés szolgáltatási tevékenység folytatására az engedélyt megadta, és a Szolgáltatót nyilvántartja (nyilvántartási adatokat ld. 1.5 pont).

A Szolgáltató és az ISO/IEC és az ITU szabványok által előírt regisztrációs eljárásnak megfelelően eljárva regisztrálja a jelen HSzSz-t.

OID szám:



1. ábra

A szabályzat a következő tanúsítványok kezelését írja le.

Nyilvános körben kibocsátott nem minősített tanúsítvány

OID: 1.3.6.1.4.1.14868.1.1.0

Nemzeti Hírközlési Hatóság regisztrációs szám: MH-13181-1/2002

Jelen dokumentum teljes neve: Trust&Sign **Hitelesítési Szolgáltatási Szabályzat Fokozott Biztonságú Elektronikus Aláíráshitelesítés Szolgáltatáshoz**. A jelen dokumentumban HSzSz-ként történik rá hivatkozás.

A HSzSz Interneten a következő címen érhető el: *http://www.mavinformatika.hu/ca/***.**

Jelen HSzSz-nek csak a Szolgáltató aláírásával ellátott változata tekinthető hitelesnek.

1.3. Hitelesítés szolgáltató és felhasználó közösség, alkalmazhatóság

A Szolgáltató által kibocsátott tanúsítványokat felhasználó közösség a következő:

- a Szolgáltatóval kapcsolatban álló hitelesítő és regisztráló szervezetek,
- a Szolgáltató elektronikus aláírásra feljogosított munkatársai,
- a szerződéses előfizetők aláírói,
- a szerződéses előfizetők informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.),
- az érintett felek.

1.3.1. Hitelesítési Politika és Szabályozási Csoport

A Hitelesítési Politika és Szabályozási Csoport a Szolgáltató által létrehozott szervezeti egység, amely a szolgáltatással kapcsolatos politikák és szabályzatok kialakításáért, elfogadásáért, karbantartásáért és adminisztrációjáért felelős. A Regisztrációs Iroda (ld. 1.3.3 pont) és az Ügyfélkapcsolati Irodák (ld. 1.3.4 pont) által létrehozott szabályokat a Hitelesítési Politika és Szabályozási Csoport ellenőrzi a Szolgáltató szabályzatainak, szerződésének és üzletpolitikájának való megfelelőség szempontjából.

A Hitelesítés Politika és Szabályozási Csoport a MÁV INFORMATIKA Kft. Biztonsági Osztálya alá van rendelve.

1.3.2. Hitelesítő Központ ("CA")

A hitelesítési politikában meghatározott hitelesítő szervezetet a Szolgáltató Hitelesítő Központja (rövidítve: CA) testesíti meg.

A Hitelesítő Központ a Szolgáltató központi eleme, amely a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, azt ezt körül vevő biztonságos fizikai környezetből (Bizalmi Központból, ld. 5.1.1 pont), valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladata a különböző osztályú és típusú aláírás létrehozó adatok és tanúsítványok előállítása, ezek nyilvános publikálása, az Ügyfélkapcsolati Irodáktól (ld. 1.3.4 pont) érkező módosítási,

felfüggesztési, újra aktivizálási, visszavonási és megszüntetési igények jelen HSzSz szerinti végrehajtása és a szolgáltatást támogató informatikai rendszer működtetése és menedzselése.

A Szolgáltató a fizikailag létező Hitelesítő Központjában működtet és menedzsel egy „Root CA”-t, amely a „Produktív CA”-k számára biztonságosan előállítja a „Produktív CA”-k szolgáltatói tanúsítványait, tanúsítvány-aláíró, infrastrukturális és rendszervezérlési kulcspárjait.

A Produktív CA-k fő feladata a Regisztrációs Iroda igényei alapján az előfizetők számára az előfizetői kulcspárok generálása, a kapcsolódó előfizetői tanúsítványok előállítása és ezek eljuttatása a Regisztrációs Irodához.

A „Root CA” és a „Produktív CA” feladatait részletesen a 2.1.2 pont ismerteti.

A Szolgáltatónál a Hitelesítő Központhoz kapcsolódó feladat-, felelősség- és hatásköröket a MÁV INFORMATIKA Kft. PKI Üzleti Egység gyakorolja.

1.3.3. Regisztrációs Iroda ("RA")

A hitelesítési politikákban meghatározott regisztráló szervezet a Szolgáltatónál a következő szervezeti egységekből áll:

- Regisztrációs Iroda (rövidítve: RA),
- Ügyfélkapcsolati Irodák, amelyek közül egy a Szolgáltató központi épületében működik.

A Regisztrációs Iroda a szolgáltatás keretein belül biztosítja az előfizetők technikai regisztrációját, a tanúsítványok felfüggesztés és visszavonás kezelését és az Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezését. Egyúttal közreműködik további elektronikus aláírással kapcsolatos szolgáltatások biztosításában: tanúsítvány előállítás, tanúsítvány kibocsátás és visszavonási állapot közzététele.
A Regisztrációs Irodához kapcsolódó feladat-, felelősség- és hatásköröket a PKI Üzleti Egység gyakorolja.

1.3.4. Ügyfélkapcsolati Irodák ("ÜKI")

Az Ügyfélkapcsolati Irodák a Szolgáltató és a vele szerződéses alapon együtt működő Társaságok (mint szerződött közreműködők) azon szervezeti egységei, amelyek az előfizetők adatainak felvételét, ellenőrzését, az igénylő személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a kérelmeknek a Regisztrációs Irodához

történő továbbítását, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el.

Egy Ügyfélkapcsolati Irodához tartozó előfizetők önálló közösséget alkothatnak, melyre a Szolgáltató, vagy a vele szerződéses alapon együtt működő Társaságok (mint szerződött közreműködők) további szabályokat is alkalmazhatnak.

Az Ügyfélkapcsolati Irodák által létrehozott szabályok nem tartalmazhatnak olyan kikötést, amely ellentétben áll a Hitelesítési Politika és Szabályozási Csoport által jóváhagyott Szabályzatokkal.

Az Ügyfélkapcsolati Irodák elérhetősége a *http://www.mavinformatika.hu/ca/* weboldalon található.

Az Ügyfélkapcsolati Irodákhoz kapcsolódó feladat-, felelősség- és hatásköröket a PKI Üzleti Egység gyakorolja.

1.3.5. Felhasználók

1.3.5.1. Előfizető

Előfizető a Szolgáltatóval, az Általános Szolgáltatási Feltételekben foglaltak szerint szerződéses viszonyban álló felhasználó, aki számára a Szolgáltató tanúsítványt bocsát ki. Előfizető lehet természetes vagy jogi személy.

Az Előfizető egyben Aláíró is, amennyiben saját maga képviseletében az aláírási jogosultsággal is rendelkezik, azaz birtokolja és használja az Aláírás létrehozó adatot.

Az Előfizető lehet jogi személy (szervezet) is. Ebben az esetben a szervezet képviselőként egy természetes személyt bíz meg, akit felruház aláírási jogosultsággal. Ez a személy a jogi személyt képviselve ír alá.

Aláíró lehet:

a) bármely természetes személy, aki személyazonosságát a regisztráció során az általa igényelt tanúsítvány osztálynak megfelelően, a HSzSz 3.1.8 pontjában előírtak szerint igazolta.

b) bármely természetes személy, aki részére a Tanúsítvány azzal a céllal kerül kibocsátásra, hogy az Aláírót más természetes vagy jogi személy (szervezet) képviseletében történő aláírásra jogosítsa fel. Ebben az esetben az Aláíró személyazonosságának ellenőrzése mellett a

regisztráció során a 3.1.8 pontban meghatározott módon a képviseleti jogosultságot is ellenőrizni kell.

1.3.5.2. Érintett fél

Az Érintett fél (Aláírás Ellenőrző) olyan természetes vagy jogi személy, aki vagy amely az elektronikus dokumentum fogadója, és egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el.

1.3.6. Alkalmazhatóság

1.3.6.1. Szabályzat hatálya

A HSzSz időbeli hatálya

A HSzSz időbeli hatálya a változáskezelési táblázatban feltüntetett jelen szabályzati verzióra érvényes hatálybalépés dátumától kezdődően határozatlan időre szól. Időbeli hatálya megszűnik a szolgáltatási tevékenység beszüntetésekor, illetve egy újabb szabályzat verzió hatályba lépésekor.

A HSzSz személyi hatálya

Az 1.3 pontban meghatározott hitelesítés szolgáltató és felhasználói közösségre terjed ki.

A HSzSz tárgyi hatálya

A következőkre terjed ki:

- az 1. pontban meghatározott szolgáltatásokra,
- a Szolgáltatónak a hitelesítés szolgáltatással valamilyen kapcsolatban álló összes objektumára, tárgyi eszközére.

1.3.6.2. Szolgáltatás szintje

A Szolgáltató jelen HSzSz-t és a bejegyzéshez szükséges egyéb adatait átadta a Nemzeti Hírközlési Hatóság részére a fokozott biztonságú hitelesítés szolgáltatóként történő nyilvántartásba vétel céljából.

A Szolgáltató a 2001. évi XXXV. sz. elektronikus aláírásról szóló törvény szerinti fokozott biztonságú szolgáltatást nyújt a következő szolgáltatási termékek vonatkozásában:

- Tanúsítvány kialakítási szolgáltatás; ebben regisztráló szolgáltatás és egyedi-név szolgáltatás, valamint megszemélyesítési szolgáltatás;
- Tanúsítvány előállítás és tanúsítvány szétosztási szolgáltatás;
- Felfüggesztési és visszavonás kezelési szolgáltatás;
- Tanúsítvány archiválási és állapotinformációs szolgáltatás, valamint adattárolási szolgáltatás;
- Tanúsítvány megújítási szolgáltatás;
- Aláírás-létrehozó eszköz fizikai megszemélyesítése (szolgáltató arculati elemeinek elhelyezése az eszközön);
- Aláírás-létrehozó eszköz logikai megszemélyesítése (tanúsítványok és magánkulcs[3] elhelyezése eszközön);

A Szolgáltatás megfelelőségét külső auditor tanúsítja.

1.3.6.3. Tanúsítványok alkalmazhatósága

A tanúsítványok alkalmazhatóságára a következő alapszabályok érvényesek:

1. Engedélyezett alkalmazási lehetőségek

   A kibocsátott magánkulcsok elektronikus dokumentumon elektronikus aláírások megtételére. A nyilvános kulcsok (amelybe egyéb célú nyilvános kulcsok nem értendők bele) a tanúsítványok aláírásának ellenőrzésére használhatók fel, a Tanúsítványba foglaltaknak megfelelően.

2. Korlátozott alkalmazási lehetőségek

   Szolgáltató területi, pénzügyi, stb. korlátozásokat szabhat saját belső hitelesítési politikája (HP) szerint, amelyeket a kibocsátott előfizetői Tanúsítványban megad.

   Egyébként a Szolgáltató nem korlátozza a kibocsátott tanúsítványok felhasználhatóságát. Az Előfizető szervezet élhet korlátozásokkal Aláíró és érintett felek tanúsítvány felhasználási tevékenységével kapcsolatosan.

3. Tiltott alkalmazási lehetőségek

[3] A jogszabályok ezt a szolgáltatást „aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése” néven nevezik.

Az előfizetői tanúsítványok más nyilvános kulcsú tanúsítványok aláírására történő felhasználása, vagy bármilyen hitelesítés szolgáltatás nyújtásához történő alkalmazása tilos.

A fentiek alapján a kibocsátott tanúsítványok (illetve az ezekhez kapcsolódó kulcspárok) felhasználhatók minden olyan számítástechnikai alkalmazásban, amely támogatja a PKI technológián alapuló elektronikus aláírási, azonosítás-hitelesítési, le nem tagadhatósági funkciókat. Amennyiben a Szolgáltató elektronikus aláírás-hitelesítés céljából bocsát ki tanúsítványt, a tanúsítványhoz kapcsolódó magán-, illetve publikus kulcsot kizárólag aláírás létrehozására, illetve ellenőrzésére lehet felhasználni a 2001. évi XXXV. sz. elektronikus aláírásról szóló törvény értelmében.

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény értelmében az elektronikus aláírásra kibocsátott Tanúsítvány, illetve az Aláírás-létrehozó adat kizárólag aláírás létrehozására használható, ezért a Szolgáltató nem vállal felelősséget az elektronikus aláírásra kibocsátott Tanúsítvány illetve az Aláírás-létrehozó adat titkosításra, vagy más, az elektronikus aláírástól eltérő felhasználásáért.

Jelen HSzSz hatálya alatt kibocsátott tanúsítványok csak az 1.3 fejezetben meghatározott hitelesítés-szolgáltató és felhasználó közösség körében használhatók az Általános Szerződési Feltételek Fokozott Biztonságú Hitelesítés Szolgáltatáshoz c. dokumentumban (továbbiakban: ÁSzF), illetve az Előfizetői Szerződésben meghatározott összeghatárok szerinti korlátokkal.

A Tanúsítvány használati lehetőségére vonatkozó fenti információk a Tanúsítványban is rögzítésre kerülnek. A feltüntetett használati információktól bármely módon eltérő használat az Aláíró egyéni felelőssége és kockázata, ahogy az ilyen módon felhasznált Tanúsítvány elfogadása az érintett fél (Aláírás Ellenőrző) felelőssége és kockázata.

1.4. Tanúsítványok típus, tanúsítvány osztály és tanúsítvány fajta

A jelen HSzSz csak a fokozott biztonságú szolgáltatás körülményei között nyilvános körben kibocsátott tanúsítványokat és az ezzel kapcsolatos szabályokat írja le.

A Tanúsítványok a létrehozott aláírás hitelességi szintje szerint három *bizalmi osztályba* sorolhatók:

- fokozott biztonságú (nem minősített),

- minősített és
- teszt

tanúsítványok osztályába,

A Tanúsítványok felhasználási területe és célja szerint kettő *használati osztály*t:

- előfizetői és
- szolgáltatói

használati osztályokat különböztetünk meg.

A használati osztályon belül megkülönböztethetünk:

- „személyes” tanúsítványokat
- „szevezeti személy” tanúsítványokat és
- „eszköz” tanúsítványokat.

A tanúsítvány osztályok és fajták jellemzőit a 1.4.1 és 1.4.2 pontok írják le.

A jelen HSzSz a nem minősített (fokozott biztonságú) bizalmi osztályon belül a következő tanúsítvány fajtákra vonatkozik:

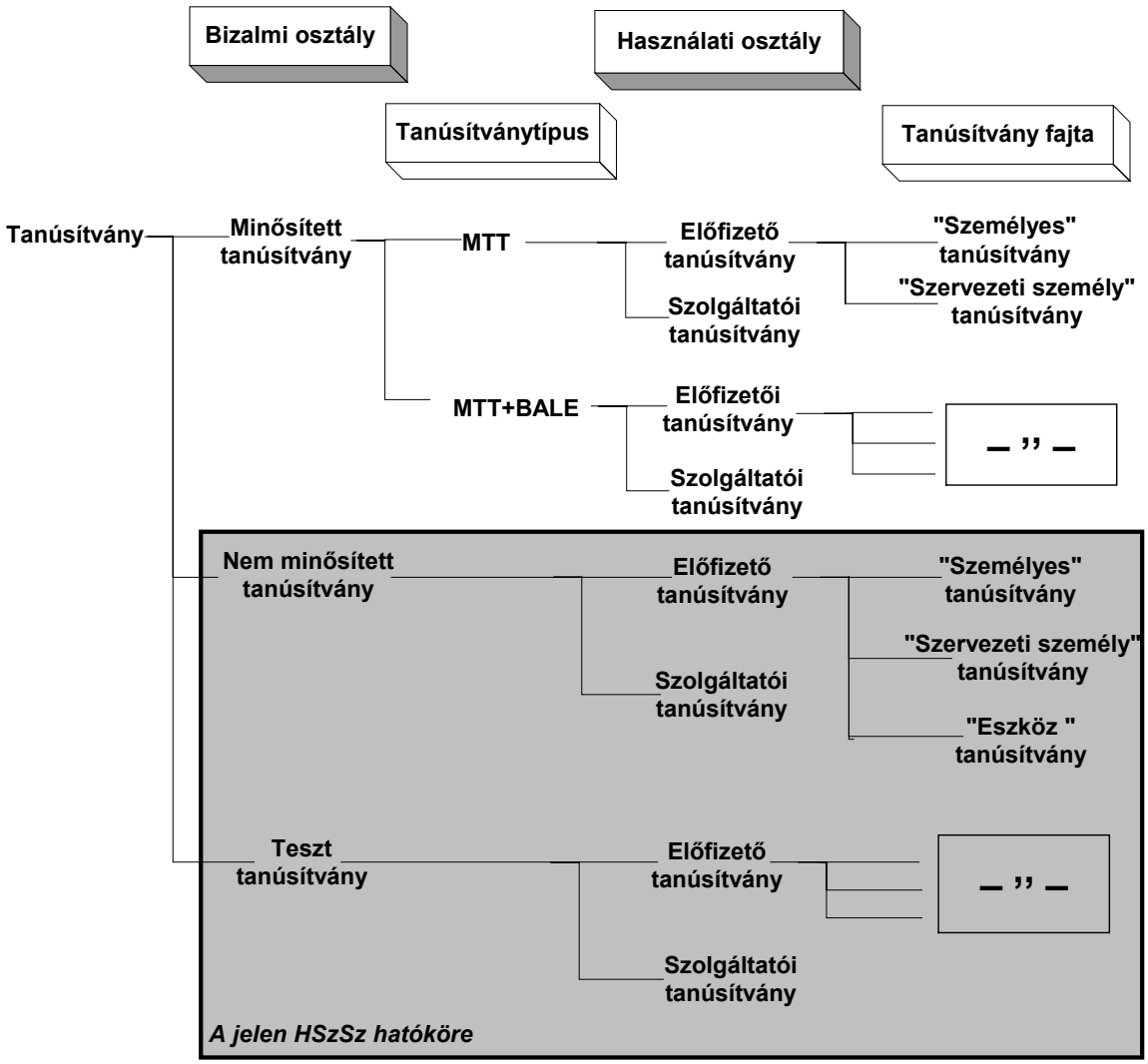
- „személyes” tanúsítvány,
- „szervezeti személy” tanúsítvány
- „eszköz” tanúsítvány.

A Szolgáltató által vállalt felelősségvállalás egy szintű.

A 2. ábra mutatja a tanúsítvány osztályok hierarchiáját. A hitelesség szintje szerinti osztályozásnál a nem minősített tanúsítványokra a hatályos jogszabályok azon előírásai érvényesek, amelyek a fokozott biztonságú szolgáltatásra vonatkoznak. A teszt tanúsítványokra vonatkozóan nincs jogszabályi követelmény és nincs felelősségvállalás.

Kötelezettségvállalással Tanúsítvány értelemszerűen csak az Előfizetőnek adható ki. A kötelezettség vállalás értékhatárát az Előfizetői Szerződés rögzíti és ez az értékhatár a Tanúsítványban (7.1.2pont) is szerepel.
A Szolgáltató felelősségének körülményeit 2.2.1 és a 2.3.1 pontok határozzák meg.

A Szolgáltató a fokozott biztonságú szolgáltatási körében csak nem minősített és teszt osztályba tartozó Tanúsítványokat bocsáthat ki.



2. ábra

A következő pontokban megadjuk az egyes Tanúsítvány osztályok és fajták meghatározását.

1.4.1. Tanúsítványok osztályai, fajtái és tulajdonságaik

1.4.1.1. Nem minősített Tanúsítvány

A CWA 14167-1:2001 szerint nem minősített tanúsítvány:

- az Európai Közösség (EK) 1999/93. direktívájának 5.2 cikkelyével összhangban levő elektronikus aláírást tanúsítja, amely gyakorlatilag olyan tanúsítványt jelent, amelyre nem

vonatkoznak a minősített tanúsítványokra előírt nemzetközi ajánlások, szabványok és a hatályos hazai jogszabályok által előírt követelmények,

- a Szolgáltató megbízható informatikai rendszerén belül használt.

A nem minősített tanúsítvánnyal hitelesített elektronikus aláírás vonatkozásában az EK 1999/93 direktíva 5.2 cikkelye kimondja, hogy a Tagállamoknak biztosítania kell, hogy egy elektronikus aláírás jogi eljárásban nem utasítható vissza, mint törvényesen hatályos és elfogadható bizonyíték csupán azon az alapon, mert az

- elektronikus formában létezik, vagy
- nem minősített tanúsítványra alapozott, vagy
- nem egy akkreditált hitelesítés szolgáltató által kibocsátott minősített tanúsítványra alapozott, vagy
- nem Biztonságos aláíró eszközzel hozták létre.

1.4.1.2. Teszt Tanúsítvány

A legalacsonyabb hitelességi és felelősség vállalási szintű osztályt képviseli. A Szolgáltató teszt tanúsítványokat kizárólag tesztelési célokból ad ki saját célra, illetve azt az Előfizető a **http://trust-sign.mavinformatika.hu** web lapon keresztül igényelheti. A Szolgáltató a kifejezetten teszt célú szolgáló tanúsítványokat a Szolgáltató Hitelesítő Központjában létrehozott logikai hitelesítő alközpont által adja ki. A kulcspár előállítása az Aláírónál történik.

A Szolgáltató a teszt tanúsítványok esetében nem végez személyes Aláíró azonosítás-hitelesítést, ezért az Aláírás létrehozó adat és eszköz, valamint a hozzátartozó tanúsítvány tartalmának az Aláíróhoz kötöttsége nem garantált.

A teszt aláírás létrehozó adatok az Aláírók által semmilyen olyan célra nem használhatók, amelynél az átvitt adatok hitelességének vagy sértetlenségének sérüléséből vagy elvesztéséből, az Aláírás létrehozó adat vagy eszköz illetéktelen kezekbe történő jutásából az Aláírónak bármilyen kára származna. Ilyen károkért a Szolgáltató semmilyen felelősséget nem vállal.

1.4.1.3. Előfizetői Tanúsítvány

Előfizetői Tanúsítvány a Szolgáltatóval az Előfizetői Szerződés által szerződéses viszonyba kerülő Előfizető számára kibocsátott Tanúsítvány, amely lehet nem minősített vagy teszt célú.

Előfizetői Tanúsítvány csak felelősség vállalással bocsátható ki, amelynek értékét az ÁSzF vagy az Előfizetővel történt megállapodás határozza meg.

Előfizetői Tanúsítvány olyan természetes személyeknek vagy szervezeteknek kerül kiadásra, amelynél az Aláírót személyes megjelenésre, saját hitelesítő dokumentumokra és írásos nyilatkozatokra alapozott biztonsági ellenőrzéssel kell a Szolgáltatónak azonosítani és hitelesíteni.

Az azonosítás-hitelesítés módját a 1. táblázat határozza meg.

Azonosítás-hitelesítés alanya	Azonosítás-hitelesítés módja
Természetes személy	Személyi igazolvány vagy útlevél bemutatása személyesen
Szervezeti személy	Az Aláíró személyi igazolványának vagy útlevélének bemutatása személyesen. Képviseleti megbízás cégszerűen aláírva.
Szervezet	Cégbíróságnál nyilvántartott gazdasági társaság esetén: 30 napnál nem régebbi cégkivonat, aláírási címpéldány. Nem cégbíróságnál nyilvántartott szervezetek esetében: a nyilvántartó szervezet igazolása. Állam-, illetve közigazgatási szervezetek esetében: az alapító dokumentum közjegyzővel hitelesített másolata, amelyet a szervezet első számú vezetőjének írásos nyilatkozatával együtt.
Eszköz	Természetes személy esetén az azonosított és hitelesített Előfizető írásos nyilatkozata az eszköz birtoklásáról és az eszköz azonosítójáról. Jogi személy esetén a szervezet és a megbízott képviselő azonosítása és hitelesítése után, a képviselőnek át kell adnia egy cégszerű aláírással ellátott nyilatkozatot az eszköz birtoklásáról és az eszköz azonosítójáról.

1. táblázat

Amennyiben a természetes személy bármely más természetes vagy jogi személyt képvisel, akkor a képviseleti jogot írásos megbízói nyilatkozattal kell igazolni. Amennyiben a természetes személy jogi személyt képvisel, akkor a szervezetnek írásban kell nyilatkoznia arról is, hogy az Aláíró hiteles személyazonosságának megállapítása a szervezeten belül már előzetesen megtörtént.

A Szolgáltató a megbízott képviselő személyt nyilvántartja és bármely, a képviselt személy nevében történő eljárás esetén a képviselő személy azonosítását-hitelesítését az Aláíró, illetve az Előfizető esetében szokásos eljárásnak megfelelően végzi el.

1.4.1.4. Szolgáltatói Tanúsítvány

A szolgáltatói tanúsítványokat Szolgáltató csak saját célra bocsátja ki, a szolgáltatási termékek előállításának biztosítására. Előfizető ezeket nem igényelheti.

A teszt célú szolgáltatói Aláírás létrehozó adat és tanúsítvány csak teszt célra használható fel a Szolgáltató feladat-, felelősség és hatáskörén belül.

1.4.2. Tanúsítvány fajták és tulajdonságaik

A Szolgáltató a következőkben meghatározott nem minősített tanúsítványokat adhatja ki előfizetők részére, illetve saját céljaira.

1.4.2.1. „Személyes" típusú tanúsítvány

Személyes típusú tanúsítványokat természetes személy igényelhet a saját nevében. A személyes típusú tanúsítvány esetében az Előfizető és az Aláíró ugyanaz a személy.

A személyes típusú tanúsítvány igénylésekor az Ügyfélkapcsolati Irodán történő azonosítás-hitelesítésnél a következő adatokat kell kezelni:

- az Aláíró neve, aláírása,
- az Aláíró okmányszáma (személyi igazolvány vagy útlevél szám),
- az Aláíró lakcíme,
- az Aláíró e-mail címe.

A tanúsítvány „Country" és „Locality" mezőjében az Igénylő lakóhelyének országkódja és helységneve, az „E" mezőben az Igénylő e-mail címe, a „Common Name" mezőben az igénylő neve szerepel. A tanúsítvány „Organization" és „Organization Unit" mezői üresen maradnak.

A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

1.4.2.2. „Szervezeti személy” típusú tanúsítvány

„Szervezeti személy” típusú tanúsítványokat természetes személy igényelhet egy adott szervezet alkalmazottjaként és/vagy tisztségviselőjeként. A szervezet - többek között - lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület, alapítvány, stb.

Ebben az esetben az Előfizetőnek a képviselt szervezet, Aláírónak a szervezetet képviselő személy számít. Az Előfizetői Szerződésben a szervezet által vállalt kötelezettségek egyetemlegesen érvényesek arra az Aláíróra, aki számára a szervezet a Tanúsítványt igényelte.

A „Szervezeti személy” típusú tanúsítványok igénylésekor az Ügyfélkapcsolati Irodán történő azonosítás-hitelesítésnél a következő adatokat kell kezelni:

- az igénylő szervezet neve, székhelye,
- annak a szervezeti egységnek a neve, e-mail címe, telefon és fax száma, amely az aláírásra kijelölt személyt megbízza,
- a képviseleti megbízás dokumentuma cégszerűen aláírva,
- az aláírásra kijelölt személy neve, aláírása,
- annak a szervezeti egységnek a megnevezése, ahol az aláírásra kijelölt személy dolgozik,
- az aláírásra kijelölt személy beosztása,
- az aláírásra kijelölt személy személyi igazolvány vagy útlevél száma,
- az aláírásra kijelölt személy telefon száma, e-mail címe.

A fentieken kívül még a következőket kell megadni:

- az aláírásra kijelölt személy kijelölését engedélyező személy neve, aláírása;
- az engedélyezőnek minden esetben cégképviseletre jogosult személynek kell lennie és ezt aláírási címpéldánnyal kell igazolni,
- az engedélyező beosztása,
- az engedélyező személy munkahelyi telefonszáma, fax-száma, e-mail címe,
- az igénylő szervezet nevében a későbbiekben eljáró képviselő személy neve, aláírása, beosztása személyi igazolvány vagy útlevél száma, hivatali telefonszám és e-mail címe,
- az igénylő szervezet által hitelesített megbízó levél, amelyben az a képviselő személyt az igénylő szervezet nevében történő eljárásra megbízza.

A tanúsítvány „Country” és „Locality” mezőjében az igénylő szervezete telephelyének országkódja és városa, az „Organization” mezőben a szervezetének neve, az „Organizational

Unit" mezőben az igényt támasztó szervezeti egység neve, az „E" mezőben a szervezeti személy e-mail címe, a „Common Name" mezőjen a szervezeti személy neve szerepel.

A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

1.4.2.3. Eszköz tanúsítvány

Eszköz tanúsítványt természetes személy vagy szervezet igényelhet az általa működtetett IP címmel rendelkező informatikai eszköz részére. Tipikus eszközök: web szerver, WAP szerver, VPN, stb. Eszköz tanúsítvány igénylésnél Előfizetőnek az a természetes vagy jogi személy számít, akivel/amellyel a szerződés megkötésre került.

Az Ügyfélkapcsolati Irodán történő azonosítás-hitelesítésnél a következő adatokat kell megadni:

- Az igénylő személy/szervezet neve, lakhelye/székhelye,
- Annak a személynek/szervezeti egységnek a neve, telefon és fax száma és e-mail címe, amely az eszközt üzemelteti.
- Az eszköz azonosítója, pl. web szerver esetén a szerver internetes, ún. host neve.

A tanúsítvány „Country" és „Locality" mezőjében a szervezet telephelyének országkódja és városa, az „Organization" mezőben a szervezet neve, az „Organizational Unit" mezőben a szervezeti egység neve, a „Common Name" mezőjében ismételten az „Organization" és az „Organizational Unit" értékek szerepelnek.

A tanúsítvány egyéb ellenőrzött adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

1.5. Szolgáltató adatai

1.5.1. Cím, cégjegyzékszám, kontakt információk

Név:	MÁV Informatika Kereskedelmi, Szolgáltató és Tanácsadó Korlátolt Felelősségű Társaság
Cégjegyzék szám:	01-09-563711
Székhely, telephely:	1012 Budapest, Krisztina krt. 37/a.
Telefonszám:	(36-1) 457-9300
Telefax szám:	(36-1) 457-9500
Internet cím:	http://www.mavinformatika.hu

Panaszok bejelentésének helye:

- Személyesen az Ügyfélkapcsolati Irodán
- írásban a Szolgáltató telephelyére címezve
- telefonon és faxon az Ügyfélkapcsolati Irodán vagy az Ügyfélszolgálatnál
- elektronikus levélben a Szolgáltató Internet címére

Illetékes fogyasztóvédelmi felügyelőség:

Budapest Főváros Közigazgatási Hivatal Fogyasztóvédelmi Felügyelőség,
1088 Budapest, József krt. 6.,
Levélcím: 1364. Budapest, Pf. 234.,
Telefon: 4594-918, telefax: 4594-870

Kapcsolat az ügyfelekkel:

A vevői kapcsolatok (általános és részletes tájékozódás, szerződéskötés, aláírás létrehozó eszköz átadása, visszavonási kérelem megerősítése, stb.) biztosítása érdekében a Szolgáltató Ügyfélkapcsolati Irodát tart fenn, melyet az ügyfelek személyesen munkanapokon 9 és 13 óra között kereshetnek fel.

Az Ügyfélkapcsolati Iroda címe: Budapest, I. Krisztina krt. 37/a.

Az Ügyfélkapcsolati Iroda munkaidőben elérhető telefonon a +36-1-457-95-78 előfizetői közvetlen számon, vagy a +36-1-457-93-00 központi számon, valamint elektronikus levélben az *ica@mavinformatika.hu* címen.

A szolgáltatással kapcsolatban felmerült kérdések megválaszolására, valamint a Trust&Sign Tanúsítványok felfüggesztésére, illetve visszavonási igény sürgős bejelentésére a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk szolgálatot) ad.

Az Ügyfélszolgálat elérhető +36 80 39-93-93-as zöldszámon, a +36-1-457-93-93 közvetlen számon, a +36-1-457-93-00 központi számon, valamint elektronikus levélben a *helpdesk@mavinformatika.hu* címen.

Szolgáltató Ügyfélkapcsolati Irodája és Ügyfélszolgálata ügyfélszolgálati naplót vezet, amelyben minden megkeresésről a következő információkat rögzíti:

- A megkereső személy vagy szervezet neve,

- A megkeresés dátuma, időpontja,
- A megkeresés témájának rövid leírása és paraméterei,
- A felvetett kérdés, probléma elintézése, dátummal, időponttal.

1.5.2. Hitelesítési Politika és Szabályozási Csoport adatai

A Hitelesítési Politika és Szabályozási Csoport elérhető a 1012 Budapest, I. Krisztina krt. 37/a címen, illetve telefonon a +36-1-457-93-75 közvetlen vagy a +36-1-457-93-00 központi számon.

2. Általános rendelkezések

2.1. Feladatok és hatáskörök

2.1.1. A MÁV INFORMATIKA Kft. feladatai és hatásköre

A MÁV INFORMATIKA Kft., mint Szolgáltató kötelezettséget vállal arra, hogy az Szervezeti és Működési Szabályzatban, a mindenkori HSzSz-ben, a hitelesítési politikákban, az ÁSzF-ben, az Előfizetői Szerződésekben és a Biztonsági Szabályzatban meghatározottak szerint jár el az előfizetők tanúsítványainak kiadásakor és kezelésekor, amelynek keretében kötelezettséget vállal az alábbiakra:

4. A Szolgáltató (a Hitelesítő Központ, a Regisztrációs Iroda, az Ügyfélkapcsolati Irodák és az Ügyfélszolgálat együttes tevékenységével) az 1. és az 1.3.6.2. pontokban megjelölt szolgáltatásokat biztosítja;

   A szolgáltatások megnevezése: Trust&Sign szolgáltatások.

5. A Szolgáltató gondoskodik a Szolgáltatóra és a szolgáltatásra vonatkozó valamennyi, a jelen HSzSz-ben részletezett állítások teljesüléséről, amennyiben azok az adott tanúsítványtípusra alkalmazhatók.
6. A Szolgáltató szolgáltatásait hozzáférhetővé teszi minden olyan igénylő számára, akinek tevékenysége kinyilvánított működési területére esik.
7. A Szolgáltató jogi személy.
8. A Szolgáltató megfelelően dokumentált megállapodásokkal és szerződéses kapcsolatokkal rendelkezik azon esetekre, amikor a szolgáltatások nyújtása alvállalkozókat, illetve más, harmadik felekkel kötött megegyezéseket érint.
9. A Szolgáltató az 1. pontban megjelölt szolgáltatásait a HSzSz szerint nyújtja.
10. A HSzSz-t a Szolgáltató vezetése hagyja jóvá; a HSzSz megfelelő megvalósításáért a Szolgáltató vezetése felel.
11. A Szolgáltató rendszeresen felülvizsgálja HSzSz-ét, az újra érvényesített szabályzat tartalmazza a szükséges módosításokat.
12. A Szolgáltató időben értesítést tesz közzé a szolgáltatási szabályzatában tervezett változtatásokról és a fenti (a 7. pont szerint történő) jóváhagyást követően az átdolgozott

szolgáltatási szabályzatát (ezen felsorolás 15. pontjában előírtak szerint) haladéktalanul hozzáférhetővé teszi.

13. A Szolgáltató mindenkor az Aláíró által szolgáltatott, az Ügyfélkapcsolati Irodák által a HSzSz-ben és Előfizetői Szerződésben meghatározott módon jóváhagyott adatok alapján bocsátja ki a Tanúsítványt.

14. A Szolgáltató a Tanúsítvány kibocsátását követően a Tanúsítvány adataiban változást nem eszközölhet.
Az Előfizető, illetve Aláíró által – a Tanúsítványban foglalt adatok változására vonatkozó – bejelentés automatikusan a Tanúsítvány visszavonását vonja maga után.
A módosított adatokkal kibocsátott Tanúsítvány új Tanúsítványnak minősül.

15. Amennyiben a Szolgáltató észlelése vagy megállapítása szerint az adatok nem felelnek meg a valóságnak, köteles ezt jelezni az Előfizető részére és kérni az adatok helyesbítését. Amennyiben a felhívásban megjelölt határidőig a helyesbítés elmarad, a Szolgáltató megtagadja a Tanúsítvány kiadását.

16. A Szolgáltató kötelezettséget vállal arra, hogy a tanúsítványigénylésnek a HSzSz-ben rögzítetteknek megfelelően történő elbírálását követően a lehető legrövidebb időn, de legkésőbb 30 munkanapon belül a Tanúsítvány feldolgozásáról intézkedik és a Tanúsítvány kibocsátásáról az Előfizetőt az Ügyfélkapcsolati Iroda útján e-mail-ben értesíti. Jogi személy képviseletére jogosító Tanúsítvány esetén az értesítés a szervezet által meghatalmazott képviselőn keresztül történik. A Szolgáltató emellett nyilvántartást vezet a szolgáltatás kérelmek státusának állásáról, melyet a HSzSz-ben meghatározott módon tesz hozzáférhetővé az Ügyfélkapcsolati Irodák részére.

17. A Szolgáltató a szolgáltatások működtetése és menedzselése során a HSzSz-ben, az ÁSzF-ben, illetve az Előfizetői Szerződésben rögzített ügyfélkapcsolati tevékenységet az Ügyfélkapcsolati Irodák által biztosítja, amely egy műszakban fogadja az igénylőket, megadja a szükséges tájékoztatást és információkat, szerződést köt, átadja a Biztonságos aláírás létrehozó eszközöket, fogadja a tanúsítvány visszavonási igényeket.
A Szolgáltató az Ügyfélszolgálata (Help Desk szolgáltatása) keretében folyamatos (7x24 órás) felügyeletet biztosít az előfizetői kérdések, panaszok és felfüggesztési igények kezelésére.

18. A Szolgáltató vezeti és közzéteszi a jogszabály szerinti nyilvántartásokat, valamint a Tanúsítvány kibocsátására vonatkozó saját szabályzatait (HSzSz, ÁSzF), Internet segítségével bárki számára folyamatosan[4] elérhető módon.
19. A Szolgáltató értesítést küld e-mail-ben a lejáró Tanúsítványokról az Előfizető és az Aláíró részére legalább 15 nappal a lejárat előtt, és kéri az Előfizető, illetve az Aláíró további intézkedését a tanúsítvánnyal kapcsolatban. Az e-mail értesítés felhívja az Előfizető és az Aláíró figyelmét arra, hogy a Tanúsítvány lejáratát követően azt nem használhatja. Amennyiben az Előfizető, illetve az Aláíró a Tanúsítvány lejártáig nem rendelkezik a Szolgáltató felé, az esetben a Tanúsítvány lejár, és a Szolgáltató adott Tanúsítványra vonatkozó szolgáltatási kötelezettsége a HSzSz-ben vállalt további adattárolási kötelezettségek kivételével megszűnik.
20. Szolgáltató a Tanúsítvány megfelelő mezőjében feltünteti, ha az ÁSzF, illetve az Előfizetői Szerződés a Tanúsítvány felhasználhatóságával kapcsolatban megjelenő összeg, területi vagy egyéb korlátozásokat.
21. A Szolgáltató felfüggeszti a Tanúsítvány érvényességét és ezt nyilvánosan elérhető helyen közzéteszi (a *http://www.mavinformatika.hu/ca/* web lapon keresztül), amennyiben:
    21.1. az Előfizető vagy az Aláíró ezt az ÁSzF-ben meghatározott módon kéri,
    21.2. a szolgáltatásokkal kapcsolatos – jogszabályban meghatározott – rendellenességről szerez tudomást,
    21.3. megalapozottan feltételezhető, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy az Aláírás létrehozó adat nem az Aláíró kizárólagos birtokában van,
    21.4. a Nemzeti Hírközlési Hatóság jogerős és végrehajtható határozatában így rendelkezik.
22. A Szolgáltató köteles a Tanúsítvány visszavonására és ennek közzétételére az alábbi esetekben:
    22.1. amennyiben ezt az Aláíró, szervezeti személy típusú Tanúsítvány esetén az általa képviselt jogi személy a mindenkori HSzSz-ben, illetve az ÁSzF-ben meghatározott módon kéri,

[4] A hét 7 napján, a nap 24 órájában.

22.2. amennyiben a képviseleti jogosultság megszűnéséről a képviselt természetes vagy jogi személy illetve a képviselő (Aláíró) a Szolgáltatónak bejelentést tesz,

22.3. amennyiben a Szolgáltató a szolgáltatással kapcsolatos – jogszabályban, HSzSz-ben meghatározott – rendellenességről vesz tudomást és a rendellenesség az ezen dokumentumokban meghatározott szabályok szerint nem orvosolható,

22.4. amennyiben tudomására jut, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy az Aláírás létrehozó adat nem az aláíró kizárólagos birtokában van,

22.5. a Szolgáltató és az Előfizető között a szerződés megszűnt,

22.6. a Hatóság jogerős és végrehajtható határozatában így rendelkezik,

22.7. a Szolgáltató a tevékenységét befejezte,

23. A Szolgáltató kötelezettséget vállal arra, hogy a részére beadott visszavonási kérelmeket a HSzSz-ben meghatározott feltételek szerint feldolgozza, és a visszavont Tanúsítványok a visszavonási listákon közzétételre kerülnek.

24. A Tanúsítványok lejárat előtti visszavonásának jogkövetkezményei az alábbiak:

24.1. a visszavont Tanúsítvány a továbbiakban a jelen HSzSz 1.3.6.3 pontjában meghatározott tevékenységek végzésére nem használható. Ha az Aláíró az Aláírás létrehozó adatot felhasználja, az aláírás ellenőrzője jogosult az elfogadás megtagadására,

24.2. a visszavonást követően nem kerül automatikusan új Tanúsítvány kibocsátásra;

Azt az új Tanúsítványok igénylésével azonos igénylési folyamatnak kell megelőznie.

25. Szolgáltató megőrzi a Tanúsítványokkal kapcsolatos elektronikus információkat és az ahhoz kapcsolódó személyes adatokat legalább a Tanúsítvány érvényességének lejáratától származó 10 évig, illetőleg – amennyiben ezen időszakban az elektronikus aláírással, illetve az azzal aláírt elektronikus dokumentummal kapcsolatosan jogvita merül fel és azt a Szolgáltatónak írásban bejelentették – a jogvita jogerős lezárásáig. Ugyanezen határidőig olyan eszközt is biztosít, mellyel a kibocsátott Tanúsítvány tartalma megállapítható.

26. A Szolgáltató tevékenységi köréből csak az új Tanúsítvány kibocsátást szüneteltetheti. A Szolgáltató köteles szüneteltetni tevékenységét, ha a Nemzeti Hírközlési Hatóság az elektronikus aláírásról szóló 2001. évi XXXV. törvény 21. § (1) bekezdés c) pontja alapján

ideiglenes intézkedésként elrendeli az új Tanúsítvány kibocsátási tevékenység szünetelését és ezt a tényt feltünteti a nyilvántartásban.

27. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről a tevékenység befejezését legalább hatvan nappal megelőzően értesítenie kell az Előfizetőket, az általa kibocsátott és még vissza nem vont Tanúsítványok Aláíróit, általuk képviselt természetes vagy jogi személyt, valamint a Nemzeti Hírközlési Hatóságot, megjelölve a 17. bekezdés szerinti szervezetet. A bejelentés időpontjától kezdve a Szolgáltató nem bocsáthat ki új Tanúsítványt. A Szolgáltató a tevékenység befejezését legalább húsz napot megelőzően köteles az általa kibocsátott, és még vissza nem vont Tanúsítványokat visszavonni. A Szolgáltató Tanúsítványok visszavonását követően a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének továbbra is köteles eleget kell tenni.
28. A Szolgáltató intézkedik az iránt, hogy legkésőbb a tevékenység befejezésekor más - vele legalább azonos besorolású - szolgáltató átvegye nyilvántartásait, így különösen a visszavont Tanúsítványok nyilvántartását, valamint ellássa a hatályos jogszabályokban foglalt feladatokat. A Szolgáltató a visszavont Tanúsítványokkal kapcsolatos minden adatot - beleértve a személyes adatokat is – átadja ezen szolgáltatónak, amely kötelezettséget vállal azoknak az 1995. évi CXXII. tv. a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. tv. módosítása szerinti kezelésére.
29. A Szolgáltató az Előfizető részére csak teszt célú kulcspár és tanúsítvány kiadására Interneten keresztül elérhető teszt CA-t létesít és üzemeltet, mely a Szolgáltató web-felülete és az alábbi általános funkciókat biztosíthatja:
    29.1. Tanúsítvány igénylése,
    29.2. Tanúsítvány-kérelmek feldolgozása, jóváhagyása és továbbítása,
    29.3. a Szolgáltató által kibocsátott Tanúsítványok letöltése,
    29.4. Tanúsítvány státuszának ellenőrzése,
    29.5. Visszavont Tanúsítványok listájának generálására, letöltése (CRL),
    29.6. Tanúsítványok visszavonásának kezdeményezése.

    Az Előfizető – a Szolgáltató által elfogadott – teszt CA-val kapcsolatos egyedi igényeit és az egyes funkciók részletes működését az Előfizetői Szerződés és mellékletei rögzítik.

30. A Szolgáltató az Előfizetői Szerződésben rögzíti a szolgáltatás díjtételeit.

2.1.2. A Hitelesítő Központok („CA”-k) feladatai és hatásköre

A Szolgáltató által működtetett Hitelesítő Központok feladata és hatásköre általában az elektronikus aláírással kapcsolatos alábbi szolgáltatás megvalósítása:

- ♦ tanúsítvány előállítás;
- ♦ közreműködés (a visszavonási listák aláírásával) a visszavonási állapot közzétételében.

A Hitelesítő Központok a tanúsítvány előállítás szolgáltatás biztosítása keretén belül:

1. ellenőrzik a regisztráló szervezettől érkező tanúsítvány kérelmet, benne az aláírandó tanúsítvány adatokat tartalmazó üzenet sértetlenségét és hitelességét,
2. feldolgozzák a regisztráló szervezettől érkező hiteles és sértetlen tanúsítvány kérelmet, melynek keretén belül előállítja a tanúsítványt (aláírja az aláírandó tanúsítvány adatokat),
3. csak tanúsítványok aláírására használják fel a tanúsítvány aláírására használt magánkulcsukat,
4. csak olyan tanúsítványokat állítanak elő, amelyek megfelelnek a HSzSz-ben meghatározott, támogatott tanúsítványtípusoknak,
5. gondoskodnak arról, hogy a tanúsítványban foglalt megkülönböztetett név egyedi legyen a Szolgáltató szolgáltatási körén belül,
6. gondoskodnak arról, hogy a Szolgáltató teljes szolgáltatási körén belül kibocsátott tanúsítványokhoz tartozó kulcsok mindvégig egyediek maradjanak,
7. megválaszolják a Regisztrációs Irodának a tőle kapott tanúsítvány kérelmet, benne elküldve az előállított tanúsítványt, biztosítva a válaszüzenet sértetlenségét és hitelességét.

A Hitelesítő Központok a visszavonási állapot közzététele szolgáltatásban való közreműködés keretén belül:

1. ellenőrzik a Regisztrációs Irodától érkező visszavonási lista aláírási kérelmet, s ebben az aláírandó tanúsítvány visszavonási lista sértetlenségét és hitelességét,
2. feldolgozzák a Regisztrációs Irodától érkező hiteles és sértetlen visszavonási lista aláírási kérelmet, melynek során aláírja a tanúsítvány visszavonási listát,
3. rendszeresen új tanúsítvány visszavonási listát készítenek a tanúsítvány állapot adatbázisból, naponta egyszer, a szolgáltatási szabályzatban meghatározott frissítési időponthoz igazodóan, mely tartalmazza a következő lista tervezett kibocsátási idejét is,

4. csak tanúsítvány visszavonási listák aláírására használják fel a tanúsítvány visszavonási listák aláírására használt magánkulcsát,
5. megválaszolják a Regisztrációs Irodától kapott visszavonási lista aláírási kérelmet, elküldve az aláírt tanúsítvány visszavonási listát, biztosítva a válaszüzenet sértetlenségét és hitelességét.

Az 1. szintű Hitelesítő Központ (Root CA) alapvető feladata és hatásköre a 2. szintű Hitelesítő Központ(ok) (Produktív CA-k) hitelesítése, ezen belül a feladatok tételesen a következők:

1. Saját kulcs-pár generálása.
2. A saját magánkulcsának MeH 12. ajánlás szerinti fokozott biztonságú védelme.
3. Saját tanúsítvány előállítása önhitelesítéssel.
4. Saját tanúsítvány nyilvánosságra hozatala.
5. Szolgáltató Hitelesítő Központok (Produktív CA-k), hitelesítési kérelmeinek fogadása és ellenőrzése.
6. Kulcs-pár generálás és Tanúsítvány előállítás Szolgáltató Hitelesítő Központok részére.
7. Szolgáltató Hitelesítő Központok Tanúsítvány visszavonási kérelmeinek feldolgozása.
8. Szolgáltató Hitelesítő Központok Tanúsítvány megújítási kérelmeinek feldolgozása.
9. Magánkulcs és Tanúsítvány Szolgáltató Hitelesítő Központokhoz történő eljuttatása.
10. Szolgáltató Hitelesítő Központok Tanúsítványainak és visszavonási listáinak publikálása a tanúsítványkönyvtárban.
11. Szolgáltató Hitelesítő Központ Tanúsítványának visszavonása, illetve felfüggesztése, amennyiben magánkulcsa kompromittálódik, vagy ennek gyanúja áll fenn.
12. Az általa tanúsított Hitelesítő Központok bizalmi és biztonsági ellenőrzése.

A 2. szintű Hitelesítő Központ alapvető feladat és hatásköre a Regisztrációs Iroda ("RA") és az általa ellenőrzött és regisztrált Előfizetők hitelesítése, ezen belül a feladatok tételesen a következők:

1. A saját Magánkulcsának MeH 12. ajánlás szerinti fokozott biztonságú védelme.
2. A Regisztrációs Iroda hitelesítési kérelmeinek fogadása és ellenőrzése.

3. A Regisztrációs Iroda és az Ügyfélkapcsolati Irodák tájékoztatása a tanúsítványkérelmek státuszáról.
4. Kulcs-pár generálás és tanúsítvány előállítás a Regisztrációs Irodák részére.
5. Kulcs-pár és tanúsítvány eljuttatása a Regisztrációs Irodákhoz.
6. Regisztrációs Irodáktól előfizetői hitelesítési kérelmek fogadása és ellenőrzése.
7. Tanúsítvány előállítás az Előfizetők részére.
8. Regisztrációs Irodáktól érkező tanúsítvány visszavonási, felfüggesztési és újraérvényesítési kérelmek feldolgozása.
9. Regisztrációs Irodáktól érkező tanúsítvány megújítási kérelmek feldolgozása.
10. Tanúsítványok és tanúsítvány visszavonási listák publikálása a tanúsítványkönyvtárban.
11. Intézkedni tanúsítványok visszavonása, illetve felfüggesztése végett, amennyiben magánkulcsa kompromittálódik, vagy ennek gyanúja áll fenn.
12. A rendelkezésre állás folyamatos[5] biztosítása a tanúsítvány felfüggesztési és visszavonási kérelmek végrehajtása érdekében.
13. A Regisztrációs Iroda bizalmi és biztonsági ellenőrzése.

2.1.3. A Hitelesítési Politika és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Politika és Szabályozási Csoport a Szolgáltató hitelesítés szolgáltatást nyújtó szervezeti egységtől függetlenül működik. Kötelessége a Szolgáltató és felhasználó Közösség igényeinek felmérése és folyamatos követése, ezek alapján a közösség működésére vonatkozó alapelvek, politikák lefektetése, s ebből levezetve a tagok tevékenységét részletesen szabályozó, az egész Szolgáltató szervezetre nézve közös szabályzatok, így hitelesítési politikák, a HSzSz, az ÁSzF, az Előfizetői Szerződések és a Biztonsági Szabályzat, készítése és rendszeres karbantartása változatkövetéssel.

A Hitelesítési Politika és Szabályozási Csoport feladatai tételesen a következők:

1. A Szolgáltató és felhasználó Közösség szabályozással kapcsolatos igényeinek felmérése.
2. A hitelesítési (tanúsítvány) politikák[6] elkészítése és karbantartása.

3. A HSzSz, az ÁSzF, az Előfizetői Szerződések és a Biztonsági Szabályzat elkészítése és karbantartása.
4. A hitelesítési politikák és a HSzSz közötti összhang rendszeres ellenőrzése és karbantartása.
5. A hitelesítés szolgáltatás támogató informatikai rendszer PKI alkalmazás szintű biztonsági ellenőrzése.
6. Szolgáltatók belső folyamatainak, tevékenységének szabályozása a közös szabályzataikon keresztül.
7. A szolgáltatók és a felhasználók közötti folyamatok szabályozása.
8. A szabályzatok karbantartása és változáskezelése.
9. A szolgáltatói szabályzatok verzióinak nyilvántartása és megőrzése.
10. A Szolgáltató és felhasználó Közösség tájékoztatása.
11. Nyilvános szabályzatok publikálása.
12. A regisztrációs folyamat szabályozása, ellenőrzése, felülvizsgálata.

2.1.4. A Regisztrációs Iroda ("RA") feladatai és hatásköre

A Regisztrációs Iroda biztosítja az alábbi elektronikus aláírással kapcsolatos szolgáltatásokat:

- elektronikus aláírás hitelesítés szolgáltatás (a továbbiakban: hitelesítés-szolgáltatás), ezen belül:
  - regisztráció,
  - felfüggesztés és visszavonás kezelés,
- Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezése.

Egyúttal közreműködik az alábbi elektronikus aláírással kapcsolatos szolgáltatások biztosításában:

- tanúsítvány előállítás,
- kibocsátás
- visszavonási állapot közzététele

A Regisztrációs Iroda a regisztráció szolgáltatás keretén belül:

[5] A hét 7 napján, a nap 24 órájában.

[6] Megfelel az RFC 2527 ajánlásban definiált Certificate Policy (CP) fogalmának

1. írásbeli indoklással visszautasítja a Tanúsítvány kiadását, amennyiben a tanúsítvány igénylés nem teljes, nem helyes, vagy egyéb módon nem felel meg az elvárt feltételeknek
2. bizalmas információként kezeli az előfizető és az Aláíró minden adatát,

A Regisztrációs Iroda a visszavonás kezelés szolgáltatás keretén belül:

1. formai szempontból ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét (lásd még 4.5.2 és 4.5.6), valamint szabályosságát (lásd még 4.5.3 és 4.5.7),
2. haladéktalanul, maximum a 4.5.4 pontban meghatározott időn belül végrehajtja a hiteles, érvényes és szabályos, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket (vagyis a kérelmezett változást átvezeti a Címtár alapját képező tanúsítvány állapot adatbázisába),
3. visszautasítja (az ok megjelölésével) a nem hiteles, érvénytelen, vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket,
4. a visszavonási kérelem elfogadása után haladéktalanul, maximum a 4.5.4 pontban meghatározott időn belül intézkedik egy tanúsítvány visszavonásáról,
5. intézkedik saját Tanúsítványának visszavonása, illetve felfüggesztése végett, amennyiben magánkulcsa kompromittálódott, vagy ennek gyanúja áll fenn,
6. folyamatosan[7], 99,9%-os rendelkezésre állással biztosítja a visszavonás kezelési szolgáltatást minden érdekelt fél számára, egyúttal szolgáltatási szabályzatában megadja az előre tervezett és rendkívüli leállások leghosszabb időtartamát.

A Regisztrációs Iroda az Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:

1. gondoskodik valamennyi általa, az Aláíró számára végrehajtott kulcs előállítás biztonságosságáról, az Aláíró magánkulcsának titkosságáról,

[7] A hét 7 napján, a nap 24 órájában.

2. az Aláíró részére biztosított kulcspárt:
   - olyan kriptográfiai eszközzel állítja elő, amely hazai tanúsítvánnyal igazolt és egyben szerepel a Nemzeti Hírközlési Hatóság által nyilvántartásba vett, tanúsított elektronikus aláírási termékek listáján is,
   - olyan algoritmus felhasználásával állítja elő, melyet a 2/2002. (IV.26) MeHVM irányelv 1. sz. melléklete az elfogadott kriptográfiai algoritmusok között megfelelő kulcs generáló algoritmusként ismer el,
   - olyan aláíró algoritmushoz és olyan kulcshosszúságban állítja elő, melyet a 2/2002. (IV.26) MeHVM irányelv 1. sz. melléklete az elfogadott kriptográfiai algoritmusok között megfelelő aláíró algoritmusként, illetve megfelelő paraméterként ismer el,
3. biztonságos módon megsemmisíti az Aláíró részére előállított magánkulcs Aláírás-létrehozó eszközön kívüli összes példányát, miután az Aláíró részére előállított kulcspárt elhelyezte az aláírás-létrehozó eszközben,
4. gondoskodik az általa megszemélyesített Aláírás-létrehozó eszköznek az Ügyfélkapcsolati Irodához a PIN-kód eljuttatásától független és biztonságos továbbításáról,
5. ellenőrzi az Aláírás-létrehozó eszköz kezelését,
6. ellenőrzi, hogy a szolgáltatáshoz felhasznált Aláírás-létrehozó eszköz a Nemzeti Hírközlési Hatóság által nyilvántartásba vett Aláírás-létrehozó eszköz-e,
7. a Biztonságos aláírás létrehozó eszköz előkészítését megfelelően biztonságos környezetben hajtja végre,
8. biztonságos módon előállítja a kezdeti aktivizáló adatot (PIN kódot), majd azt az Aláírás-létrehozó eszköztől elkülönítve eljuttatja az Ügyfélkapcsolati Irodához,
9. biztosítja, hogy a Szolgáltató alkalmazottai nem élhetnek vissza az Aláírás-létrehozó eszközzel,
10. biztosítja saját Aláírás létrehozó adatainak biztonságos használatát és tárolását.

A Regisztrációs Iroda a tanúsítvány előállítás szolgáltatásban való közreműködés keretén belül:

1. a Tanúsítvány kibocsátásához szükséges ellenőrzések és visszaigazolások sikeres befejeződése után a Hitelesítő Központ felé tanúsítvány kibocsátási kérelem üzenetet indít el,
2. feldolgozza a teljes, pontos, hiteles és teljesíthető tanúsítvány megújítási kérelmeket az alábbi módon:

- tanúsítványfrissítés kérelme esetén az Aláíró korábbi Tanúsítványában szereplő érvényességi időt meghosszabbítja, a többi adat és kulcspár változatlan megtartása mellett,
- tanúsítvány aktualizálás kérelme esetén nyilvántartásba veszi az Aláíró megváltozott új adatait, a korábbi Tanúsítvány visszavonja és a megváltozott adatokkal új Tanúsítványt állít elő,
- tanúsítvány kulcscsere kérelme esetén a korábbi Tanúsítvány visszavonja, új kulcspárt generál és új Tanúsítványt állít elő,

3. biztosítja az aláírandó Tanúsítványt is tartalmazó tanúsítvány kérelem üzenet sértetlenségét, hitelességét és bizalmasságát.

A Regisztrációs Iroda a tanúsítvány kibocsátás szolgáltatásban való közreműködés keretén belül:

1. fogadja a Hitelesítő Központtól kapott új tanúsítványokat, valamint ellenőrzi ezek hitelességét és sértetlenségét,
2. kezdeményezi az új tanúsítványok[8] elküldését a címtárhoz, biztosítva a kérést tartalmazó üzenet hitelességét és sértetlenségét.

A Regisztrációs Iroda a visszavonási állapot közzététele szolgáltatásban való közreműködés keretén belül:

1. rendkívüli esetben[9] új Tanúsítvány visszavonási listát készít tanúsítvány állapot adatbázisából, mely tartalmazza a visszavonási lista lejáratának idejét is,
2. kéri a Hitelesítő Központtól az új Tanúsítvány visszavonási lista kibocsátását, (a visszavonási lista aláírási kérelemben), biztosítva az ezt tartalmazó üzenet hitelességét és sértetlenségét,

2.1.5. Az Ügyfélkapcsolati Iroda feladatai és hatásköre

Az Ügyfélkapcsolati Iroda szolgáltatás igénylés esetén az Igénylők, az előfizetők és az érintett felek részére nyújtott ügyfélkapcsolati tevékenység regisztráció szolgáltatásán belül:

[8] Amennyiben az Aláíró hozzájárult ehhez.

[9] Rendkívüli esetnek számít a Szolgáltató szolgáltatói magánkulcsának kompromittálódása, illetve jelentős számú új tanúsítvány visszavonási kérelem beérkezése.

1. gondoskodik az Igénylő megfelelő azonosításáról, illetve arról, hogy a Tanúsítványt igénylő formanyomtatványok teljesek, pontosak és kellőképpen hitelesek legyenek;
2. ellenőrzi a 3.1 pontban és az ÁSzF-ben előírt adatszolgáltatási követelmények szerint megadott adatok alapján a szolgáltatást igénylő ügyfél (természetes, illetve szervezeti személy) személyazonosságát és a leendő Aláíró és/vagy időbélyeg kérő fél 1 pontban meghatározott jellemzőit;
3. összegyűjti, illetve meghatározza a regisztráció során valamennyi, a 1 pontban meghatározott, Tanúsítványba kerülő adatot, ellenőrzi az Igénylő által átadott dokumentumok valódiságát, érvényességét, sértetlenségét és hitelességét,
4. összeveti egymással és a valósággal az egyes iratokon szereplő adatokat (így különösen a Tanúsítványt személyesen igénylő ügyfél fotóját az arcával, aláírását a helyszíni aláírásával),
5. ellenőrzi a dokumentumok érvényességét, valódiságát valós idejű nyilvántartásokban is,
6. nyilvántartásba vesz minden, a regisztráció során felvett, a 4.1 pontban meghatározott információt,
7. megőrzi a 6. pontbeli nyilvántartásokat a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított tíz évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig.
8. bizalmas információként kezeli az előfizető és az Aláíró minden adatát, kivéve azokat, amelyeket a 2.8.2 pont tárgyal. A Szolgáltató a birtokába jutott bizalmas információkat a személyes adatok védelméről szóló 1992 évi LXIII. törvénynek megfelelően kezeli, s csak a 2.8.3-2.8.7 pontokban említett esetekben és személyek részére fedi fel őket
9. korlátozás nélkül biztosítja az Aláíró számára a rá vonatkozó regisztrációs és egyéb információhoz történő hozzáférést (lásd 2.8.7).

Az Ügyfélkapcsolati Iroda a visszavonás kezelés szolgáltatás keretén belül:

1. ellenőrzi a tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmek hitelességét és érvényességét (lásd még 4.5.2 és 4.5.6), valamint szabályosságát (lásd még 4.5.3 és 4.5.7),
2. visszautasítja (az ok megjelölésével) a nem hiteles, érvénytelen, vagy szabálytalan, tanúsítvány visszavonásra, felfüggesztésre, vagy felfüggesztés megszüntetésére vonatkozó kérelmeket,

3. a visszavonási kérelem elfogadása után haladéktalanul, maximum a 4.5.4 pontban meghatározott időn belül intézkedik egy tanúsítvány visszavonásáról,
4. tájékoztatja a visszavont, illetve felfüggesztett Tanúsítvány tulajdonosát Tanúsítványa állapotának változásáról.

Az Ügyfélkapcsolati Iroda az Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:

1. gondoskodik valamennyi általa, az Aláíró számára előállított Aláírás-létrehozó eszköz, az Aláírás-létrehozó adat és a PIN kód biztonságos kezeléséről és az Aláírónak történő biztonságos átadásukról,
2. biztosítja, hogy a Szolgáltató alkalmazottai nem élhetnek vissza az Aláírás-létrehozó eszközzel.

Az Ügyfélkapcsolati Iroda a tanúsítvány előállítás szolgáltatásban való közreműködés keretén belül:

1. kezdeti tanúsítvány előállítás esetén a regisztráció szolgáltatás 3., 4., és 5. pontjaiban leírt módon összegyűjtött, Tanúsítványba kerülő adatokat ellenőrzi az adott tanúsítványtípushoz kapcsolódó hitelesítési, ellenőrzési eljárás szerint,
2. az Aláíró adatainak változása, illetve kulcscsere kérelem esetén ellenőrzi a már korábban nyilvántartásba vett Aláírótól érkező tanúsítvány megújítási kérelem teljességét, pontosságát, hitelességét és teljesíthetőségét a 3.1.1 pontban a kezdeti regisztrációnál meghatározott ellenőrzési módszerrel. Adatváltozás esetén a Szolgáltató a bejelentést elfogadja telefonon történő bejelentéssel vagy minősített elektronikus aláírással hitelesített elektronikus kérelemmel is, de a megváltozott adatokat tartalmazó Tanúsítvány kiállításához szükséges az Aláíró személyes megjelenése, mert azonosítás-hitelesítését el kell végezni.

2.1.6. A Címtárral (Tanúsítványtárral) kapcsolatos feladatok és kötelezettségek

A Tanúsítványokkal kapcsolatos felfüggesztési, illetve visszavonási kérelmeket a Szolgáltató Ügyfélkapcsolati Irodája naponta 9-13 óra között, Ügyfélszolgálata (Help Desk-je) napi 24 órában folyamatosan fogadja. A Szolgáltató az általa kibocsátott előfizetői Tanúsítványokat és a Visszavont Tanúsítványok Listáját (CRL) közcélú Internet segítségével bárki számára hozzáférhető és folyamatosan elérhető módon közzéteszi.

A Szolgáltató a Címtár kibocsátás szolgáltatás keretén belül:

1. közzé teszi az általa kibocsátott előfizetői Tanúsítványokat[10] a kibocsátást követően haladéktalanul, de legrosszabb esetben 24 órán belül;
2. biztosítja a Címtár folyamatos[11] elérhetőségét, még rendkívüli üzemeltetési helyzet esetén is;

Annak érdekében, hogy a Címtár elérési útvonala bárki számára hozzáférhető legyen, Szolgáltató az 1.2 pontban, az Előfizetői Szerződésben és a *http://www.mavinformatika.hu/ca/* weboldalon felsorolja azokat az Internet címeket, ahol a Hitelesítő Központonként vezetett nyilvántartások elérhetők. A Címtár elérési útvonala Produktív Hitelesítő Központonként változhat.

A Szolgáltató a Címtár a visszavonási állapot közzététele szolgáltatás keretén belül:

1. közzé teszi a hiteles és sértetlen új tanúsítvány visszavonási listát;

   Előfizetői kérelem vagy a Szolgáltató alapos indokkal meghozott döntése alapján történő Tanúsítvány felfüggesztést vagy visszavonást a Szolgáltató belső nyilvántartásában haladéktalanul, de legrosszabb esetben 1 órán belül végre kell hajtani. A felfüggesztés vagy a visszavonás publikálása a legközelebbi közzétételi időpontban történik meg.
2. biztosítja a legfrissebb tanúsítvány visszavonási lista folyamatos[12] elérhetőségét, még rendkívüli üzemeltetési helyzet esetén is;

A visszavont és felfüggesztett tanúsítványokra vonatkozó közzétételi időpontja, valamint a visszavonási listák frissítésének időintervalluma a 1.2 pontban megadott web lap címen érhető el az Előfizetők, az Aláírók és az Érintett felek által.

2.1.7. Az Igénylő, az Előfizető és Aláíró feladatai és hatásköre

Az Igénylő, az Előfizető, illetve az Aláíró kötelessége a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a tanúsítvány és magánkulcs igénylése és felhasználása során, ezen belül köteles:

1. az Igénylő a Tanúsítvány igénylése előtt megismerni és elfogadni a Szolgáltató ÁSzF-ét és a HSzSz-ét,

[10] Amennyiben az Aláíró hozzájárult ehhez.

[11] A hét 7 napján, a nap 24 órájában.

2. az Előfizető az Ügyfélkapcsolati Irodánál személyesen megjelenő Igénylőt, aki a Tanúsítványt és az ezzel kapcsolatos műveleteket igényli, meghatalmazással ellátni,
3. az Igénylő a HSzSz és az ÁSzF-et az alkalmazásában álló vagy vele szerződéses kapcsolatban álló Aláírókkal megismertetni, különösen az elektronikus aláírás biztonságos használatával, technikai feltételeivel és jogi következményeivel kapcsolatosan,
4. a Tanúsítvány igénylését és a kulcs-pár felhasználását úgy végezni, hogy az harmadik fél jogait ne sértse,
5. az Előfizető a Tanúsítvány kiadásához szükséges aláírói adatokat ellenőrizni, ennek érdekében a Tanúsítvány kibocsátására vonatkozó kérelem érvényesítését megelőzően köteles az Aláírót azonosítani,
6. az Előfizető teljes, pontos, valós és hiteles adatokat szolgáltatni a Szolgáltató részére az igényelni kívánt tanúsítványtípus és fajta követelményeinek megfelelően az Aláíró személyazonosságát, szervezeti identitását és a regisztrációhoz szükséges egyéb jellemzőket illetően,
7. az Előfizető és az Aláíró megismerni a Magánkulcsának átvétele és felhasználása előtt a magánkulcs tárolásával, s az elektronikus aláírás megtételével kapcsolatos technikai, jogi, biztonsági követelményeket és feltételeket,
8. az Aláíró biztosítani az Aláírás-létrehozó eszközének és adatának, valamint a PIN kódjának védelmét,
9. az Aláíró Aláírás-létrehozó adatát aláírásra csak az Aláírás-létrehozó eszközzel használni;

   az Aláíró nem jogosult a Tanúsítványban megadott nyilvános kulcs titkos párját újabb Tanúsítványok vagy bármely más formátumú tanúsított kulccsal használni.
10. az Előfizető, illetve az Aláíró 3 (három) munkanapon belül jelezni Szolgáltatnál a regisztráció során felvett adataiban történő változásokat, különös tekintettel a tanúsítványba foglalt adatokra,
11. az Előfizető az Aláíró figyelmét külön felhívni arra, ha az Előfizetői Szerződés a Tanúsítvány felhasználhatóságával kapcsolatban összeg, területi vagy egyéb korlátozásokat köthet ki,
12. az Aláíró az Aláírás-létrehozó adatát csak a vele közölt valamennyi korlátozásnak megfelelően használhatja,

[12] A hét 7 napján, a nap 24 órájában.

13. az Aláíró tudomásul venni, hogy magánkulcsának védelme és az elektronikus aláírás készítése kizárólag a saját felelőssége, ezért ezzel - így különösen a magánkulcsának illetéktelen harmadik személyhez kerülésével - kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
14. az Aláíró tájékoztatni az Érintett felet arról, hogy a HSzSz-ben meghatározott aláírás ellenőrzés lépéseinek elmulasztásából eredő következményekért az Érintett fél felel,
15. az Előfizető az ÁSzF módosításáról szóló értesítést követően 72 órán belül az Aláírókat írásban tájékoztatni a változásokról;

    amennyiben az Előfizető nem fogadja el az ÁSzF módosítását, jogosult a hatálybalépést követően 15 napon belül 15 napos felmondási idővel az Előfizetői Szerződést felmondani.
16. az Aláíró azonnal intézkedni tanúsítványának visszavonása, illetve felfüggesztése végett, amennyiben
    - tudomására jut, hogy a Tanúsítványban foglalt adatok nem felelnek meg a valóságnak, tartalmában, a regisztrációs adatokban pontatlanság van, illetve azokban változás következett be,
    - az Aláírás létrehozó adat és/vagy a PIN kód nem az Aláíró kizárólagos birtokában van (elveszett, ellopták, esetleg kompromittálták), vagy ennek alapos gyanúja áll fenn,
17. kompromittálódás esetén az alany magánkulcsának használatát azonnal és véglegesen megszakítani,
18. az Előfizető az Előfizetői Szerződésben rögzített szolgáltatási díjakat a Szolgáltatónak megfizetni,
19. az Aláíró vagy az Előfizető a Tanúsítvánnyal ellátott elektronikus dokumentummal kapcsolatos jogvita megindulásáról köteles haladéktalanul tájékoztatni a Szolgáltatót.

Ezeken kívül:

20. az Aláíró jogosult arra, hogy a magánkulcsot birtokolja és a jogszabályokban meghatározott módon elektronikus aláíráshoz, a HSzSz-ben és az Előfizetői Szerződésben rögzített tevékenységhez csak (a tanúsítványban is feltüntetett névmegadás szerint) saját, illetve szervezete nevében felhasználja,
21. az ÁSzF tartalmazza az Előfizetői Szerződésnek az Előfizető, illetve a Szolgáltató által történő rendes vagy soron kívüli felmondásának feltételeit,
22. az Aláíró tudomásul veszi, hogy a magánkulcsával készített elektronikus aláírás a saját elektronikus aláírásának minősül, és viseli ennek jogkövetkezményeit;

23. az Aláíró a Tanúsítványt csak a HSzSz-nek, valamint a hatályos jogszabályi rendelkezéseknek megfelelően használhatja; elektronikus aláírás csak Tanúsítvány érvényességi ideje alatt készíthető,

2.1.8. Érintett fél feladatai és hatásköre

Az Érintett félnek kötelessége Szolgáltató szabályzatainak megfelelően a legnagyobb gondossággal eljárni az Elektronikus aláírás és a tanúsítvány elbírálásakor, ezen belül:

1. az Elektronikus aláírás elfogadása előtt meg kell értenie az Elektronikus aláírással kapcsolatos technikai, jogi, biztonsági és egyéb vonatkozásokat,
2. meg kell ismernie Szolgáltató nyilvánosan elérhető szabályzatait (HSzSz, ÁSzF) és az Elektronikus aláírással ellátott dokumentum alapján végzett bármilyen tevékenység a Szolgáltató szabályzatának elfogadását jelenti,
3. az Elektronikus aláírás ellenőrzését el kell végeznie az Aláíró tanúsítványának segítségével, meggyőződve az üzenet eredetiségéről és az aláírás valódiságáról,
4. a Tanúsítványban feltűntetett azonosító alapján, és egyéb adatok, törvényesen rendelkezésre álló módszerek segítségével az aláíró személyéről egyértelműen meg kell győződnie,
5. a Tanúsítvány érvényességét és hatályosságát ellenőriznie kell,
6. el kell végeznie a teljes tanúsítási lánc vizsgálatát az alábbiak szerint:
   - a Tanúsítvány kibocsátójának azonosítója alapján a Kibocsátó kilétéről meg kell győződnie;
   - a Kibocsátó Tanúsítványának segítségével az Aláíró Tanúsítványának integritásáról meg kell győződnie;
   - a Tanúsítvány állapotát ellenőriznie kell a Tanúsítvány visszavonási listák (CRL) áttanulmányozásával;
   - át kell tanulmányoznia a Tanúsítvány összes attribútumát, és az adott tranzakcióra vonatkozó előírásoknak, valamint józan megfontolásoknak megfelelően döntést hozni az aláírás elfogadásáról,
7. az Elektronikus aláírás elfogadását vissza kell utasítani, ha az Elektronikus aláírás, az aláíró tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata, annak érvénytelenségére utal, illetve ha az az adott kontextusban nem elfogadható; az aláírás elfogadása nem jelenti az aláírt üzenet tartalmának tudomásul vételét vagy elfogadását.

2.2. A hitelesítés szolgáltató és felhasználó közösség tagjainak felelőssége

1.1.1. A MÁV INFORMATIKA Kft. felelőssége

Általános Szabály

A MÁV INFORMATIKA Kft., mint Szolgáltató azzal, hogy aláír egy, a jelen HSzSz 1.4.2 pontja szerint meghatározott Tanúsítványt, illetve időbélyeget – és ezzel jelzi az 1.3.5 pontban meghatározott felhasználó közösség és az érintett felek felé ezen HSzSz használatát –, csak azért vállalja a felelősséget, hogy a tanúsítvány előállítása, kibocsátása, közzététele, visszavonása, a Visszavonási Lista közzététele és az időbélyegzés tevékenységek a jelen HSzSz-ben előírtaknak teljes mértékben megfelelnek, és a Szolgáltató megteszi a szükséges intézkedéseket ahhoz, hogy a Szolgáltató maga és az előfizetők is a jelen HSzSz előírásainak megfelelően járjanak el.

A Szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag a hibájából, kötelezettségeinek megszegéséből, valamint a neki felróható okokból bekövetkező, bizonyítható károkért tartozik helyt állni. Általában a Szolgáltató nem vállal felelősséget, ha a Szolgáltató által kibocsátott Tanúsítvány a jelen HSzSz-ben előírtaktól eltérő módon kerül felhasználásra. Így a Szolgáltató nem felelős az olyan károkért, mely abból adódott, hogy az Érintett fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok és Szolgáltató HSzSz-e szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

A Szolgáltató felelősségére a következő részletes szabályok mérvadók:

- Amennyiben a jelen HSzSz szabályai megszegésével a Szolgáltató a vele szerződéses jogviszonyban nem álló Érintett félnek kárt okoz, vagy a tanúsítvány Érintett fél általi, – a HSzSz szerint történő – felhasználása ellenére, az Érintett fél kárt szenved, azért a Magyar Köztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény 339. §-ának megfelelően a Szolgáltató felelős, azzal a korlátozással, hogy a kártérítés mértéke Tanúsítvány típusonként és egyedi tanúsítványonként is maximált összegű az Általános Szolgáltatási Feltételek vagy az Előfizetői Szerződés vonatkozó feltételei szerint.
- A Szolgáltató köteles a Tanúsítvány megfelelő mezőjében feltüntetni, ha az Előfizetői Szerződésben a Tanúsítvány felhasználhatóságával kapcsolatban összeg, területi vagy egyéb

korlátozásokat köt ki. Ezen korlátokat meghaladó ügyletekben kibocsátott és aláírt elektronikus dokumentumokból származó követelésekért, illetve az így okozott kárért a Szolgáltató nem felel.

- A Szolgáltató kizárja felelősségét, ha az aláírás ellenőrzés lépései a HSzSz-ben meghatározott módon bármi okból – beleértve Szolgáltatónál keletkező működtetési és/vagy menedzselési problémát is – nem hajthatóak végre az aláírás ellenőrzésének időpontjában, és az elektronikus aláírás, illetve az aláírással ellátott dokumentum az aláírás ellenőrzője által ennek ellenére elfogadásra kerül.
- Szolgáltató HSzSz vagy az előfizetői szerződés megszegéséből származó károk esetén a vele szerződéses jogviszonyban álló Előfizetővel szemben a Polgári Törvénykönyv szerződésszegésért való felelősség szabályai szerint felelős.
- A Szolgáltató a teszt célú magánkulcsok kompromittálódásából, a tanúsítványokkal és a kulcspárokkal történő bármilyen visszaélésből származó károkért felelősséget nem vállal.
- A Szolgáltató nem vagyoni felelőssége az Előfizető és Érintett fél felé a Polgári Törvénykönyv nem vagyoni felelősségről szóló szabályai szerint alakul.
- A tanúsítvány lejárat előtti megszüntetése esetén, a kártérítési felelősség korlátozásáról a 2.3. pont rendelkezik.

2.2.2. A Hitelesítő Központok felelőssége

A Hitelesítő Központok felelősségének belső megosztása nem érinti a szolgáltató társaság egységes jogi felelősségét.

Az 1. szintű „Root CA”

- felelős a közvetlenül alá rendelt hitelesítő központok és szervezetek hitelesítésért,
- nem felelős az alá rendelt hitelesítő szervezetek működéséért.

A 2. szintű (produktív) Hitelesítő Központ felelőssége:

- felelős az általa kibocsátott tanúsítványok hitelességéért.
- felelős az általa létrehozott alárendelt hitelesítő központok hitelesítésért,
- felelős az alárendelt regisztrációs irodák működéséért.
- nem felelős az Előfizetők aláírási és más hitelesítő központok által kibocsátott magánkulcsok és tanúsítványok felhasználási tevékenységért,
- nem felelős az Érintett felek aláírás ellenőrzési és tanúsítvány elbírálási tevékenységért.

2.2.3. Hitelesítési Politika és Szabályozási Csoport felelőssége

A Hitelesítési Politika és Szabályozási Csoport felelős az ÁSzF, a HSzSz és a Szolgáltató minden szervezeti egysége által kibocsátott más szabályzatok ellentmondás-mentességéért, megfelelő értelmezhetőségéért és használhatóságáért, azok törvényi megfelelőségéért, érvényesítéséért és betartatásáért.

A Hitelesítési Politika és Szabályozási Csoport nem felelős az Előfizetők, az Érintett felek, és a felhasználó közösség szervezetei által kibocsátott szabályzatokért.

2.2.4. A Regisztrációs Iroda felelőssége

A Regisztrációs Iroda felelős:

- a regisztrációs adatok ellenőrzéséért,
- az általa generált kulcspárok megfelelőségéért, az Aláírás-létrehozó adat, az Aláírás-ellenőrző adat és a Tanúsítvány összetartozásáért és a Tanúsítvánnyal együtt történő Aláírás-létrehozó eszközre írásért,
- az Aláírás-létrehozó eszköz és az aktivizáló (PIN) kód összetartozásáért.

2.2.5. Az Ügyfélkapcsolati Iroda felelőssége

Az Ügyfélkapcsolati Iroda felelős:

- az előfizetők személyazonosságának és szervezeti identitásának megállapításáért és a bemutatott dokumentumok alapján történő ellenőrzéséért,
- a felvett regisztrációs adatok ellenőrzéséért,
- a regisztrációs adatoknak a Hitelesítő Központba történő bizalmas, hiteles és sértetlen eljuttatásáért,
- a tanúsítvány visszavonási igény bejelentője személyazonosságának és szervezeti identitásának megállapításáért és a bemutatott dokumentumok alapján történő ellenőrzéséért,
- az előfizetői pénzek kezeléséért.

2.2.6. Előfizető és az Aláíró felelőssége

Az Előfizetőnek és az Aláírónak büntetőjogi felelőssége áll fenn Szolgáltatóval szemben, ha a regisztráció során megadott adatai nem valódiak és/vagy nem hitelesek és ezzel a Szolgáltatónak kárt okoz.

Az Előfizetőnek kártérítési felelőssége áll fenn Szolgáltatóval szemben azokért a veszteségekért és károkért, melyeket a regisztráció során megadott helytelen adataival, vagy az azokban bekövetkezett változások be nem jelentésével, vagy egyéb kötelezettségeinek be nem tartásával számára okoz. Az Előfizető felelős azért, ha magánkulcsát nem a HSzSz-ben, az ÁSzF-ben és a vonatkozó jogszabályokban meghatározott módon és célra használta.

Az Előfizető és az Aláíró felelős a magánkulcs biztonságos megőrzéséért, a kulcs tartalom és a PIN kód illetéktelenek tudomására jutásának megakadályozásáért.

A Szolgáltató nem vállal felelősséget a magánkulcs hordozó elvesztéséből, vagy a kulcs biztonságának egyéb módon történő sérüléséből, elvesztéséből, illetve a PIN kód illetéktelen tudomásra jutásból származó károkért.

2.2.7. Érintett fél felelőssége

Érintett fél felelőssége fennáll a tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a tanúsítvány érvényességének és hatályosságának ellenőrzése során nem a tanúsítványtípus, a szolgáltatási szabályzat, illetve a hatályos jogszabályok szerint jár el.

Az Érintett fél felelős az elektronikus aláírás és a Szolgáltató által kibocsátott tanúsítványok elfogadása során tanúsított körültekintő ellenőrzésért, valamint a Szolgáltató nyilvánosan elérhető HSzSz-e rá vonatkozó részének megismerésért, a 2.1.8 pontban meghatározott kötelezettségeinek betartásáért.

Az Érintett fél felelőssége fennáll, ha a tanúsítvány érvényességének és hatályosságának ellenőrzése során nem a HSzSz, illetve a hatályos jogszabályok szerint jár el.

2.3. A pénzügyi felelősség korlátjai

2.3.1. Kártérítés

A Szolgáltató nem felelős az olyan kárért, amely abból adódott, hogy az Érintett fél a tanúsítványok, illetve az elektronikus aláírások hitelességének ellenőrzésénél nem a hatályos jogszabályok, szerződéses feltételek, a HSzSz, valamint az Előfizetői Szerződés szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

Az Aláírás létrehozó adat, illetve eszköz illetéktelen kezekbe kerülés esetén a Szolgáltató nem felelős egészen az Előfizető vagy Aláíró által tett bejelentés időpontjáig azért a kárért, amely abból származik, hogy az Előfizető, illetve az Aláíró nem a HSzSz-ben előírt biztonságos feltételek mellett tárolta, használta az Aláírás létrehozó adatot, illetve eszközt, és emiatt az illetéktelen felhasználásra került. Az előfizetők és az érintett felek kártérítési felelősséggel tartoznak a Szolgáltatóval szemben azokért a veszteségekért és károkért, amelyeket kötelezettségeik be nem tartásával okoznak számára.

A Szolgáltató felelősségének korlátait – kártérítés felső határa - az ÁSzF, illetve az Előfizetői Szerződés szerint kell értelmezni. Szolgáltató – helytállási kötelezettsége esetén – csak az ÁSzF-ben, illetve az Előfizetői Szerződésben megjelölt összeghatárig köteles kártérítésre.

A Szolgáltatással kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben a Szolgáltató a hibájából, kötelezettségeinek megszegéséből, neki felróható okból bekövetkező bizonyítható károkért tartozik helyt állni.

A Szolgáltató megfelelő megoldásokkal rendelkezik a műveleteiből és tevékenységeiből származó kötelezettségek fedezésére, különösképpen a kárfelelősség kockázatára vonatkozóan.

A Szolgáltató rendelkezik a jelen dokumentumban foglaltakkal összhangban álló üzemeltetéshez szükséges pénzügyi stabilitással és erőforrásokkal.

2.3.2. Megbízotti kapcsolatok

Azáltal, hogy a Szolgáltató az Előfizetők részére tanúsítványokat bocsát ki, semmilyen körülmények között nem tekinthető az Előfizetők vagy az Érintett felek ügynökének, megbízottjának, képviselőjének, vagy bármilyen más, az Előfizetői Szerződésben meghatározottól eltérő funkciójú partnerének a hitelesítési tevékenysége vonatkozásában.

2.3.3. Adminisztratív eljárások

A Szolgáltató a vagyoni felelősségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelősség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megőrzi (archiválja) azokat. (Részletesebben lásd a 4.5 és 4.6 alfejezeteket.)

A Szolgáltató Szervezeti és Működési Szabályzatában kerültek meghatározásra azok az adminisztrációs folyamatok, amelyek az Aláírás létrehozó eszköz és tanúsítvány kibocsátást támogatják.

Ilyenek:

- Az igénylők adatainak nyilvántartása, tárolása, archiválása,
- Az Előfizetők, Aláírók tanúsítványainak, a Visszavonási listák tárolása, archiválása,
- Számlázás, számlázási adatok nyilvántartása, archiválása,
- A Szolgáltató által üzemeltetett PKI rendszer elemeinek nyilvántartása,
- Hitelesítési tevékenység és biztonsági audit eljárások,
- Minőségbiztosítási eljárások.

2.4. Értelmezés és alkalmazás

2.4.1. Alkalmazott jogszabályok

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. Szerződéseire és szabályzataira, és azok teljesítésére, a magyar jog az irányadó, és azok a magyar jog szerint értelmezendők.

A Szolgáltató tevékenységére elsősorban a következő jogszabályok mérvadók:

- 2001. évi XXXV. törvény az elektronikus aláírásról[13]
- 100/2000. (VI. 23.) Korm. rendelet az információs társadalom megvalósításával összefüggő feladatokról, az informatikai kormánybiztos feladat- és hatásköréről
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.
- 1014/2001. (III.5.) Korm. határozat az elektronikus aláírásról szóló törvény alapelveiről és az ezzel kapcsolatban szükséges intézkedésekről szóló 1075/2000. (IX.13.) Korm. határozat módosításáról.
- 151/2001. (IX. 1.) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat-és hatásköréről, valamint eljárásainak részletes szabályairól.
- 20/2001. (XI.15.) MeHVM rendelet a Hírközlési Felügyeletnek az elektronikus aláírással összefüggő minősítéssel nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról.
- 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- 15/2001. (VIII. 27.) MeHVM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról.
- 1026/2002. (III. 26.) Kormányhatározat a kormányzati elektronikus aláírási rendszer kiépítésével összefüggő egyes feladatokról és a kormányzati központi kormányzati hitelesítés-szolgáltató felállításáról.
- 47/2002. (III. 26.) Korm. rendelet a kormányzati elektronikus aláírási rendszer kiépítésével összefüggő egyes kormányrendeletek módosításáról

[13] A 2001. évi XXXV. törvényt kiegészítő, felsorolt alacsonyabb szintű jogszabályok a 2002 május 31.-i állapotot tükrözik.

- 7/2002 (IV.26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről.

Ezeken túlmenően a Szolgáltató

- az üzleti titkok vonatkozásában az 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról,
- a személyes adatok vonatkozásban az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról és az 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. tv. Módosításáról

szerint jár el.

Szolgáltató figyelembe veszi még az Európai Parlament és Európa Tanács az elektronikus aláírások közösségi programjáról szóló 1999/93/EK irányelvét, a vonatkozó ITU szabványokat, az Internet közösség RFC ajánlásait és az Európai Unió Távközlési Szabványok Intézetének (ETSI) vonatkozó szabványait.

2.4.2. Érvénytelenség, hatályosság, megszűnés, értesítések

2.4.2.1. Érvénytelenség

Amennyiben a Szolgáltató szerződéseinek vagy szabályzatainak valamely pontja érvénytelenné vagy érvényesíthetetlenné válna, az az egész szabályzat vagy szerződés egyéb pontjainak érvényességét nem érinti.

A jelen HSzSz minden olyan rendelkezése, amely a felelősségek, a kötelezettségek, garanciák és a kártérítés korlátaira vonatkoznak, azok függetlenül más intézkedésektől, önmagukban értelmezendők és érvényesítendők.

2.4.2.2. Hatályosság

Jelen HSzSz időbeli hatálya az 1.3.6.1 pontnak megfelelően a Nemzeti Hírközlési Hatóság engedélyének keltétől a szolgáltatási tevékenység megszűntéig tart. A HSzSz személyi és tárgyi hatályát az 1.3.6.1 pont tartalmazza.

Jelen HSzSz 1.3.6.1. fejezete érvényben marad a HSzSz hatályának végét követően is (a hatályosság megszűnésének módjától függetlenül) mindazon tanúsítványokkal kapcsolatosan, melyet jelen tanúsítványtípus hatálya alatt bocsátott ki a Szolgáltató

2.4.2.3. Megszűnés

Jelen HSzSz és az ÁSzF a közösség résztvevőinek valamennyi kötelezettségét, felelősségét és jogát tartalmazza. A HSzSz egyetlen pontja sem értelmezhető a jelen dokumentumba foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében, beleértve a Szolgáltató és más szervezet jövőbeli esetleges összeolvadásának esetét is. A HSzSz csak írott és hitelesített formában módosítható, a Nemzeti Hírközlési Hatóság által vezetett tanúsítványtípus nyilvántartásban való átvezetés mellett.

A jelen HSzSz a Szolgáltató fokozott biztonságú szolgáltatásának befejezésével tekintendő megszűntnek.

2.4.2.4. Értesítések

Az Előfizetők, az Érintett felek vagy bármely harmadik fél az Ügyfélkapcsolati Irodát naponta 9-13 óráig megkeresheti személyesen telefonon, írásban, e-mail-ben vagy faxon. Naponta 24 órás szolgálattal áll rendelkezésre telefonos vagy e-mail megkeresés esetén a Szolgáltató Ügyfélszolgálata (Help Desk-je). Az írásban vagy elektronikus úton történő kommunikáció esetében a feladó nevét és elérhetőségét fel kell tüntetni és a feladónak a küldeményt hitelesítenie kell.

A Szolgáltató az Előfizetőket és Érintett feleket tipikusan a web oldalain, illetve az Ügyfélkapcsolati szolgálaton történő közzététellel tájékoztatja. Az Előfizetőket esetenként írásban vagy elektronikus úton is értesítheti.

2.4.3. Vitás kérdések kezelése

Bármely vitás kérdés felmerülése esetén az Előfizetőnek, az Érintett félnek, vagy bármely harmadik félnek kötelessége a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása a kérdés minden vonatkozását érintően, a vita jogi útra terelése előtt.

A panaszt az Előfizetőt nyilvántartó Ügyfélkapcsolati Irodán vagy az Ügyfélszolgálatnál (Help Desk-nél) lehet írásban vagy szóban előterjeszteni. A panasz előterjesztésétől számított 10 munkanapon belül a Szolgáltató kivizsgálja azt és írásban válaszol.

A szerződő felek kölcsönösen megállapodnak abban, hogy jogvitáikat mindenkor megkísérlik békés úton tárgyalások útján rendezni. Amennyiben ez az egyeztetés kezdetétől számított 30

napon belül nem vezet eredményre, arra az esetre a Felek kölcsönösen alávetik magukat a Kereskedelmi és Iparkamara mellett szervezett Állandó Választott Bíróság kizárólagos illetékességének. A Választott Bírósági eljárás nyelve a magyar, az eljárásban irányadó jog a mindenkor hatályos magyar anyagi és eljárásjog.

A jelen HSzSz-ben nem szabályozott kérdésekben a mindenkor hatályos magyar jogszabályok rendelkezései irányadók, különös tekintettel a Polgári Törvénykönyv, az elektronikus aláírásról szóló 2001. évi XXXV. törvény, az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról, valamint az 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. törvény módosításáról törvények rendelkezésire. Jelen HSzSz-ben szereplő kifejezéseket és jogintézményeket a magyar nyelv szabályi szerint, a szavak általánosan elfogadott mindennapi jelentése szerint, valamint a magyar jogszabályok alapján kell értelmezni.

2.5. Díjak

A mindenkor érvényes szolgáltatási díjakat a Szolgáltató a *„http://www.mavinformatika.hu/ca/”* web oldalon keresztül teszi közzé. A Szolgáltató jogosult az árlistát egyoldalúan módosítani.

A módosítást Szolgáltató köteles a fenti web oldalon közzétenni. Az előfizetőkre vonatkozó hatályos szolgáltatási díjak az Előfizetői Szerződésben kerülnek rögzítésre.

A módosított árlista a közzétételt illetve az értesítést követő 15. napon lép hatályba. Azok az előfizetők, akik a módosítást nem fogadják el, jogosultak az Előfizetői Szerződésüket legkésőbb a módosítás életbe lépésének napjáig 30 napos felmondási idővel felmondani. A szerződés felmondása egyben a kiadott Tanúsítvány iránti visszavonási kérelemnek is tekintendő és a Szolgáltató jogosult a Tanúsítványt Címtárából törölni.

A Szolgáltató a következő pontokban ismertetett díjtípusokat ajánlja fel az Előfizetőnek.

2.5.1. Tanúsítvány kibocsátás és megújítás

Szolgáltató a kibocsátott tanúsítványokért éves fenntartási díjat számol fel az Előfizető felé, amely tartalmazza a tanúsítvány kibocsátásának, Címtárban történő közzétételének az érvényesség időtartamára, valamint lejárat utáni archiválásának a díját.

2.5.2. Tanúsítvány hozzáférés

Szolgáltató a közzétett tanúsítványok eléréséért nem számol fel díjat az érintett felek irányában.

2.5.3. Visszavonás és állapot információ hozzáférés

Szolgáltató a közzétett visszavonási információ eléréséért nem számol fel díjat az érintett felek irányába.

2.5.4. Egyéb szolgáltatásokra vonatkozó díjak

Szolgáltató a kibocsátott tanúsítványok visszavonásáért, felfüggesztéséért és újraérvényesítéséért eljárási díjat számol fel az Előfizető felé, mely tartalmazza a tanúsítvány megváltozott állapotának a címtárban visszavonási lista formájában történő közzétételének díját. Újraérvényesítésért csak abban az esetben számít fel a Szolgáltató díjat, ha a felfüggesztést az Aláíró vagy az Előfizető kérte.

2.5.5. Visszatérítési elvek

Az Előfizető a számára kibocsátott Tanúsítvány éves fenntartási díjának visszakérésére a következő esetekben jogosult:

- a kibocsátott Tanúsítvány valamely adata a Szolgáltató hibájából fakadóan nem megfelelő,
- a kibocsátott Tanúsítvány, magánkulcs és aktivizáló adat nem összetartozó,
- a kibocsátott Aláírás-létrehozó eszközön szereplő adatok a Szolgáltató hibájából fakadóan nem megfelelők,[14]
- a kibocsátott Aláírás-létrehozó eszköz, az aktivizáló kód és a kulcsok nem összetartozók,
- a Szolgáltató egyéb hibát követ el a tanúsítvány kibocsátásakor,
- a Szolgáltató bizonyítottan nem tartja be valamely kötelezettségét Előfizető tanúsítványának kezelésekor.

A díj visszatérítésére előfizetőnek a tanúsítvány kibocsátását, illetve megújítását követő 30 naptári napon belül a regisztrációt végző regisztráló szervezetnél kérvényt[15] kell beadnia szolgáltató részére. A kérvény pozitív elbírálása esetén a Szolgáltató a Tanúsítványt díjmentesen

[14] Pl. a kártya fizikai megszemélyesítése nem megfelelő.
[15] Erre vonatkozóan a Szolgáltatónak formanyomtatvánnyal rendelkezik.

visszavonja és a fenntartási díjat az Előfizető számára a megjelölt bankszámlaszámra 20 naptári napon belül visszautalja.

A Tanúsítvány kibocsátását, illetve megújítását követő 30 naptári napon túl az Előfizető kizárólag csak a Szolgáltató bizonyított szerződés- vagy kötelezettségszegése esetén jogosult díjvisszafizetésre.

Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

2.6. Közzététel

2.6.1. Szolgáltatói információk közzététele

A Szolgáltató gondoskodik arról, hogy a tanúsítványok és az azokhoz kapcsolódó kikötései és egyéb feltételei az előfizetők és az érintett felek rendelkezésére álljanak. Különösképpen:

- a kibocsátott előfizetői és szolgáltatói tanúsítványok (tanúsítványtár közzététele),
- a visszavont előfizetői és szolgáltatói tanúsítványok (visszavonási lista – CRL - közzététele),
- A Szolgáltató, az Előfizetők és az Érintett felek rendelkezésére bocsátja a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, köztük az alábbiakat:
  - az alkalmazott tanúsítványtípus, beleértve egy egyértelmű nyilatkozat arra vonatkozóan, hogy a tanúsítványtípus a nyilvánosság részére kibocsátott tanúsítványokra vonatkozik, és hogy megköveteli-e bármilyen speciális termék, alkalmazás vagy eszköz használatát a kibocsátandó tanúsítvánnyal összekapcsolt kulcspár alkalmazására,
  - a tanúsítványok használatára vonatkozó bárminemű korlátozás,
  - az Előfizető kötelezettségei a 2.1.7 alfejezetben meghatározottaknak megfelelően,
  - a tanúsítvány ellenőrzésének mikéntjére vonatkozó információ, beleértve a tanúsítvány visszavonási állapot ellenőrzésére vonatkozó követelményeket, oly módon, hogy az Érintett fél "ésszerű módon hagyatkozhasson" a tanúsítványra (lásd 2.1.8),
  - a felelősség vállalásra vonatkozó bármilyen korlátozást, beleértve azokat az okokat/ használatokat, amelyek esetén a Szolgáltató elfogadja, illetve visszautasítja a felelősség vállalását (lásd 2.3),
  - az az időtartam, amíg a regisztrációs információt (lásd 4.6) megőrzik,
  - az az időtartam, amíg a Szolgáltató eseménynaplóját (lásd 4.5.3) megőrzik,
  - reklamációkra és viták rendezésére vonatkozó eljárások (lásd 2.4.3),

- az alkalmazandó jogi rendszer (lásd 2.4.1) és
- az, hogy a Szolgáltatónak az adott tanúsítványtípusnak való megfelelősége értékelésre került-e, s hogy ez milyen tanúsító rendszeren keresztül történt (lásd 2.7).

♦ A Szolgáltató elérhetővé teszi az előző pontban meghatározott információkat web oldalain keresztül, közérthetően megfogalmazva, elektronikusan továbbítható formában.

Tanúsítványok nyilvánosságra hozatala keretében a Szolgáltató gondoskodik arról, hogy a tanúsítványok szükség esetén az ügyfelek (előfizetők, alanyok és az érintett felek) rendelkezésre álljanak.

Részletesebben:

♦ az előállítás után a teljes és pontos tanúsítvány rendelkezésre áll azon Előfizető vagy Aláíró számára, akinek a Tanúsítvány kibocsátásra került,
♦ a tanúsítványok csak azokban az esetekben érhetők el más számára, ha az előfizető és az alany hozzájárult ehhez,
♦ a Szolgáltató az érintett felek rendelkezésére bocsátja a Tanúsítvány használatával kapcsolatos kikötéseket és feltételeket,
♦ egy adott Tanúsítvánnyal kapcsolatban a vonatkozó kikötések és feltételek könnyen azonosíthatók.

A tanúsítvány visszavonásának és felfüggesztésének nyilvánosságra hozatala keretében a Szolgáltató gondoskodik arról, hogy hiteles és érvényes tanúsítvány visszavonási kérelmek esetén a tanúsítványok időben visszavonásra, s ezen információ nyilvánosságra kerüljön. Részletesebben:

♦ a Szolgáltató a HSzSz-ében dokumentálja a tanúsítványok visszavonásának eljárásait, beleértve az alábbiakat:
  - a visszavonási állapot információk nyilvánosságra hozatalánál használt mechanizmusok,
  - a legnagyobb késedelem a visszavonási kérelem fogadása, és az összes érintett fél rendelkezésére álló információk állapotának megváltozása között;
♦ tájékoztatja a visszavont, illetve felfüggesztett tanúsítvány tulajdonosát (ahol ez alkalmazható, az előfizetőt is) tanúsítványa állapotának megváltozásáról,
♦ biztosítja, hogy a tanúsítvány visszavonási listákra teljesüljenek az alábbiak:

- minden egyes visszavonási lista tartalmazza a következő visszavonási lista kibocsátási időpontját,
- új visszavonási lista közzétehető a következő visszavonási lista kibocsátására megadott időpont előtt is,
- a visszavonási listát a hitelesítő szervezet a Szolgáltató nevében elektronikusan aláírja.

A Szolgáltató információ közzétételi kötelezettségét az alábbiak szerint teljesíti:

- Legalább két országos napilapban és az 1.2 pontban megadott web lapon hirdetést jelentet meg a szolgáltatás beindításáról az 1. szintű Hitelesítő Központ tanúsítványának aláírásával, a szolgáltatás beszüntetéséről, új tanúsítvány típus, osztály vagy fajta bevezetéséről, valamint magánkulcsának kompromittálódásáról amennyiben ilyen esemény bekövetkezik.

  A Szolgáltató az általa működtetett hitelesítő egységek tanúsítványát a következő módszerekkel teheti közzé:

  - Az 1. szintű Hitelesítő Központ („root”; önhitelesített) tanúsítványát a http://www.trust-sign.mavinformatika.hu web lapon teszi közzé. A "root" tanúsítványok esetében ez az egyetlen módszer tekinthető hivatalos formának.
  - Minden nyilvános Hitelesítő Központ tanúsítványát közzé teszi Címtárában, valamint Internetes honlapján keresztül.
  - Az egyes Hitelesítő Központok tanúsítványa beépítésre kerülhet különböző alkalmazásokba.
  - Az Előfizető részére a végfelhasználói tanúsítvánnyal együtt átadja (lásd 4.2 pont!).
- A Szolgáltató a Címtárban (Tanúsítványtárban) tárolja és internetes honlapon teszi elérhetővé a kibocsátott előfizetői és szolgáltatói tanúsítványokat, köztük a Root CA és a produktív Hitelesítő Központok tanúsítványait, valamint a tanúsítvány visszavonási listákat (CRL).
- A Szolgáltató saját web oldalain keresztül elérhetővé teszi a HSzSz-t, az ÁSzF-et, az egyéb nyilvános szabályzatokat, valamint a Regisztrációs szervezetek listáját, elérhetőségét az 1.2 pontban megadott elérhetőséggel.
- Szolgáltatónak csak saját elektronikus aláírásával ellátott dokumentumai tekinthetőek eredetinek. A dokumentumok nyomtatott változatai semmilyen formában sem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokat a következő módszerekkel teszi közzé:

- A kérelmező Aláíró részére elküldi védett kommunikációs protokollt alkalmazva.
- Az Aláíró részére átadja az aláírás-létrehozó eszközön.
- Az érintett felek részére közzéteszi a nyilvános Címtárában, amennyiben ehhez az Aláíró és az előfizető hozzájárult (a hozzájárulás formája a tanúsítványigénylő űrlapon ennek írásos jelölése).

A Szolgáltató az általa működtetett Hitelesítő Központok tanúsítványával kapcsolatos állapot információkat a következő módszerekkel teszi közzé:

- Az 1. szintű Hitelesítő Központ tanúsítványának állapotváltozásáról egy országos terjesztésű napilapban tesz közzé hirdetést. A gyökér tanúsítványok esetében ez az egyetlen módszer tekinthető hivatalos formának.
- A 2. szintű Hitelesítő Központok tanúsítványának állapotváltozását a Címtárában hozza nyilvánosságra.

A Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokkal kapcsolatos állapot információkat a Címtárában hozza nyilvánosságra.

2.6.2. A közzététel gyakorisága

- A Szolgáltató a kibocsátott tanúsítványokat a Tanúsítványtárban (Címtárban) publikálja a 2.6.4 pontban megadott elérhetőséggel. A Tanúsítvány visszavonási listát a 4.4.9 pontnak megfelelő gyakorisággal tesz közzé.
- A Szolgáltató a HSzSz-ben és az ÁSzF-ben tervezett változásokról a hatályba lépést megelőzően 30 nappal tájékoztatja a Nemzeti Hírközlési Hatóságot, s a változásokkal egységes szerkezetbe foglalva közzéteszi egyéb nyilvános szabályzatait pedig a hatályba lépést megelőző 30 nappal hozza nyilvánosságra.
- A Szolgáltató az egyes tanúsítványok nyilvánosságra hozatala kapcsán a következő gyakorlatot követi:
  - Az általa működtetett root hitelesítő egységek tanúsítványát a kibocsátást követő 10 munkanapon belül teszi közzé.
  - Az általa működtetett felhasználói hitelesítő egységek tanúsítványai a címtárában 24 órán belül, Internetes honlapján 5 munkanapon belül megjelennek.

- A Hitelesítő Központok tanúsítványának alkalmazásokban való megjelenése esetleges. Amennyiben erre vonatkozó megállapodás történik, arról a Szolgáltató http://trust-sign.mavinformatika.hu web lapján 15 munkanapon belül értesítést tesz közzé.
- A Szolgáltató a végfelhasználói tanúsítványokat a kibocsátást követően, a regisztrációs eljárás részeként átadja az Előfizető részére.
- A Szolgáltató a végfelhasználói tanúsítványokat a Címtárában az előállítást követően 24 órán belül teszi közzé.

2.6.3. Elérési szabályok

♦ A Szolgáltató belső adatbázisait és egyéb adatállományait csak és kizárólag a Szolgáltató Biztonságpolitikája és Biztonsági Szabályzata által meghatározott szerepkörű és jogosultságú munkatársai érhetik el egyénileg differenciált erős azonosítás-hitelesítési és feljogosítási eljárás után.

A Szolgáltató minden Előfizető és Érintett fél számára elérhetővé teszi web oldalait és Címtárát olvasás céljából. A Címtárban keresési lehetőséget biztosít a tanúsítvány sorszáma és az azonosítója alapján. A Címtár és a web oldalak tartalmát csak és kizárólag a Szolgáltató módosítja.

A visszavonásra vonatkozó kérelmeket hitelesíteni kell, ezért a Szolgáltató feldolgozás előtt ellenőrzi, hogy hiteles forrásból származnak-e. Az ilyen jellegű kérelmeket meg kell erősíteni.

A Szolgáltató a nyilvánosságnak bocsát ki tanúsítványt, ezért a visszavonási állapotokat tartalmazó tanúsítvány visszavonási listák nyilvánosak, szabványos felületen bárki által elérhetők.

A Szolgáltató belső adatbázisait és egyéb adatállományait csak és kizárólag a Szolgáltató Biztonságpolitikája és Biztonsági Szabályzata által meghatározott szerepkörű és jogosultságú munkatársai érhetik el egyénileg differenciált erős azonosítás-hitelesítési és feljogosítási eljárás után.

2.6.4. Címtár

A Szolgáltató a tanúsítványokat, a tanúsítványok használatára vonatkozó kikötéseket és feltételeket, valamint a tanúsítvány visszavonási listákat címtárán keresztül teszi hozzáférhetővé.

Az Aláíró vagy az Érintett fél a *http://trust-sign.mavinformatika.hu* web lapon érheti el a Címtárat.

2.7. A megfelelőség vizsgálata

A Szolgáltatót fokozott biztonságú szolgáltatóként 2002. október 30.-án a Nemzeti Hírközlési Hatóság nyilvántartásba vette.

A Nemzeti Hírközlési Hatóság a Szolgáltató bejelentése alapján a jelen dokumentumban megnevezett tanúsítványtípusokat nyilvántartásába felvette.

A Szolgáltató olyan elektronikus aláírási termékeket használ „elektronikus aláírás hitelesítés-szolgáltatás" szolgáltatásához (kulcspárok előállításához, a kibocsátott tanúsítványok és tanúsítvány visszavonási listák aláírásához, valamint az ehhez szükséges magánkulcsok tárolásához), amelyek szerepelnek a Nemzeti Hírközlési Hatóság „tanúsított elektronikus aláírási termékek" listáján. Konkrét ismertetésük a HSzSz 6.1.7 és 6.2.1 pontjaiban található.

A Szolgáltató az „Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezése" szolgáltatásához olyan Aláírás -létrehozó eszközt használ fel, mely szerepel a Nemzeti Hírközlési Hatóság „tanúsított elektronikus aláírási termékek" listáján. Konkrét ismertetésük a HSzSz 6.1.7 és 6.2.1 pontjaiban található.

A Szolgáltató a hitelesítő tevékenységét és a hitelesítés szolgáltatást támogató informatikai rendszert, valamint annak személyi és fizikai környezetének biztonságát auditáltatja:

1. a saját szervezetén belüli, a Szervezeti és Működési Szabályzatban megjelölt, nem a Szolgáltató alá rendelt, belső auditor szervezettel,
2. független külső auditor céggel.

A Szolgáltató szolgáltatási rendszerének következő elemeit vizsgáltatja:

- az Aláírás-létrehozó eszközét, melyet magánkulcsainak tárolására használ.
- az Aláírás-létrehozó eszközöket, melyeket az előfizetők számára biztosít.
- A végfelhasználói és szolgáltatói tanúsítványok kezeléshez felhasznált elektronikus aláírási termékeit.
- A végfelhasználói és szolgáltatói tanúsítványok kezeléshez használt rendszereit és módszereit.

A vizsgálathoz a Szolgáltató külső szervezetet vesz igénybe (lásd 2.7.2 pont!). Szolgáltató e külső vizsgálatokon túl saját belső ellenőrzési rendszerrel is rendelkezik, amely rendszeresen vizsgálja a korábbi vizsgálatok jelentéseiben szereplő hiányosságok megszüntetését.

2.7.1. Vizsgálatok gyakorisága

A vizsgálatokat Szolgáltató a Szervezeti és Működési Szabályzatban, illetve a Biztonsági Szabályzatban megjelölt rendszerességgel, minimum évente egyszer megismételteti, azt a törvényi feltételek vagy szabályzataiban bekövetkezett jelentősebb változások esetén, döntése alapján, soron kívül elvégezteti.

2.7.2. Az átvizsgáló szervezet megnevezése/jellemzői

A belső hitelesítési tevékenységre és az informatikai biztonságra vonatkozó auditot a Szolgáltató informatikai biztonsági menedzsere, a külső auditot a Szolgáltató olyan, széles körben ismert auditor céggel végezteti el, amely szakértelmét bizonyítani tudja a nyilvános kulcsú infrastruktúra, és informatikai biztonság, valamint az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában.

Az auditot a fokozott biztonságú hitelesítés szolgáltatás regisztrációja előtt az EDIPORT Kft. végezte el. Ezután a rendszeres auditálások a HSzSz 6.5.2 pontja szerinti rendben történnek.

2.7.3. Az átvizsgáló szervezet és a vizsgált fél kapcsolata

A belső auditot a Szolgáltató hitelesítés szolgáltatást végző szervezeti egységétől független informatikai biztonsági menedzser, a külső auditot nyilvános kulcsú infrastruktúra illetve informatikai biztonsági termék és szállítótól független külső auditor cég végzi el**.**

2.7.4. A vizsgálatok kiterjedése

Az auditorok két fő területet, a hitelesítés szolgáltatás és az informatikai biztonság területét vizsgálják, abból a szempontból, hogy Szolgáltató hitelesítő és biztonsági rendszere, annak személyi és fizikai környezete megfelel-e a mindenkori hatályos törvényi előírásoknak, valamint a Szolgáltató saját szabályzatainak, első sorban a Tanúsítvány politikáknak, a HSzSz-nek, a Biztonságpolitikának és a Biztonsági Szabályzatnak.

2.7.5. Hiányosságok kezelése

A Nemzeti Hírközlési Hatóságtól rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltató késlekedés nélkül megszünteti a vizsgálatot végző Nemzeti Hírközlési Hatóságtól kapott információ és ajánlások alapján.

A Szolgáltató által kezdeményezett auditok vizsgálati jelentést a Szolgáltató vezetőjének és a Hitelesítési Politika és Szabályozási Csoportnak nyújtja be.

A jelentésben megállapított hiányosságok következménye két szintű lehet:

1. A hiányosságok nem sértik alapvetően a Szolgáltató tevékenységébe vetett bizalmat, vagy az informatikai biztonságot. A Szolgáltató változatlan formában folytatja tevékenységét, de köteles a hiányosságokat 30 napon belül megszüntetni. A hiányosságok megszüntetésére vonatkozó konkrét intézkedéseket a Hitelesítési Politika és Szabályozási Csoport dolgozza ki és ellenőrzi a végrehajtásukat. Az intézkedéseket a Szolgáltató első számú vezetője hagyja jóvá.

   Amennyiben a korrekciós intézkedések 30 napon belül nem kerülnek végrehajtásra, akkor a Szolgáltatónak a hiányosságok által érintett funkcióit, tevékenységét fel kell függesztenie az intézkedések ellenőrzésének befejezéséig. Amennyiben ez a létrehozandó aláírás létrehozó adatok, eszközök biztonságát vagy a tanúsítványok, visszavonási listák hitelességét veszélyezteti, akkor ezen tevékenységet és a tanúsítványokat fel kell függeszteni.

2. Amennyiben a hiányosságok alapvetően érintik a Szolgáltató egyes tevékenységeit, vagy az informatikai biztonság egyes területeit, a Szolgáltatónak fel kell függesztenie a hiányosságok által érintett tevékenységeit a hiányosságok megszüntetéséig. Amennyiben ez a létrehozandó aláírás létrehozó adatok, eszközök biztonságát vagy a tanúsítványok, visszavonási listák hitelességét veszélyezteti, akkor ezen tevékenységet és a kibocsátott tanúsítványokat fel kell függeszteni. A hiányosságok megszüntetésére vonatkozó konkrét intézkedéseket a Hitelesítési Politika és Szabályozási Csoport dolgozza ki és ellenőrzi a végrehajtásukat. Az intézkedéseket a Szolgáltató első számú vezetője hagyja jóvá.

3. Amennyiben a hiányosságok a Szolgáltatóba vetett bizalmat alapvetően megingatják, a teljes tevékenységét fel kell függeszteni és a kibocsátott tanúsítványokat vissza kell vonni.

2.7.6. Eredmény kommunikációja

A Hitelesítési Politika és Szabályozási Csoport javaslatot tesz arra, hogy az audit jelentés mely részei tekinthetők publikusnak. A javaslatot a Szolgáltató vezetője hagyja jóvá. A teljes jelentés belső használatra szolgáló anyag. Azt a Szervezeti és Működési Szabályzatban meghatározott szervezeti egységek vezetői kapják meg. A publikus részt a Szolgáltató a *http://www.mavinformatika.hu/ca/* web oldalon teszi közzé.

A Szolgáltató nem köteles a feltárt konkrét hiányosságokat nyilvánosságra hozni, s azok nem adhatnak alapot a Szolgáltató kötelezettségszegésének bizonyítására. Szolgáltató nem tartozik kártérítési felelősséggel az általa elvégeztetett vizsgálatok alapján feltárt hibák után.

2.8. Bizalmasság – Adatkezelési szabályzat

2.8.1. Bizalmas információk

A Szolgáltató gondoskodik a jogszabályoknak való megfelelésről. Ennek keretén belül:

- A fontos bejegyzéseket védi az elveszéstől, tönkretételtől és hamisítástól. A jogszabályoknak való megfelelés, valamint az alapvető üzleti tevékenységek támogatása érdekében szükség van bizonyos bejegyzések biztonságos megőrzésére is. (lásd 4.6),
- gondoskodik az adatvédelmi törvényeknek való megfelelésről,
- megfelelő technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénytelen kezelése ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen,
- nyilvántartásba veszi az előfizetővel aláírt megállapodást, beleértve az alábbiakat:
  - hozzájárulás az alábbi szolgáltatások során felhasznált információ hitelesítés-szolgáltató által történő nyilvántartásba vételéhez: regisztrálás, az alanyok eszközzel való ellátása, esetleges későbbi visszavonás,
  - hozzájárulás a nyilvántartásba vett információ harmadik félhez történő továbbításához, a Szolgáltató szolgáltatásainak leállítása esetén, az erre az esetre vonatkozó szabályzat megkövetelt feltételei szerint,
  - hogy az előfizető megköveteli-e és az alany hozzájárul-e a tanúsítvány közzétételéhez és milyen feltételek mellett,

- gondoskodik arról, hogy a regisztrációs eljárás során az adatvédelmi jogszabályok követelményeit figyelembe vegyék,
- ellenőrzési politikája csak annyi bizonyítékot követel meg az azonosításhoz, mely elégséges a tanúsítvány tervezett felhasználásához,
- gondoskodik az Aláíróra vonatkozó információ bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk[16] hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja,
- védi a regisztrációs adatok bizalmasságát (és sértetlenségét) az előfizetővel/alannyal folytatott, illetve a hitelesítő szervezet – regisztráló szervezet – címtár rendszerkomponensek közötti adatcsere során is.

A legmagasabb érzékenységi szintet bizalmasság szempontjából az Aláírók és a hitelesítés szolgáltatók aláírás létrehozó adatai képezik, ezen belül a legérzékenyebb a szolgáltatói Aláírás létrehozó adat, mert kompromittálódása a Szolgáltató tevékenységének azonnali felfüggesztésével jár. Ezért ezeket az adatokat, illetve az ezeket hordozó eszközöket fokozott biztonsággal kell tárolni és használni. Az Aláírás létrehozó adat biztonságáért a teljes felelősséget az adat tulajdonosa viseli.

A Szolgáltató tevékenysége során a következő bizalmas adatköröket kezeli:

1. a Szolgáltató üzleti titkai,
2. más Társaságok által a Szolgáltatónak átadott üzleti titkok,
3. az Előfizetők, az Aláírók és a saját munkatársainak személyes adatai.

Az 1. és 2. pontokban meghatározott üzleti titkok kezelésére az 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról és a Szolgáltató Titokvédelmi Szabályzata mérvadó. Így például egyik szerződő fél sem jogosult az Előfizetői Szerződés teljesítése kapcsán tudomására jutott bármely adatot, tényt, információt, tervet vagy dokumentumot a másik fél előzetes írásbeli hozzájárulása nélkül harmadik személynek átadni.

A felek az üzleti titok megsértésével okozott kárért a polgári jog általános szabályai szerint felelnek.

[16] vagy nevükben az Előfizető

A személyes adatok vonatkozásban az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról és az 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. törvény módosításáról szóló törvény.

A Fentiek értelmében a Szolgáltató az Előfizetők és az Aláírók személyes adatait csak a közöttük fennálló Előfizetői Szerződéssel összhangban levő célokra használhatja fel, harmadik félnek azokat az Előfizetők és az Aláírók írásos hozzájárulása nélkül nem adhatja át, kivéve a 2.8.4 pontban meghatározott eseteket. A Szolgáltató a birtokába került személyes adatokat az adott adat rögzítéséhez kapcsolódó tanúsítvány lejártát, illetve a tanúsítvánnyal összefüggésbe hozható jogi eljárás lezárását követő 10 évig (2001. évi XXXV. törvény 9.§ (7.) bek.) őrzi meg.

Az Előfizető és az Aláíró a tanúsítvány igénylésével hozzájárul ahhoz, hogy a Szolgáltató személyes adatait (a Titokvédelmi és a Biztonsági Szabályzatainak megfelelő módon) tárolja és kezelje. A hozzájárulás egyaránt vonatkozik az adatok alannyal és előfizetővel való megosztására (ha a két fél különbözik), s nyilvántartásba vett információk harmadik félhez történő továbbítására, a szolgáltató szolgáltatásainak leállítása esetén[17]. A tanúsítványigénylő űrlapon az Előfizetőnek és az Aláírónak jeleznie kell a tanúsítvány nyilvánosságra hozatalához történő egyhangú hozzájárulását. Szolgáltató az előfizetői adatokat kizárólag csak a hitelesítési-szolgáltatással összefüggésben használja fel.

A Szolgáltató által kezelt adatok egy része a tanúsítványba foglalva, valamint a Szolgáltató címtárán keresztül nyilvánosságra kerül a nyilvános kulcs tulajdonosának azonosítása céljából, másik részét a Szolgáltató védett módon tárolja az Előfizető és az Aláíró azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából

2.8.2. Nem bizalmas információk

A Szolgáltató nem bizalmas információként kezeli mindazon adatokat, melyet a tanúsítványba belefoglal[18]. Az Előfizető és az Aláíró tudomására kell hozni szerződéskötéskor, hogy mely személyes adatai fognak a Címtárban hozzáférhető tanúsítványokban szerepelni és a regisztrációs lapon ezeket külön jelölni kell.

[17] 2001. évi XXXV. Törvény az elektronikus aláírásról 16. § (2) bek.

[18] Függetlenül attól, hogy az Előfizető hozzájárul-e (az Aláíró nevében) a tanúsítvány nyilvánosságra hozásához.

Nem bizalmas információk, adatok még azok a Szolgáltatóhoz kapcsolódó adatok is, amelyeket a Szolgáltató vezetője publikusnak minősít, illetve amelyekről a hatályos jogszabályok így rendelkeznek, pl. az ÁSzF és a HSzSz.

2.8.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése

A Szolgáltató az általa kibocsátott tanúsítványok visszavonását és felfüggesztését tanúsítvány-visszavonási listákban (CRL[19]) teszi közzé, a 7.2 pontban meghatározott tartalommal, jellemzőkkel, illetve az ezekben általa támogatott keresési lehetőségekkel.

A Szolgáltató a tanúsítvány visszavonás okát feltünteti a visszavonási listában. Ezen kívül a visszavonással kapcsolatos minden egyéb információt, adatot bizalmasan kezel.

2.8.4. Feltárás törvényi meghatalmazással rendelkezők részére

A Szolgáltató az elektronikus aláírás felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az érintett személyazonosságát igazoló adatok tekintetében - a 2001. évi XXXV. törvény 11.§ paragrafusa alapján adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak.

Az adatátadás tényét rögzíteni kell, az adatátadásról a Szolgáltató az Aláírót nem tájékoztathatja.

2.8.5. Feltárás törvényi meghatalmazással rendelkezők részére

A Szolgáltató a Tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az aláíró személyazonosságát igazoló adatokat átadhatja az ellenérdekű peres félnek vagy képviselőjének feltárhat bizalmas felhasználói információkat, illetőleg azt közölheti a megkereső bírósággal a 2001. évi XXXV. törvény 11.§ paragrafusa alapján.

A Szolgáltató rögzíti az információszolgáltatás tényét, és arról tájékoztatja az Előfizetőt és az Aláírót.

[19] CRL: Certification Revocation List

2.8.6. Feltárás tulajdonos kérésére

Szolgáltató a törvényi meghatalmazással rendelkezők részére történő adatszolgáltatáson túl más Társaság üzleti titkát, az Előfizetők és az Aláírók nem nyilvános személyes adatait csak az Illető Társaság illetve Előfizető írásos (hagyományos vagy elektronikus aláírással ellátott) meghatalmazása alapján tárhatja fel harmadik fél részére.

2.8.7. Feltárás más esetekben

Szolgáltatónak tevékenysége befejezésekor nyilvántartásait, a bizalmas adatokkal együtt, át kell adnia más - vele azonos besorolású – szolgáltató részére a 2001. évi XXXV. törvény 16. § (2.) bek. szerint.

2.9. Szellemi tulajdonhoz fűződő jogok

A Szolgáltató által ügyfelei részére kibocsátott Tanúsítvány és az ennek megfelelő kulcspár tulajdonosa az Előfizető, teljes jogú használója pedig az Aláíró, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

A Szolgáltató a Tanúsítványt a kikötéseiben és feltételeiben ismertetett módon közzéteheti, sokszorosíthatja, visszavonhatja, s egyéb módon kezelheti.

A visszavonási információ a Szolgáltató tulajdonát képezi.

A Szolgáltató által az alany részére kibocsátott egyedi azonosító a Szolgáltató tulajdonát képezi.

A Tanúsítványban szereplő megkülönböztető név használatára a megnevezett alany jogosult.

Az Aláíró egyedi azonosítójában szereplő bármilyen védjegy, szervezeti- és személynév, vagy egyéb adat az Előfizető vagy az Aláíró tulajdonát képezheti.

A Szolgáltató szabályzatai, szerződéses feltételei a Szolgáltató tulajdonát képezik.

A tanúsítványban szereplő hitelesítő azonosító a Szolgáltató tulajdonát képezi.

3. Azonosítás és hitelesítés

3.1. Kezdeti regisztráció

A Szolgáltató a kezdeti regisztrálás során:

- gondoskodik arról, hogy az Előfizető tanúsítvány kérelmei pontosak, hitelesek és teljesek legyenek;
- megfelelő, illetékes források igazolásán alapulva megvizsgálja az alanyok és előfizetők azonosságára vonatkozó bizonyítékokat, valamint nevük és a hozzá kapcsolódó adatok pontosságát.

3.1.1. Nevek típusa

A tanúsítványokban szereplő név (Hitelesítés szolgáltató, illetve Aláíró név) megadás az ITU-T X.500 „Information Technology - Open Systems Interconnection - The directory: Overview of concepts, models and services" ajánlása (továbbiakban X.500) egyedi név formátum (Distinguished Name form) előírásainak felel meg.

3.1.2. Név jelentése, szemantikája

A tanúsítványban szerepeltetendő nevek megadásakor a következő szabályok szerint kell eljárni:

- álnevek használata megengedett, jelölése: „~álnév~" formátumú,
- a személyek nevének felvétele során a személyi igazolványban vagy az útlevélben szereplő írásmód kerül követésre, azaz a Tanúsítványba az azonosítás-hitelesítés alapjául szolgáló dokumentumban szereplő név kerül névmegadásként; ettől eltérő névmegadás álnévnek minősül,
- az azonosító nem tartalmazhat olyan speciális karaktereket, amelyek megjelenítése az általánosan használt ügyfél alkalmazásokban nem lehetséges helyesen,
- az azonosító mezői esetében a magyar ABC ékezetes karakterei helyett azok ékezet nélküli megfelelőit kell használni.

3.1.3. Különböző névmegadási formák értelmezési szabályai

A nevek formátumát az 1.4.2 fejezetben meghatározott tanúsítványfajták névmegadási szabályaival adtuk meg.

A névmegadási formák értelmezése érdekében érintett feleknek a jelen HSzSz 1.4.2 és 3.1.1 pontjaiban leírtak alapján kell eljárniuk. Amennyiben a névmegadási formák, illetve a Tanúsítványban foglalt adatok értelmezésével kapcsolatban az Érintett félnek segítségre lenne szüksége, akkor a Szolgáltatóval közvetlenül is felveheti a kapcsolatot.
A Szolgáltató ilyen esetben az Aláíró és az Előfizető egyéb adatairól többlettájékoztatást nem ad, csak a Tanúsítványban feltüntetett adatok értelmezését segítő információt.

3.1.4. Nevek egyedisége

A Szolgáltató biztosítja címtárában a tulajdonosazonosítók egyediségét. Erről elsődlegesen az Aláíró e-mail címének a névmegadásban való szerepeltetése gondoskodik. A Szolgáltató a név azonosító kiosztásakor ellenőrzi, hogy az adott e-mail cím nem szerepel-e egy más személy részére korábban kibocsátott Tanúsítványban. Ha szerepel, és a Tanúsítvány név azonosítójának egyéb mezői sem biztosítják az egyediséget, akkor a Szolgáltató fenntartja magának a jogot a név olyan megváltoztatására, amely továbbra is jellemző az Aláíróra, de biztosítja a megkülönböztethetőséget.

A Szolgáltató biztosítja, hogy a teljes működési ciklusa alatt egy Tanúsítványban az általa használt megkülönböztetett nevet sohasem fogja egy másik egyedhez rendelni.

3.1.5. Név igénylési viták feloldása

Az Aláírót egyértelműen a tanúsítványban megadott név és a tanúsítvány sorozat száma különbözteti meg a többi Aláírótól. Ezen kívül a névmegadásnál a Common Name mezőben az Aláíró neve mellett az e-mail címet is szerepel, annak érdekében, hogy biztosított legyen a név megkülönböztetés, arra az esetre, ha tanúsítvány sorozat száma és az Aláíró neve nem elég ehhez.

Amennyiben e két adat nem biztosítja a megkülönböztethetőséget a Szolgáltató fenntartja magának a jogot a név olyan megváltoztatására, amely továbbra is jellemző az Aláíróra, de biztosítja a megkülönböztethetőséget.

Az Előfizetőnek egy bizonyos azonosítóra való igényét a tanúsítványkérelemben kell jeleznie. Az előfizetői azonosítók kiosztása a beérkezett tanúsítványkérelmek elbírálásának sorrendje szerint történik. Ha a kérelmezett azonosító már korábban kiosztásra került, a Szolgáltató az egyediséget szolgáló eljárásait követve eltérő azonosítót oszt ki.

A Szolgáltató – lehetőségei szerint – a névkiosztás során ellenőrzi az Aláíró jogosultságát a feltüntetett nevek használatára. Szolgáltató fenntartja magának a jogot az igényelt nevek kiosztásának visszautasítására. Jogszerűtlen név- vagy adathasználat miatt, amennyiben erre bíróság kötelezi, vagy másik fél megalapozott módon bizonyítani tudja jogosultságát, a Szolgáltatónak jogában áll visszavonni a kérdéses tanúsítványt.

3.1.6. Védjegyek elismerésének és hitelesítésének módszere

A tanúsítványkérelemmel az Előfizető kifejezi, hogy a benne foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik fél jogait. Szolgáltatónak nem kötelessége a védjegyek jogos használatának ellenőrzése, és nem vállal közvetítő vagy döntnöki szerepet ilyen jellegű viták feloldásában. Szolgáltató nem garantálja Előfizetők számára védjegyeik feltüntetését a tanúsítványban. Előfizető részéről egy védjegy megszerzése nem tekintendő olyan eseménynek, mely alapján a tanúsítvány megújítását kell, hogy kezdeményezze.

A Tanúsítvány Kibocsátó azonosítója a „Trust&Sign” védjegyet tartalmazza. A védjegy a hitelesítés-szolgáltató szervezet, a MÁV INFORMATIKA Kft. tulajdona.

3.1.7. Az Aláírás létrehozó adat birtoklás ellenőrzésének módszere

Az 1.4 pontban meghatározott összes tanúsítvány osztály és fajta szerinti kulcspár generálása a Szolgáltató Hitelesítő Központjában történik. Előfizetőnél kulcspár generálás csak a tesztcélú Aláírás létrehozó eszköz igénylése esetén valósul meg.

Központi kulcs generálás esetén az Aláírás létrehozó és az ellenőrző adat birtoklásának és egymáshoz tartozásának ellenőrzésére nincs szükség, csupán az Aláíróhoz eljutatott Aláírás létrehozó eszköz, illetve adat átvételének igazolására van szükség. Az Aláírás létrehozó eszköz személyes átvételénél az Előfizető írásban igazolja az Aláírás létrehozó eszköz és a PIN kód

átvételét. Az átvétel után az Előfizető teljes felelősséget visel az Aláírás létrehozó eszköz és a PIN kód biztonságos használatáért és megőrzésért.

3.1.8. Személyes azonosság hitelesítése „Személyes” tanúsítvány igénylése esetén

A természetes személy Igénylőnek (Előfizetőnek) a tanúsítványkérelemhez csatolnia kell a Szolgáltató által biztosított tanúsítványigénylő űrlapot kitöltve és aláírva.

A természetes személy hitelesítéséhez a következő adatokat kéri az Ügyfélkapcsolati Iroda:

- az Igénylő neve, aláírása,
- az Igénylő okmányszáma (személyi igazolvány vagy útlevél szám),
- az Igénylő lakcíme,
- az Igénylő e-mail címe.

Ezen adatokat személyi igazolvány vagy útlevél személyes bemutatásával kell hitelesíteni.

Az Ügyfélkapcsolati Iroda az átadott azonosító-hitelesítő dokumentumok érvényességének és hitelességének biztonságos megállapítása érdekében kiegészítő ellenőrzést végezhet a Szolgáltató Biztonsági Szabályzatában szabályozott módon.

Az Előfizető írásbeli nyilatkozatot ad arra vonatkozóan, hogy:

- a Tanúsítvány kibocsátásával és fenntartásával kapcsolatos és minden egyéb járulékos költséget vállal,
- a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat.

A Tanúsítvány kérelem nem fogadható el, amennyiben az okmányok személyhez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel.

3.1.9. Szervezeti identitás hitelesítése „Szervezeti személy” tanúsítvány igénylése esetén

Az igénylő szervezetnek (Előfizetőnek) a tanúsítványkérelemhez csatolnia kell a Szolgáltató által biztosított tanúsítványigénylő űrlapot kitöltve, és a szervezet képviseletére jogosult vezető tisztségviselőinek az aláírásával ellátva.

A szervezeti személy hitelesítéséhez a következő adatokat kéri az Ügyfélkapcsolati Iroda:

- az igénylő szervezet neve, székhelye,

- annak a szervezeti egységnek a megnevezése, ahol a szervezeti személy (továbbiakban: Aláíró) dolgozik,
- az Aláíró neve, aláírása,
- az Aláíró beosztása (az előfizető szervezet és szervezeti egység viszonya az Aláíróhoz)
- az Aláíró személyi igazolvány vagy útlevél száma,
- az Aláíró telefon száma, e-mail címe.
- az Aláírót megbízó dokumentum cégszerűen aláírva (a dokumentum tartalmazza a megbízó szervezet vagy szervezeti egység nevét, e-mail címét, telefon és fax számát),
- az előfizető szervezet egyértelmű hozzájárulása ahhoz, hogy:
  - a Tanúsítvány kibocsátásra kerüljön,
  - a szervezet vagy szervezeti egysége neve a Tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön,
  - az Aláíró neve a Tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön,
  - a Szolgáltató a kezdeti regisztráció során a szervezeti azonosság hitelesítésére elfogad minősített aláírással ellátott elektronikus okiratot is az Igénylőtől, abban az esetben, ha az Előfizetővel ebben előzetesen megegyezik. Ez esetben az Előfizető szervezeti azonosságának hitelesítése, s a szervezeti adatok felvétele a megegyezés során történik, az elektronikus okirat „már csak” az Előfizető hozzájárulását tartalmazza az Aláíró részére történő Tanúsítvány kibocsátásához,
  - az Előfizető kapcsolattartókat nevez meg a Szolgáltató részére, akik aláírási joggal rendelkeznek a Tanúsítvány kibocsátását illetően; a Szolgáltató később e személyeknek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén,
  - az előfizető szervezet kötelezettséget vállal arra, hogy:
    - a Tanúsítvány kibocsátásával és fenntartásával kapcsolatos és minden egyéb járulékos költséget vállal,
    - a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat.

A fentieken kívül még a következőket kell megadni:

- az Aláíró kijelölését engedélyező személy neve (az engedélyezőnek minden esetben cégképviseletre jogosult személynek kell lennie és ezt aláírási címpéldánnyal kell igazolni),
- az engedélyező személy beosztása,

- az engedélyező személy munkahelyi telefonszáma, fax-száma, e-mail címe.

Ezen adatokat a következő dokumentumokkal kell hitelesíteni:

- képviseleti megbízás cégszerűen aláírva,
- A Kapcsolattartó azonosítás-hitelesítése személyi igazolvány vagy útlevél bemutatásával személyesen
- Az Aláíró(k) azonosítás-hitelesítése személyi igazolvány vagy útlevél bemutatásával személyesen; A Szolgáltató eltekint az Aláíró(k) személyes azonosítás-hitelesítésétől abban az esetben, ha ezt az előfizető szervezet elvégezte és a képviseleti megbízásban írásban igazolja. Az Aláíró(k) azonosítás-hitelesítéséhez kapcsolódó minden felelősség ebben az esetben az előfizető szervezetre hárul.
- cégbíróságnál nyilvántartott gazdasági társaságok esetében 30 napnál nem régebbi cégkivonat,
- nem cégbíróságnál nyilvántartott szervezetek esetében a nyilvántartó szervezet igazolása, pl. alapítványok esetében Fővárosi Bíróság, egyéni vállalkozók esetében az illetékes önkormányzat, ügyvédek esetében az Ügyvédi Kamara, könyvvizsgálók esetében a Könyvvizsgálói Kamara,
  igazságügyi szakértők esetében az Igazságügyi Minisztérium, stb.,
- állam-, illetve közigazgatási szervezetek esetében az alapító dokumentum közjegyzővel hitelesített másolata, amelyet a szervezet első számú vezetőjének írásos nyilatkozata kísér,
- aláírási címpéldány, amely a szervezet aláírásra jogosult vezetőinek nevét és aláírását tartalmazza;
  gazdasági társaságok esetében a cégbírósági bejegyzést, más – nem gazdasági – szervezetek esetében a szervezet hivatalos bejegyzését is mellékelni kell a kérelemhez.

Az Ügyfélkapcsolati Iroda a bemutatott iratok és okmányok érvényességét és hitelességét ellenőrzi. Szervezeti személy típusú tanúsítvány igénylés esetén az Ügyfélkapcsolati Iroda az aláírási jogosultság ellenőrzése céljából adategyeztetést végezhet a cégnyilvántartással[20].

Az Ügyfélkapcsolati Iroda szervezeti személy azonosítás-hitelesítése során köteles a Tanúsítvány kibocsátását megtagadni, amennyiben

[20] 2001. évi XXXV. törvény 12. § (2) b)

- az okmányok személyhez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel,
- a bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel,
- a cégnyilvántartással végzett adategyeztetés a bemutatott adatoktól eltérő eredményt ad,
- a szervezet kiléte nem állapítható meg minden kétséget kizáróan,
- nem egyértelmű a szervezet felhatalmazása a Tanúsítvány kibocsátására.

Szervezet részéről teszt tanúsítvány nem igényelhető.

3.1.10. Eszköz identitás hitelesítése

Előfizetői osztályú eszköz tanúsítvány igénylésekor az eszköz azonosításához és hitelesítéséhez a következőben megadott adatokat kéri az Ügyfélkapcsolati Iroda.

Természetes személy esetén:

- az Előfizető személyes identitása hitelesítéséhez szükséges adatok a 3.1.9 pont szerint.
- az Előfizető írásos nyilatkozata az eszköz birtoklásáról és azonosítójáról.

Jogi személy esetén:

- az előfizető szervezet identitása hitelesítéséhez szükséges adatok a 3.1.9 pont szerint
- annak a szervezeti egységnek a neve, telefon és fax száma és e-mail címe, amely az eszközt üzemelteti,
- az előfizető szervezet cégszerű aláírással ellátott írásos nyilatkozata az eszköz birtoklásáról és azonosítójáról,
- az előfizető szervezet egyértelmű hozzájárulása ahhoz, hogy:
  - a tanúsítvány kibocsátásra kerüljön,
  - a szervezet és szervezeti egysége neve a tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön,
  - az eszköz azonosítója a tanúsítvány tulajdonosazonosító mezőjében feltüntetésre kerüljön,
  - az Előfizető kapcsolattartókat nevez meg a Szolgáltató részére, akik aláírási joggal rendelkeznek a tanúsítvány kibocsátását illetően, a Szolgáltató később e személyeknek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén,

- az előfizető szervezet kötelezettségvállalása melyben:
  - a tanúsítvány kibocsátásával és fenntartásával kapcsolatos és minden egyéb járulékos költséget vállal,
  - a Szolgáltató szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat.

Ezen adatokat a következőben megadott dokumentumokkal kell hitelesíteni.

Természetes személy esetén:

- személyi igazolvány vagy útlevél bemutatása személyesen,
- az Előfizető írásos nyilatkozata az eszköz birtoklásáról és azonosítójáról.

Jogi személy esetén:

- 30 napnál nem régebbi cégkivonat, aláírási címpéldány,
- képviseleti megbízás cégszerűen aláírva,
- az előfizető szervezet cégszerű aláírással ellátott írásos nyilatkozata az eszköz birtoklásáról és azonosítójáról.

Az Ügyfélkapcsolati Iroda köteles a szerződéskötéstől elállni, és a Regisztrációs Iroda köteles a tanúsítvány kibocsátását megtagadni, amennyiben az azonosítás-hitelesítés vagy az azt követő ellenőrzések során az eszköznek az Előfizetőhöz tartozásával, annak eredetiségével kapcsolatban kétség merül fel.

3.2. Érvényes tanúsítvány megújítása (tanúsítvány frissítése)

Egy érvényes (nem lejárt és nem visszavont) tanúsítvány megújítására az alábbi lehetőségek vannak:

- tanúsítványfrissítés, amikor a Szolgáltató érvényes magánkulcsával az új tanúsítványban a tanúsítvány alanyának változatlan (régi) nyilvános kulcsát és változatlan egyéb adatait írja alá új érvényességi időtartamra,
- tanúsítvány aktualizálás, amikor a Szolgáltató érvényes magánkulcsával az új tanúsítványban a tanúsítvány alanyának változatlan (régi) nyilvános kulcsát és megváltozott új adatait írja alá új érvényességi időtartamra,

- tanúsítvány kulcscsere, amikor a Szolgáltató érvényes magánkulcsával az új tanúsítványban a tanúsítvány alanyának új nyilvános kulcsát és változatlan egyéb adatait írja alá új érvényességi időtartamra.

Tanúsítványának lejárta előtt, az Előfizető az Előfizetői Szerződésben meghatározott időpontban (ha a Szerződés erről nem intézkedik, akkor a lejárat előtt 15 nappal korábban) e-mailben kap értesítést a Szolgáltatótól a tanúsítvány megújítás szükségességéről.

A Szolgáltató által kibocsátott előfizetői tanúsítványok érvényességi ideje 1 év.

Előfizetői tanúsítvány megújítása akkor lehetséges, ha:

- a tanúsítvány érvényes,
- a tanúsítvány nem szerepel a tanúsítvány visszavonási listán, mint visszavont vagy felfüggesztett tanúsítvány,
- a kezdeti regisztráció alkalmával rögzített összes adat még érvényes, (azok is melyek a tanúsítványban nem, csak szolgáltató belső nyilvántartásában szerepelnek),
- a tanúsítványhoz tartozó magánkulcs nem kompromittálódott.

Ha mindezen feltételek nem teljesülnek, alanynak új tanúsítványt kell igényelnie a kezdeti regisztráció módszerével.

Minden második évben a tanúsítvány megújítási eljárás megegyezik a „Kezdeti regisztráció” fejezetben leírtakkal. Közbenső megújítás esetén a felhasználó adatainak újbóli regisztrációjára nincs szükség. Ennek feltétele, hogy a felhasználó nyilatkozzon, hogy a kezdeti regisztrációkor magadott adatai nem változtak, különös tekintettel a tanúsítványban megjelenő adatokra.

3.3. Érvénytelen tanúsítvány megújítása

Tanúsítvány megújítása nem lehetséges a tanúsítvány érvényességének lejárta után, illetve ha a tanúsítvány visszavont vagy felfüggesztett állapotban van. Ezen esetekben új tanúsítványt kell igényelni, a regisztrációs eljárás újbóli végrehajtásával.

3.4. Felfüggesztés és visszavonási kérés

Felfüggesztés és visszavonási kérés személyes megjelenéssel vagy hitelesített elektronikus üzenetváltással történhet. A tanúsítvány visszavonási kérés azonosítási és hitelesítési vonatkozásai megtalálhatók a 4.4 fejezetben.

A Szolgáltató gondoskodik arról, hogy az előző pontban meghatározott, egy már korábban nála nyilvántartásba vett Aláírótól származó, tanúsítvány visszavonási vagy felfüggesztési kérelem teljes, pontos és kellőképpen hiteles legyen. Ennek érdekében a Szolgáltató a 4.4 pont szerint dokumentálja a tanúsítványok visszavonásának, felfüggesztésének eljárásait, beleértve az alábbiakat:

- milyen okból kifolyólag függeszthető fel egy tanúsítvány,
- mi a felfüggesztett állapot maximális időtartama,
- ki adhat be visszavonási kérelmeket,
- hogyan lehet ezeket beadni,
- mik a visszavonási kérelmek megerősítésére vonatkozó esetleges követelmények.

4. A működésre vonatkozó követelmények

4.1. Tanúsítványigénylés

Tanúsítvány a Szolgáltatótól az Ügyfélkapcsolati Irodánál igényelhető, az adott tanúsítvány osztálynak megfelelő, a 3.1.8 - 3.1.9 pontokban meghatározott azonosítás-hitelesítési feltételek mellett, a regisztrációs eljárás lefolytatásával.

a. A Szolgáltatónak azt megelőzően, hogy egy Előfizetővel szerződéses kapcsolatot létesít, tájékoztatnia kell az Előfizetőt a Tanúsítvány használatával kapcsolatos kikötésekről és feltételekről a 3.1.9 pontban megadottak szerint. A kapcsolatfelvételkor – amennyiben az Igénylő Aláírás létrehozó adat és eszköz használati igényét egyértelműen jelzi – Tanúsítvány űrlapot kap az Ügyfélkapcsolati Iroda munkatársától.
b. A Tanúsítvány űrlap átvételét követően a Szolgáltató tájékoztatási kötelezettségét tájékoztató kiadványnak (Tájékoztató, ÁSzF) az Igénylő részére történő átadásával teljesíti. Igénylőnek módja van e dokumentumok helyszínen történő áttanulmányozására és helyszíni konzultációra, de azok, valamint a Tanúsítvány igénylő űrlap megtalálható szolgáltató honlapján is, így előzetesen is áttekinthető[21] és kitölthető. Amennyiben az Előfizető igényli, az Ügyfélkapcsolati Iroda az egyéb nyilvános dokumentumok tanulmányozásának lehetőségét is biztosítja, valamint szóban válaszol az Igénylő, a szerződéskötéssel kapcsolatos további kérdéseire.

   A Tájékoztató tartalma:

   - A HSzSz-nek az Előfizető szempontjából legfontosabb szabályokat, feltételeket tartalmazó kivonata, (természetesen az Igénylő az Ügyfélkapcsolati Iroda által megadott elérhetőségen a HSzSz-t teljes egészében is elolvashatja).
   - A Szolgáltató további nyilvános dokumentumainak szerepe és elérhetősége.
   - Egyéb technikai eligazítás.
c. A Szolgáltató az Aláírót is tájékoztatja kötelességeiről.

[21] Az űrlap a regisztrációs adatok mellett tartalmazza a szükséges nyilatkozatokat és igénylő fizikai címét, illetve más jellemzőit, amelyek leírják, hogy hogyan lehet felvenni vele a kapcsolatot.

d. Az Előfizetőnek meg kell adnia egy fizikai címet, illetve más jellemzőket (lásd HSzSz 3.1 pont), amelyek leírják, hogy az Előfizetővel hogyan lehet felvenni a kapcsolatot.
e. A személyes és szervezeti identitások hitelesítése, űrlapon szereplő adatok formai és tartalmi ellenőrzése.

   A személy- és szervezeti azonosság, valamint a szervezethez tartozás megállapítása a 3.1.8 és 3.1.9 fejezetekben leírtak alapján történik. Amennyiben az azonosság nem állapítható meg minden kétséget kizáróan, vagy valamely az űrlapon feltüntetett adat nem helyes, akkor az igénylési eljárás félbeszakad. Szolgáltató az űrlapot visszaadja igénylő részére, akinek lehetősége van az adatok korrigálására, s újbóli igénylésre.
f. A regisztrációhoz szükséges dokumentumok és adatok formai és tartalmi ellenőrzése után a regisztrációt végző személy ellenőrzi a regisztrációs űrlapon szereplő adatok egyezőségét az Előfizető dokumentumaiban szereplő adatokkal.
g. Ha az adatok helyesek, az űrlap tartalmát rögzíti az Ügyfélkapcsolati Iroda informatikai rendszerében, ellenkező esetben az űrlapot visszaadja.
h. Az Aláíró azonosítójának (egyedi nevének) megállapítása a 3.1 pontban tárgyaltaknak megfelelően történik.
i. Az Előfizetői szerződés megkötése a Szolgáltató előfizetői szerződés mintájának megfelelően. Az Igénylő aláírásával Előfizetővé válik és egyúttal nyilatkozik arról is, hogy a Szolgáltató feltételei és kikötései, saját kötelezettségei vonatkozásában tájékoztatást kapott, azokat elfogadja. Az aláírással az Előfizető hozzájárul a szolgáltatások során felhasznált információknak a Szolgáltató által történő nyilvántartásba vételéhez, Tanúsítványa és az azzal kapcsolatos állapot információ szolgáltatói címtárban való közzétételéhez, s ezen információ harmadik félhez történő továbbításához a Szolgáltató szolgáltatásainak leállítása esetén, illetve egyéb jogszabályok által meghatározott esetekben, a Szolgáltató szabályzatai által meghatározott módon.

   Az Előfizető aláírása igazolja azt is, hogy az Előfizető:
   - vállalja az aláírás-létrehozó eszköz használatát, védelmét,
   - garantálja feltüntetett adatainak valódiságát,
   - az adatok későbbi változásairól a Szolgáltatót értesíti.
j. Az Ügyfélkapcsolati Iroda nyilvántartásba vesz minden, az Aláíró azonosságának igazolására használt információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és

az annak érvényességével kapcsolatos esetleges korlátozásokat. A dokumentációkról az Ügyfélkapcsolati Iroda másolatot készít.

k. A Tanúsítványigénylő űrlap tartalmát az Ügyfélkapcsolati Iroda nyilvántartásába veszi és archiválásra kerül mind elektronikus, mind papír formában.

l. Az Ügyfélkapcsolati Iroda nyilvántartásba veszi az Előfizetővel aláírt nyilatkozatokat[22], beleértve az alábbiakat:
   - az Előfizető kötelezettségeivel (lásd 3.1.9) történő egyetértést,
   - az Előfizető beleegyezését az aláírás-létrehozó eszköz használatára vonatkozóan,
   - hozzájárulás az alábbi szolgáltatások során felhasznált információ Szolgáltató által történő nyilvántartásba vételéhez: regisztrálás, az előfizetők eszközzel való ellátása (beleértve az Előfizetőhöz történő továbbítást is), bármely ezt követő visszavonás, illetve ezen információ harmadik félhez történő továbbítása (a Szolgáltató szolgáltatásainak leállítása esetén HSzSz által megkövetelt feltételek szerint),
   - hogy az Előfizető megköveteli-e, az Aláíró pedig hozzájárul-e a Tanúsítvány közzétételéhez és milyen feltételek mellett,
   - annak megerősítését, hogy a Tanúsítványban szereplő információ helyes[23].

   A Szolgáltató megőrzi a d)-f) pontokban megnevezett nyilvántartásokat 10 évig[24], illetőleg a velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig.

Sikeres regisztráció után az Ügyfélkapcsolati Iroda a tanúsítvány igényt a Regisztrációs Iroda felé továbbítja, amellyel elbírálási igényt támaszt a fölérendelt Hitelesítő Központ felé. A Regisztrációs Iroda a kedvező elbírálás után a hitelesítés szolgáltatást támogató informatikai rendszerbe a tanúsítvány kibocsátási igényt beviszi.

A Szolgáltató lehetővé teheti 1 évnél régebben aktív ügyfelei részére tanúsítvány frissítés esetén, hogy tanúsítványaik frissítésére vonatkozó bejelentésüket ne személyesen tegyék meg. Ebben az esetben az Előfizetőnek írásban meg kell erősítenie, hogy az adatai az előző tanúsítvány igénylés

[22] Az Előfizető ezen megállapodás különböző pontjaihoz a regisztráció különböző fázisai során is hozzájárulhat. Például a Tanúsítványban szereplő információ helyességére vonatkozó megállapodás a megállapodás egyéb szempontjait követően is megköthető.

[23] A fenti megállapodás elektronikus formát is ölthet.

[24] A 2001. évi XXXV. törvény 9. § (7) pontja legalább 10 év megőrzési időt követel meg.

óta nem változtak meg. Ez után a rendelkezésére álló adatok alapján történik meg a tanúsítvány kibocsátás. A 4.1 pontban leírt regisztrációs űrlap kitöltésnek ekkor is meg kell történnie a Tanúsítvány átadása előtt. Ilyen egyszerűsített igénylés azonban csak egyszer adható be a Szolgáltatóhoz, a következő igénylésnél az azonosítás-hitelesítést a **Hiba! A hivatkozási forrás nem található.** pont szerint el kell végezni.

4.2. Tanúsítvány kibocsátás

Az elkészült Tanúsítványt a Szolgáltató a következő módon juttatja el az Előfizetőhöz:

- az Előfizető, az Aláíró vagy az eredetileg regisztrált képviselője személyesen átveheti az Ügyfélkapcsolati Irodán, vagy
- utólagosan letöltheti a nyilvános Címtárból

A Szolgáltató biztonságosan fenntartja az általa kibocsátott tanúsítványok hitelességét.
Különösképpen:

- Előállítása után a teljes és pontos Tanúsítvány rendelkezésére áll azon Előfizető vagy Aláíró számára, akinek a Tanúsítvány kibocsátásra került.
- A Tanúsítvány kibocsátás eljárása biztonságosan kapcsolódik a megfelelő regisztrációhoz, illetve a különböző tanúsítvány megújítási eljárásokhoz.
- Az Aláíró számára a Szolgáltató által megvalósított kulcspár előállításra:
  - a Tanúsítvány kibocsátás eljárása biztonságosan kapcsolódik a Szolgáltató általi kulcspár előállításhoz;
  - az Aláíró Aláírás létrehozó adatát tartalmazó Aláírás létrehozó eszközt biztonságosan továbbítják az Előfizetőhöz.

A Szolgáltató csak akkor bocsát ki egy új Tanúsítványt az Aláíró korábbiakban tanúsított Aláírás ellenőrző adatának felhasználásával (Tanúsítvány frissítés), ha annak kriptográfiai biztonsága még megfelelő az új Tanúsítvány tervezett élettartamára, és nincsenek arra utaló jelek, hogy az alany Aláírás létrehozó adata kompromittálódott. A Szolgáltató legfeljebb egy alkalommal újít meg egy Tanúsítványt ily módon.

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

- az Igénylő benyújtotta kérelmét a Regisztrációs Irodának,

- az Aláíró (akinek nevében az Igénylő eljár, amennyiben nem azonos az Aláíróval) azonos a kérelemben szereplő alannyal (subject),
- az Igénylő jogosult a kérelemben szereplő Aláíró nevében kérelmet benyújtani,
- a Regisztrációs Iroda bejegyezte a tanúsítványkérelmet.

A Szolgáltató a Tanúsítvány kibocsátását visszautasíthatja, amennyiben:

- a bemutatott iratok és okmányok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel,
- a cégnyilvántartással végzett adategyeztetés a bemutatott adatoktól eltérő eredményt ad,
- a személy szervezethez tartozása nem egyértelmű,
- a szervezet kiléte nem állapítható meg minden kétséget kizáróan,
- nem egyértelmű a szervezet felhatalmazása a tanúsítvány kibocsátására.

A tanúsítvány elkészítését és kibocsátását a regisztráció során felvett elektronikus űrlap alapján végzi a Hitelesítő Központ.

A Hitelesítő Központ az előállított tanúsítványt visszaküldi a Regisztrációs Irodához. Amennyiben a tanúsítványkérelem visszautasításra kerül ennek tényéről és okáról a Regisztrációs Iroda értesítést kap.

A Szolgáltató lehetővé teheti 1 évnél régebben aktív ügyfelei részére, hogy tanúsítványok ismételt igénylése esetén az igénylést ne személyesen tegyék meg. Ebben az esetben az Előfizetőnek írásban meg kell erősítenie, hogy az adatai az előző tanúsítvány igénylés óta nem változtak meg. Ez után a rendelkezésére álló adatok alapján történik meg a tanúsítvány kibocsátás. A 4.1 pontban leírt regisztrációs űrlap kitöltésnek ekkor is meg kell történnie a tanúsítvány átadása előtt.

4.3. Tanúsítvány elfogadás

A Regisztrációs Iroda, a Szolgáltató felelősségi körében eljárva az elkészült Tanúsítványt ellenőrzi, Aláírás létrehozó eszközre írja az Aláírás létrehozó adattal együtt, majd az eszközt és a PIN kódot személyesen adja át az Ügyfélkapcsolati Irodában megjelent Előfizetőnek. Teszt célú tanúsítvány kibocsátása esetén az Aláírás létrehozó adat generálása az Aláírónál történik saját felelősségére. Tanúsítvány elfogadási eljárás szüksége nem merül fel.

Előfizetői szerződés megkötése esetén az átadás során átadásra kerül:

- az Aláírás létrehozó eszköz, rajta az Aláírás létrehozó adattal és a tanúsítvánnyal,
- az aláírt regisztrációs űrlap egy eredeti példánya,
- a tájékoztató brosúra,
- az aláírt Előfizetői Szerződés egy példánya.

Az aláírás létrehozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

Amennyiben a regisztrációs eljárás és az Aláírás létrehozó eszköz átadása között az Előfizetővel a személyes kapcsolat megszakadt, az Előfizető személyazonosságát újra ellenőrizni kell az Aláírás létrehozó eszköz átadása előtt.

A személyes, illetve postai úton történő átadásnál a kulcshordozót kizárólag a regisztrációs űrlapon megjelölt Aláíró, illetve eszköz tanúsítvány esetén az Előfizető írásban feljogosított meghatalmazottja veheti át.

A magánkulcs és a Tanúsítvány elfogadása az Aláírás létrehozó adat első felhasználásával történik meg.

A tanúsítvány elfogadásával együtt az Előfizetőnek írásban kell megerősíteni a következőket:

- ismeri, érti és elfogadja jelen és kapcsolódó nyilvánosan hozzáférhető szabályzatokat,
- minden adat, amit a Szolgáltatónak a Tanúsítvány kiadásának céljából átadott, a valóságnak megfelel és azok átadása önkéntes volt,
- a Tanúsítványban szereplő minden adat az Előfizető tudomásával és egyetértésével került a Tanúsítványba,
- a Tanúsítvány érvényességét befolyásoló tényekről haladéktalanul értesíti a Szolgáltatót,
- mindent megtesz annak érdekében, hogy jogosulatlan személy nem férjen hozzá az Aláírás létrehozó adathoz,
- ismeri az elektronikus aláírás megfelelő használatának módját, tisztában van az elektronikus aláírás használatának technikai feltételeivel és jogi következményeivel,
- minden egyes elektronikus aláírást, amely a Tanúsítványban szereplő az Aláírás ellenőrző adat párjával készült, az Aláíró saját elektronikus aláírásának ismeri el,
- tudomással bír arról, hogy az elektronikus aláírással ellátott elektronikus iratok az írásbafoglalás jogszabályi követelményének megfelelnek,
- minden aláírás az elfogadott és érvényes (vissza nem vont, nem lejárt) Tanúsítvány alapján készült,

- a Tanúsítványt kizárólag törvényes célokra, jogszerűen, a jelen és kapcsolódó szabályzatoknak és törvényi előírásoknak megfelelően használja,
- tisztában van azzal, hogy az Aláírás létrehozó adat védelme és az elektronikus aláírás készítése kizárólag a Felhasználó felelőssége, s ezzel kapcsolatban a Szolgáltatót semmiféle felelősség nem terheli,
- az Aláíró végfelhasználó, azaz nem hitelesítés szolgáltató, és nem fogja a tanúsítványban megadott Aláírás ellenőrző adat párját újabb tanúsítványok vagy bármely más formátumú tanúsított Aláírás ellenőrző adat, visszavonási lista kiadására használni; hacsak erről külön írásbeli szerződésben a Szolgáltatóval meg nem egyezett,
- felhatalmazza a Szolgáltatót a Tanúsítvány nyilvánosságra hozatalával, és saját vagy más nyilvános címtárakban történő elhelyezésével.

A Szolgáltató elutasítja a tanúsítványkérelmeket, ha az azonosítás-hitelesítési és regisztrációs feltételek a jelen HSzSz szerint nem biztosíthatók az igényelt Tanúsítvány osztályának és típusának előírt módon.

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

Elutasítás után a kérelmező új kérelemmel fordulhat a Szolgáltatóhoz.

Az Aláírás létrehozó adat használatba vétele előtt az Előfizetőnek kötelessége ellenőrizni a Tanúsítványban feltűntetett adatainak helyességét. Amennyiben bármilyen rendellenességet talál az Aláírás létrehozó adatot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonása érdekében.

4.4. Tanúsítvány visszavonás és felfüggesztés

A Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatásokat nyújt. A Tanúsítvány visszavonása a Tanúsítvány állapotát végérvényesen érvénytelenre állítja. A Tanúsítvány felfüggesztett állapotban csak ideiglenesen lehet, az engedélyezett időtartam (lásd 4.4.8 pont) után állapotát újra érvényesre kell állítani, vagy vissza kell vonni. A felfüggesztett Tanúsítvány mindaddig, míg felfüggesztett állapotban van, ugyanúgy érvénytelenként kezelendő, mint a visszavont.

A visszavont/felfüggesztett Tanúsítványhoz tartozó magánkulcs használatát azonnal meg kell szüntetni, illetve fel kell függeszteni. A visszavont Tanúsítványhoz tartozó aláíró magánkulcsot a visszavonást követően azonnal meg kell semmisíteni. A megsemmisítéséig a magánkulcs ugyanolyan felügyeletben részesítendő, mintha érvényes lenne.

A visszavonási/felfüggesztési kérelmek fogadását és azoknak a sikeres ellenőrzés utáni végrehajtását a Szolgáltató mindennap 24 órában, 99,9%-os rendelkezésre állással biztosítja úgy, hogy esetenként a visszavonási/felfüggesztési kezelés kiesése nem lehet több, mint 3 óra.

4.4.1. Visszavonáshoz vezető körülmények

Az Előfizető, az Aláíró vagy az eredetileg regisztrált képviselő a következő körülmények fennállása esetén kezdeményezi a visszavonást:

- a magánkulcs kompromittálódása, vagy annak gyanúja,
- a Biztonságos aláírás-létrehozó eszköz elvesztése, eltulajdonítása, megrongálódása,
- a Biztonságos aláírás-létrehozó eszközt védő aktivizáló adat (PIN kód) kompromittálódása, vagy annak gyanúja,
- a magánkulcs átvételének visszautasítása,
- a Tanúsítványban feltűntetett hibás adatok,
- az Előfizetőnek a Tanúsítványban feltűntetett adatainak megváltozása,
- az Aláírónak a Tanúsítványban feltűntetett adatainak megváltozása,
- a Tanúsítványban feltűntetett szervezet adatainak megváltozása,
- a Tanúsítványban feltűntetett Aláíró és szervezet kapcsolatának megváltozása vagy megszűnése[25].

miatt.

Visszavonási kérelmet mérlegelés nélkül teljesíteni kell, ha az Aláíró, az Előfizető vagy a kezdeti regisztráláskor nyilvántartásba vett képviselő kéri.

A Szolgáltató kezdeményezése alapján:

- a Tanúsítvány felfüggesztési idejének lejárata,
- amennyiben a törvény erre kötelezi,

[25] A 2001. évi XXXV. törvény 10. § (3)

- az ÁSzF, Előfizetői Szerződés megszegése az Előfizető és/vagy az Aláíró által,
- az Előfizető és/vagy az Aláíró kötelezettségeinek be nem tartása,
- az Előfizetői szerződés megszűnése,
- a Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról,
- a Tanúsítványban feltűntetett kibocsátó adatok megváltozása
- a hitelesítési szolgáltatás megszűnése,
- a Regisztrációs Iroda megszűnése,
- a Szolgáltató valamely magánkulcsának kompromittálódása

miatt.

Harmadik fél, pl. Érintett fél kezdeményezése alapján.

Egyéb visszavonáshoz vezető körülmények:

- az Aláíró halála, az Előfizető megszűnése,
- jogszabály kötelező ereje.

4.4.2. Visszavonás kérelmezése

Tanúsítvány visszavonását az előző pontban feltüntetett körülmények alapján az Előfizető, annak a kezdeti regisztrációkor nyilvántartásba vett képviselője, a Szolgáltató, hatósági szervezet vagy más harmadik fél kezdeményezheti. Az Előfizetőnek és Szolgáltatónak kötelessége, harmadik félnek joga, a feltűntetett esetekben a visszavonás azonnali kezdeményezése.

A visszavonási kérelmet be lehet nyújtani személyesen és írásban a Szolgáltató Ügyfélkapcsolati Irodájánál vagy Ügyfélszolgálatánál (Help Desk-nél). Amennyiben a bejelentő akadályoztatása miatt a visszavonási igényét személyesen nem tudja bejelenteni, akkor telefonon vagy elektronikusan aláírt e-mail-ben a Tanúsítvány felfüggesztését kérheti (lásd 4.4.6 pont) és az ettől számított 30 napon belül megteheti a visszavonás személyes bejelentését.

A visszavonási kérelemnek a következő adatokat kell tartalmazni:

- a Tanúsítvány sorszáma,
- a visszavonást kérő megnevezése,
- a visszavonást kérő e-mail címe,
- a visszavonás oka.

4.4.3. Visszavonási eljárás

Visszavonási igényt mind szerződéses előfizetői, mind teszt célú tanúsítványra be lehet nyújtani. A visszavonási eljárás első lépéseként a Szolgáltató Ügyfélkapcsolati Irodája vagy a munkaidőn kívül Ügyfélszolgálata (Help Desk) azonosítja a bejelentőt, aki lehet:

- természetes személy Előfizető esetén maga az Aláíró vagy az általa megbízott és a Szolgáltató által nyilvántartott képviselője,
- jogi személy Előfizető esetén maga az Aláíró vagy a jogi személy által megbízott és a Szolgáltató által nyilvántartott képviselő,

E-mail-el történő bejelentés esetén az Aláíró tanúsítványa érvényességének ellenőrzése után a nyilvános kulccsal történő sikeres kibontás azonosítja és hitelesíti az Aláírót.

Az Ügyfélkapcsolati Irodánál az Iroda munkaidején belül bejelentett visszavonási kérelmeket a bejelentő azonosítása-hitelesítése, valamint a visszavonási kérelem formai és tartalmi ellenőrzése után haladéktalanul a Hitelesítő Központhoz kell továbbítani, amely azokat ismét ellenőrzi.

Az Ügyfélkapcsolati Iroda munkaidején kívül a telefonon jelentkező bejelentőt Help Desknél az erre feljogosított munkatárs felfüggesztési jelszóval azonosítja, valamint a kérelmet formailag és tartalmilag ellenőrzi. Amennyiben az ellenőrzések pozitív eredménnyel zárulnak, a feljogosított ügyeletes a Tanúsítvány felfüggesztését és közzétételét elvégzi. A visszavonás kérelmezése ténylegesen az Ügyfélkapcsolati Irodában személyes megjelenés útján, legkésőbb 30 napon belül, a bejelentő megnyugtató azonosítás-hitelesítését követően fog megtörténni.

Ha az okok nem megalapozottak, az adatok helytelenek, vagy a kérelmező személye nem állapítható meg, akkor a Szolgáltató a visszavonási kérelmet visszautasítja.

A visszavont Tanúsítvány bekerül a következő alkalommal kibocsátott Tanúsítvány visszavonási listába.

Szolgáltató a visszavonás megtörténtéről vagy visszautasításáról elektronikusan aláírt e-mail-ben értesíti az Előfizetőt és a visszavonás kérelmezőjét.

A Szolgáltató nem állítja vissza érvényesre a már egyszer véglegesen visszavonásra került tanúsítványokat.

Végfelhasználói tanúsítvány visszavonását és felfüggesztését a Szolgáltató akkor is nyilvánosságra hozza, ha a Tanúsítvány közzétételéhez az Előfizető nem járult hozzá.

4.4.4. Visszavonási kérelemre vonatkozó türelmi idő

A visszavonási kérelem esetén a bejelentési kötelezettség azonnali, a Szolgáltató ennek végrehajtását soron kívül végrehajtja a kérelem elfogadása után. A legnagyobb késedelem a visszavonási kérelem fogadása, illetve az összes érintett fél rendelkezésére álló információ visszavonási állapotának megváltoztatása között: 24 óra.

A Tanúsítvány érvényességének lejárata előtti - bármely okból történő - visszavonása esetén a tanúsítványt a továbbiakban joghatályosan nem lehet felhasználni.

A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok:

- A visszavonási kérelem bejelentésének a Szolgáltatóhoz történő megérkezéséig az ÁSzF-nek megfelelően az Előfizető felelős a felmerülő károkért.
- A visszavonási kérelem megérkezésétől a visszavonás tényének Címtárban való megjelenésig a Szolgáltató felelős a felmerülő károkért.
- A visszavonás Címtárban való megjelenése után az Érintett fél felelős a felmerülő károkért.

Az Érintett fél, amennyiben a tudomására jut adott tanúsítvány érvénytelenségére utaló információ, nem hagyatkozhat kizárólag a Címtárban megjelenő érvényességi adatokra.

4.4.5. Felfüggesztéshez vezető körülmények

Az Előfizető, az Aláíró vagy az eredetileg regisztrált képviselő a következő körülmények fennállása esetén kezdeményezi a felfüggesztést:

- a magánkulcs kompromittálódásának gyanúja,
- a Biztonságos aláírás-létrehozó eszköz elvesztése, eltulajdonításának gyanúja,
- a Biztonságos aláírás-létrehozó eszközt védő aktivizáló adat (PIN kód) kompromittálódásának gyanúja,

miatt.

A felfüggesztési kérelmet mérlegelés nélkül teljesíteni kell, ha az Aláíró, az Előfizető vagy a kezdeti regisztrációkor nyilvántartásba vett képviselő kéri.

A Szolgáltató a regisztrációs adatok valótlanságának alapos gyanúja esetén kezdeményezheti a felfüggesztést. Mindenképpen meg kell győződnie a gyanú alaposságáról, illetve alaptalanságáról és ennek függvényében kell dönteni a Tanúsítvány visszavonásáról.

Harmadik fél kezdeményezése alapján, amikor a Tanúsítvány hitelességével kapcsolatosan kétely vagy alapos gyanú merül fel.

Általános szabály az, hogy a Szolgáltató egy Tanúsítvány hitelességével kapcsolatosan felmerülő kétely vagy a hitelesség sérülésének alapos gyanúja esetén, dönthet a Tanúsítvány felfüggesztéséről. Ilyen esetekben a Szolgáltatónak a felfüggesztett állapot időtartama alatt intézkednie kell a körülmények tisztázása, s szükséges esetén a Tanúsítvány visszavonása érdekében. Tanúsítvány felfüggesztését harmadik fél is kérheti, amennyiben bizonyítani tud olyan körülményt, mely alapján Előfizetőnek vagy Szolgáltatónak kezdeményeznie kellene a visszavonást.

Amennyiben az Előfizető kötelessége a Tanúsítvány visszavonásának kérelmezése, de személyes megjelenése akadályoztatva van, vagy nem lehetséges, akkor haladéktalanul intézkednie kell Tanúsítványának felfüggesztése érdekében.

4.4.6. Felfüggesztés kérelmezése

A Tanúsítvány felfüggesztésére vonatkozó kérelem a következő módokon nyújtható be a Szolgáltatónak:

- elektronikusan aláírt e-mail írásával, a küldő, a tanúsítvány azonosításához szükséges adatok, és a felfüggesztést indokoló okok feltüntetésével,
- személyes megjelenéssel az Ügyfélkapcsolati Irodánál,
- az Ügyfélszolgálat (Help Desk) telefonszámán.

A telefonon keresztül történő bejelentésénél a bejelentőt a visszavonási jelszóval kell hitelesíteni.

A felfüggesztési kérelemnek a következő adatokat kell tartalmazni:

- a Tanúsítvány sorszáma,
- a felfüggesztést kérő megnevezése,
- a felfüggesztést kérő email címe,
- a felfüggesztés oka.

Harmadik fél csak személyesen vagy elektronikus aláírással ellátott e-mailben kérheti egy tanúsítvány felfüggesztését. A visszavonási jelszó megadása harmadik fél számára nem kötelező, de meg kell adnia a személyes adatait is (lakcím, személyi igazolvány száma), s személyes

megjelenés esetén a személyazonosságát is igazolnia kell. Elektronikusan aláírt e-mail esetén a kérelmező tanúsítványa és személyazonossága leellenőrizendő.

Teszt célú tanúsítványra a visszavonás nem értelmezett, így ilyen igényt benyújtani nem lehet.

4.4.7. Felfüggesztési eljárás

A felfüggesztési eljárás első lépéseként Szolgáltató azonosítja és hitelesíti a bejelentőt, majd ellenőrzi a kérelemben szereplő okokat és a kérelmező adatait. Amennyiben azok helytelenek, a kérelem nem megalapozott, vagy a kérelmező személye nem megállapítható, akkor Szolgáltató a felfüggesztési kérelmet visszautasítja.

Amennyiben a kérelmet az Előfizető terjesztette be, a szolgáltatónak nincs mérlegelési joga a végrehajtás tekintetében. A bejelentett felfüggesztési kérelmeket a Regisztrációs Iroda a Hitelesítő Központnak továbbítja.

Szolgáltató a felfüggesztés megtörténtéről, vagy visszautasításáról elektronikusan aláírt e-mail-ben értesíti az Előfizetőt és a felfüggesztés kérelmezőjét.

A felfüggesztési kérelem bejelentésének és végrehajtásának az Aláírás létrehozó adat kompromittálódása esetén késlekedés nélkül, minden más műveletet megelőzve meg kell történnie az észlelést követően.

4.4.8. Felfüggesztett állapotra vonatkozó korlátozások

Legfeljebb 30 naptári napig lehet egy Tanúsítvány felfüggesztett állapotban. Ha a Szolgáltató a felfüggesztésről határozott, akkor ezen időszakon belül dönt a Tanúsítvány állapotáról.

Amennyiben Szolgáltató nem képes ezen időszak alatt a körülmények kivizsgálására, akkor a tanúsítványt visszavonja. Az Előfizető igénye estén részére új Tanúsítványt bocsát ki térítésmentesen.

Ha a felfüggesztést az Előfizető, vagy a Tanúsítványban feltüntetett szervezet kérte, akkor a kérelmezőnek ezen időszak alatt értesítenie kell a Szolgáltatót a Tanúsítvány érvényesítése vagy visszavonása felől. Ha ilyen értesítés nem történik Szolgáltató a Tanúsítványt visszavonja.

A felfüggesztés megszüntetése a felfüggesztési időszak vége előtt is kérvényezhető. A felfüggesztés megszűntetésének eredménye a Tanúsítvány újra érvényesítése vagy annak visszavonása lehet.

A felfüggesztés megszüntetésének feltételei a következők:

- A felfüggesztést megszüntetését kérheti ugyanaz a személy, az Aláíró, az Előfizető vagy a kezdeti regisztrációkor nyilvántartásba vett képviselője,
- a felfüggesztés megszüntetését kérő személyt azonosítani és hitelesíteni kell, ennek során kérni kell tőle a felfüggesztési jelszót is.

A felfüggesztés megszüntetésének kéréséhez a következő adatokat kell megadni:

- a felfüggesztett Tanúsítvány sorszáma,
- a felfüggesztés megszüntetést kérő megnevezése,
- a felfüggesztést megszüntetést kérő e-mail címe,
- a felfüggesztés megszüntetés kérés oka.

4.4.9. CRL kibocsátás gyakorisága

A Szolgáltató Tanúsítvány visszavonási listát legalább 24 óránként bocsát ki. A Tanúsítvány visszavonási listában megadja a Visszavonási lista érvényességi idejét. Tanúsítvány visszavonási lista a megjelölt tervezett idő előtt is kibocsátható.

A visszavonási listában a visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre. A felfüggesztett tanúsítványok az újbóli érvényesítés hatására kerülhetnek ki a listából. Visszavont tanúsítványok a Tanúsítvány lejárta után 1 évvel törlődnek a listából.

A visszavonási lista elérhetőségét a Szolgáltató minden nap 24 órában, 99,9%-os rendelkezésre állással biztosítja úgy, hogy az esetenkénti elérhetőség kiesés nem lehet több, mint 3 óra.

4.4.10. CRL ellenőrzési követelmények

A Visszavonási lista ellenőrzése az érintett felek részére kötelező a tanúsítványok elfogadását megelőzően. A Tanúsítványhoz tartozó visszavonási lista elérhetőségét a Tanúsítvány tartalmazza. A lista ellenőrzésének arra kell vonatkozni, hogy a kérdéses Tanúsítványt a lista tartalmazza-e, a lista hiteles és sértetlen, s a kérdéses tranzakció szempontjából időben releváns-e.

A Tanúsítvány visszavonási listában a Szolgáltató által közzétett érvénytelen, vagy felfüggesztett tanúsítvány elfogadásából keletkező bárminemű kár Érintett felet terheli. Lásd még a 2.2.7 pontot.

4.4.11. On-line visszavonási státusz-szolgáltatás

A Szolgáltató on-line visszavonási állapot-szolgáltatást nem ad.

4.4.12. On-line visszavonás ellenőrzési követelmények

A Szolgáltató on-line visszavonási állapot-szolgáltatást nem ad.

4.4.13. Visszavonási állapot közlés más formái

A Szolgáltató nem alkalmaz a Tanúsítvány visszavonási listától különböző visszavonási állapot közlő eljárást.

A tanúsítványt igénybe vevő Érintett feleknek ugyanakkor, minden hagyományosan alkalmazott, és ésszerűen elvárható módszert igénybe kell venniük az általuk tanúsítvány segítségével ellenőrzött műveletek biztonsága érdekében. Amennyiben módjuk van az aláírás és tanúsítvány érvényességének más forrásból való ellenőrzésére, akkor azt a tanúsítvány állapotától függetlenül is meg kell tenniük.

Amennyiben Érintett fél más forrásból tudomást szerezhet, vagy ésszerű és elvárható gondossággal más forrásból megbizonyosodhat a tanúsítvánnyal igazolt művelet érvényességéről, akkor ezeket a lépéseket a tanúsítvány állapotától függetlenül is meg kell tennie. Szolgáltató ilyen esetekben nem felelős a bekövetkező károkért.

4.4.14. Visszavonási állapot közlés más formáinak ellenőrzési követelményei

Szolgáltató nem alkalmaz a Tanúsítvány visszavonási listától különböző visszavonási állapot közlő eljárást.

4.4.15. Magánkulcs kompromittálódás speciális követelményei

Az Aláírás létrehozó adat kompromittálódása, vagy vélelmezett kompromittálódása esetén a tanúsítvány visszavonásáról azonnal intézkedni kell. Alapos gyanú esetén az Aláírás létrehozó adat használatát azonnal fel kell függeszteni.

Kompromittálódott magánkulcs tovább nem használható. A kompromittálódott Aláírás létrehozó adat a megsemmisítéséig ugyanolyan felügyeletben részesítendő, mint egy érvényes Aláírás létrehozó adat.

Az Előfizetőnek kötelessége a kompromittálódott Aláírás létrehozó adat által esetlegesen érintett felek értesítése, és minden intézkedés megtétele az esetleges károk megelőzése és enyhítése érdekében.

4.5. Biztonsági audit eljárások

A Szolgáltató hitelesítés támogató informatikai rendszerének biztonsági naplózását és annak auditálását a jelen HSzSz mellett a Szolgáltató biztonsági szabályzata szabályozza részletesen.

4.5.1. Naplózott esemény típusok

A Szolgáltató hitelesítés támogató informatikai rendszerén az 5.3 pontban meghatározott szerepkörű munkatársai által végzett műveletek naplózásra kerülnek, amelyeket a regisztráció, a tanúsítvány igénylés, az Aláírás létrehozó és ellenőrző adatpár generálása, az Aláírás létrehozó eszköz megszemélyesítése, a tanúsítvány létrehozása és kibocsátása során hajtanak végre.

A Szolgáltató gondoskodik arról, hogy naplózásra kerüljön valamennyi regisztrációval kapcsolatos esemény, beleértve a Tanúsítvány megújítására (Tanúsítványfrissítésre, Tanúsítvány aktualizálására és Kulcscserére) vonatkozó kérelmeket is.

A tanúsítvány előállítással kapcsolatosan:

- A Szolgáltató naplózza a szolgáltatói kulcsok életciklusával kapcsolatos összes eseményt.
- A Szolgáltató naplózza a tanúsítványok életciklusával kapcsolatos összes eseményt.

Az Aláírók Aláírás létrehozó eszközzel való ellátásával kapcsolatosan[26]:

- A Szolgáltató naplóz minden általa gondozott kulcs életciklusával kapcsolatos eseményt.
- A Szolgáltató naplózza az Aláírás-létrehozó eszközök készítésével kapcsolatos valamennyi eseményt.

A visszavonás kezeléssel kapcsolatosan:

- A Szolgáltató gondoskodik a visszavonással kapcsolatos összes kérés, valamint az ezek eredményét képező összes tevékenység naplózásáról.

[26] Az „Aláírás-létrehozó eszközön az Aláírás-létrehozó adat elhelyezése” szolgáltatás keretén belül.

A naplóbejegyzések a bejegyzés pontos idejét, a tevékenység időpontját (ha az a bejegyzés idejétől eltér) és végrehajtóját is tartalmazzák.

A hitelesítés támogató informatikai rendszer operációs rendszere szintjén a Biztonság politikában és a Biztonsági Szabályzatban meghatározott események kerülnek naplózásra.

4.5.2. Napló adatok feldolgozásának gyakorisága

A nyilvános kulcsú hitelesítés (PKI) alkalmazás és az operációs rendszer szintű biztonsági esemény és audit naplók operatív (napi) ellenőrzését csak a rendszer auditorok végezhetik csak olvasási jogosultsággal.

A rendszer auditorok a Szolgáltató informatikai biztonsági menedzserének jelentik a rendellenességeket, aki félévente rendszeres belső auditot, illetve szúrópróbaszerű eseti ellenőrzéseket végez.

4.5.3. Napló adatok tárolási ideje

A naplózások – a Működtetési és Menedzselési Utasításban előírt heti gyakorisággal – kerülnek mentésre a szükségessé váló rendszer visszaállítás érdekében. A naplózások havonta egyszer kerülnek archiválásra a szükségessé váló visszakeresés, újbóli használat céljából. A 16/2001. (IX. 1.) MeHVM rendelettel összhangban az archivált naplókat keletkezésüktől számított 10 évig meg kell őrizni. Papír alapú naplókat csak abban az esetben kell megőrizni, ha nincs elektronikus megfelelőjük.

4.5.4. Napló adatok védelme

A hitelesítés szolgáltatás támogató informatikai rendszer biztonsági szempontból legkritikusabb elemei – így a naplóik is –, fokozott biztonságú fizikai környezetben vannak.
A naplók elektronikus aláírással hitelesítettek és hozzáférési jogosultsággal nem rendelkezők által nem olvashatók. A biztonsági és esemény naplókhoz csak az SO-k, a rendszer auditor, az informatikai biztonsági adminisztrátor, valamint a külső auditor férhetnek hozzá, csak olvasási joggal.

A Szolgáltató az eseményeket oly módon naplózza, ami nem törölhető, illetve nem tehető könnyen tönkre azon időtartam alatt, amíg azokat meg kell őrizni.

A Szolgáltató biztosítja a tanúsítványok és kulcsok gondozására[27] vonatkozó napló rekordok bizalmasságát és sértetlenségét.

4.5.5. Napló adatok mentési eljárásai

A hitelesítés szolgáltatás támogató informatikai rendszer különböző moduljaiban elkészült naplók egy központi mentő szerveren összegyűjtésre kerülnek. A mentő szerver és az egyedi eszközök tartalmának mentése hetente egyszer rendszeresen megtörténik.

4.5.6. Napló adatok gyűjtési rendszere

A mentést tartalmazó adathordozók első példányának tárolása a Hitelesítő Központban biztonságos helyen történik. A mentésekről biztonsági másolat készül, mely földrajzilag elkülönülten, a Szolgáltató Biztonsági Adattárában kerül elhelyezésre.

4.5.7. Rendkívüli eseményekről történő értesítés

A hitelesítés szolgáltatás támogató informatikai rendszerre, annak fizikai és személyi környezetére kiható súlyos üzemzavari és katasztrófa események megelőzéséről, kezeléséről és a rendszer visszaállításáról részletesen az Üzletmenet-folytonossági Terv intézkedik, a lényeges intézkedéseket a 4.8. fejezet tartalmazza.

Az üzletmenet-folytonosságot veszélyeztető, sértő, illetve megszüntető események az Üzletmenet-folytonossági Tervben súlyossági osztályokba vannak sorolva. Ez a Terv a szokásos üzletmenet-folytonossági tervekhez képest annyiban különbözi, hogy részletesen szabályozza az 1. és a 2. szintű Hitelesítő Központok saját Aláírás létrehozó adatainak, aktiváló adatainak (PIN kódok, jelszavak) kompromittálódása esetén elvégzendő teendőket.

A hitelesítés szolgáltatás leállását eredményező súlyos üzemzavari vagy katasztrófa, illetve a szolgáltatói Aláírás létrehozó és aktiváló adatait kompromittáló események esetén haladéktalanul értesítésre kerülnek:

- a Szolgáltatónak az Üzletmenet-folytonossági Tervben meghatározott felső vezetői,
- a Válságstáb vezetője és tagjai,

[27] Minden a tanúsítványokkal és kulcsokkal kapcsolatos művelet ide értendő. A hardverek (pl. UPS) és más biztonsági berendezések (pl. tűzfalak) valamint az operációs rendszerek és egyéb szoftverek (pl. vírusvédelmi szoftverek) naplóállományai külön kategóriát jelentenek.

- ♦ szükség esetén az ilyen események kezelésére szerződéssel lekötött szerviz cégeknek, az Üzletmenet-folytonossági Tervben megnevezett munkatársai.

4.5.8. Sebezhetőség kiértékelése

A hitelesítés szolgáltatás támogató informatikai rendszernek és annak fizikai és személyi környezetének a biztonsági sebezhetőségét két szempontból kell mérni:

1. Az informatikai rendszer által kezelt adatok bizalmasságának, hitelességének és sértetlenségének (röviden: az információvédelem) sérülése vagy elvesztése, ebbe beletartozik a Szolgáltató saját Aláírás létrehozó adatainak és aktiváló adatainak kompromittálódás elleni védelme is,
2. Az informatikai rendszer által kezelt adatok rendelkezésre állásának sérülése vagy elvesztése, amelynek kritikus mértékét az Üzletmenet-folytonossági Tervben meghatározott sebezhetőségi rés (a szolgáltatások kiesésének elviselhető mértéke egy hónapra vetítve, 7*24 órás folyamatos üzemet feltételezve) határozza meg.

Az aktuális sebezhetőségi szintek a biztonsági ellenőrzése és kiértékelése a 6.5.2 pont 3. táblázata szerinti rendszerben történik.

4.6. Adatarchiválás

A Szolgáltató gondoskodik arról, hogy a Tanúsítványra vonatkozó minden lényeges információ megfelelő ideig rögzítésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében[28].

4.6.1. A tárolt események típusai

A Szolgáltató gondoskodik arról, hogy rögzítésre kerüljön az összes regisztrációs információ, beleértve az alábbiakat is:

- az Igénylő által a regisztráció támogatása céljából benyújtott dokumentum(ok) típusa,
- az azonosító dokumentumok egyedi azonosító adatai (például az Igénylő jogosítvány száma),

[28] A tanúsítványokra vonatkozó rekordok regisztrációs információt és a Szolgáltató környezeti, kulcs- és tanúsítvány gondozási eseményeire vonatkozó fontos információt tartalmaznak.

- az Igénylő és azonosító dokumentumok (beleértve az aláírt, az Előfizetővel kötött megállapodást másolatainak tárolási helyszíne,
- az Előfizetővel kötött megállapodás esetleges egyedi választásai (például a tanúsítvány közzétételéhez történő hozzájárulás),
- a kérelmet elfogadó regisztrációs felügyelő (RO) azonosítója,
- a fogadó Hitelesítő Központ és/vagy a küldő Ügyfélkapcsolati Iroda neve, amennyiben ez értelmezhető.

A tanúsítványokra vonatkozó valamennyi naplóbejegyzés archiválásra kerül (lásd 3.1.9).

Azon eseményeket, mely a fent említett naplóbejegyzéseken túl kerülnek archiválásra (a biztonságos környezet fenntartásának és utólagos ellenőrizhetősége és bizonyíthatósága céljából), a Szolgáltató jelen HSzSz-e határozza meg.

4.6.2. Az archívum megőrzési időtartama

A Szolgáltató a 3.1.9 d) és e) pontjában megnevezett nyilvántartásokat a 3.1.9 g pontban meghatározott ideig megőrzi, illetve jogi eljárásban a tanúsítványokon keresztül történő bizonyításhoz szükséges ideig.

A Szolgáltató a tanúsítványokra vonatkozó napló adatokat (lásd 3.1.9 pontot) a 16/2001. (IX.1.) MeHVM rendelettel összhangban a keletkezésüktől számított 10 évig megőrzi.

A biztonságos környezet fenntartásának utólagos ellenőrizhetősége és bizonyíthatósága érdekében archivált egyéb naplóbejegyzések megőrzési időtartama 10 év.

4.6.3. Az archívum védelme

A Szolgáltató Biztonsági Adattárában olyan fizikai védelmet biztosít, amely fenntartja a tanúsítványokra vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét.

A Biztonsági Adattárba történő belépéshez csak az Szolgáltató informatikai biztonsági vezetője, a kijelölt SO és a rendszer auditor rendelkezik jogosultsággal.

A Biztonsági Adattárba történő hagyományos vagy elektronikus adattovábbítás csak biztonságos megoldással (az utóbbi esetben rejtjelezve, elektronikusan aláírva és időpecséttel ellátva) történhet.

A Biztonsági Adattárba érkező iratokat és adathordozókat az érkezési időpontot is tartalmazó nyilvántartásba kell venni, amellyel követni kell az előforduló irat és adathordozó mozgásokat (kivétel, visszaadás, megsemmisítés).

A Szolgáltató megfelelő műszaki és szervezeti védelmi intézkedéseket hoz, amelyek megvédik a személyes adatokat a felhatalmazás nélküli, illetve törvénytelen feldolgozás ellen, valamint a személyes adatok véletlen elveszése, megsemmisülése, illetve károsodása ellen.

4.6.4. Az archívum mentési folyamatai

Az elektronikus másolati példányban létező, archiválásra kijelölt adatok havonta egyszer mentésre kerülnek egyszer írható médiára. A Szolgáltató tanúsítványokra vonatkozó naplóadatokat teljes körűen és a bizalmasságot garantáló módon archiválja.

4.6.5. A rekordok időbélyegzésére vonatkozó követelmények

Lásd 4.6.3!

4.6.6. Az archívum gyűjtési rendszere

Az archivált adathordozók egy-egy példánya a Szolgáltató Biztonsági Adattárában kialakított archívumban és a tartalék helyszínen kerülnek elhelyezésre.

4.6.7. Archív információ hozzáférését és ellenőrzését végző eljárások

A Szolgáltató az archívumhoz Ügyfélkapcsolati Irodáján keresztül biztosít hozzáférést.
A hozzáférés az Aláírónak és az Előfizetőnek a rá vonatkozó adatokhoz lehetséges, más feleknek a 2.8.5, 2.8.6 és 2.8.7 pontok szerint. A Szolgáltató a jogosultságot minden esetben ellenőrzi, és azt naplózza.

4.7. Kulcs csere

Szolgáltató által kibocsátott végfelhasználói tanúsítványok érvényességi ideje 1 év.
Az érvényesség kezdete a kibocsátás ideje. Az aláírás létrehozó adatok érvényességi ideje megegyezik a tanúsítvány érvényességi idejével. Szolgáltató lehetőséget biztosít az előfizetők részére a tanúsítvány lejártát megelőző 30 napos időszakban arra, hogy a tanúsítványt megújítsák, a hozzá tartozó kulcspár cseréje mellett.

Előfizetői tanúsítvány egy alkalommal frissíthető, egy éves időtartamra. A frissítés igénylése a 3.2 pontban leírtak szerint történhet. A második frissítési kérelemnél az Aláírónak új Tanúsítványt kell igényelnie a kezdeti regisztráló eljárás módszerével és új kulcspár előállítása mellett. A kulcspár generálást a Trust&Sign szolgáltatások esetében mindig a Szolgáltató végzi.

A megújított tanúsítvány érvényességének kezdete a megújítás időpontja lesz. Az eredeti tanúsítvány a megújított tanúsítvány kibocsátásával egyidejűleg visszavonásra kerül.

A Szolgáltatói Aláírás létrehozó adatok megújítására előre tervezetten abban az esetben kerül sor, ha a kulcs érvényessége lejár, és azt nem hosszabbítják meg. Ebben az esetben a Szolgáltató a lejáratot megelőzően intézkedik az új, a szolgáltatói Aláírás létrehozó adat létrehozásának szabályai szerint történő előállításra és annak elkészültét valamint digitális lenyomatának publikálását követően, az előfizetők igénye alapján megkezdi részükre az új magánkulccsal aláírt tanúsítványok kiadását. A nem tervezett kulcs változtatás esetei a 4.8 pontban találhatók.

4.8. Katasztrófa elhárítás, Aláírás létrehozó adat kompromittálódás

A Szolgáltató gondoskodik arról, hogy katasztrófa esetén, beleértve a saját aláírás-létrehozó magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is, az üzemeltetés amint csak lehetséges helyreálljon.

A Szolgáltató Üzletmenet-folytonossági Tervében a katasztrófa események az üzletment-folytonosságot sértő események legszigorúbb osztályát képezik, így katasztrófa megelőzési és elhárítási intézkedések a Terv szerves részét képezik. A következő pontokban szereplő esetekre az Üzletmenet-folytonossági Terv részletes intézkedéseket tartalmaz.

4.8.1. Hardver, szoftver, vagy adatsérülés esete

A hardver és/vagy szoftver meghibásodások, valamint egyéb üzemzavarok osztálybasorolástól függő intézkedéseket vonnak maguk után. Katasztrófa helyzetben az Üzletmenet-folytonossági Tervben előírt „azonnali reakció” intézkedéseket kell foganatosítani, azaz értesíteni kell:

- a Szolgáltató meghatározott felső vezetőit,
- a Válságstáb vezetőjét és tagjait,
- szükség esetén a szerződéssel lekötött szerviz cégeknek, az Üzletmenet-folytonossági Tervben megnevezett munkatársai.

A Válságstáb első intézkedései:

- a katasztrófa esemény azonosítása és behatárolása,
- A katasztrófa esemény további hatásainak korlátozása,
- A károk azonosítása, a további károk keletkezésének megakadályozása, illetve mérséklése és a kárérték becslése.

A Válságstáb további intézkedései a hitelesítés szolgáltatást támogató informatikai rendszer részleges vagy teljes visszaállítására vonatkoznak a katasztrófa tartalék helyszínen.

4.8.2. Egy szolgáltatói egység nyilvános kulcsának visszavonása

Egy szolgáltatói kulcs visszavonása esetén a Szolgáltató az alábbiakat vállalja:

- a visszavonásról tájékoztatja az összes előfizetőt és érintett felet,
- jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok vagy visszavonási állapot információ már nem érvényes(ek).

A Szolgáltató a szolgáltatói kulcs kompromittálódását előidéző okok megszüntetése érdekében helyreállítja a biztonságos környezetet, valamint szükség esetén új kulccsal és új tanúsítvánnyal látja el szolgáltatói egységét, valamint a kompromittálódás által érintett aláírókat.

Katasztrófa esemény osztályba sorolt az Elsődleges Hitelesítő Központ („Root CA”), illetve a Szolgáltató operatív hitelesítő Aláírás létrehozó adatainak, az aktiváló adatoknak és a hardver biztonsági moduloknak az együttes kompromittálódása. Az Üzletmenet-folytonossági Terv forgatókönyvet tartalmaz az ilyen típusú katasztrófa események kezelésére.

A katasztrófa esemény a szolgáltatás azonnali felfüggesztésével jár és amennyiben a kompromittálódás ténye bizonyítást nyer, úgy az összes tanúsítványt vissza kell vonni. A szolgáltatások felfüggesztésének tényéről a Szolgáltató értesíti a felhasználó Közösség tagjait, valamint a Nemzeti Hírközlési Hatóságot.

4.8.3. Egy szolgáltatói egység kulcsának kompromittálódása

Egy szolgáltatói kulcs kompromittálódása esetén a Szolgáltató az alábbiakat vállalja:

- a kompromittálódásról tájékoztatja az összes előfizetőt és érintett felet,
- jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok vagy visszavonási állapot információ már nem érvényes(ek).

A Szolgáltató a szolgáltatói kulcs kompromittálódását előidéző okok megszüntetése érdekében helyreállítja a biztonságos környezetet, valamint a végfelhasználók számára új Aláírás ellenőrző adatot biztosít új tanúsítvány kiadásával.

Katasztrófa esemény osztályba sorolt a Root Hitelesítő Központ, illetve a Szolgáltató operatív hitelesítő Aláírás létrehozó adatainak, az aktiváló adatoknak és a hardver biztonsági moduloknak az együttes kompromittálódása.

Ez az esemény a hitelesítő szolgáltatás azonnali felfüggesztésével jár és amennyiben a kompromittálódás ténye bizonyítást nyer a Visszavonási listát meg kell szüntetni és erről, valamint a szolgáltatás felfüggesztésének tényéről a Szolgáltató értesíti a Szolgáltató és a felhasználó Közösség tagjait és a Nemzeti Hírközlési Hatóságot.

4.8.4. Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően

A súlyos üzemzavari és a katasztrófa esetet – többek között – az különbözteti meg, hogy katasztrófa esetén nagy valószínűséggel nem csak az informatikai rendszer, hanem annak a fizikai környezete is megsemmisül részben vagy egészben. Ez utóbbi esetben az Üzletmenet-folytonossági Tervben meghatározott módon a Válságstáb intézkedik a (katasztrófa) tartalékhelyszínre történő áttelepülésről és az informatikai rendszer részleges vagy teljes visszaállításáról a Biztonsági Adattárban korábban elhelyezett mentések segítségével.

4.8.5. Üzletmenet-folytonossági Terv

A Szolgáltató rendelkezik Üzletmenet-folytonossági tervvel, amely részletes intézkedési forgatókönyveket tartalmaz a különböző osztályú üzemzavari, illetve katasztrófa események kezelésére. Ez a dokumentum biztonsági okokból nem nyilvános.

4.9. A hitelesítés-szolgáltatási tevékenység megszüntetése

A Szolgáltató a szolgáltatás megszűnése esetén késlekedés nélkül értesíti a Szolgáltató és a felhasználó Közösség tagjait és a Nemzeti Hírközlési Hatóságot. Amennyiben a megszűnés tervezett, az értesítés legkevesebb 60 nappal megelőzi a szolgáltatás leállítását.

A Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezd más szolgáltatókkal a szolgáltatás átvételéről. A tárgyalások végeredményéről tájékoztatja a közösséget. Az értesítést a Szolgáltatás

nyújtásában részt vevő szervezeteknek és az Előfizetőknek elektronikus aláírásával ellátott e-mailben küldi el, s az Érintett felek tájékoztatása végett a web oldalain is közzé teszi.

A bejelentéssel egyidejűleg a Szolgáltató leállítja:

- tanúsítvány előállítás szolgáltatást (ezen belül a tanúsítvány megújítását),
- kezdeti regisztráló szolgáltatást (egyéb regisztráló szolgáltatások tovább élnek),
- tanúsítvány kibocsátás szolgáltatást (ezen belül a tanúsítványok archiválását),
- aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatást.

Szolgáltató a tervezett megszűnés előtt 20 nappal intézkedik az előfizetői tanúsítványok és saját felhasználású tanúsítványok visszavonásáról.

Ezzel egyidejűleg leállítja a következő szolgáltatásokat:

- visszavonás kezelési szolgáltatás.
- visszavonási állapot közzététele szolgáltatás.

Szolgáltató nem biztosít a szokásosnál és a jogszabályokban előírtnál nagyobb mértékű adatszolgáltatást a megszűnéskor.

Eljárás regisztrációs szervezet megszűnése esetén:

- Az Ügyfélkapcsolati Iroda megszűnése előtt 60 nappal értesíti azon Előfizetőket, akik a megszűnő Regisztrációs Irodától kapott, a Szolgáltató által kibocsátott érvényes tanúsítvánnyal rendelkeznek. Az értesítésben jelzi, hogy a tanúsítványt milyen határidővel vonja vissza, és tájékoztatja az Előfizetőt arról, hogy mely Regisztrációs Szervezeteknél igényelhet díjmentesen új tanúsítványt.
- Az Ügyfélkapcsolati Iroda megszűnéséről a felhasználó Közösség tagjait Szolgáltató a web oldalain történő közzététel útján tájékoztatja.

5. Fizikai, eljárásrendi, és humán biztonsági szabályozások

A Szolgáltató gondoskodik arról, hogy kellő, az elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések és az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra. Ezen belül:

- A Szolgáltató kockázat elemzést végzett üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és működési eljárások meghatározása érdekében.
- A Szolgáltató felelősséget vállal minden elektronikus aláírással kapcsolatos szolgáltatásért, még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki. A Szolgáltató egyértelműen meghatározza a harmadik felek felelősségét, és megfelelő konstrukciók biztosítják azt, hogy a harmadik felek a Szolgáltató által megkövetelt összes ellenőrzés végrehajtására legyenek szorítva. A Szolgáltató felelősséget vállal valamennyi fél fentiekre vonatkozó gyakorlatának nyilvánosságra hozására.
- A Szolgáltató vezetősége (mely felelős a Szolgáltató informatikai biztonság politikájának meghatározásáért, és e politika által érintett valamennyi alkalmazott részére történő közzétételért) az információ biztonságára vonatkozó útmutatót hagyott jóvá és adott ki.
- A Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a Szolgáltató vezetőségének kell jóváhagynia[29].
- A Szolgáltató a Biztonsági Szabályzatában dokumentálta, majd megvalósította és folyamatosan fenntartja a hitelesítési szolgáltatásokat nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait[30].

[29] Az informatika biztonság kezelésével kapcsolatban útmutatásként lásd a MeH 12. ajánlást és az ISO/IEC 17799-et.

[30] Ajánlott, hogy ez a Biztonsági Szabályzat azonosítsa a nyújtott szolgáltatásokkal kapcsolatos valamennyi fontos célt és potenciális veszélyt, valamint az ezen veszélyek hatásainak elkerülése, illetve korlátozása érdekében szükséges védelmi intézkedéseket. Ajánlott leírnia az arra vonatkozó szabályokat, irányelveket és eljárásokat, hogy a meghatározott szolgáltatásokat és az ezekkel kapcsolatos biztonsági garanciákat hogyan biztosítják.

- A Szolgáltató gondoskodik az informatikai biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősség más szervezethez, illetve egységhez lettek kiadva.
- A Szolgáltató biztonsági műveleteiért a végső felelősség a felső vezetőségéé. Ezen biztonsági műveletek közé az alábbiak tartoznak:
    - üzemeltetési eljárások és felelősségek
    - biztonsági rendszerek tervezése és elfogadása
    - káros szoftver elleni védelem
    - erőforrás gazdálkodás
    - hálózat menedzselés
    - a biztonsági napló aktív felügyelete, eseményelemzések és nyomkövetések
    - adathordozó eszköz kezelése és biztonsága
    - adat és szoftver csere

  E felelősségeket a Szolgáltató biztonsági műveletei kezelik, azokat szakértő üzemeltető személyzet hajthatja végre.

A Szolgáltató gondoskodik arról, hogy eszközei és információi megfelelő szintű védelemben részesüljenek. A Szolgáltató valamennyi informatikai értékéről leltárt vezet, ezek védelmi követelményeit osztályokba sorolja és minősíti, az elvégzett kockázat elemzéssel összhangban

A Szolgáltató fizikai, eljárásrendi (adminisztratív) és humán biztonsági szabályozásait a Trust&Sign Szolgáltatások Biztonsági Szabályzata tartalmazza részletesen. A Trust&Sign Szolgáltatások Biztonsági Szabályzata biztonsági okokból nem nyilvános.

A szolgáltatást támogató informatikai rendszer, annak személyi és fizikai környezete a MeH ITB 12. ajánlás szerint a fokozott biztonsági osztályba tartozik, amely egyértelműen meghatározza a Hitelesítő Központok és a Regisztrációs Iroda informatikai rendszereinek, személyi és fizikai környezetének biztonsági követelményeit.

A következő pontok csak a vonatkozó lényeges intézkedéseket tartalmazzák.

5.1. Fizikai biztonsági szabályozások

5.1.1. Hitelesítő Központok

Ebben a pontban az Elsődleges (Root) Hitelesítő Központon kívül a fizikai objektumokban létező (nem logikai) másodlagos hitelesítő központok fizikai biztonsági szabályairól lesz szó.

A hitelesítő központok legmagasabb védelmi szintet képező objektuma a Bizalmi Központ, amely a biztonsági szempontból legkritikusabb hardver/szoftver elemeket tartalmazza. Ez az objektum fokozott biztonsági osztályba sorolt, amely a következő, a MeH ITB 12. ajánlás szerinti főbb fizikai védelmi követelményeknek felel meg:

- a fokozott biztonsági szintnek megfelelő szilárdságú határoló felületek,
- a Bizalmi Központ bejárati ajtaja és a technikai helyiség ajtaja a MABISZ ajánlásában meghatározott I-es kategóriájú, a perszonalizációs helyiség ajtaja MABISZ III. kategóriájú.
- a Bizalmi Központ objektum előtt biztonsági szegmens van kialakítva, amelybe anti-passback és naplózási tulajdonságokkal bíró beléptető rendszeren keresztül lehet csak bejutni,
- a biztonsági szegmensbe és a Bizalmi Központba történő bejutást és az ott történő mozgásokat video kamerás biztonsági rendszer figyeli,
- a Bizalmi Központ felett, illetve a közvetlen környezetében nincs nagyobb áteresztő képességű víz, szennyvíz, gáz vagy erősáramú vezeték,
- a Bizalmi Központ rendelkezik klimatizálással, mozgásérzékelő és tűz- és füstjelző rendszerrel,
- A Bizalmi Központ IT eszközei két, egymástól független külső betáplálással támogatott, Diesel aggregátoros szünetmentes tápáramellátó rendszerrel rendelkeznek,
- a Bizalmi Központban a szerverek biztonsági kabinetekben vannak elhelyezve,
- a Bizalmi Központra és a kabinetekre a Biztonsági Szabályzat egy fejezetét képező kulcskezelés szabályozás érvényes,
- A Bizalmi Központ az MSZ 274/5T:1993 szabvánnyal összhangban LPZ2 zónahatárig kiépített másodlagos villámvédelemmel ellátott,
- A Bizalmi Központba csak a Biztonsági Szabályzatban meghatározott szerepkörű vezetők és munkatársak léphetnek be,

- A mentési és a primer szoftver adathordozók, a nyers és a megszemélyesített Aláírás létrehozó eszközök besugárzás és fizikai behatás ellenálló biztonsági szekrényekben tároltak.
- A működtetési és menedzselési, valamint a biztonsági dokumentáció elektronikusan tárolt.

5.1.2. Regisztrációs Iroda

A regisztrációs tevékenység a Bizalmi Központ perszonalizációs helyiségében folyik, amely az előző pontban ismertetett fokozott biztonságú fizikai védelemmel van ellátva. Itt találhatók a regisztrációs munkahelyek és munkaállomások.

5.2. Eljárásrendi szabályozások

A Szolgáltató Eljárásrendi Szabályait három szabályzat tartalmazza:

- a Szervezeti és Működési Szabályzat, amely részletesen meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes munkaköröket és az azokhoz kapcsolt feladat-, felelősség és hatásköröket,
- a jelen HSzSz,
- a Trust&Sign Szolgáltatások Biztonsági Szabályzata, amely részletesen szabályozza az adatokhoz és az informatikai rendszerekhez, valamint a személyi és a fizikai környezethez kapcsolódó biztonsági szabályokat.

Jelen pont 2. táblázatában a hitelesítő szolgáltatáshoz kapcsolódó szerepköröket, azok feladat-, felelősség és hatáskörei kerülnek összefoglalásra.

Szerepkör	Feladatkör	Felelősségi kör	Hatáskör
A Szolgáltató vezetője	A Szolgáltató szervezet irányítása és ellenőrzése	Folyamatos és biztonságos szolgáltatás. A Trust&Sign Rendszer és adat tulajdonosa	A Szolgáltató munkáltatói jogköre. A teljes szervezet szintjén dönt
A PKI Üzleti Egység vezetője	A Szolgáltató szervezet szolgáltatási tevékenységének irányítása és ellenőrzése	Folyamatos és biztonságos szolgáltatás. Trust&Sign Rendszer működtetésének egy-személyi felelős vezetője	A Szolgáltató szervezet szintjén dönt, intézkedik.
Ügyfélkapcsolati Iroda vezetője	Az ügyfélkapcsolati tevékenység irányítása és ellenőrzése.	Az ügyfelek biztonságos azonosítása-hitelesítésének ellenőrzése.	Az ügyfélkapcsolati tevékenység ellenőrzése.

Hitelesítés Pol. és Szab. Csop. Vezető	Politikák, szabályzatok kialakítása, PKI belső ellenőrzés	Politikák, szabályzatok és gyakorlat összhangja	Politikák, szabályzatok érvényesítése, PKI belső audit
A Szolgáltató IB vezetője	IB tevékenység irányítása, ellenőrzése a Szolgáltató minden területén.	IB kockázatok elviselhető szinten tartása	IB intézkedések, IB belső ellenőrzés.
Üzemeltetés vezető	Az IT rendszer üzemeltetés irányítása	Az üzemeltetés folyamatossága, minősége, biztonsága	Intézkedés az IT rendszer minden szintjén üzemeltetési kérdésekben
Üzemeltető adminisztrátor	Üzemeltetési adminisztráció, hibaelhárítás, karbantartás	Az üzemeltetés folyamatossága, minősége	Operatív intézkedés az üzemeltetés területén
IB adminisztrátor	Biztonsági beállítások, adminisztráció, karbantartás	Az üzemeltetés biztonsága	Operatív ellenőrzés, operatív intézkedés
Hitelesítő biztonsági felügyelő (Security Officer /SO/)	RO kulcsok, tanúsítványok létrehozása	Saját kulcs, PKI alkalmazás és adatok biztonsága	RO és ügyfél kulcsok, tanúsítványok létrehozása. RO hatásköre is lehet.
Regisztrációs felügyelő (Registration Officer /RO/)	Regisztrációs Iroda irányítása. Előfizető regisztráció, kulcs, tanúsítvány igénylése, kulcs megszemélyesítése	Regisztrációs Iroda folyamatos működtetése.	Regisztrációs Irodán intézkedési jog. SO hatásköre nem lehet.
Rendszer operátor	Üzemeltetési rutin tevékenységek PKI szinten.	A PKI alkalmazás üzemeltetésének folyamatossága,	Rutin operátori tevékenység az Üzemeltetési Kézikönyv szerint
Rendszer vizsgáló (auditor)	Operatív funkcionális és biztonsági ellenőrzések.	Funkcionális és biztonsági hiányosságok, visszaélések felfedése.	Biztonsági és audit naplók ellenőrzése.

2. táblázat

Az egyes munkakörökben elvárt azonosítás és hitelesítés

A *Hitelesítő Központnál* valamennyi bizalmi munkakört betöltő munkatársának (SO-k, IB adminisztrátor, működtető adminisztrátor, operátor, valamint rendszer auditor) azonosítása és hitelesítése egy intelligens kártyaolvasóba helyezésével, majd az azt aktivizáló PIN kód megadásával történik[31] A hitelesítésre használt kártya (a kombinált kártya másik chip-jére alapozva) egyben a zárt körletbe való bejutást is lehetővé teszi.

[31] Tehát az alkalmazott hitelesítés egy birtokláson és egy tudáson alapuló mechanizmus kombinációján alapul.
Lehetséges példák még (különböző erősségű, különböző veszélyek ellen védelmet biztosító hitelesítési mechanizmusokra):

- változó, egyszer használatos jelszó megadása, melyet egy a rendszerhez nem csatolandó, külön hardver token szolgáltat időtől és felhasználótól függő módon, mindig másképpen, s melyet a központi szerver oldalon folyamatosan utána számolva ellenőriznek,

Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani.

A Regisztrációs Iroda valamennyi bizalmi munkakört betöltő munkatársának azonosítása és hitelesítése egy intelligens kártyaolvasóba helyezésével, majd az azt aktivizáló PIN kód megadásával történik. A hitelesítésre használt kártya lényegében megegyezik a Hitelesítő Központnál használt kártyával, csak az utóbbin nincs rajta az előbbi közelítéses 2. chipje[32].

Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani.

5.3. Humán szabályozások

A Szolgáltató gondoskodik arról, hogy személyzeti, illetve a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák a Szolgáltató működésének megbízhatóságát. Különösképpen:

- A Szolgáltató kellő számú, az elektronikus aláírással kapcsolatos szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező személyzetet alkalmaz.
- A Szolgáltató valamennyi bizalmi munkakört betöltő munkatársa független minden olyan ütköző érdektől, ami hátrányosan érinthetné a hitelesítés-szolgáltató tevékenységeinek semlegességét.

A Szolgáltató (ideiglenes és állandó) munkatársainak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaleírásokkal rendelkeznek. A munkaleírások meghatározzák a beosztás érzékenységét, a feladatok és a hozzáférési szintek, a háttér-ellenőrzés, az alkalmazott képzettség és tudatosság alapján. Ahol erre szükség van, megkülönböztetik az általános funkciókat és a hitelesítés-szolgáltató specifikus funkciókat. A munkaleírások meghatározzák az egyes feladatokhoz szükséges létszámot is. A munkaleírások tartalmazzák a szakismeretre és a tapasztalatra vonatkozó követelményeket is.

- biometrikus hitelesítés (pl. a felhasználó ujjlenyomatának ellenőrzésével),
- fix jelszó megadása.

[32] Ebből következően az SO saját (kombinált) kártyájával beléphet ebbe a gépterembe is.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

A Szolgáltató olyan személyzetet alkalmaz, amely rendelkezik a kínált szolgáltatáshoz szükséges szakértői tudással, tapasztalattal és minősítésekkel.

A Szolgáltató kellő számú, a hitelesítési szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező személyzetet alkalmaz.

A vezető személyzet tapasztalattal rendelkezik az elektronikus aláírási technológia terén, ismeri a biztonsági felelősséggel tartozó munkatársakra vonatkozó biztonsági eljárásokat, valamint gyakorlattal rendelkezik az informatika biztonság és a kockázat elemzés területein.

5.3.2. Biztonsági háttér ellenőrzésekre vonatkozó eljárások

A 2. táblázatban meghatározott szerepkörök mindegyikéhez történő személy hozzárendelésnél az átlagosnál magasabb szintű biztonsági ellenőrzés történik. Közülük a következők minősülnek biztonsági szempontból kulcsszerepkörnek:

- A Szolgáltató üzleti egység vezetője
- Hitelesítés Pol. és Szab. Csop. Vez.
- A Szolgáltató IB menedzsere
- IB adminisztrátor
- Hitelesítő biztonsági felügyelő (Security Officer /SO/),
- Regisztrációs felügyelő (Registration Officer /RO/),
- rendszer vizsgáló (auditor).

A szerepkörökhöz csak fokozott biztonsági ellenőrzéssel lehet személyt rendelni, amelyhez szükséges a szerepkörre kijelölt személy hozzájárulása, ugyanakkor a fokozott ellenőrzés a szerepkör betöltésének alapfeltétele.

A fokozott biztonsági ellenőrzés fontosabb intézkedései:

- Újonnan felvett személy csak 1 éves próba idő után töltheti be a szerepkört,
- Felvételkor, illetve a szerepkörhöz történő hozzárendeléskor:
  - több azonosító dokumentumból történő azonosítás-hitelesítés
  - életrajzi adatok, információk ellenőrzése,
  - anyagi helyzet ellenőrzése,

- családi helyzet ellenőrzése,
- személyiség vizsgálat.

A szerepkörhöz történő hozzárendeléskor:

- pontos és írásos munkaköri leírást kell adnia a fölérendelt vezetőnek,
- Gondoskodni kell a megfelelő helyettesítésről betegség, szabadság, egyéb okú távollét esetére,
- titoktartási nyilatkozatot kell a kijelölt személlyel aláíratni, amelyben 5év titoktartási kötelezettség szerepel a Szolgáltatótól történő kilépés utáni időponttól számítva,
- a szükséges mértékű oktatásban kell a kijelölt személyt részesíteni, annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és gyakorolni tudja.

Kilépéskor:

- A kilépésről szóló döntés meghozatalakor a kilépő fizikai és logikai belépési és hozzáférési jogosultságait azonnal meg kell szüntetni. A kilépő ezután az informatikai biztonsági menedzser kíséretében léphet be még egyszer a munkahelyi környezetébe, a személyes dolgai elvitele céljából.
- A kilépő személy számítógépes tevékenységét legalább két hétre visszamenőlegesen le kell ellenőrizni.
- Vissza kell venni az Aláírás létrehozó eszközét, azonnal és dokumentáltan meg kell semmisíteni azt. A kapcsolódó tanúsítvány(oka)t azonnal vissza kell vonni.
- Minden, a kilépőnél levő dokumentációt és ügyiratot vissza kell venni, különös tekintettel a biztonsági és/vagy minősített adatokat információkat tartalmazó anyagokra.

A visszaadott anyagokról tételes átvételi jegyzőkönyvet kell felvenni.

Nem tölthet be bizalmi munkakört az a személy, aki akár az alap, akár egy időszakos biztonsági ellenőrzésen a „elfogadhatatlanul nagy biztonsági kockázat” minősítést kapja[33].

Az időszakos biztonsági ellenőrzésre rendszeres időnként kerül sor:

- IB adminisztrátorok, SO-k és RO-k esetében 3 évente,
- működtető adminisztrátorok, valamint operátorok esetében 5 évente.

[33] A már bizalmi munkakört betöltő munkatársaktól való, biztonsági okokból történő megválást az alkalmazható legdiszkrétebb módon hajtják végre.

5.3.3. A felhatalmazás nélküli tevékenységek büntető következményei

Valamennyi bizalmi munkakört betöltő munkatárs esetén, a munkakörbe kinevezéskor a foglalkoztatási dokumentumok részeként

- írásos tájékoztatást kapott jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról,
- munkaköri leírást kapott, mely tartalmazta az őt érintő biztonsági feladatokat,
- titoktartási nyilatkozatot írt alá, melyben a biztonsági intézkedések be nem tartásával járó, őt érintő következmények (büntető szankciók) is megfogalmazódtak.

Mindezek tartalmazzák azokat a munkajogi - vagy büntető következményeket, melyek a különböző fegyelem- munkaköri kötelezettség- illetve törvénysértést szankcionálják.

Amennyiben egy munkatárs (gondatlanságból fakadóan vagy szándékosan) megsérti a fenti szabályokat, ellene büntető intézkedéseket hoznak, amelyek az elkövetés módjától és következményétől függően a jutalom megvonástól fegyelmi eljárás indításán és kártérítésen át, egészen a hatósági feljelentésig terjedhet.

5.3.4. A szerződéses alkalmazottakra vonatkozó követelmények

A Szolgáltató bizalmi munkakörben csak vele 1 évnél hosszabb munkaviszonyban álló személyt alkalmaz.

Az egyéb feladatok ellátására, alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket (külső munkavállalókat és ideiglenes alkalmazottakat egyaránt) a Szolgáltató csak az „ellenőrzött beszállítók” listájáról választ. Az ellenőrzött beszállítókkal a PKI Üzleti Egység előzetesen írásos megállapodást köt, melyben vállalta a Szolgáltató biztonságpolitikájának elfogadását.

Valamennyi szerződő fél - még a tényleges munkavégzés megkezdése előtt – titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során későbbiekben megismerendő üzleti/vállalati titkokat illetéktelen személynek fel nem fedi, s egyéb módon sem hasznosítja. A titoktartási nyilatkozat záró része tartalmazza a megszegése esetén alkalmazandó szankciókat is.

A külső munkavállalók és ideiglenes alkalmazottak szakmai kiképzésben, továbbképzésben nem részesülnek, erre nem kötelezettek[34].

5.3.5. A személyzet számára biztosított dokumentációk

A személyzet számára biztosítandó dokumentációt a 9.1 pont sorolja fel.

[34] A külső munkavállalókat eleve úgy választják meg, hogy az adott munkafeladathoz minden szakmai ismerettel és gyakorlattal rendelkezzenek. Az ideiglenes alkalmazottak olyan jellegű munkát végeznek, melyhez nincs szükség ki- és továbbképzésre.

6. Műszaki biztonsági óvintézkedések

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

Az informatikai rendszer szállítója hitelesítés-szolgáltatási rendszer kiépítésében jelentős tapasztalatokkal rendelkezik, nemzetközileg elismert technológiát alkalmaz.

6.1. Kulcs-pár előállítás és telepítés

6.1.1. Kulcs-pár előállítás

A Szolgáltató maga generálja a kulcspárt biztonságos szoftver modulban vagy magán a kártyán (on-board). Nem fogad el az Előfizető által generált Aláírás létrehozó adatot, illetve eszközt. Az Aláírás létrehozó eszköz (chip kártya) megszemélyesítése a Szolgáltatónál – fokozott biztonságú környezetben – üzemelő kártyamegszemélyesítő rendszeren történik.

Az Aláírás létrehozó adat elhelyezésére a Szolgáltató csak Tanúsítvány kibocsátással és a kibocsátott Tanúsítvány chip kártyán történő elhelyezésével együtt vállalkozik.

A chip kártya megszemélyesítés szolgáltatáshoz vizuális – egy oldali nyomással történő – grafikus megszemélyesítése is kapcsolódik az Előfizetői Szerződésben meghatározott adattartalommal. A Szolgáltató a Tanúsítványt tartalmazó chip kártyához a Szolgáltató PIN kódot biztosít.

Teszt célú Aláírás létrehozó adat teszt CA-n keresztül történő igényléskor a kulcspár generálása az Aláírónál történik.

A Szolgáltatói saját kulcspár előállítása:

- A Szolgáltatónál történő kulcselőállítást fizikailag védett környezetben, bizalmi munkakört betöltő személyzet végzi, legalább kettős ellenőrzés[35] mellett. A kulcspár előállítási funkció végrehajtására felhatalmazott személyzet körét a Szolgáltató, HSzSz-ének megfelelve, a lehető legkisebbre korlátozza.

[35] Két személy együttes jelenlétével

- A Szolgáltató a kulcs előállítását olyan algoritmussal valósítja meg, melyet jogszabály ismer el erre a célra alkalmasnak.[36]

A Szolgáltató által más felek számára előállított kulcspár előállítás:

- A Szolgáltató által saját szervezeti egységei /Címtár, Regisztrációs Iroda/ számára előállított kulcsokat biztonságos módon, egy olyan algoritmussal állítja elő, melyet jogszabály ismer el erre a célra alkalmasnak[37].
- A Szolgáltató által az alanyok számára előállított kulcsokat biztonságos módon, egy olyan algoritmussal állítja elő, melyet jogszabály ismer el erre a célra alkalmasnak [38].
- Az Aláírás-létrehozó eszköz elkészítését (logikai és fizikai megszemélyesítését) a Szolgáltató ellenőrzi.

A Hitelesítő Központ az alábbi kulcspárokat használja

- A végfelhasználói tanúsítványokat aláíró kulcs,
- a Regisztrációs Iroda tanúsítványait aláíró kulcs,
- visszavonási lista aláíró kulcs,
- az SSL protokollhoz felhasznált kulcspár.

Valamennyi kulcspárt saját maga generálja, egy védett kriptográfiai hardver modulban. A generált magánkulcsok (a 6.2.4 alatt részletezett) mentést (klónozást) leszámítva, teljes életciklusuk alatt a kriptográfiai hardverekben marad, megsemmisítéséig azt sehová nem kell továbbítani.

Az SSL protokollhoz felhasznált kulcspárt szintén saját maga generálja, egy másik védett kriptográfiai hardver modulban.

A Regisztrációs Iroda az alábbi kulcspárokat használja:

- Az archiválandó regisztrációs adatokat és tranzakciókat aláíró kulcs,
- Az SSL protokollhoz felhasznált kulcspár.

[36] A 2/2002 (IV.26) MeHVM irányelv 1. sz. melléklete felsorolja a megfelelőnek elismert kulcspár előállítási algoritmusokat.

37 A 2/2002 (IV.26) MeHVM irányelv 1. sz. melléklete felsorolja a megfelelőnek elismert kulcspár előállítási algoritmusokat.

[38] A 2/2002 (IV.26) MeHVM irányelv 1. sz. melléklete felsorolja a megfelelőnek elismert kulcspár előállítási algoritmusokat.

A fenti kulcspárokat a Regisztrációs Iroda számára a Hitelesítő Központ generálja, védett kriptográfiai hardver modulban. A generált magánkulcs teljes életciklusa alatt a kriptográfiai hardverben marad, megsemmisítéséig azt sehová nem kell továbbítani.

A végfelhasználók kulcspárjait a Regisztrációs Iroda kezdeményezésére a PKI alkalmazás generálja egy védett kriptográfiai hardver modulban. A minősített aláíró kulcs védett csatornán átkerül a Biztonságos aláírás-létrehozó eszközre, s előállítása helyén azonnal és minden későbbi reprodukálást kizáró módon megsemmisül. Ezt követően a magánkulcs teljes életciklusa alatt csak a biztonságos aláírás-létrehozó eszközön (intelligens kártya) marad, a végfelhasználókhoz való továbbítása magának az intelligens kártyának a végfelhasználóhoz történő továbbítását jelenti.

6.1.2. Az Aláírás létrehozó adat felhasználóhoz történő eljuttatása

A Szolgáltató amikor kulcsokat generál más felek (Regisztrációs Iroda és Aláírók) számára:

- az általa más felek számára előállított kulcsokat az Előfizető vagy az Aláíró által történő személyes átvételig biztonságos módon tárolja,
- az általa más felek számára előállított magánkulcsot az Előfizetőnek vagy az Aláírónak úgy adja át, hogy a magánkulcs titkossága ne sérüljön,
- az átadást követően csak az Aláíró férhet hozzá saját magánkulcsához,
- a Szolgáltató biztonságosan ellenőrzi az Aláírás-létrehozó eszköz elkészítését,
- a Szolgáltató a nem megszemélyesített Aláírás-létrehozó eszközt is biztonságosan tárolja.
- a Szolgáltató biztonságosan ellenőrzi az Aláírás-létrehozó eszköz kiiktatását és újraaktivizálását,
- a Szolgáltató az Aláírás-létrehozó eszköz aktivizálási adatait (PIN kód) biztonságosan készíti el és az aláírás-létrehozó modultól elkülönítve osztja szét.

Az Előfizető vagy az Aláíró számára:

- olyan algoritmus felhasználásával kell előállítaniuk az alany kulcsait, melyet jogszabály a tanúsítványtípusban azonosított kulcshasználatra megfelelőnek ismer el,
- olyan kulcshosszúságot és algoritmust kell alkalmazniuk, amelyet jogszabály a tanúsítványtípusban azonosított kulcshasználatra megfelelőnek ismer el.

Egy Előfizetőnek a megszemélyesített és legyártott chip kártyákat (az Aláírás-létrehozó eszközt aktivizáló PIN kódot tartalmazó zárt borítékkal együtt) személyesen kell átvennie, az átvétel írásos elismerésével.

Az átadás során átadásra kerül:

- Kulcshordozó eszköz és rajta a magánkulcs, illetve a tanúsítvány
- Az aláírt regisztrációs űrlap egy példánya
- Tájékoztató füzet
- Az aláírt Előfizetői Szerződés egy példánya

A kulcshordozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

6.1.3. Aláírás ellenőrző adat eljuttatása a tanúsítvány kibocsátóhoz

Az Előfizető tanúsítványba foglalandó nyilvános kulcsa a Regisztrációs Irodától PKCS#10 tanúsítványigénylés formában, a Regisztrációs Szervezet magánkulcsával elektronikusan aláírt elektronikus üzenetben kerül a Hitelesítő Központhoz.

6.1.4. Hitelesítő Szervezet Aláírás ellenőrző adatának eljuttatása a felhasználókhoz

A Szolgáltató a Hitelesítő központok Root CA által aláírt nyilvános kulcsait saját Címtárában teszi mindenki számára elérhetővé[39].

Az itt közzétett Tanúsítvány ellenőrzéséhez szükséges Root CA nyilvános kulcs közzététel az alábbi módon valósul meg:

- A hitelesítő központ a Root CA-tól egy tokenen kapja meg a nyilvános kulcsot, amelyet két SO személyesen hoz el a Root CA-tól.
- A Regisztrációs Iroda a Root CA-tól egy tokenen kapja meg a nyilvános kulcsot, amelyet két SO személyesen hoz el a Root CA-tól.
- Az aláírók a Root CA nyilvános kulcsát a Regisztrációs Iroda által feltöltött Aláírás létrehozó eszközön (intelligens kártyán) kapják meg a személyes átvételkor.

A fentieken kívül a Root CA nyilvános kulcsa megszerezhető, illetve ellenőrizhető közvetlenül is, mivel a Szolgáltató CA közzéteszi a Root CA nyilvános kulcsát a *http://www.mavinformatika.hu/ca/* web lapon keresztül.

---

[39] Mivel a Hitelesítő Központ nem önaláírt, hanem a Root CA által aláírt tanúsítványt alkalmaz, ezért a saját nyilvános kulcsának közzétételére használt módszer mindenki számára (aki rendelkezik a Root CA nyilvános, tanúsítvány ellenőrzéshez szükséges kulcsával) megbízható.

A produktív hitelesítő központok nyilvános kulcsai azok Tanúsítványába foglalva a Címtárba íródnak. A hitelesítő központok tanúsítványai felkerülnek a Szolgáltató nyilvános web oldalaira is a *http://www.mavinformatika.hu/ca/* címen.

A tanúsítványok letölthetők és a felhasználó kliens-alkalmazásába installálhatók. A Szolgáltató Ügyfélkapcsolati Irodája, kérés esetén, telefonon is rendelkezésre áll a digitális lenyomat egyeztetése céljából.

6.1.5. Kulcs méretek

Az Elsődleges (1. szintű) Hitelesítő Központ ("Root CA")
aláíró kulcsának mérete: 2048 bit
kommunikációs kulcsának mérete: 1024 bit

A 2. szintű Hitelesítő Központ („Produktív CA”)
aláíró kulcsainak mérete: 2048 bit
kommunikációs kulcsának mérete: 1024 bit

A Regisztrációs Iroda
kommunikációs kulcsának mérete: 1024 bit

Az Aláírók (Előfizetők)
aláíró kulcsainak mérete: 1024 bit

A Szolgáltató folyamatosan figyelemmel kíséri a technikai fejlődést és ennek függvényében szükség esetén gondoskodik kulcshosszak növeléséről.

6.1.6. Előfizetői Aláírás ellenőrző adat előállításához használt paraméterek előállítása

A végfelhasználói Aláírás ellenőrző adat generálásához használt paraméterek előállítását a PKI alkalmazás végzi.

6.1.7. Előfizetői Aláírás ellenőrző adat előállításához használt paraméterek előállítása

A Hitelesítő Központ és a Regisztrációs Iroda az elektronikus aláírás létrehozására az RSA[40] algoritmust használja.

RSA algoritmussal van aláírva a rendszer által kibocsátott minden tanúsítvány, és ezt az algoritmust használják a rendszeren belül is a letagadhatatlanság (regisztrációs pontokról küldött adatok, tranzakciók aláírása, központi regisztráló szervezet által archivált adatok, tranzakciók) biztosítására.

Az Aláírók számára kibocsátott tanúsítványok az RSA aláíró algoritmusokhoz használhatók.

Az előfizetői Aláírás ellenőrző adat generálásához használt paraméterek előállítását teszt cél esetében a PKI alkalmazás, a szerződéses viszonyban álló Aláírók esetében az Aláírást létrehozó eszköz on board elvégzi.

6.1.8. Szoftveres / hardveres kulcsgenerálás

A Szolgáltatóra vonatkozóan szoftveresen Aláírás létrehozó eszközben történik a kulcsgenerálás, amelyet a Szolgáltató saját aláírású tanúsítvánnyal hitelesít.

Az előfizetői kulcsokat a Szolgáltató vagy Aláírás létrehozó eszközben vagy PKI alkalmazással hozza létre.

6.1.9. Kulcs felhasználási célok

A Szolgáltató Előfizető részére kulcs-párt elektronikus aláírási vagy azonosítás-hitelesítési céllal bocsát ki.

Ennek érdekében az Előfizetők részére kibocsátott tanúsítványok bővítmény (Extension) részében található „KeyUsage” mezőbe felhasználási területtől és céltól függően „digitalSignature” és „nonRepudiation” kulcshasználati módoknak megfelelő kijelölést alkalmaz.

Azonosítás-hitelesítési célú tanúsítványban a „Key Usage” mezőbe a „Digital Signature” módot, és a „Key Usage” kiterjesztéseként a „clientAuth” módot állítja be.

40 Az RSA algoritmust (Rivest, Shamir and Adleman Algorithm) az alábbi szabvány írja le részletesen: International Organization for Standardization, “ISO/IEC 14888-3: Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms,” 1999.

A kulcspár kizárólag arra a célra használható, amelyre a Szolgáltató kibocsátotta, a HSzSz-nek és az Előfizetői Szerződés feltételeinek megfelelően.

6.2. Aláírás létrehozó adat védelme

6.2.1. Kriptográfiai modulra vonatkozó szabványok

Az Előfizetők Aláírás létrehozó adatának tárolására Szolgáltató olyan eszközt bocsát ki, mely teljesíti a FIPS 140-1 Level 3 követelményeket

Az Aláírás létrehozó adatot a Szolgáltató PIN kóddal védve bocsátja ki. Az Aláírás létrehozó adat dokumentált átvétele után az Előfizető felelős az Aláírás létrehozó eszköz, az Aláírás létrehozó adat, valamint a PIN kód védelméért.

A Szolgáltató saját kulcsainak tárolására chip kártyát alkalmaz, amely teljesíti legalább a FIPS 140-1 Level 3 követelményeket.

6.2.2. A több- szereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése

A Szolgáltatónál egyedül a Hitelesítő Központban nem alkalmazzák az „n-ből m” ellenőrzést.

6.2.3. Aláírás létrehozó adat letét

Szolgáltató nem nyújt magánkulcs letét szolgáltatást. Az Előfizetői Aláírás létrehozó adatot, vagy annak előállítására, visszafejtésére alkalmas programot, adatot nem tárol.

6.2.4. Aláírás létrehozó adat mentése

Szolgáltató az Előfizető aláírói Aláírás létrehozó adatot semmilyen formában nem menti, vagy tárolja.

6.2.5. Aláírás létrehozó adat archiválása

Szolgáltató Előfizetői Aláírás létrehozó adatot nem archivál.

6.2.6. Aláírás létrehozó adat kriptográfiai modulba helyezése

A Szolgáltató nem alkalmaz hardveres kriptográfiai modult.

6.2.7. Aláírás létrehozó adat aktiválása

Az előfizetői Aláírás létrehozó adat aktiválása a felhasználó által történik a jelszó vagy PIN kód megadásával, azokban az esetekben, amikor az Aláírás létrehozó adat használatára szükség van. Az Aláírás létrehozó eszközt az Aláírás létrehozó adat aktiváláskor sem hagyja el, az eszközről leolvasni nem lehet.

6.2.8. Aláírás létrehozó adat deaktiválása

Az előfizetői Aláírás létrehozó adatok deaktiválását a felhasználó alkalmazása végzi az Aláíró kijelentkezésekor, vagy amikor az Aláíró az Aláírás létrehozó eszközt eltávolítja az olvasóból.

6.2.9. Aláírás létrehozó adat megsemmisítése

Az előfizetői Aláírás létrehozó adat lejárta után az Aláírás létrehozó eszköz fizikai megsemmisítését az Előfizetőnek saját felelősségi körében úgy kell elvégezni, hogy az semmilyen körülmények között ne legyen újra felhasználható.

A szolgáltatói Aláírás létrehozó adatok megsemmisítése a Szolgáltató kötelessége.

6.3. Kulcs-pár kezelés egyéb aspektusai

6.3.1. Aláírás ellenőrző adat archiválása

Az előfizetői tanúsítványokat Szolgáltató az érvényesség lejáratától számított 10 évig archiválja. Az archív adatállományt Szolgáltató az erre a célra létrehozott Aláírás létrehozó adatával aláírja, s legalább két példányban menti.

Az adathordozók egyik példányát Szolgáltató a Hitelesítő Központjában, a másik példányt a földrajzilag távol eső Biztonsági Adattárában tárolja a megőrzési idő végéig.

6.3.2. Aláírás létrehozó és ellenőrző adatok felhasználási ideje

A Root CA aláíró kulcshoz tartozó Tanúsítvány érvényességi ideje:	10 év
A Produktív CA aláíró kulcsához tartozó Tanúsítvány érvényességi ideje:	max. 10 év

Az RO kommunikációs kulcsához
tartozó Tanúsítvány érvényességi ideje: max. 3 év

Az előfizetői aláírók aláíró
kulcsához tartozó Tanúsítvány érvényességi ideje: 1 év

Valamennyi fenti Tanúsítvány (és a benne foglalt nyilvános kulcs) érvényességének kezdete a kibocsátás időpontjával egyezik meg.

Valamennyi fenti Tanúsítvány esetén a megfelelő magánkulcs érvényességi ideje megegyezik a Tanúsítvány érvényességi idejével.

6.4. Aktiválási adatok

6.4.1. Aktiválási adatok generálása és installációja

A Regisztrációs Iroda által kibocsátott Aláírás-létrehozó eszközök aktivizáló adatait (PIN kódjait) a PKI alkalmazás állítja elő.

6.4.2. Aktiválási adatok védelme

A Regisztrációs Iroda az általa kibocsátott Aláírás-létrehozó eszközök aktivizáló adatait (PIN kódjait) műszaki[41] és szervezési[42] intézkedésekkel védi, majd az Aláírás-létrehozó eszköztől elkülönítve[43] osztja szét.

Előfizetői Aláírás létrehozó adatának kizárólag csak az Aláíró által történő birtoklása az alapvető feltétel az elektronikusan aláírt adat, dokumentum hitelességének biztosítására. Emiatt az Előfizetőnek saját felelősségi körében kell biztosítania a kizárólagos birtoklást. Amennyiben ez sérül vagy elvszik, illetve ennek alapos gyanúja fennáll, akkor az Előfizetőnek ezt haladéktalanul jelentenie kell az őt regisztráló Irodánál, amely azonnal intézkedik a tanúsítvány visszavonásáról.

[41] A PIN kódok generálása, kinyomtatása és borítékolása egy zárt láncú, automatikus, ember által megszakíthatatlan folyamattal történik.
[42] A címzettekhez történő továbbításig, a rendszerüzemeltetők gondoskodnak a beborítékolt PIN kódok biztonságos tárolásáról.
[43] Az elkülönítés úgy van biztosítva, hogy a PIN kódok és intelligens kártyák szétosztása, illetve átadása külön lezárt borítékokban történik.

Az Előfizető Aláírás létrehozó adatának aktiválási adatát a Szolgáltató az Aláírás létrehozó adat előállítása után megsemmisíti, büntetőjogi felelőssége mellett nem hozza harmadik fél tudomására.

Az Előfizető bármikor megváltoztathatja a jelszavát vagy PIN kódját.

A Szolgáltató a saját aktiválási adatait a MeH 12. ajánlás által meghatározott fokozott biztonsági szinten védi a 2.8 fejezetben (Bizalmasság – Adatkezelési szabályzat), a 4.5 fejezetben (Biztonsági audit eljárások), 5. fejezetben (Fizikai, eljárásrendi, és humán biztonsági szabályozások), és a 6.5 fejezetben (Számítógép biztonsági szabályok) meghatározott biztonsági intézkedésekkel.

6.4.3. Aktiválási adatok egyéb aspektusai

Az előfizetői aktiválási adatát Szolgáltató nem tárolja, és nem állítja újra elő az Előfizető, harmadik fél, vagy hatóság kifejezett kérése esetén sem.

Az aktiváló adat elvesztése, elfelejtése vagy illetéktelen kezekbe történő jutása esetén minden esetben új aktiválási adatot kell előállítani.

6.5. Számítógép biztonsági szabályok

6.5.1. Számítógép biztonság technikai követelményei

A Számítógép biztonság technikai követelményeit a MeH 12. ajánlás szerinti fokozott biztonsági osztálybasorolás határozza meg.

A Szolgáltató olyan megbízható informatikai rendszert alkalmaz, mely az alábbi termékeken alapul:

- operációs rendszer,
- PKI alkalmazás,
- kriptográfiai hardver modulok,
- tűzfalak,
- behatolás detektorok.

Az operációs rendszerek által megvalósított biztonsági funkciók az alábbiak:

- biztonsági naplózás (a rendszeradminisztrátori hozzáférések és tevékenységek rögzítése, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása),
- a felhasználói adatok védelme (a hozzáférés ellenőrzési szabályok alapjainak érvényre juttatása /rendszer fájlok védelme, a felhasználói adatok csak alkalmazáson keresztüli elérésének biztosítása/, a tárolt adatok sértetlenségének védelme /beleértve a vírusok, káros és engedély nélküli szoftverek elleni védekezés támogatását is/, a maradvány információ védelmének megvalósítása),
- azonosítás és hitelesítés (a rendszeradminisztrátorok azonosítása és hitelesítése, az operációs rendszer által biztosított funkciók elérésének sikeres hitelesítéshez kötése),
- biztonságkezelés (a biztonsági szerepkörök kezelése, a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
- a biztonsági funkciók megbízható védelme (alap biztonsági tesztelés végrehajtása, biztonságos állapot megőrzése hiba esetén, a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása, a különböző alkalmazói folyamatok által használt tartományok elkülönítése).

A PKI alkalmazás által megvalósított biztonsági funkciók az alábbiak:

- biztonsági naplózás (a rendszerüzemeltetői hozzáférések és tevékenységek rögzítése),
- kommunikáció (a Hitelesítő Központ és a Regisztrációs Iroda 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:

- biztonsági naplózás (a saját funkcióihoz való hozzáférések rögzítése, a saját belső biztonsági napló védelme, az ehhez való hozzáférés rendszervizsgáló szerepkörre korlátozása),
- 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).

A tűzfal és a behatolásdetektáló 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),

6.5.2. Számítógép biztonsági értékelések

A Szolgáltató olyan megbízható informatikai rendszereket alkalmaz, melyek a MeH 12. ajánlás szerinti fokozott biztonsági osztálybasorolás követelményeit kielégíti. Ez összhangban van az ITSEC F-B1/E3, illetve a Common Criteria ajánlás AL4 biztonsági osztályok követelményeivel.

A számítógép biztonsági értékelések rendszerét az 3. táblázat mutatja.

Biztonsági ellenőrzés típusa	Végzi	Rendszeresség

Operatív	IT infrastruktúra	Informatikai biztonsági adminisztrátor	Naponta
	PKI alkalmazás	Rendszer auditor	Naponta
Belső ellenőrzés	IT infrastruktúra	Informatikai biztonsági menedzser	Félévente egyszer
	PKI alkalmazás	Hitelesítési Politika és Szabályozási Csoport	Félévente egyszer
Külső ellenőrzés	IT infrastruktúra	Külső auditor	Évente egyszer
	PKI alkalmazás	Külső auditor	Évente egyszer

3. táblázat

6.6. Életciklus technikai szabályok

6.6.1. Rendszerfejlesztési szabályok

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató társasági szintű Informatikai biztonságpolitikája és az Informatikai Biztonsági Szabályzat tartalmazza, amelyek pontosan meghatározzák az előkészítés, a projekt, a működtetés és menedzselés és a visszavonás/rekonstrukció ciklus időszakok feladatait és az alkalmazott módszertanokat.

6.6.2. Biztonságkezelési szabályok

A biztonságkezelési szabályok a Szolgáltató társasági szintű Informatikai biztonságpolitikája, valamint a társasági és a rendszer szintű Informatikai Biztonsági Szabályzatok tartalmazzák. A Szolgáltató hitelesítés támogató informatikai rendszere vonatkozásában a rendszer szintű szabályzat a Biztonsági Szabályzat.

6.6.3. Életciklus biztonsági értékelések

Az életciklus biztonsági értékelések a 3. táblázat szerinti rendszerben történnek.

6.7. Hálózati biztonsági szabályok

A Szolgáltató hitelesítés szolgáltatás támogató informatikai rendszere fokozott biztonsági osztályba sorolt. A Szolgáltató társasági szintű informatikai, valamint a hálózati biztonságpolitikájának és biztonsági architektúrájának megfelelően a 2. szintű Hitelesítő Központok és a Regisztrációs Iroda közötti biztonságos kommunikáció valósul meg. Mindegyik objektum informatikai rendszerénél a védett belső és a külső hálózatok biztonságos elválasztását tűzfal és betörés figyelő rendszer (IDS) biztosítja.

6.8. Kriptográfiai modul ellenőrzése

A Szolgáltató fokozott biztonságú szolgáltatáshoz nem alkalmaz hardver kriptográfiai modult.

7. Tanúsítvány és kulcs-visszavonási profil

Az ebben a fejezetben bemutatott, ITU-T X.509 ajánlás szerinti tanúsítvány profil mezőit és azok értelmezését általában mutatjuk be.

7.1. Tanúsítvány profil

7.1.1. Alap mezők

A Szolgáltató által kibocsátott végfelhasználói tanúsítványok alap mezői a következők:

Mezőnév	**Érték vagy szabály**
Verzió *Version*	Szolgáltató az RFC 2459-nek megfelelő tanúsítványokat bocsát ki. Az Előfizető és Érintett fél által alkalmazott eljárásoknak és alkalmazásoknak támogatnia kell az ilyen típusú tanúsítványok helyes kezelését. Szolgáltató a kibocsátott tanúsítványok „Version” mezőjébe V3 értéket ír.
Sorozatszám *Serial Number*	A kibocsátó Hitelesítő Központon belül egyedi szám 12 karakter hosszúságú.
Algoritmus azonosító *Signature Algorithm Identifier*	Szolgáltató tanúsítványt hitelesítő elektronikus aláírásának algoritmus azonosítója, pl. sha1WithRSAEncryption
Aláírás *Signature*	Szolgáltató tanúsítványt hitelesítő elektronikus aláírása az RFC 2459 szerint generálva és kódolva.
Kibocsátó *Issuer*	A tanúsítványt kibocsátó Hitelesítő Központ és egység egyedi azonosítója egyedi X.500 név formátumot szerint, UTF8String formátumban. c=hu, o=MÁV INFORMATIKA Kft., ou=CA, cn=ICA0
Érvényesség *Valid From & Valid To*	A tanúsítvány érvényességének kezdete és vége. UCT szerinti érték, az RFC 2459 szerinti kódolással. Validity from: 2002. április 4. 10:53:14 Validity to: 2003. április 4. 10:53:14

Mezőnév	Érték vagy szabály
Tulajdonosazonosító *Subject*	Tulajdonos egyedi neve egyedi X.500 név formátumot szerint, UTF8String formátumban. Természetes személynél: c=hu, l=Budapest, e=<e-mail cím>, cn=Kiss János Szervezeti (pl. MÁV Rt.) személynél: c=hu,l=Budapest, e=<e-mail cím>, o=MAV Rt., ou=<MAV Rt. szervezeti egység név>, cn=Kiss János/<e-mail cím> Szervezeti (pl. MÁV Rt.) pozíciónál: c=hu, o=MAV Rt., ou=<MAV Rt. szervezeti egység név>, cn=<beosztás> (pl. igazgató)
Alany nyilvános kulcsának algoritmus azonosítója *Subject Public Key Algorithm Identifier*	Alany nyilvános kulcs algoritmusának azonosítója, pl. rsaEncryption
Alany nyilvános kulcsa *Subject Public Key Value*	Alany nyilvános kulcsa.
Kibocsátó egyedi azonosító *Issuer Unique Identifier*	Nem kitöltött.
Alany egyedi azonosító *Subject Unique Identifier*	Nem kitöltött.

7.1.2. Tanúsítvány kiterjesztések

A Szolgáltató az ITU-T X.509 ajánlás 3. verziójának megfelelő tanúsítvány kiterjesztéseket támogatja.

Mezőnév	Érték vagy szabály	Kritikus
Tanúsítvány-típusok *Certificate Policies*	PolicyIdentifier = X.X.X.X[44] PolicyQualifier = http://trust-sign.mavinformatika.hu UserNotice = ”*A tanúsítvány értelmezéséhez és elfogadásához a Szolgáltató HSzSz-ében foglaltak szerint kell eljárni, amelyek megtalálhatók a következő Internetes web oldalon: http://trust-sign.mavinformatika.hu”*	Nem
Alapvető megkötések *Basic Constraints*	Subject type = End Entity Path Length Constraint = None	Nem
Kulcshasználat	digitalSign	Nem

[44] Ide kerül a hivatkozott tanúsítványtípus azonosítója

Mezőnév	Érték vagy szabály	Kritikus
Key Usage	nonRepudiation	
Kulcshasználat kiterjesztés[45] *Key Usage*	ClientSign	Nem
CRL szétosztási pont *CRL Distribution Points*	ldap://ldap.mavinformatika.hu/	Nem

Valamennyi fenti kiterjesztés kitöltésre kerül.

A Szolgáltató által kibocsátott tanúsítványok nem tartalmazhatnak álnevet.

A kiterjesztési mezők feldolgozásáért az Előfizető és Érintett fél alkalmazása és eljárása felelős. A Szolgáltató semmilyen körülmények között nem hibáztatható a kiterjesztés, vagy a szabályzatokban foglaltak figyelmen kívül hagyása, téves értelmezése miatt.

7.2. Kulcs-visszavonási profil

A szolgáltató által kibocsátott visszavonási listák alap mezői a következők:

Mezőnév	Érték vagy szabály
Verzió *Version*	A visszavonási lista a [12] ajánlás hányadik verziójának felel meg (lásd 7.2.1 alfejezet).
Algoritmus azonosító *Signature Algorithm Identifier*	Szolgáltató visszavonási listát hitelesítő elektronikus aláírásának algoritmus azonosítója: sha1RSA (OID=1.2.840.113549.1.1.5).
Aláírás *Signature*	Szolgáltató visszavonási listát hitelesítő elektronikus aláírása az RFC 2459 szerint generálva és kódolva.
Kibocsátó *Issuer*	A visszavonási listát kibocsátó hitelesítő szervezet és egység egyedi azonosítója.
Hatályba lépés *Effective Date*	A visszavonási lista hatályba lépésének kezdete. A szolgáltató által kibocsátott tanúsítványok esetében ez megegyezik a kibocsátás idejével. UCT szerinti érték, az RFC 2459 szerinti kódolással.
Következő kibocsátás *Next Update*	A következő visszavonási lista kibocsátásának ideje. UCT szerinti érték, az RFC 2459 szerinti kódolással.

[45] Csak azonosítás-hitelesítés célú felhasználás esetén kell megadni.

Visszavont tanúsítványok *Revoked Certificates*	A visszavont tanúsítványok listája a tanúsítvány sorozatszámával és a visszavonás idejével.

7.2.1. Verzió szám(ok)

A Szolgáltató ITU-T X.509 ajánlás 2. verziója szerinti tanúsítvány visszavonási listákat bocsát ki.

7.2.2. „Tanúsítvány visszavonási lista" és „Tanúsítvány visszavonási lista bejegyzési" kiterjesztések

A Szolgáltató által használt visszavonás bejegyzési kiterjesztések a következők:

Mezőnév	**Érték vagy szabály**	**Kritikus**
Visszavonás oka *reasonCode*	A visszavonás oka	Nem
Érvénytelenség ideje *Invalidity Date*	A magánkulcs megbízhatatlanná válásának ideje	Nem
Útmutató *Hold Instruction*	A felfüggesztett tanúsítvány kezelése	Nem

Szolgáltató a kiterjesztéseket nem köteles kitölteni.

A Szolgáltató által kitöltött visszavonási lista kiterjesztések a következők:

Mezőnév	**Érték vagy szabály**	**Kritikus**
CRL sorozatszám *CRL number*	A visszavonási lista egyesével növekvő sorozatszáma	Nem

A visszavonási lista kiterjesztés és visszavonás bejegyzési kiterjesztések feldolgozásáért az Előfizető és Érintett fél alkalmazása és eljárása felelős. Szolgáltató semmilyen körülmények között nem hibáztatható a kiterjesztések figyelmen kívül hagyása vagy téves értelmezése miatt.

8. HSzSz adminisztráció

8.1. A HSzSz változáskezelés

8.1.1. HSzSz változtatási eljárások

A Szolgáltató szervezetén belül Hitelesítési Politika és Szabályozási Csoport működik, amely a HSzSz karbantartásáért felelős. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz, s a változtatásokat életbe lépteti.

A változtatásokat gyűjtve a Hitelesítési Politika és Szabályozási Csoport belső nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. A Szolgáltató a változásokat kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A HSzSz módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

8.1.2. Értesítés nélkül változtatható elemek

A Szolgáltató fenntartja a jogot, hogy a szabályzat nem lényegi elemeit előzetes értesítés és bejelentés nélkül változtassa. Ilyenek lehetnek a helyesírási hibák, formai változtatások, különböző kontaktadatok (web címek, telefonszámok), és egyéb olyan elemek, melyek a tanúsítványok biztonsági szintjét, felhasználhatóságát a legkisebb mértékben sem módosítják.

8.1.3. Értesítéssel változtatható elemek

Minden a tanúsítványok biztonsági szintjét, felhasználhatóságát érintő módosító változtatás értesítésköteles a 8.2 fejezet szerint.

8.1.4. Észrevételek kezelése

A 8.2 fejezet szerint közzétett új HSzSz-el kapcsolatos észrevételeket szolgáltató a hatályba lépést megelőző 14 naptári napig fogadja a http://trust-sign.mavinformatika.hu címen. A HSzSz észrevételekkel módosított változatát szolgáltató a hatályba lépést megelőző 7. naptári nap zárja le és teszi közzé.

8.1.5. Szabályzati objektumazonosítót vagy mutatót változtató módosítások

Minden olyan jelentősebb módosítás, melyet a Szolgáltató csak az újonnan kibocsátásra kerülő tanúsítványok esetében alkalmaz (s a már kibocsátottak esetében nem) a HSzSz verziószámának fő jegyét, s a szabályzat objektumazonosítóját is módosítja. E szabályzatok az előző főbb verziótól eltérő web címen kerülnek közzétételre, így csak az újonnan kibocsátott tanúsítványok mutatói fognak rá hivatkozni.

8.2. Közzétételi és tájékoztatási elvek

8.2.1. A HSzSz-ben nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyezteti. A Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen HSzSz több ilyet is megemlít). A 2.7 pontban leírt vizsgálati eljárások ezeket a dokumentumokat is vizsgálják.

8.2.2. A HSzSz közzététele

A Szolgáltató szabályzatainak a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően 30 nappal közzéteszi web oldalán, a http://trust-sign.mavinformatika.hu címen. Szolgáltató alkalmanként ezt megelőzően is tájékoztatja a közösséget a tervezett változtatásairól.

8.3. HSzSz elfogadási eljárások

A jelen HSzSz az RFC 2527 szabványnak való megfelelőségét közzététel előtt a Szolgáltató megvizsgálta. A vizsgálatot a Szolgáltató, illetve a külső auditor is elvégzi a 3. táblázatban megadott rendszerességgel.

A szabályzat törvényeknek való megfelelőségét a Nemzeti Hírközlési Hatóság is vizsgálja a HSzSz hatálybalépését megelőzően.

A Szolgáltató HSzSz-ét, a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően 30 nappal átadja a Nemzeti Hírközlési Hatóság részére.

A Szolgáltató alkalmanként ezt megelőzően is konzultál a Nemzeti Hírközlési Hatóságtól a tervezett változtatásairól.

9. Hivatkozások és Meghatározások

9.1. Hivatkozások

Hivatkozott törvények, kormányrendeletek, MeH rendeletek:

- 2001. évi XXXV. törvény az elektronikus aláírásról,
- 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,
- 151/2001. (IX. 1.) Korm. rendelet a Hírközlési Felügyeletnek az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól,
- 15/2001. (VIII. 27.) MeHVM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról.
- 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.
- 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról,
- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról,
- 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. törvény módosításáról szóló törvény.

A Szolgáltató hivatkozott dokumentumai:

- A MÁV INFORMATIKA Kft. Szervezeti és Működési Szabályzata,
- A MÁV INFORMATIKA Kft. Iratkezelési Szabályzata
- A MÁV INFORMATIKA Kft. Titokvédelmi Szabályzata
- A MÁV INFORMATIKA Kft. Informatikai Biztonságpolitikája
- A MÁV INFORMATIKA Kft. Informatikai Biztonsági Szabályzata
- Általános Szerződési Feltételek Fokozott Biztonságú Hitelesítés Szolgáltatáshoz
- Előfizetői Szerződés Minta
- A Trust&Sign Szolgáltatás Biztonságpolitikája
- A Trust&Sign Szolgáltatás Biztonsági Szabályzata
- A Trust&Sign Szolgáltatás Üzletmenet-folytonossági Terve
- A Trust&Sign Szolgáltatás Üzemeltetési Kézikönyve

Hivatkozott ajánlások, szabványok:

- ITU-T X.509 “Information technology - Open Systems Interconnection - The Directory: Public -key and attribute certificate frameworks” ajánlás 3. verziója,
- Internet Közösség RFC 2459 ajánlása,
- Internet Közösség RFC 2527 ajánlása,
- Internet Közösség RFC 3039 ajánlása,
- Európai Unió ETSI TS 101 456 szabvány,
- Európai Unió ETSI TS 101 862 szabvány,
- NIST FIPS 140-1 Level 1-3,
- American Bar Association (ABA) PKI Assessment Guidelines (PAG),
- a CWA 14167-1, és a CWA 14172-1,-2,-3,-4 CEN Workshop Agreement-ek
- MeH 12. ajánlás,
- ITSEC,
- Common Criteria.

9.2. Meghatározások

Aláírás-létrehozó adat: olyan egyedi adat (jellemzően kriptográfiai magánkulcs), amelyet az aláíró az elektronikus aláírás létrehozásához használ.

Aláírás-ellenőrző adat: olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), amelyet az elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.

Aláírás-létrehozó eszköz: olyan hardver, illetve szoftver eszköz, amelynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

Aláíró: az a természetes személy, akihez az elektronikus aláírás hitelesítés-szolgáltató (a továbbiakban: hitelesítés szolgáltató) által közzétett aláírás-ellenőrző adatok jegyzéke szerint az aláírás-ellenőrző adat kapcsolódik.

Biztonságos aláírás-létrehozó eszköz: az e törvény 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz.

Biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy;

Elektronikus aláírás: elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum.

Elektronikus aláírás ellenőrzése: az elektronikus dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, valamint a tanúsítvány felhasználásával.

Elektronikus aláírás felhasználása: elektronikus adat elektronikus aláírással történő ellátása, illetve elektronikus aláírás ellenőrzése.

Elektronikus aláírás hitelesítés-szolgáltató: a 6. § (2) bekezdése szerinti tevékenységet végző személy (szervezet).

Elektronikusan történő aláírás: elektronikus aláírás hozzárendelése, illetve logikailag való hozzákapcsolása az elektronikus adathoz.

Elektronikus aláírási termék: olyan szoftver vagy hardver, amely elektronikus aláírással kapcsolatos szolgáltatások nyújtásához, így különösen elektronikus aláírások, illetőleg időbélyegző készítéséhez vagy ellenőrzéséhez használható.

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adat, amely elektronikus aláírással van ellátva.

Elektronikus irat: olyan elektronikus dokumentum, amelynek funkciója szöveg betűkkel való közlése, és a szövegen kívül az olvasó számára érzékelhetően kizárólag olyan egyéb adatokat foglal magában, melyek a szöveggel szorosan összefüggenek, annak azonosítását (pl. fejléc), illetve könnyebb megértését (pl. ábra) szolgálják.

Elektronikus okirat: olyan elektronikus irat, amely nyilatkozattételt, illetőleg nyilatkozat elfogadását, vagy nyilatkozat kötelezőnek elismerését foglalja magában.

Fokozott biztonságú elektronikus aláírás: elektronikus aláírás, amely megfelel a következő követelményeknek:

a. alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető,

b. olyan eszközzel hozták létre, mely kizárólag az aláíró befolyása alatt áll,

c. a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően az iraton, illetve dokumentumon tett - módosítás érzékelhető.

Időbélyegző: elektronikus irathoz, illetve dokumentumhoz végérvényesen hozzárendelt, illetőleg az irattal vagy dokumentummal logikailag összekapcsolt igazolás, amely tartalmazza a bélyegzés időpontját, és amely a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden - az igazolás kiadását követő - módosítás érzékelhető.

Igénylő: a nem minősített tanúsítvány iránti igényt benyújtó személy;

Informatikai rendszer: a szolgáltató által a szolgáltatói kulcspár kezeléséhez, az aláírás-létrehozó adat előállításához, a tanúsítványok kibocsátásához, a kibocsátott tanúsítványt tartalmazó nyilvántartáshoz, a visszavonási nyilvántartásokhoz és a visszavonás kezelési szolgáltatáshoz, valamint e tevékenységek informatikai védelméhez használt, az Eat. 3. számú mellékletének f) pontja szerinti megbízható rendszerek és termékek;

Kriptográfiai kulcs: olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a rejtjelezéshez vagy a visszaállításhoz, különösen az elektronikus aláírás előállításához vagy ellenőrzéséhez szükséges;

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 kezelő személy;

Rendkívüli üzemeltetési helyzet: olyan, a szolgáltató üzemmenetében zavart okozó rendkívüli helyzet, amikor a szolgáltató rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség;

Szolgáltatási szabályzat: a 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.

Szolgáltatói kulcspár: a szolgáltatói magánkulcs és a szolgáltatói nyilvános kulcs;

Szolgáltatói magánkulcs: olyan kriptográfiai magánkulcs, amelyet a hitelesítés-szolgáltató vagy az időbélyegzést nyújtó szolgáltató saját elektronikus aláírási szolgáltatásának igazolására, így különösen a tanúsítvány kibocsátására, a visszavonási nyilvántartásokra, az időbélyegzésre, a naplózáshoz, az archiváláshoz használ;

Szolgáltatói nyilvános kulcs: olyan kriptográfiai nyilvános kulcs, amelyet a szolgáltatói magánkulcs használatával létrehozott elektronikus aláírás ellenőrzésére használnak;

Tanúsítvány: hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírásellenőrző adatot a 9. § (3), illetőleg (4) bekezdése szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát.

Tanúsítvány kibocsátása: a tanúsítvány átadása az aláírónak, valamint a szolgáltató nyilvántartásában a tanúsítvány elérhetővé tétele az aláíró által meghatározott kör részére;

Visszavonás kezelése: az Eat. 14. §-ban meghatározott esetekben a kibocsátott tanúsítványok visszavonására és felfüggesztésére vonatkozó eljárások lefolytatása;

Visszavonási nyilvántartások: nyilvántartások a felfüggesztett, illetőleg a visszavont tanúsítványokról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját.