MÁV Szolgáltató Központ

Zártkörűen Működő Részvénytársaság

Szolgáltatási szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz (HSZSZ-M)

Verziószám	**9.0**
OID szám	**1.3.6.1.4.1.14868.1.2.9**
Hatósági nyilvántartásba vétel napja	**2013.05.03.**
Hatósági nyilvántartásba vétel száma	EF/11965-3/2013
Hatálybalépés dátuma	**2013.05.28.**

© **Copyright MÁV Szolgáltató Központ Zrt.** – Minden jog fenntartva

HSZSZ-M verziók

Verzió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2002.09.30	A fokozott biztonságú szolgáltatói regisztrálásra előkészített, a HIF részére átadott változat.	Bodlaki Ákos		
2.0	2002.11.29	HSZSZ-M minősített tanúsítványtípusokra, véleményezésre átadott változat	Bodlaki Ákos		
2.1	2003.03.31.	A minősítési eljárásra átadott változat kiegészítve és módosítva a HIF észrevételeivel	Bodlaki Ákos		
2.2	2003.07.30	Időbélyegzés szolgáltatás minősítési eljárására beadott 1.0 változattal kapcsolatos észrevételekkel módosítva.	Bodlaki Ákos		
2.2.1	2004. 01. 20.	Formai és sajtóhibák javítása, belső ellentmondások megszűntetése szakértői észrevételek alapján. Felülvizsgált és javított változat	Néder Ferenc		
2.3	2004. 08. 23.	A 2004. évi LV. törvény hatásainak átvezetése	Néder Ferenc		
3.0	2005. 07. 21.	Felülvizsgált, OCSP[1]-vel bővített változat	Néder Ferenc		
4.0	2006. 04. 13.	Felülvizsgált, az NHH észrevételei alapján javított, a 2004. évi CXL. törvény (a közigazgatási hatósági eljárás és szolgáltatás általános szabályai) előírásainak megfelelő változat	Néder Ferenc		
5.0	2007. 08. 06.	Felülvizsgált, az RFC3647 szabvány szerint átdolgozott, az NHH észrevételei alapján javított változat	Néder Ferenc	Kovács Árpád, PKI SZE vezető	Hosszú Sándor István, vezérigazgató
6.0	2008. 01. 01.	A Szolgáltató adatainak változásával korrigált változat	Néder Ferenc	Juhász György, PKI SZE vezető	Hosszú Sándor István, vezérigazgató
7.0	2008. 05. 26.	Az új CA szoftver és HSM modul használatba vételevel hatályos, OCSP szolgáltatás nélküli változat	Néder Ferenc	Juhász György, PKI SZE vezető	Hosszú Sándor István, vezérigazgató
7.1	2010. 05. 18.	BALE információkkal és HSM modul tanúsítványára vonatkozó adatokkal kiegészített, és az NHH által kért módosításokat tartalmazó változat	Kővári Ferenc	Néder Ferenc	Juhász György HBSZE vezető
7.2	2010.09.24.	Új, Gemalto BALE információkat tartalmazó változat	Kővári Ferenc	Néder Ferenc	Juhász György HBSZE vezető
8.0	2011.12.01.	Algoritmusváltás és viszontazonosítás szolgáltatás törlése miatt módosuló változat	Kővári Ferenc	Kovács Gergely	Katus Gábor vezérigazgató
9.0	2013.04.23	Névváltozás kapcsán aktualizált változat	Néder Ferenc	Kővári Ferenc	Sánta Zoltán vezérigazgató

[1] OCSP: On-line Certificate Status Protocol, magyarul: valós idejű tanúsítvány-állapot lista

TARTALOMJEGYZÉK

1. Bevezetés 8

1.1. Áttekintés 8

1.2. A dokumentum neve és azonosítója 8

1.3. A Szolgáltató és a felhasználói közösség 10

1.3.1. Szolgáltató adatai 10

1.3.2. A Szolgáltató regisztráló, hitelesítő és szolgáltató egységei 11

1.3.3. Felhasználói közösség 11

1.3.4. A Közigazgatási Gyökér Hitelesítés-szolgáltató 12

1.4. Tanúsítványhasználat 13

1.4.1. A szolgáltatások szintje 13

1.4.2. Tanúsítványok alkalmazhatósága 13

1.4.3. Időbélyegek alkalmazhatósága 13

1.5. A szolgáltatási szabályzat adminisztrációja 14

1.5.1. Szabályzat hatálya 14

1.5.2. Kapcsolattartó személy 14

1.5.3. Változáskezelés 14

1.5.4. Közzétételi és tájékoztatási elvek 14

1.5.5. Elfogadási eljárások 14

1.6. Meghatározások 15

1.7. Hivatkozások 17

1.8. Tanúsítványok jellemzői és típusai 19

1.8.1. Minősített tanúsítványok jellemzői 19

1.8.2. Tanúsítványok felhasználási területük szerint 19

1.8.3. Tanúsítvány típusok 20

1.9. Időbélyegek jellemzői 20

2. Általános rendelkezések 21

2.1. Feladatok és hatáskörök 21

2.1.1. A Szolgáltató feladatai és hatásköre 21

2.1.2. Az Előfizető és az Aláíró feladatai és hatásköre 22

2.1.3. Érintett félre vonatkozó ajánlások 23

2.2. Felelősségek 23

2.2.1. A Szolgáltató felelőssége 23

2.2.2. Az Előfizető és az Aláíró felelőssége 24

2.2.3. Érintett fél felelőssége 24

2.3. Értelmezés és alkalmazás 24

2.3.1. Alkalmazott jogszabályok 24

2.3.2. Hatályosság, megszűnés, értesítések 24

2.3.3. Vitás kérdések kezelése 25

2.4. Közzététel 25

2.4.1. Adatbázisok 25

2.4.2. A tanúsítványokra, időbélyegekre vonatkozó információk közzététele 25

2.4.3. A közzététel gyakorisága 26
3. Azonosítás és hitelesítés 27
3.1. Megnevezési konvenciók 27
3.1.1. Nevek típusa 27
3.1.2. Nevek szemantikája 27
3.1.3. Nevek egyedisége 27
3.1.4. Név igénylési viták feloldása 27
3.1.5. Álnevek használata 28
3.1.6. Védjegyek elismerésének és hitelesítésének módszere 28
3.2. Regisztráció 28
3.2.1. Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere 28
3.2.2. Azonosítás „Személyes" tanúsítvány igénylése esetén 28
3.2.3. Azonosítás „Szervezeti személy" („Munkatársi") tanúsítvány igénylése esetén 28
3.2.4. Szervezet azonosítása közigazgatásban alkalmazható tanúsítványok igénylése esetén 30
3.2.5. Személy azonosítása közigazgatásban alkalmazható tanúsítványok igénylése esetén 30
3.2.6. Időbélyegzés szolgáltatás igénylése 30
3.2.7. Adategyeztetés 31
3.2.8. Együttműködési képességek 31
3.2.9. Viszontazonosítás 31
4. A tanúsítvány-életciklusra vonatkozó szabályok 32
4.1. Tanúsítványigénylés 32
4.1.1. Ki nyújthat be tanúsítványkérelmet 32
4.1.2. A tanúsítványigénylés folyamata és a résztvevők felelőssége 32
4.2. A tanúsítvány kérelem feldolgozása 32
4.2.1. Azonosítási és hitelesítési funkciók megvalósítása 32
4.2.2. A tanúsítványkérelem jóváhagyása vagy visszautasítása 32
4.2.3. A tanúsítványigénylések feldolgozásának időtartama 32
4.3. Tanúsítvány kibocsátás 32
4.4. Tanúsítvány elfogadás 33
4.4.1. Tanúsítvány közzététele a hitelesítés-szolgáltató által 33
4.4.2. A további szereplők értesítése a tanúsítvány kibocsátásáról 33
4.5. Kulcspár és tanúsítvány illetve időbélyeg használat 33
4.5.1. Az alany magánkulcs- és tanúsítvány használata 33
4.5.2. Az érintett felek nyilvános kulcs- és tanúsítvány használata 33
4.6. Tanúsítványok érvényessége, megújítása (tanúsítvány frissítése) 34
4.6.1. A tanúsítványok érvényessége 34
4.6.2. A tanúsítványok megújítása (tanúsítványok frissítése) 34
4.6.3. Érvénytelen tanúsítványok megőrzése 34
4.7. Kulcscsere 34
4.8. Tanúsítvány-módosítás 34
4.9. Tanúsítványok visszavonása és felfüggesztése 35
4.9.1. Visszavonáshoz vagy felfüggesztéshez vezető körülmények 35
4.9.2. Visszavonás kérelmezése 36

4.9.3. Visszavonási kérelemre vonatkozó eljárás 36
4.9.4. A felfüggesztési kérelemre vonatkozó eljárás 36
4.9.5. Kivárási idő visszavonási/felfüggesztési kérelem esetén 37
4.9.6. A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok 37
4.9.7. Felfüggesztett állapotra vonatkozó korlátozások, újraérvényesítés 38
4.9.8. A visszavonási információ ellenőrzése az érintett felek részéről 38
4.9.9. Visszavonási lista (CRL) és kibocsátásának gyakorisága 38
4.9.10. A visszavonási lista előállítása és közzététele közötti közötti leghosszabb idő 38
4.9.11. A visszavonási listák ellenőrzése 38
4.9.12. Visszavonási állapot közlés más formái 38
4.9.13. Intézkedések magánkulcs kompromittálódás esetén 39
4.10. Kulcsletét 39
4.11. Időbélyegzés 39
4.11.1. Az időbélyegzés szolgáltatás igénylése 39
4.11.2. Az időbélyegzés szolgáltatás szintje 39
4.11.3. Az időbélyegzés kérelmek teljesítése 39
4.11.4. Az időbélyeg érvényességének ellenőrzése 39
4.12. OCSP szolgáltatás 40
5. Fizikai, eljárásrendi, és humán biztonsági szabályozások 41
5.1. Fizikai biztonsági szabályozások 41
5.1.1. Hitelesítő Központok 41
5.1.2. Regisztrációs Iroda 41
5.2. Eljárásrendi szabályozások 41
5.3. Humán szabályozások 42
5.3.1. Bizalmi munkakörök 42
5.3.2. Az egyes feladatokhoz szükséges személyzeti létszámok 43
5.3.3. A bizalmi munkakörökben elvárt azonosítás és hitelesítés 43
5.3.4. Egymást kizáró munkakörök 43
5.3.5. Személyzetre vonatkozó előírások 43
5.3.6. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények 44
5.3.7. Biztonsági háttér ellenőrzésekre vonatkozó eljárások 44
5.3.8. Képzési követelmények 45
5.3.9. A felhatalmazás nélküli tevékenységek büntető következményei 45
5.3.10. A szerződéses alkalmazottakra vonatkozó követelmények 45
5.4. Naplózási eljárások 45
5.4.1. Naplózott esemény típusok 45
5.4.2. Napló adatok védelme 46
5.4.3. Naplók feldolgozásának gyakorisága 46
5.4.4. Napló adatok tárolása 46
5.4.5. A napló fájlok megőrzési időtartama 46
5.5. Adatok archiválása 46
5.5.1. A tárolt adatok típusai 46
5.5.2. Az archívum megőrzési időtartama 47

5.5.3. Az archívum védelme 47
5.5.4. Az archívum hozzáférését és ellenőrzését végző eljárások 47
5.6. Felülhitelesítés 47
5.7. A Szolgáltató kulcscseréje 47
5.8. A folyamatos üzemmenet biztosítása 47
5.8.1. A szolgáltatások azonnali felfüggesztése 48
5.8.2. Biztonsági képesség rendkívüli üzemeltetési helyzetben 48
5.8.3. Rendkívüli eseményekről történő értesítés 48
5.8.4. Minimális szolgáltatás rendkívüli üzemeltetési helyzetben 48
5.8.5. Üzletmenet-folytonossági terv 48
5.9. A szolgáltatási tevékenység megszüntetése 48
6. Műszaki biztonsági óvintézkedések 50
6.1. Kriptográfiai kulcspár előállítás és aláírás-létrehozó eszköz megszemélyesítés 50
6.1.1. Kulcspár előállítás 50
6.1.2. Az aláírás-létrehozó eszköz megszemélyesítése 50
6.1.3. Az aláírás-létrehozó adat eljuttatása az Aláíróhoz (Előfizetőhöz) 50
6.1.4. Az Aláírók aláírás-ellenőrző adatának eljuttatása az érintett feklekhez 50
6.1.5. A Szolgáltató aláírás-ellenőrző adatainak eljuttatása a felhasználói közösséghez 51
6.1.6. Kulcs méretek, algoritmosok 51
6.1.7. Előfizetői aláírás-ellenőrző adat előállításához használt paraméterek előállítása 51
6.1.8. Szolgáltatói kulcsgenerálás 51
6.1.9. Kulcs felhasználási célok 51
6.2. Aláírás-létrehozó adat védelme 51
6.2.1. Az aláírási termékre vonatkozó szabályok 51
6.2.2. A kriptográfiai modulra vonatkozó szabályok 52
6.2.3. A több-szereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése 52
6.2.4. Aláírás-létrehozó adat letét, mentés, archiválás 52
6.2.5. Aláírás-létrehozó adat védelme 52
6.2.6. Aláírás-létrehozó adat aktiválása 52
6.2.7. Aláírás-létrehozó adat deaktiválása 52
6.2.8. Aláírás-létrehozó adat megsemmisítése 52
6.3. Kulcspár kezelés egyéb aspektusai 52
6.3.1. Aláírás-ellenőrző adat (az előfizetői tanúsítványok) megőrzése 52
6.3.2. Aláírás-létrehozó és aláírás-ellenőrző adatok felhasználási ideje 53
6.4. Aktiválási adatok 53
6.4.1. Aktiválási adatok generálása és installációja 53
6.4.2. Aktiválási adatok védelme 53
6.4.3. Aktiválási adatok egyéb aspektusai 53
6.5. Az időszinkronizálás megvalósítása 54
6.6. Számítógép biztonsági szabályok 54
6.6.1. Számítógép biztonság technikai követelményei 54
6.6.2. Számítógép biztonsági értékelések 55
6.7. Életciklus technikai szabályok 55

6.7.1. Rendszerfejlesztési szabályok 55
6.7.2. Biztonságkezelési szabályok 55
6.7.3. Életciklus biztonsági értékelések 55
6.8. Hálózati biztonsági szabályok 56
6.9. Kriptográfiai (HSM) modul ellenőrzése 56
7. Tanúsítvány és tanúsítvány-visszavonási profil 57
7.1. Tanúsítvány profil 57
7.1.1. Alap mezők 57
7.1.2. Tanúsítvány kiterjesztések 57
7.1.3. Közigazgatásban alkalmazható tanúsítványok 57
7.2. Tanúsítvány-visszavonási profil 57
7.3. Időbélyeg profil 57
8. A megfelelőség vizsgálata 58
8.1.1. Vizsgálatok gyakorisága 58
8.1.2. Az átvizsgáló szervezet megnevezése/jellemzői 58
8.1.3. Hiányosságok kezelése 58
8.1.4. Eredmény kommunikációja 58
9. Egyéb üzleti és jogi kérdések 59
9.1. Díjak 59
9.1.1. Tanúsítvány kibocsátás 59
9.1.2. Tanúsítvány hozzáférés 59
9.1.3. Visszavonási lista hozzáférés 59
9.1.4. Időbélyegzés 59
9.1.5. Egyéb szolgáltatásokra vonatkozó díjak 59
9.1.6. Visszatérítési elvek 59
9.2. Anyagi felelősség és annak korlátai 59
9.3. Bizalmasság – Adatkezelési szabályok 60
9.3.1. Bizalmas információk 60
9.3.2. Nem bizalmas információk 60
9.3.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése 60
9.3.4. Feltárás törvényi meghatalmazással rendelkezők részére 61
9.3.5. Információszolgáltatás polgári eljárás keretében 61
9.3.6. Feltárás tulajdonos kérésére 61
9.3.7. Feltárás más esetekben 61
9.4. Szellemi tulajdonhoz fűződő jogok 61
10. Tevékenységért viselt felelősség és helytállás 62
10.1. A hitelesítés-szolgáltatói felelősség és helytállás 62
10.2. Az előfizetői felelősség és helytállás 62
10.3. Az érintett fél felelőssége 62
10.4. Érvényességi időtartam 62
10.5. Irányadó jog 62

1. Bevezetés

A MÁV Szolgáltató Központ Zrt[2]. 2003. áprilisától nyújt a 2001. évi XXXV. törvényben (röviden: Eat.) meghatározott minősített elektronikus aláírással kapcsolatos szolgáltatásokat. A minősített elektronikus aláírás hitelesítés-szolgáltatását 2003. augusztusától minősített időbélyegzés-szolgáltatássalegészítette ki. A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (röviden: Ket.) 2005. november 1-jétől a közigazgatásban lehetővé teszi az elektronikus ügyintézést, illetve rendelkezik annak legfőbb szabályairól. A MÁV Szolgáltató Központ Zrt. élve a törvény kínálta lehetőséggel, , szolgáltatásai körét 2006. májusától kiterjesztette a Ket. hatálya alá tartózó hitelesítés-szolgáltatásokra.

E dokumentum a MÁV Szolgáltató Központ Zrt. (továbbiakban Szolgáltató) az Eat. hatálya alá tartozó minősített elektronikus aláírással kapcsolatos szolgáltatásaira vonatkozó eljárási és működési szabályokat tartalmazza.

A Szolgáltató szolgáltatásait a vele előfizetői szerződéses viszonyban álló *Előfizetők* részére nyújtja. A Szolgáltató az elektronikus aláírások és időbélyegek hitelességét ellenőrző *érintett felek* részére bizonyos szolgáltatási elemeket hozzáférhetővé tesz.

A minősített elektronikus aláírással kapcsolatos szolgáltatások (továbbiakban: szolgáltatások) keretében a Szolgáltató az Eat.-ban meghatározott szolgáltatások közül a következőket nyújtja:

a. elektronikus aláírás hitelesítés-szolgáltatás (a továbbiakban: hitelesítés-szolgáltatás)

b. aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése

c. időbélyegzés-szolgáltatás

A HSZSZ-M további fejezeteiben a „*szolgáltatások*” kifejezés alatt a fenti három szolgáltatás bármelyike, vagy azok tetszőleges kombinációja értendő.

1.1. Áttekintés

Jelen HSZSZ-M célja, hogy összefogja azokat a szabályokat, adatokat és információkat, melyeket a Szolgáltató szolgáltatásaival kapcsolatba kerülő feleknek ismerni szükséges vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát és annak megítélését a szolgáltatásokat igénybe vevők számára, hogy az ismertetett szolgáltatási gyakorlat, a kibocsátott tanúsítványok, illetve időbélyegek mennyiben felelnek meg az elvárásaiknak. A HSZSZ-M és egyéb, a HSZSZ-M-ben hivatkozott publikus dokumentumok, ajánlások, szabványok tartalmának megismerése után, a tanúsítványok felhasználói közösségének egyértelműen meg kell tudni állapítani a tanúsítványok kezelésének módját, az általuk garantált hitelesség és biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügy garanciákat, jogi felelősségvállalásokat.

Jelen HSZSZ-M vonatkozik az {Sz24} „*Hitelesítési Rend nyilvános körben kibocsátott biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványokra (HR-MTT+BALE)*” hatálya alá tartozó előfizetői tanúsítványokra.

A közigzgatásban alkalmazható előfizetői tanúsítványok esetében a szabályzat elfogadja a {J11} „*Közigazgatási, ügyfélhez kapcsolódó, biztonságos aláírás-létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend*”-et [MHR_Ü] és a {J12} „*Közigazgatási, köztisztviselőhöz kapcsolódó, biztonságos aláírás-létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend*”-et [MHR_K], a Szolgáltató az ott rögzített követelményeket elfogadja, szolgáltatásaiban érvényesíti. Jelen szabályzat előbb felsorolt hitelesítési rendeknek való megfelelőségét a Közigazgatási Gyökér Hitelesítés-szolgáltató felülhitelesítéssel igazolja.

Jelen szabályzat vonatkozik még az {Sz26} Időbélyegzés Szolgáltatási Rend (ISZR) követelményei szerint kiadott minősített időbélyegekre is.

1.2. A dokumentum neve és azonosítója

A Szolgáltató jelen dokumentumot az ISO/IEC és az ITU szabványok által előírt regisztrációs eljárásnak megfelelően eljárva regisztrálja.

A jelen dokumentum teljes neve:	Szolgáltatási szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz. A jelen dokumentumban és a kapcsolódó szabályzatokban HSZSZ-M-ként történik rá hivatkozás.
Azonosítója:	HSZSZ-M
OID:	1.3.6.1.4.1.14868.1.2.9
Első hatálybalépés időpontja	2003. április 3.

[2] A társaság neve korábban (2013.04.01-et megelőzően) MÁV INFORMATIKA Zrt. volt

A HSZSZ-M nyomtatott formában a Szolgáltató ügyfélkapcsolati irodáiban, elektronikus változata a szolgáltatások internetes honlapján érhető el. A szabályzatnak csak a Szolgáltató aláírásával ellátott változata tekinthető hitelesnek.

1.3. A Szolgáltató és a felhasználói közösség

1.3.1. Szolgáltató adatai

Név: MÁV Szolgáltató Központ Zrt.

Cégjegyzék szám: 01-10-045838

Székhely: 1087 Budapest, Könyves Kálmán krt. 54-60.

Telephely: 1012 Budapest, Krisztina krt. 37/a.

Levelezési cím: 1426 Budapest Pf. 24

Telefonszám: (36-1) 457-9300

Telefax szám: (36-1) 457-9500

Internetes honlap címe: *http://www.mavinformatika.hu/*

Szolgáltatások internetes honlapjának címe: *http://www.mavinformatika.hu/ca/*

Illetékes fogyasztóvédelmi felügyelőség:

Budapest Főváros Kormányhivatal Fogyasztóvédelmi Felügyelőség

Cím: 1052 Budapest, Városház u. 7.

Postacím: 1364 Budapest, Pf.: 144.

Telefonszám: +36 30 940 7039, +36 1 328 0185, Telefax: +36 1 411 0116

Email: *fogyved_kmf_budapest@nfh.hu*

Kapcsolat az ügyfelekkel:

Az ügyfélkapcsolatok (általános és részletes tájékozódás, szerződéskötés, aláírás létrehozó eszköz átadása, visszavonási kérelem megerősítése, stb.) biztosítása érdekében a Szolgáltató Ügyfélkapcsolati Irodákat tart fenn, melyeket az ügyfelek személyesen azok nyitvatartási idejében kereshetnek fel. A mindenkori nyitvatartási rendeket a Szolgáltató a szolgáltatásainak internetes honlapján teszi közzé.

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

A központi 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 a *hiteles@mavinformatika.hu* címen.

A területi ügyfélkapcsolati irodák címe és elérhetősége a szolgáltatások internetes honlapján keresztül érhető el.

A tanúsítványok felfüggesztésére a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk szolgálatot) ad. Az Ügyfélszolgálat elérhető a +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.

Panaszok bejelentésének helye:

a. személyesen az Ügyfélkapcsolati Irodákban

b. írásban a Szolgáltató székhelyére címezve

c. telefonon az Ügyfélkapcsolati Irodákban vagy az Ügyfélszolgálatnál

d. elektronikus levélben a *mavinformatika@mavinformatika.hu* és a *hiteles@mavinformatika.hu* címeken

Nyilvántartásba vétel:

A Nemzeti Média- és Hírközlési Hatóság (korábban: Hírközlési Felügyelet) a MÁV Szolgáltató Központ Zrt.-t minősített hitelesítés-szolgáltatóként 2003. április 3.-án nyilvántartásba vette.
A nyilvántartásba vétel (regisztráció) száma: MH-2460-8/2003.

1.3.2. A Szolgáltató regisztráló, hitelesítő és szolgáltató egységei

1.3.2.1. Ügyfélkapcsolati Irodák ("ÜKI")

Az Ügyfélkapcsolati Irodák (rövidítve: ÜKI) a Szolgáltató és a vele szerződéses alapon együttműködő Társaságok (mint szerződött közreműködők) azon szervezeti egységei, amelyek az előfizetői tanúsítvány kérelmek összeállítását és az elkészült tanúsítványok és eszközök átadását végzik, valamint az adminisztrációs feladatokat látják el.

1.3.2.2. Regisztrációs Iroda ("RA")

A Regisztrációs Iroda (rövidítve: RA) a szolgáltatás keretein belül biztosítja az előfizetők technikai regisztrációját, a tanúsítványok felfüggesztés és visszavonás kezelését és az aláírás-létrehozó adat adathordozó eszközre helyezését.

1.3.2.3. Hitelesítő Központ ("CA")

A Hitelesítő Központ (rövidítve: CA) a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, az ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladata a kulcspárok és tanúsítványok előállítása, a tanúsítványok közzététele.

1.3.2.4. Időbélyegző egység („TSA”)

Az időbélyegző egység (rövidítve: TSA) a Hitelesítő Központ erőforrásaival szorosan együttműködve az időbélyegzés szolgáltatást támogató informatikai rendszer központi erőforrásaiból, az ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladata az időbélyegek előállítása.

1.3.3. Felhasználói közösség

A Szolgáltató által kibocsátott tanúsítványokat felhasználó közösség a következő:

a. a Szolgáltató regisztráló és hitelesítő egységei, a szolgáltatást működtető elektronikus aláírásra feljogosított munkatársai

b. az Előfizetők és az Előfizetők feljogosított munkatársai,

c. a Ket. hatálya alá tartozó felhasználók, mint minősített elektronikus aláírást alkalmazó személyek

d. az Előfizetők és az Aláírók informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.)

e. az érintett felek

Szolgáltató által kibocsátott időbélyegek felhasználói közössége általában megegyezik a fentiekkel, azzal a kitétellel, hogy időbélyegzés szolgáltatást – tanúsítvány nélkül – önállóan is lehet igényelni.

1.3.3.1. Előfizető

Előfizető a Szolgáltatóval szerződéses viszonyban álló felhasználó, aki számára a Szolgáltató tanúsítványt és/vagy időbélyeget bocsát ki. Előfizető lehet természetes vagy jogi személy. A szerződési feltételeket a {Sz25} „*Általános Szerződési Feltételek PKI szolgáltatásokhoz*” (továbbiakban: ÁSZF-PKI) tartalmazza.

Az Előfizető lehet egyben Aláíró is, ha saját maga birtokolja és használja az aláírás-létrehozó eszközt.

Az Előfizető lehet jogi személy vagy jogi személyiség nélküli szervezet is. Az Aláíró(k) ebben az esetben a szervezet munkatársa(i).

1.3.3.2. Közigazgatási szervek

A közigazgatási szervek az előfizetők azon csoportja, melyek a {J2} Ket. hatálya alá tartoznak [lásd: Ket. 12. § (3) és (4) bekezdés].

1.3.3.3. Aláíró (alany)

Aláíró (alany) az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében, vagy szervezet képviseletében aláírásra jogosult.

Aláíró lehet:

a. bármely természetes személy, aki személyazonosságát a regisztráció során a jelen szabályzat 3.2.2 pontjában előírtak szerint igazolta,

b. bármely természetes személy, aki részére a tanúsítvány azzal a céllal kerül kibocsátásra, hogy jogi személy (szervezet) képviseletében legyen jogosult aláírni. Ebben az esetben az Aláíró személyazonosságának ellenőrzése mellett a regisztráció során a 3.2.3 pontban meghatározott módon a képviseleti jogosultságot is ellenőrizni kell.

c. az Aláíró (alany) definíciójára a közigazgatásban alkalmazható tanúsítványok esetében a Szolgáltató elfogadja és alkalmazza a {J11} [MHR_Ü] 1.3.3 és {J12} [MHR_K] 1.3.3 pontokat.

1.3.3.4. Érintett fél

Az Érintett fél az a személy vagy eszköz, aki vagy amely a magánkulcs felhasználó nyilvános kulcsához tartozó tanúsítvány ellenőrzése során a nyilvános kulcsú technikára (elektronikus aláírásra) hagyatkozva jár el:

a. az Érintett fél olyan természetes személy vagy eszköz, aki vagy amely az aláírt és/vagy időbélyegzett elektronikus dokumentum fogadója és aki vagy amely egy tanúsítvánnyal hitelesített elektronikus aláírásra hagyatkozva jár el az aláírás, és/vagy az időbélyeg hitelességének ellenőrzésekor.

b. az érintett fél definíciójára a közigazgatásban alkalmazható tanúsítványok esetében a Szolgáltató elfogadja és alkalmazza a {J11} [MHR_Ü] 1.3.4 és az {J12} [MHR_K] 1.3.4 pontokat.

Az Érintett fél az aláírás ellenőrzésekor az Aláíró nyilvános kulcsához tartozó tanúsítvány érvényességének ellenőrzésére hagyatkozva jár el.

1.3.4. A Közigazgatási Gyökér Hitelesítés-szolgáltató

A Szolgáltató a közigazgatásban alkalmazható tanúsítványok esetében magára nézve kötelezőnek ismeri el a Közigazgatási Gyökér Hitelesítés-szolgáltató (KGyHSz) által kiadott {J10} hitelesítési rendet és a KGyHSz felügyeleti jogát.

1.4. Tanúsítványhasználat

1.4.1. A szolgáltatások szintje

Szolgáltató az általa nyújtott szolgáltatások vonatkozásában **minősített szolgáltatóként** szerepel az Eat. 19.§.-a szerinti Hatósági nyilvántartásokban.

Ennek megfelelően, Szolgáltató hitelesítés-szolgáltatását jelen szabályozás keretében az Eat. 2.§. 17. pontjában meghatározott **minősített elektronikus aláírás** hitelesítéséhez nyújtja, az általa kibocsátott tanúsítványok az Eat. 2.§. 19. pontja szerint **minősített tanúsítványok**. Hasonlóan, Szolgáltató által jelen szabályozás keretében nyújtott időbélyegzés szolgáltatást minősített szolgáltatóként végzi.

1.4.2. Tanúsítványok alkalmazhatósága

A tanúsítványok alkalmazhatóságára a következő alapszabályok érvényesek:

- **A kibocsátott tanúsítványokhoz kapcsolódó magánkulcsok az elektronikus aláírások megtételére használhatók fel.**
- **A tanúsítványok illetve a nyilvános kulcsok az elektronikus aláírások ellenőrzésére használhatók fel.**

A Szolgáltató által jelen szabályzat hatálya alatt kibocsátott tanúsítványok (illetve az ezekhez kapcsolódó kulcspárok) felhasználhatók minden olyan számítástechnikai alkalmazásban, amelyek támogatják a PKI technológián alapuló elektronikus aláírási funkciókat.

Jelen szabályzat hatálya alatt kibocsátott tanúsítványok csak az 1.3.2.4 fejezetben meghatározott hitelesítés-szolgáltató és felhasználó közösség körében használhatók.

A Szolgáltató nem vállal felelősséget a kibocsátott tanúsítványok, illetve az ezekhez kapcsolódó kulcspárok kibocsátási céltól eltérő felhasználásáért.

Az időbélyegzéshez kibocsátott szolgáltatói tanúsítványokat, illetve aláíró kulcsokat a Szolgáltató kizárólag időbélyegek hitelesítésére illetve aláírására használja.

1.4.2.1. Megfelelő tanúsítványhasználat

A kibocsátott tanúsítványokhoz tartozó privát kulcs csak elektronikus állományok aláírására, a publikus kulcs pedig csak az aláírás ellenőrzésére használható fel, a tanúsítványba foglaltaknak megfelelően.

1.4.2.2. Korlátozott alkalmazási lehetőségek

Szolgáltató az ÁSZF-PKI-ban és az előfizetői szerződésben felhasználási, területi, pénzügyi, stb. korlátozásokat szabhat. A korlátozásokat a kibocsátott előfizetői tanúsítványban is megadja.

Az Előfizető szervezet élhet korlátozásokkal Aláíró és érintett felek tanúsítvány felhasználási tevékenységével kapcsolatosan.

1.4.2.3. Tiltott tanúsítványhasználat

A Szolgáltató és az Előfizető eltérő megállapodásának hiányában tilos az előfizetői magánkulcs felhasználása más nyilvános kulcsú tanúsítványok aláírására, vagy az előfizetői tanúsítványok alkalmazása bármilyen hitelesítés szolgáltatás nyújtásához.

1.4.3. Időbélyegek alkalmazhatósága

Szolgáltató által kiadott időbélyegek elektronikus aláírásokhoz, elektronikus üzenetekhez, tetszőleges elektronikus dokumentumokhoz vagy állományokhoz kapcsolhatók hozzá igazolva azok létezését az adott időpontban.

1.5. A szolgáltatási szabályzat adminisztrációja

1.5.1. Szabályzat hatálya

A HSZSZ-M aktuális verziójának időbeli hatálya a hatálybalépés dátumával kezdődik és határozatlan időre szól. Időbeli hatálya megszűnik egy újabb szabályzatverzió hatályba lépésével vagy a szolgáltatási tevékenység beszüntetésekor.

A HSZSZ-M személyi hatálya a felhasználó közösségre terjed ki.

A HSZSZ-M tárgyi hatálya a következőkre terjed ki:

a. az 1. pontban meghatározott szolgáltatásokra,

b. a Szolgáltatónak a hitelesítés-szolgáltatással kapcsolatban álló összes objektumára és tárgyi eszközére.

1.5.2. Kapcsolattartó személy

A Szolgáltató részéről a kapcsolattartó személy a PKI szolgáltatásokért általánosan felelős vezető. Elérhetőségét a Szogáltató az ügyfélkapcsolati irodákon keresztül biztosítja.

1.5.3. Változáskezelés

1.5.3.1. Változtatási eljárások

A Szolgáltató szervezetén belül Hitelesítési Rend és Szabályozási Csoport működik, amely a HSZSZ-M karbantartásáért felelős. A szolgáltatási szabályzat hitelesítési rendeknek való megfeleléséért a Hitelesítési Rend és Szabályozási Csoport, illetve annak vezetője felel. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, az új szabályzat verziókat jóváhagyásra előterjeszti, elektronikus aláírással hitelesíti, a hatályon kívül helyezett szabályzatokat arhiválja.

A szabályzatot a Szolgáltató vezetése hagyja jóvá és lépteti hatályba.

A szolgáltatási szabályzat módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

1.5.3.2. Kapcsolattartás, észrevételek kezelése

A szabályzattal, illetve a szolgáltatással kapcsolatos észrevételeket a Szolgáltató vezetésének kell címezni.

A HSZSZ-M-el kapcsolatos észrevételeket Szolgáltató az Ügyfélkapcsolati Iroda útján fogadja.

1.5.4. Közzétételi és tájékoztatási elvek

1.5.4.1. A HSZSZ-M-ben nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyeztetik. A Szolgáltató több belső biztonsági és egyéb szabályzattal {Sz19} –{Sz23}, {Sz27}, {Sz28} rendelkezik, melyeket bizalmasan, üzleti titokként kezel.

1.5.4.2. A HSZSZ-M közzététele

A Szolgáltató a HSZSZ-M-t a szolgáltatások internetes honlapján teszi közzé.

1.5.5. Elfogadási eljárások

A jelen HSZSZ-M szerkezetében és tartalmában követi az RFC 3647 szabványt azzal az eltéréssel, hogy a szabályzat nem tartalmazza a nem értelmezhető vagy lényegi előírásokat nem tartalmazó fejezeteket, illetve tartalmaz az RFC-ben nem tárgyalt fejezeteket is.

A Szolgáltató a jelen HSZSZ-M-t indokolt esetben, de legalább évente felülvizsgálja.

A szabályzat jogszabályoknak való megfelelőségét a Nemzeti Média- és Hírközlési Hatóság (NMHH) vizsgálja a HSZSZ-M aktuális változatának hatálybalépését megelőzően.

Módosítás esetén a Szolgáltató a HSZSZ-M változtatásokkal egybeszerkesztett új verziójának tervezetét felülvizsgálat és nyilvántartásba vétel céljából átadja a Nemzeti Média- és Hírközlési Hatóság Hivatalának. A Szolgáltató alkalmanként ezt megelőzően is konzultál az NMHH-val és/vagy a Közigazgatási Gyökér Hitelesítés-szolgáltatóval a tervezett változtatásairól. A HSZSZ-M új változata hatályba léptetésének feltétele, hogy azt a Nemzeti Média- és Hírközlési Hatóság nyilvántartásba vette.

A közigazgatásban alkalmazható tanúsítványok kibocsátásának feltétele, hogy a Szolgáltató tanúsítványát a Közigazgatási Gyökér Hitelesítés-szolgáltató felülhitelesítette.

1.6. Meghatározások

Alany: A hitelesítés-szolgáltató által kiadott tanúsítványban azonosított természetes személy, aki a tanúsítványban szereplő nyilvános kulcsnak megfelelő magánkulcsot birtokolja.

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 elektronikusan aláírt elektronikus dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ

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

Aláíró: az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult

Biztonságos aláírás-létrehozó eszköz: az Eat. 1. számú mellékletében foglalt követelményeknek eleget tevő, az Eat. 7. § (5) – (6) bekezdés szerinti tanúsítással rendelkező aláírás-létrehozó eszköz

Biztonsági tisztviselő, biztonsági menedzser: a hitelesítés-szolgáltatás biztonságáért, a biztonsági irányelvek és szabályzatok érvényre juttatásáért általánosan felelős személy

Elektronikus aláírás: elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat

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

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

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

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

Elektronikus aláírás érvényesítése: annak tanúsítása minősített elektronikus aláírás vagy e szolgáltatás tekintetében minősített szolgáltató által kibocsátott időbélyegző elhelyezésével, hogy az elektronikus dokumentumon elhelyezett elektronikus aláírás vagy időbélyegző, illetve az azokhoz kapcsolódó tanúsítvány az időbélyegző elhelyezésének időpontjában érvényes volt

Elektronikus aláírási termék: olyan szoftver vagy hardver, illetve más elektronikus aláírás alkalmazáshoz kapcsolódó összetevő, amely elektronikus aláírással kapcsolatos szolgáltatások nyújtásához, így különösen elektronikus aláírások, illetőleg időbélyegző készítéséhez vagy ellenőrzéséhez használható

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes

Érintett fél: Az Érintett fél (aláírás Ellenőrző) olyan természetes vagy jogi személy, aki vagy amely, az aláírt és/vagy időbélyegzett elektronikus dokumentum fogadója, és egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az aláírás, és/vagy az időbélyeg hitelességének ellenőrzésekor.

Érvényességi lánc: az elektronikus dokumentum vagy annak lenyomata, és azon egymáshoz rendelhető információk sorozata, (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás-ellenőrző adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató elektronikus aláírás-ellenőrző adatára és annak visszavonására vonatkozó információk), amely alapján megállapítható, hogy az elektonikus dokumentumon elhelyezett fokozott biztonságú vagy minősített aláírás, illetve időbélyegző, valamint az azokhoz kapcsolódó tanúsítványok az aláírás és időbélyegző elhelyezésének időpontjában érvényes volt

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

a. alkalmas az aláíró azonosítására,

b. egyedülállóan az aláíróhoz köthető,

c. olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak és

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

Hitelesítési rend: olyan szabálygyűjtemény, mely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára.

Időbélyegzés: az a folyamat, melynek során az elektronikus dokumentumhoz olyan igazolás rendelődik, amely tartalmazza a bélyegzés hiteles időpontját, és amely a dokumentumhoz oly módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető

Időbélyeg: elektronikus dokumentumhoz végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegzés időpontjában változatlan formában létezett

Időbélyegzés szolgáltatási rend: olyan szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely időbélyegző felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára

Igénybe vevő: elektronikus aláírással kapcsolatos szolgáltatást igénybe vevő természetes személy, jogi személy vagy jogi személyiség nélküli szervezet

Igénylő: a 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 titkosításhoz (rejtjelezéshez) vagy annak visszaállításához, továbbá az elektronikus aláírás előállításához vagy az elektronikus aláírás hitelességének ellenőrzéséhez szükséges

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

a) a képzett lenyomat egyértelműen származtatható az adott elektronikus dokumentumból;

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

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

Minősített elektronikus aláírás: olyan - fokozott biztonságú – elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki

Minősített hitelesítés-szolgáltató: az Eat. szabályai szerint nyilvántartásba vett, minősített tanúsítványt a nyilvánosság számára kibocsátó hitelesítés szolgáltató

Minősített szolgáltató: a minősített hitelesítés-szolgáltató és az Eat. 6. § (1) bekezdésének *b)-d)* pontjában meghatározott szolgáltatásokat nyújtó olyan szolgáltató, amely a szolgáltatók nyilvántartásában valamely szolgáltatás tekintetében minősített szolgáltatóként szerepel

Minősített tanúsítvány: az Eat. 2. számú mellékletében foglalt követelményeknek megfelelő olyan tanúsítvány, amelyet minősített szolgáltató bocsátott ki

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: hitelesítés-szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a hitelesítés-szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős 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: az Eat. 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat

Szolgáltató: elektronikus aláírással kapcsolatos szolgáltatást nyújtó természetes személy, jogi személy vagy jogi személyiség nélküli szervezet

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 digitális igazolás, amely a belefoglalt nyilvános kulcsot (aláírásellenőrző adatot) az Eat. 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

1.7. Hivatkozások

A Szolgáltató által nyújtott szolgáltatásokra elsősorban a következő jogszabályok vonatkoznak:

{J1} 2001. évi XXXV. törvény az elektronikus aláírásról (a továbbiakban: Eat.)

{J2} 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (a továbbiakban: Ket.)

{J3} 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

{J4} 78/2010. (III.25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól

{J5} 9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról

{J6} 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

{J7} 4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról

{J8} 7/2002 (IV. 26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről

{J9} Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára

{J10} A Közigazgatási Gyökér Hitelesítés-szolgáltató Hitelesítési rendje
(azonosító: [KGyHSz_HR], OID: 0.2.216.1.100.42.1.200.2.0)

{J11} Közigazgatási, ügyfélhez kapcsolódó, biztonságos aláírás-létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend
(azonosító: [MHR_Ü] OID: 0.2.216.1.100.42.101.1.2.1)

{J12} Közigazgatási, köztisztviselőhöz kapcsolódó, biztonságos aláírás-létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend
(azonosító: [MHR_K] OID: 0.2.216.1.100.42.101.2.2.1)

{J13} 2/2002. (IV. 26) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

A Szolgáltató által hivatkozott szabványok és szabályozói dokumentumok:

{Sz1} ISO/IEC 15408 1999: Információ technológia - Biztonsági módszerek - Informatikai biztonság értékelési kritériumai (1-3 részek)

{Sz2} RFC 3647 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és szolgáltatási szabályzat keretrendszer)

{Sz3} RFC 3739 (Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil)

{Sz4} RFC 2459 illetve RFC 3280 (Internet X.509 Nyilvános kulcsú infrastruktúra – Tanúsítvány és Tanúsítvány visszavonási lista profil)

{Sz5} Internet Közösség RFC 2527 ajánlása

{Sz6} ETSI TS 101 862 (Minősített tanúsítvány profil),

{Sz7} ETSI TS 101456 (Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények)

{Sz8} RFC – 3161 (Internet X. 509 nyilvános kulcsú infrastruktúra időbélyeg protokoll)

{Sz9} ETSI TS 102 023 (2003. 04) (Időbélyegzés szolgáltatókra vonatkozó követelmények)

{Sz10} ETSI TS 101 861 szabvány (Időbélyegzés profil)

{Sz11} IETF RFC 2560 szabvány

{Sz12} NIST FIPS 140-1 Level 1-3 (Kriptográfiai modulok biztonsági követelményei)

{Sz13} CEN 14167-2 munkacsoport egyezmény: „Védelmi profil hitelesítés-szolgáltató aláíró műveleteit megvalósító kriptográfiai modulra" (MCSO-PP, HSM-PP),

{Sz14} Common Criteria (CC, Közös /Informatikai Biztonsági/ Követelmények) az Európai Közösség, az Egyesült Államok és Kanada közös ajánlása az IT termékek biztonsági minősítésének követelményeire

{Sz15} American Bar Association (ABA)

{Sz16} PKI Assessment Guidelines (PAG)

{Sz17} CWA 14167-1, és a CWA 14172-1,-2,-3,-4 CEN Workshop Agreement-ek

{Sz18} MSZ ISO/EC 27001 szabvány

{Sz19} A MÁV Szolgáltató Központ Zrt. Szervezeti és Működési Szabályzata

{Sz20} A MÁV Szolgáltató Központ Zrt. Iratkezelési Szabályzata

{Sz21} A MÁV Szolgáltató Központ Zrt. Titokvédelmi Szabályzata

{Sz22} A MÁV Szolgáltató Központ Zrt. Adatvédelmi és adatbiztonsági szabályzata

{Sz23} A MÁV Szolgáltató Központ Zrt. Információbiztonsági szabályzata

{Sz24} Hitelesítési Rend
nyilvános körben kibocsátott biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványokra (HR-MTT+BALE)

{Sz25} Általános Szerződési Feltételek a PKI szolgáltatásokhoz (ÁSZF-PKI)

{Sz26} Időbélyegzés Szolgáltatási Rend (ISZR)

{Sz27} A PKI szolgáltatások biztonsági szabályzata

{Sz28} A PKI szolgáltatások üzletmenet-folytonossági terve

Ezeken túlmenően a Szolgáltató az üzleti titkok vonatkozásában az 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szerint jár el, a személyes adatok vonatkozásban az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseit veszi figyelembe .

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.

1.8. Tanúsítványok jellemzői és típusai

1.8.1. Minősített tanúsítványok jellemzői

Minősített tanúsítvány az Eat. 2. számú mellékletében foglalt követelményeknek megfelelő olyan tanúsítvány, amelyet minősített hitelesítés-szolgáltató bocsátott ki. A Szolgáltató által kibocsátott minősített tanúsítványok tartalmazzák:

- annak megjelölését, hogy a tanúsítvány minősített tanúsítvány,
- a tanúsítványt kibocsátó Szolgáltató és székhelyének (ország-) azonosítóját
- az aláíró nevét vagy (a közigazgatásban alkalmazható tanúsítványokat kivével) egy álnevet, ennek jelzésével,
- az aláírónak külön jogszabályban, a szolgáltatási szabályzatban vagy az általános szerződési feltételekben meghatározott speciális jellemzőit, a tanúsítvány szándékolt felhasználásától függően,
- azt az aláírás-ellenőrző adatot (publikus kulcsot), amely az aláíró által birtokolt aláírást készítő adatnak felel meg,
- a tanúsítvány érvényességi idejének kezdetét és végét, valamint azt az időtartamot, ameddig a hitelesítés-szolgáltató az Eat. 9. § (7) bekezdés szerinti feladatot a tanúsítvány vonatkozásában ellátja,
- a tanúsítvány azonosító kódját
- a Szolgáltató fokozott biztonságú elektronikus aláírását,
- a tanúsítvány használhatósági körére vonatkozó esetleges korlátozásokat,
- a tanúsítvány felhasználásának korlátait,
- más személy (szervezet) képviseletére jogosító elektronikus aláírás tanúsítványa esetén a tanúsítvány ezen minőségét és a képviselt személy (szervezet) adatait.

A Szolgáltató által jelen szabályozás keretében kibocsátott minősített tanúsítványok további jellemzőit az 1.6 pontban megnevezett {J11}, {J12}, és {Sz24} hitelesítési rendek írják le. Ez utóbbi Szolgáltató saját hitelesítési rendje, amelyhez kapcsolódó tanúsítványtípus legfontosabb jellemzőit a következő alpont ismerteti.

1.8.1.1. Nyilvános körben kibocsátott és biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványtípus (MTT+BALE)

Az MTT+BALE olyan tanúsítványtípus, amely:

a. megfelel az Eat. 2. számú mellékletében meghatározott követelményeknek

b. olyan Szolgáltató adta ki, amely teljesíti az Eat. 3. számú mellékletében meghatározott követelményeket

c. olyan biztonságos aláírás-létrehozó eszköz került felhasználásra, amely eleget tesz az Eat. 1. számú mellékletében meghatározott követelményeknek

d. nyilvános körben került kibocsátásra.

A Szolgáltató által kibocsátott minősített tanúsítványok a fenti követelményeknek megfelelve olyan elektronikus aláírások igazolására használhatók, amelyek az aláírás jogi követelményeit az elektronikus formájú adatok vonatkozásában ugyanolyan módon kielégítik, mint egy kézírásos aláírás a papír-alapú dokumentumok vonatkozásában. Az ilyen körülmények között készített elektronikus aláírást ***minősített elektronikus aláírás***-nak kell tekinteni.

1.8.2. Tanúsítványok felhasználási területük szerint

1.8.2.1. Előfizetői tanúsítványok

Az Előfizetői tanúsítványok a Szolgáltatóval szerződéses viszonyban álló Előfizetők számára kerülnek kibocsátásra.

Az Előfizetői tanúsítványokat leíró hitelesítési rendek objektum-azonosítói (OID):

1.3.6.1.4.1.14868.2.2.2 (HR-MTT+BALE)

0.2.216.1.100.42.101.1.2.1 [MHR_Ü]

0.2.216.1.100.42.101.2.2.1 [MHR_K]

Előfizetői tanúsítvány olyan magánszemélyeknek vagy szervezeteket képviselő természetes személyeknek kerül kiadásra, akiknél a Szolgáltató az Aláírót személyes megjelenésre, saját hitelesítő dokumentumokra és írásos nyilatkozatokra alapozott biztonsági ellenőrzéssel azonosítja.

Ha az Aláíró természetes személy bármely más természetes vagy jogi személyt képvisel, akkor a képviseleti jogot írásos megbízói nyilatkozattal kell igazolni.

Kötelezettség vállalással csak Előfizetői tanúsítvány adható ki. A kötelezettségvállalás értékhatárát az Előfizetői Szerződés rögzíti és ezt az értékhatárt a Szolgáltató a tanúsítványban feltünteti.

1.8.2.2. Szolgáltatói tanúsítványok

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

A saját kiadású Szolgáltatói tanúsítványok objektum-azonosítója (OID): 1.3.6.1.4.1.14868.1.2

1.8.3. Tanúsítvány típusok

A Szolgáltató a szolgáltatói tanúsítványok tekintetében nem alkalmaz típus-megkötést.

A Szolgáltató a következő típusú Előfizetői tanúsítványokat adhatja ki:

1.8.3.1. „Személyes” tanúsítvány

„Személyes” típusú tanúsítványt európai uniós állampolgárságú természetes személy igényelhet a saját nevében.

Személyes tanúsítványok természetes személyek részére kerülnek kibocsátásra. A személyes tanúsítvány esetében az Előfizető és az Aláíró jellemzően ugyanaz a személy

A tanúsítvány „Country” és „Locality” mezőjében az Előfizető lakóhelyének országkódja és helységneve, a „Common Name” (CN) mezőben az Előfizető neve vagy álneve szerepel. Az „E” mezőben opcionálisan az Előfizető e-mail címe szerepel. A tanúsítvány „Organization” és „Organization Unit” mezői üresen maradnak.

Ha a tanúsítvány CN mezőjében nem az aláíró személyazonosító igazolványában szereplő név kerül megadásra, úgy ez a név álnévként kerül rögzítésre.

A közigazgatásban alkalmazható tanúsítványok szerkezete és adattartalma megfelel a {J9} az Informatikai és Hírközlési Minisztérium ajánlása szerinti követelményeknek és a {J11} - {J12} hitelesítési rendeknek, így pl.: az email cím a „SubjectAltName” mezőben szerepel, ill. a tanúsítvány CN mezőiben csak valós nevek szerepelhetnek, álnév használata kizárt.

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

1.8.3.2. „Szervezeti személy” („Munkatársi”) tanúsítvány

„Szervezeti személy” vagy más néven „Munkatársi” tanúsítványokat természetes személy igényelhet egy adott szervezet alkalmazottjaként és/vagy tisztségviselőjeként.

Ebben az esetben az Előfizető a szervezet, az Aláíró a szervezetet képviselő személy. Az Előfizetői Szerződésben a szervezet által vállalt kötelezettségek egyetemlegesen érvényesek a szervzetet képviselő Aláíróra.

A tanúsítvány „Country” mezőjében a szervezet telephelyének országkódja, az „Organization” mezőben a szervezet neve, a „Common Name” (CN) mezőben a munkatárs (aláíró) neve szerepel. Opcionálisan szerepel a „Locality” mezőben a szervezet telephelyének városa, az „Organizational Unit” mezőben a szervezeti egység neve és az „E” mezőben a munkatárs (aláíró) e-mail címe.

Ha a tanúsítvány CN mezőjében nem az aláíró személyazonosító igazolványában szereplő név kerül megadásra, úgy ez a név álnévként kerül rögzítésre.

A közigazgatásban alkalmazható tanúsítványok szerkezete és adattartalma megfelel a {J9} az Informatikai és Hírközlési Minisztérium ajánlása szerinti követelményeknek és a {J11} - {J12} hitelesítési rendeknek, így pl.: az email cím a „SubjectAltName” mezőben szerepel, ill. a tanúsítvány CN mezőiben csak valós nevek szerepelhetnek, álnév használata kizárt.

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

1.9. Időbélyegek jellemzői

Időbélyeget a Szolgáltató a vele szerződéses viszonyban álló Előfizetők számára bocsát ki a minősített időbélyegekre vonatkozó {Sz26} Időbélyegzés Szolgáltatási Rend (objektum-azonosító: 1.3.6.1.4.1.14868.3.6) szerint.

A Szolgáltató az időbélyegeket az Előfizetők regisztrációja során a számukra kiosztott hozzáférés jogosultság (authentikációs tanúsítvány) vizsgálatát és elfogadását követően bocsátja ki.

2. Általános rendelkezések

2.1. Feladatok és hatáskörök

2.1.1. A Szolgáltató feladatai és hatásköre

1. A Szolgáltató gondoskodik a szolgáltatásokra vonatkozó valamennyi, a jelen HSZSZ-M-ben részletezett állítás teljesüléséről, amennyiben azok az adott tanúsítványtípusra vagy időbélyegre alkalmazhatók.
2. A Szolgáltató szolgáltatásait nyilvánosan elérhetővé teszi.
3. A Szolgáltató jogi személy.
4. A Szolgáltató rendszeresen felülvizsgálja és újra kiadja HSZSZ-M-ét.
5. A Szolgáltató mindenkor az Előfizető által átadott és az Ügyfélkapcsolati Irodák által ellenőrzött adatok alapján bocsátja ki a tanúsítványokat. A Szolgáltató a tanúsítvány kibocsátását követően a tanúsítvány adataiban nem változtathat.
6. A Szolgáltató a Tanúsítványtárában teszi közzé az általa kibocsátott, visszavonási listákban a felfüggesztett és visszavont előfizetői tanúsítványokat. A Tanúsítványtár, a visszavonási listák és az időbélyegzés szolgáltatás elérhetőségét a Szolgáltató 99,9%-os rendelkezésre állással biztosítja úgy, hogy az elérhetőség kiesése esetenként nem lépheti túl a 3 órás időtartamot.
7. A Szolgáltató kötelezettséget vállal arra, hogy az előfizető regisztrációját követően a tanúsítvány kiadására intézkedik és erről az Előfizetőt értesíti. Tanúsítvány kiállítására ezt követően legkésőbb 30 naptári napon belül kerül sor.
8. A Szolgáltató a szolgáltatások működtetése és menedzselése során az ügyfélkapcsolati tevékenységet Ügyfélkapcsolati Irodák által biztosítja.
9. A Szolgáltató rendkívüli üzemeltetési helyzetben is biztosítja tanúsítványtára és visszavonási nyilvántartásai elérhetőségét, visszavonás kezelési, visszavonási állapot közzétételi és időbélyegzés szolgáltatását minden érdekelt fél számára. Ügyfélszolgálata útján folyamatos felügyeletet biztosít a tanúsítvány visszavonási és felfüggesztési igények fogadására és kezelésére.
10. A Szolgáltató vezeti és az internetes honlapján keresztül bárki számára folyamatosan elérhetővé teszi a jogszabály szerinti nyilvántartásokat és a tanúsítvány kibocsátására vonatkozó saját szabályzatait.
11. A Szolgáltató a lejárat előtti 30 napban értesítést küldhet a lejáró tanúsítványokról az Előfizető részére.
12. Szolgáltató a tanúsítványban feltünteti az Előfizetői Szerződésben rögzített, a tanúsítvány felhasználhatóságával kapcsolatos korlátozásokat.
13. A Szolgáltató indokolt esetben felfüggeszti vagy visszavonja a tanúsítványt és ezt a szolgáltatások internetes honlapján közzéteszi.
14. Szolgáltató megőrzi a tanúsítványokkal kapcsolatos adatokat és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejáratától számított 10 évig, illetőleg – amennyiben ezen időszakban az elektronikus aláírással vagy 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.
15. Ha a Szolgáltató be kívánja fejezni tevékenységét, erről legalább hatvan nappal korábban értesíti az Előfizetőket és a Nemzeti Média- és Hírközlési Hatóságot. A bejelentés időpontjától kezdve a Szolgáltató nem bocsáthat ki új tanúsítványt. A Szolgáltató a tevékenység befejezése előtt legalább húsz nappal visszavonja az általa kibocsátott és még érvényes tanúsítványokat. A Szolgáltató a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének eleget tesz.
16. A Szolgáltató intézkedik az iránt, hogy legkésőbb a tevékenysége 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.

2.1.1.1. Az Ügyfélkapcsolati Iroda feladatai és hatásköre

Az Ügyfélkapcsolati Iroda szolgáltatás igénylés és teljesítés keretén belül:

1. felveszi a regisztráció során az előfizető adatait és elkészíti az előfizetői szerződést,
2. összegyűjti, illetve meghatározza a tanúsítványba kerülő adatokat,
3. megőrzi a nyilvántartásokat,
4. bizalmas információként kezeli az Előfizető és az Aláíró minden adatát, kivéve azokat, amelyeket a tanúsítványba kerülnek,
5. gondoskodik az aláírás-létrehozó eszköz és a PIN kód biztonságos kezeléséről és az Előfizetőnek történő biztonságos átadásáról,

6. a tanúsítvány kezelési eljárások során korlátozás nélkül biztosítja az Aláíró számára a rá vonatkozó regisztrációs és egyéb adatokhoz történő hozzáférést,
7. fogadja a tanúsítvány visszavonásra, felfüggesztésre, vagy a felfüggesztés megszüntetésére vonatkozó kérelmeket,
8. felfüggesztési/visszavonási kérelem elfogadása után intézkedik a tanúsítvány felfüggesztéséről/visszavonásáról,
9. tájékoztatja a visszavont, illetve felfüggesztett tanúsítvány tulajdonosát tanúsítványa állapotának változásáról,
10. fogadja az Aláíró adatainak változására vonatkozó bejelentéseket.
11. időbélyegzés-szolgáltatás esetén biztosítja az Előfizető részére a szolgáltatáshoz való hozzáférés jogosultságot (jellemzően authentikációs tanúsítványt).

2.1.1.2. A Hitelesítési Rend és Szabályozási Csoport feladatai és hatásköre

A Hitelesítési Rend és Szabályozási Csoport feladata a Szolgáltató és felhasználói közösség igényeinek felmérése és folyamatos követése, ezek alapján a közösség működésére vonatkozó alapelvek lefektetése, s ebből levezetve a tagok tevékenységét részletesen szabályozó, az egész Szolgáltató szervezetre nézve közös szabályzatok, így a hitelesítési rendek, a HSZSZ-M, az ISZR, az ÁSZF-PKI, és a biztonsági szabályzatok, készítése és rendszeres karbantartása. A szolgáltatási szabályzat hitelesítési rendeknek való megfeleléséért a Hitelesítési Rend és Szabályozási Csoport, illetve annak vezetője felel.

A Hitelesítési Rend és Szabályozási Csoport feladatai tételesen a következők:

1. A hitelesítési-, és időbélyegzési rendek elkészítése és karbantartása.
2. A szolgáltatási szabályzatok elkészítése és karbantartása.
3. A hitelesítési rendek és a szolgáltatási szabályzatok közötti összhang biztosítása.
4. A hitelesítési rendek és szolgáltatási szabályzatok verzióinak nyilvántartása és megőrzése.
5. A hitelesítési rendek és szolgáltatási szabályzatok hitelesítése és publikálása.
6. A regisztrációs folyamat szabályozása, ellenőrzése és felülvizsgálata.

2.1.1.3. Az Ügyfélszolgálat feladata

A tanúsítványokkal kapcsolatos felfüggesztési, illetve visszavonási kérelmeket a Szolgáltató Ügyfélszolgálata telefonon és elektronikus levélben folyamatosan (napi 24 órában) fogadja.

2.1.2. Az Előfizető és az Aláíró feladatai és hatásköre

Az Előfizető és az Aláíró kötelessége a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatás igénybevétele során. Ennnek során az Előfizető és az Aláíró köteles:

1. Önmagát az Ügyfélkapcsolati Irodán hiteles okmányokkal igazolni.
2. A tanúsítvány igénylését és magánkulcsának felhasználását úgy végezni, hogy az harmadik fél jogait ne sértse.
3. Az Előfizető a regiszrtráció során a tanúsítvány kiadásához szükséges adatokat ellenőrizni.
4. Az Aláíró saját érdekében biztosítani az aláírás-létrehozó eszközének és PIN kódjának védelmét.
5. az Előfizető saját érdekében biztosítani az időbélyegzés hozzáférés titkos adatait (jellemzően az authentikációs tanúsítvány magánkulcsát),
6. az Előfizető az Aláíró figyelmét külön felhívni arra, ha az Előfizetői Szerződés a tanúsítvány felhasználhatóságával kapcsolatban összeg, területi vagy egyéb korlátozásokat tartalmaz,
7. 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.
8. az Előfizető vagy az Aláíró azonnal intézkedni a tanúsítvány visszavonása, illetve felfüggesztése végett, amennyiben
   - 8.1.1 tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, tartalmában, a regisztrációs adatokban pontatlanság van, illetve azokban változás következett be,
   - 8.1.2 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,
9. az Aláíró vagy az Előfizető elektronikus aláírással, időbélyeggel ellátott elektronikus dokumentummal kapcsolatos jogvita megindulásáról köteles haladéktalanul tájékoztatni a Szolgáltatót.
10. Az időbélyeget felhasználók kötelesek a kért időbélyeg vétele után meggyőződni arról, hogy az időbélyeget a Szolgáltató elektronikusan aláírta, az aláírás az időbélyegzésre szolgáló kulccsal történt-e és a hozzátartozó tanúsítvány érvényes-e.

Továbbá:

1. Az Aláíró jogosult arra, hogy a magánkulcsot birtokolja és a jogszabályokban meghatározott módon elektronikus aláíráshoz felhasználja.
2. Az Aláíró tudomásul veszi, hogy a magánkulcsával készített elektronikus aláírás a saját elektronikus aláírásának minősül, és viseli ennek jogkövetkezményeit
3. az Aláíró a tanúsítványt csak a jelen HSZSZ-M-nek, valamint a hatályos jogszabályi rendelkezéseknek megfelelően használhatja.

2.1.3. Érintett félre vonatkozó ajánlások

Az érintett fél részére ajánlott megismerni a Szolgáltató nyilvánosan elérhető HSZSZ-M-je rá vonatkozó részét.

2.1.3.1. Ajánlás az elektronikus aláírás elbírálása során

Az Érintett félnek ajánlott (a Szolgáltató szabályzataiban leírtaknak megfelelően) a legnagyobb gondossággal eljárni az elektronikus aláírás és a tanúsítvány elbírálásakor, ezen belül:

1. ajánlott elvégeznie az elektronikus aláírás ellenőrzését, az ún. tanúsítási lánc vizsgálatával az alábbiak szerint:
   1.1. az Aláíró tanúsítványának segítségével meggyőződni az Aláíró tanúsítványt kibocsátó (hitelesítés-szolgáltató) kilétéről;
   1.2. a hitelesítés-szolgáltató tanúsítványának segítségével meggyőződni az Aláíró tanúsítványának integritásáról;
   1.3. az Aláíró tanúsítványának állapotát (érvényességét) ellenőrizni a tanúsítvány visszavonási listák (CRL) áttanulmányozásával;
   1.4. áttanulmányozni az Aláíró tanúsítványának összes attribútumát, és az adott tranzakcióra vonatkozó előírásoknak, valamint józan megfontolásoknak megfelelően döntést hozni az aláírás elfogadásáról vagy elutasításáról,
2. nem szabad elfogadni az elektronikus aláírást, ha az elektronikus aláírás, az aláíró tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata, annak érvénytelenségére utal; az aláírás elfogadása nem jelenti az aláírt üzenet tartalmának tudomásul vételét vagy elfogadását.
3. Az ellenőrzés a tanúsítvány érvényességének lejárta után is elvégezhető, mert a Szolgáltató az Eat. 9.§ (7. bek.) alapján a tanúsítványokat és a tanúsítványok ellenőrzéséhez szükséges adatokat a tanúsítvány lejártát követő 10 évig, illetve az aláírt és/vagy időbélyegzett dokumentummal kapcsolatban felmerült jogvita lezárásáig megőrzi, így a tanúsítványokkal kapcsolatos elektronikus információkat és ahhoz kapcsolódó személyes adatokat elő lehet keresni és a tanúsítvány érvényességét ellenőrizni lehet. A tanúsítvány tartalmának megállapításához a Szolgáltató megfelelő eszközt biztosít.

2.1.3.2. Ajánlás az időbélyeg ellenőrzése során

Időbélyeg ellenőrzése során ajánlott meggyőződni arról, hogy az időbélyeg valóban a lebélyegzett dokumentumhoz tartozik-e és az időbélyeg aláírása érvényes-e.

Az időbélyeget aláíró kulcs tanúsítványának ellenőrzésére vonatkozóan általában érvényesek a 2.1.3.1 pontban leírt, a tanúsítvány ellenőrzésre vonatkozó szabályok.

2.2. Felelősségek

2.2.1. A Szolgáltató felelőssége

A Szolgáltató azzal, hogy aláír egy, a jelen HSZSZ-M 1.8.3 pontja szerint meghatározott tanúsítványt, időbélyeget,– és ezzel jelzi az 1.3.2.4 pontban meghatározott felhasználó közösség felé ezen HSZSZ-M használatát – azért vállalja a felelősséget, hogy a tanúsítvány előállítása, kibocsátása, közzététele, visszavonása, a visszavonási listák közzététele, az időbélyegzés tevékenységek a jelen HSZSZ-M-ben előírtaknak teljes mértékben megfelelnek, és a Szolgáltató megteszi a szükséges intézkedéseket ahhoz, hogy a Szolgáltató maga és az Előfizetők is a jelen HSZSZ-M előírásainak megfelelően járjanak el.

A Szolgáltató a vele szerződéses jogviszonyban álló Előfizetővel szemben a szerződésszegésért való felelősség szabályai szerint felelős az elektronikus aláírással aláírt elektronikus dokumentummal okozott kárért, ha megszegte a jelen HSZSZ-M-ben, az ÁSZF-PKI-ban vagy az előfizetői szerződésben előírtakat, továbbá az Eat. 7. § (2) bekezdésében, a 9-11. §-okban vagy a 14.§-ban foglaltakat. E szabályok megtartását kétség esetén a szolgáltatónak kell bizonyítania.

A Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a Magyar Köztársaság Polgári Törvénykönyvéről szóló 1959. évi IV. törvény 339. §-a szerint felelős az elektronikus aláírással aláírt elektronikus dokumentummal okozott kárért, ha mulasztása bizonyítható.

A felelősségvállalás mértékét, mely tanúsítvány típusonként és egyedi tanúsítványonként is maximált összegű, az Előfizetői Szerződésben kell rögzíteni.

A Szolgáltató nem vállal felelősséget, ha a Szolgáltató által kibocsátott tanúsítvány a jelen HSZSZ-M-ben előírtaktól eltérő módon kerül felhasználásra. Így a Szolgáltató nem felelős az olyan károkért, melyek abból adódtak, hogy az Érintett fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok és Szolgáltató jelen HSZSZ-M-e szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

A Szolgáltató azáltal, hogy az Előfizetők részére tanúsítványokat, időbélyegeket bocsát ki, semmilyen körülmények között sem tekinthető az Előfizetők vagy az érintett felek ügynökének, megbízottjának, képviselőjének, vagy bármilyen más, az Előfizetői Szerződésben meghatározottól eltérő funkciójú partnerének a hitelesítési tevékenysége vonatkozásában.

2.2.2. Az Előfizető és az Aláíró felelőssége

Az Előfizetőnek és az Aláírónak felelőssége áll fenn a regisztráció során megadott adatainak valódiságával kapcsolatban.

Az Előfizetőnek kártérítési felelőssége áll fenn a 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 jelen HSZSZ-M-ben, az ÁSZF-PKI-ban és a vonatkozó jogszabályokban meghatározott módon és célra használta.

Az Előfizető vagy az Aláíró köteles azonnal tájékoztatni a hitelesítés-szolgáltatót az aláírás-létrehozó adatnak illetéktelen személy tudomására jutásáról vagy elvesztéséről.

Az Előfizető vagy az Aláíró köteles három napon belül tájékoztatni a hitelesítés-szolgáltatót, ha:

a. az azonosításához szükséges személyazonosító adatokról, más személy (szervezet) képviseletében történő aláírásra jogosító elektronikus aláírás esetén a képviseletre, illetőleg aláírásra jogosult személy személyazonosító adatairól, a cégadatokról, továbbá mindezek változásáról;

b. az aláírással vagy az így aláírt elektronikusan aláírt elektronikus dokumentummal, illetve a tanúsítvánnyal kapcsolatban észlelt - a szolgáltatási szabályzatban meghatározott - rendellenességről;

c. a tanúsítvánnyal ellátott elektronikusan aláírt elektronikus dokumentummal, időbélyeggel kapcsolatos jogvita megindulásáról.

Az Előfizető illetve az Aláíró felelős az aláírás-létrehozó eszköz biztonságos megőrzéséért, az aláírás-létrehozó adat és a PIN kód valamint az időbélyegzés szolgáltatáshoz kapcsolódó authentikációs tanúsítvány magánkulcsa illetéktelenek tudomására jutásának megakadályozásáért.

A Szolgáltató nem vállal felelősséget a biztonságos aláírás-létrehozó eszköz hordozó elvesztéséből, vagy az aláírás-létrehozó adat (magánkulcs) biztonságának egyéb módon történő sérüléséből, elvesztéséből, illetve a PIN kód illetéktelen személy tudomására jutásából származó károkért.

2.2.3. Érintett fél felelőssége

Az Érintett fél felelős az elektronikus aláírás és a Szolgáltató által kibocsátott tanúsítványok illetve időbélyegek elfogadása során tanúsított körültekintő ellenőrzésért, az adott helyzetben elvárható magatartás tanúsításáért.

Érintett fél felelőssége fennáll a tanúsítvány vagy időbélyeg elfogadásából fakadó bármely következményért és kárért, ha a tanúsítvány vagy időbélyeg érvényességének ellenőrzése során nem az irányadó jogszabályok szerint vagy nem az adott helyzetben általában elvárható gondossággal jár el.

2.3. Értelmezés és alkalmazás

2.3.1. 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 vonatkozó fő jogszabályok felsorolását az 1.7 fejezet tartalmazza.

2.3.2. Hatályosság, megszűnés, értesítések

2.3.2.1. Hatályosság

A HSZSZ-M, az ÁSZF-PKI és az előfizetői szerződés a felhasználói közösség résztvevőinek valamennyi kötelezettségét, felelősségét és jogát tartalmazza.

A HSZSZ-M csak írott és hitelesített formában módosítható, a Nemzeti Média- és Hírközlési Hatóság által vezetett nyilvántartásban való átvezetés mellett.

A HSZSZ-M személyi és tárgyi hatályát az 1.5.1 pont tartalmazza.

2.3.2.2. Megszűnés

A HSZSZ-M a Szolgáltató minősített hitelesítés-szolgáltatásának vagy időbélyegzés szolgáltatásának befejezésével tekintendő megszűntnek.

2.3.2.3. Értesítések

A Szolgáltató az Előfizetőket és Érintett feleket tipikusan a szolgáltatások internetes honlapján történő közzététellel, illetve az ügyfélkapcsolati irodákban elérhető dokumentumokkal tájékoztatja. Az ügyfélkapcsolati irodák az Előfizetőket esetenként írásban vagy elektronikus úton is értesíthetik.

Az Előfizetők és az Érintett felek vagy bármely harmadik fél az Ügyfélkapcsolati Irodát megkeresheti írásban postai úton, e-mail-ben vagy faxon, továbbá ügyfélfogadási időben személyesen vagy telefonon.

A Szolgáltató Ügyfélszolgálata folyamatos szolgálattal áll rendelkezésre telefonos vagy e-mail megkeresés esetén.

2.3.3. Vitás kérdések kezelése

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

Panaszt az Előfizetőt nyilvántartó Ügyfélkapcsolati Irodán vagy az Ügyfélszolgálatnál lehet írásban vagy szóban előterjeszteni. A panaszt a Szolgáltató az előterjesztéstől számított 20 munkanapon belül kivizsgálja és ennek eredményéről a panaszost írásban tájékoztatja.

A jogvitáik rendezésére vonatkozó szabályokat az {Sz25} ÁSZF-PKI tartalmazza.

2.4. Közzététel

2.4.1. Adatbázisok

2.4.1.1. Tanúsítványtár

A Szolgáltató az általa kibocsátott tanúsítványokat Tanúsítványtárában helyezi el.

Az Aláíró vagy az Érintett fél a szolgáltatások internetes honlapján keresztül érheti el a Tanúsítványtár adatait.

A Tanúsítványtár elérhetőségét a Szolgáltató folyamatosan (az év minden napján, 24 órában), 99,9%-os rendelkezésre állással biztosítja úgy, hogy a Tanúsítványtár szolgáltatás kiesése nem lépheti túl esetenként a 3 órás időtartamot.

2.4.1.2. Naplók, regisztrációs adatok

A Szolgáltató a működése során keletkező naplófájlokat, regisztrációs adatokat belső adatbázisokban, fokozottan védett körülmények között tárolja.

2.4.1.3. Az adatbázisok elérésének szabályozása

A Szolgáltató minden Előfizető és érintett fél számára elérhetővé teszi a szolgáltatások internetes honlapját, azon keresztül Tanúsítványtárát és visszavonási listáit olvasás céljából. A Tanúsítványtárban keresési lehetőséget biztosít a tanúsítványokban tárolt adatok alapján.

A Szolgáltató belső adatbázisait és egyéb adatállományait a jogszabályokban meghatározott kötelezettségeken túl csak és kizárólag a Szolgáltató biztonsági szabályzatai által meghatározott szerepkörű és jogosultságú munkatársai érhetik el.

2.4.2. A tanúsítványokra, időbélyegekre vonatkozó információk közzététele

A Szolgáltató gondoskodik arról, hogy a tanúsítványok, az időbélyegek és az azokhoz kapcsolódó kikötései és egyéb feltételei az előfizetők és az érintett felek rendelkezésére álljanak. Ezek közé tartozik különösképpen:

a. a hitelesítési rendek, szolgáltatási szabályzatok

b. a tanúsítványok, illetve az időbélyegek használatára vonatkozó ismertetők, nyomtatványok

c. a kibocsátott előfizetői és szolgáltatói tanúsítványok

d. a felfüggesztett és visszavont előfizetői és szolgáltatói tanúsítványok

e. szolgáltatói közlemények

A Szolgáltató a szolgáltatói információkat elektronikus formában szolgáltatásai internetes honlapján keresztül teszi elérhetővé. Szolgáltatónak csak saját elektronikus aláírásával ellátott dokumentumai tekinthetők eredetinek. Az elektronikus dokumentumok nyomtatott változatai nem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

A Szolgáltató hiteles nyomtatott dokumentumai az Ügyfélkapcsolati Irodán férhetők hozzá.

2.4.3. A közzététel gyakorisága

Tanúsítványok, kikötések és feltételek nyilvánosságra hozatala:

A Szolgáltató a kibocsátott előfizetői tanúsítványokat - az érintett alany, illetve előfizető hozzájárulása esetén - a Tanúsítványtárban 24 órán belül közzéteszi és azok elérhetőségét az Interneten keresztül korlátozás nélkül, folyamatosan, a 2.1.1/6. pont szerinti rendelkezésre állással biztosítja.

A Szolgáltató általa működtetett hitelesítő központok szolgáltatói tanúsítványait a Tanúsítványtárában 24 órán belül közzéteszi és azok elérhetőségét az Interneten keresztül korlátozás nélkül, folyamatosan, a 2.1.1/6. pont szerinti rendelkezésre állással biztosítja.

Visszavonási állapot információk nyilvánosságra hozatala:

a. A Szolgáltatónak a visszavonási és felfüggesztési kérelem fogadásától számított 3 órán belül meg kell állapítania a kérelem érvényességét (a kérelmező jogosultságát), és visszavonási listájában át kell vezetnie az érvényes kérelem szerinti visszavonási állapot megváltozását.

b. A Szolgáltató a kérelem szerint módosított visszavonási állapotot az a.) pontban foglaltak teljesítését követő 1 órán belül teszi közzé a visszavonási listájában.

c. A Szolgáltató a tanúsítvány visszavonási listákat (beleértve ezek bármely változatát is) legalább 24 óránként teszi közzé.

A Szolgáltató a visszavonási listák elérhetőségét az Interneten keresztül korlátozás nélkül, folyamatosan, a 2.1.1/6. pont szerinti rendelkezésre állással biztosítja.

3. Azonosítás és hitelesítés

3.1. Megnevezési konvenciók

3.1.1. Nevek típusa

A tanúsítványban szereplő név (betű-, szóköz- és ékezet-helyesen) azonos a személyazonosság igazolására elfogadott hatósági személyazonosító igazolványban (személyi igazolvány, jogosítvány vagy útlevél) feltüntetett valódi névvel. Az ettől eltérő névmegadás álnévnek minősül.

A tanúsítványokban szereplő névmegadás az ITU-T[3] X.500 ajánlásának felel meg: X.500 formátum (ITU-T X.501 /ISO/IEC 9594-2:1997, RFC 2459).

3.1.2. Nevek szemantikája

Megnevezési konvenciók:

Természetes személy alany esetében a tanúsítványban feltüntetett név azonos a személyazonosság igazolására elfogadott hatósági személyazonosító igazolványban foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve CN és SN mezőkkel (CN=Teljes név=Vezetéknév+Keresztnév, SN=Vezetéknév), az UTF-8 kódolást használva.

A Szolgáltatót fenntartja a jogot, hogy a tanúsítvány adatok egyedi elbírálás alapján, az Előfizető egyetértésével az előzőektől eltérő írásmód vagy karakterkészlet használatával kerüljenek rögzítésre.

Nem természetes személy alany vagy álnév használata esetében a tanúsítványban feltüntetett név megegyezik az Előfizető által megadott névvel az UTF-8 kódolást használva.

A Szolgáltató fenntartja a jogot az egyes személyeket vagy csoportokat esetlegesen sértő (pl. jóízlést, szemérmet, etnikai hovatartozást sértő) álnevek és egyéb adatok megadásának elutasítására.

A Ket. hatálya alá tartozó név típusok ([MHR+_Ü], [MHR+_K] 3.1.1 pontok):

Természetes személy alany esetében a személyazonosság igazolására elfogadott hatósági személyazonosító igazolványban (személyi igazolvány, jogosítvány vagy útlevél) foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve CN és SN mezőkkel (CN = Teljes név = Vezetéknév + Keresztnév, SN = Vezetéknév), az UTF-8 kódolást használva.

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

A tanúsítványok CN mezőiben csak valós nevek szerepelhetnek, álnév használata kizárt.

3.1.3. Nevek egyedisége

A Szolgáltató biztosítja tanúsítványtárában a tulajdonosazonosítók egyediségét, azaz gondoskodik arról, hogy az általa kiadott tanúsítványokban használt megkülönböztető nevet (DN) sohasem fogja egy másik entitáshoz rendelni. Erről a Szolgáltató elsődlegesen az alany neve és e-mail címének a névmegadásban való szerepeltetésével gondoskodik. A Szolgáltató a megkülönböztető név kiosztásakor ellenőrzi, hogy az adott név és e-mail cím szerepel-e egy más alany részére korábban kibocsátott tanúsítványban. Ha igen, és a tanúsítvány egyéb névmezői sem biztosítják az egyediséget, akkor a Szolgáltató fenntartja magának a jogot a megkülönböztető név olyan megváltoztatására, amely továbbra is jellemző az alanyra, mint magánkulcs felhasználóra, de biztosítja a megkülönböztethetőséget.

A nevek kiadására vonatkozó igények teljesítését a Szolgáltató érkezési sorrendben végzi.

3.1.4. Név igénylési viták feloldása

A magánkulcs felhasználót a tanúsítványban megadott név és a tanúsítvány sorozat száma különbözteti meg egyértelműen a többi magánkulcs felhasználótól.

A Szolgáltató – lehetőségei szerint – a névkiosztás során ellenőrzi a magánkulcs felhasználó 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] „Information Technology - Open Systems Interconnection - The directory: Overview of concepts, models and services”

3.1.5. Álnevek használata

Álnév használata esetén a CN mezőben található szöveg '~' (tilde) karakterrel kezdődik és végződik (pl. CN= „~Ludas Matyi~").

A közigazgatásban alkalmazható tanúsítványok DN (megkülönböztető név) mezőiben csak valós nevek szerepelhetnek, álnév használata kizárt.

3.1.6. Védjegyek elismerésének és hitelesítésének módszere

A regisztrálással az Előfizető kifejezi, hogy a tanúsítványban 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.

3.2. Regisztráció

A regisztrálás során:

a. Az Előfizető kitölti a regisztrációs űrlapot és átadja az Ügyfélkapcsolati Iroda részére,

b. a regisztrációs űrlap elfogadásával Szolgáltató gondoskodik az Előfizetői Szerződés előkészítéséről és intézkedik az előfizetői kulcspár és tanúsítvány elkészítésére,

c. Az előfizetői tanúsítvány elkészültével értesíti az Előfizetőt és egyezteti vele a tanúsítvány és az Előfizetői Szerződés átvételének módját.

A regisztrációs űrlap egyúttal az Előfizetői Szerződés szerepét is betöltheti.

Ha egy Előfizető csak időbélyegzés szolgáltatást igényel, a regisztráció egyszerűsített eljárással történik a 3.2.6 pont szerint.

3.2.1. Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere

Az Aláíró számára az aláírás-létrehozó adat és az aláírás-ellenőrző adat (kriptográfiai kulcspár) előállítása a szolgáltatás keretében a Szolgáltató által történik kiemelt biztonságú környezetben. A kriptográfiai kulcspár a biztonságos aláírás-létrehozó eszközön (BALE) áll elő, ezért az aláírás-létrehozó adat és az aláírás-ellenőrző adat birtoklásának és egymáshoz tartozásának ellenőrzésére nincs szükség, csupán az aláírás-létrehozó eszköz átvételének igazolása szükséges. A biztonságos aláírás-létrehozó eszköz személyes átvételénél az Aláíró aláírásával igazolja az aláírás-létrehozó eszköz és a PIN kód átvételét.

3.2.2. Azonosítás „Személyes" tanúsítvány igénylése esetén

Természetes személy, mint Előfizető a regisztrációs űrlap kitöltésével igényelhet tanúsítványt. Az űrlapon a következő Előfizetői adatokat kell megadni:

a. név,

b. álnév, amennyiben annak megjelölésére az Előfizető igényt tart,

c. személyazonosítására használt okmány száma (személyi igazolvány, jogosítvány vagy útlevél szám),

d. lakcím,

e. anyja neve,

f. születési hely és idő,

g. e-mail cím,

A regisztrációs űrlapot a Szolgáltató biztosítja; azon további adatok megadására vonatkozó mezők is rendszeresíthetők.

Természetes személyt az Ügyfélkapcsolati Iroda hatósági személyazonosító igazolvány (személyi igazolvány, jogosítvány vagy útlevél) személyes bemutatásával azonosít.

Az Ügyfélkapcsolati Iroda a bemutatott személyazonosító igazolvány érvényességét és hitelességét ellenőrzi (lásd: 3.2.7. 1. pont).

A Szolgáltató megtagadhatja a tanúsítvány igénylését, ha az okmányok személyhez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel.

3.2.3. Azonosítás „Szervezeti személy" („Munkatársi") tanúsítvány igénylése esetén

Az igénylő szervezet mint Előfizető a regisztrációs űrlap kitöltésével igényelhet tanúsítványt és azt a szervezet képviseletére jogosult vezető tisztségviselő aláírásával kell hitelesíteni.

A szervezeti személy (továbbiakban: Aláíró) azonosításához a következő adatokat kéri az Ügyfélkapcsolati Iroda:

a. az igénylő szervezet neve, székhelye
b. annak a szervezeti egységnek a megnevezése, ahol az Aláíró dolgozik
c. az Aláíró neve
d. az Aláíró beosztása (az előfizető szervezet és szervezeti egység viszonya az Aláíróhoz)
e. személyazonosítására használt okmány száma (személyi igazolvány, jogosítvány vagy útlevél szám),
f. az Aláíró e-mail címe
g. az Aláírót megbízó dokumentum cégszerűen aláírva (a dokumentum tartalmazza a megbízó szervezet vagy szervezeti egység nevét, e-mail címét, telefon+fax számát)
h. az előfizető szervezet egyértelmű hozzájárulása ahhoz, hogy:
- a tanúsítvány kibocsátásra kerüljön
- a szervezet vagy szervezeti egysége neve a tanúsítvány tulajdonos-azonosító mezőjében feltüntetésre kerüljön
- az Aláíró neve a tanúsítvány tulajdonos-azonosító mezőjében feltüntetésre kerüljön
- a Szolgáltató a regisztráció során a szervezeti azonosság hitelesítésére elfogad minősített aláírással ellátott elektronikus okiratot is 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:

a. az Aláíró kijelölését engedélyező személy neve (az engedélyezőnek minden esetben a szervezet képviseletére jogosult személynek kell lennie és ezt hiteles dokumentumokkal (pl. aláírási címpéldánnyal) kell igazolni)
b. az engedélyező személy beosztása
c. az engedélyező személy munkahelyi telefonszáma, fax-száma, e-mail címe

Ezen adatokat a következő dokumentumokkal kell hitelesíteni:

a. személyazonosítására használt okmány (személyi igazolvány, jogosítvány vagy útlevél), bemutatása személyesen (Aláíró, Kapcsolattartó)
b. cégszerűen aláírt képviseleti megbízás
c. cégbíróságnál nyilvántartott gazdasági társaságok esetében 30 napnál nem régebbi cégkivonat
d. 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.,
e. állam-, illetve közigazgatási szervezetek esetében az alapító dokumentum közjegyzővel hitelesített másolata, amelyet a szervezet első számú vezetőjének írásos nyilatkozata kísér,
f. 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 érvényessége és hitelessége, valamint az aláírási jogosultság ellenőrzése céljából adategyeztetést végez (lásd: 3.2.7. pont).

Az Ügyfélkapcsolati Iroda szervezeti személy azonosítás-hitelesítése során köteles a tanúsítvány kibocsátását megtagadni, ha

a. a bemutatott okmányok személyhez tartozásával, valódiságával vagy érvényességével kapcsolatban kétsége merül fel
b. a csatolt dokumentumok valódiságával vagy érvényességével kapcsolatban kétsége merül fel
c. a cégnyilvántartással végzett adategyeztetés a bemutatott adatoktól eltérő eredményt ad
d. a szervezet kiléte nem állapítható meg minden kétséget kizáróan
e. nem egyértelmű a szervezet felhatalmazása a tanúsítvány kibocsátására.

3.2.4. Szervezet azonosítása közigazgatásban alkalmazható tanúsítványok igénylése esetén

a) Ha az ***ügyfél*** tanúsítványával kifejezetten jelezni kívánja, hogy ő egy adott szervezethez tartozik, akkor a regisztrációhoz magával kell vinnie az adott szervezet nevében aláírásra jogosult személy által kiállított és aláírt, az adott szervezet nevét is tartalmazó meghatalmazást arra, hogy a szervezet képviseletében a tanúsítványt használja, az aláírásra jogosító aláírási címpéldányt, valamint a szervezet azonosságát is hitelesítő dokumentumot.
A természetes személyt külön is azonosítani kell a 3.2.5. pont szerint.

b) Egy közigazgatási szervet ***képviselő*** természetes személynek a regisztrációhoz magával kell vinnie egy, az adott közigazgatási szerv által kiállított és közokiratba foglalt, a közigazgatási szerv nevét is tartalmazó meghatalmazást arra, hogy a hivatal képviseletében a hitelesítés-szolgáltatónál előforduló ügyekben eljárjon, mely meghatalmazás egyúttal a szervezet azonosságát is hitelesíti.
A természetes személyt külön is azonosítani kell a 3.2.5. pont szerint.

3.2.5. Személy azonosítása közigazgatásban alkalmazható tanúsítványok igénylése esetén

A személy azonosságának hitelesítését a Szolgáltató a 3.2.2 pontban leírtakon felül a következők szerint biztosítja:

a) A regisztrációhoz az igénylőnek személyesen kell megjelennie a Szolgáltató Ügyfélkapcsolati Irodájában.

b) A regisztráció során az igénylő személyazonosságát a személyazonosság igazolására alkalmas hatósági igazolvány alapján ellenőrizni kell.

c) A regisztráció és a személyazonosság ellenőrzése alapjául szolgáló, rögzítendő adatok helyességét az igénylőnek nyilatkozatban, saját kezű aláírásával ellátva kell igazolnia.

d) A b) pont szerinti hatósági igazolvány azonosító adatait, a megadott adatok egyezését és a hatósági igazolvány érvényességét a Szolgáltató regisztrációs szervezete közhiteles nyilvántartásban ellenőrzi.

e) A regisztrációt végző szervezet regisztrációban részt vevő ügyintézőjének aláírásával kell igazolnia, hogy a hatósági igazolványon szereplő arckép megfeleltethető az igénylő arcának és az igazolványban szereplő aláírás azonos a c) pont szerinti nyilatkozatot igazoló aláírással.

h) A ***köztisztviselők*** számára történő tanúsítvány kibocsátást megelőző regisztrációt az alábbiak kezdeményezhetik:

- a hatóságot képviselő természetes személy a Szolgáltató előtt, ha a regisztrációhoz benyújtja a hatóság által kiállított és közokiratba foglalt, a közigazgatási szerv nevét tartalmazó, a hivatal képviseletére feljogosító meghatalmazást;
- a hatóság, ha a regisztrációs szervezet a természetes személy azonosítását külső helyszíni regisztráció útján – szükség szerint a hatóság által kijelölt közigazgatási szerv közreműködésével – végzi el.

i) A h) pont első bekezdése szerinti (a Szolgáltató előtti) regisztráció esetén a Szolgáltató a meghatalmazást kiállító hatóságot – a regisztrációban érintett köztisztviselő adatainak megadása nélkül – a tanúsítvány kibocsátásának tényéről és a hatóság által kiadott meghatalmazásban foglalt iktatószámról értesíti.

3.2.6. Időbélyegzés szolgáltatás igénylése

Időbélyegzés szolgáltatást igényelhet:

a. természetes személy

b. jogi személy (szervezet)

Az időbélyegzés szolgáltatás igénybe vétele a Szolgáltató és az Előfizető között megkötött szolgáltatási szerződés keretében lehetséges. Ezen szerződés keretében az Előfizető írásbeli nyilatkozatot ad arra vonatkozóan, hogy a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri, s elfogadja azokat.

Az időbélyegzés szolgáltatás igénybe vételére vonatkozó szerződés megkötése érdekében az Ügyfélkapcsolati Iroda az előfizető személy illetve szervezet azonosítása érdekében a 3.2.6.1 pontban leírt egyszerűsített azonosítási eljárást alkalmazza.

Az Ügyfélkapcsolati Iroda az időbélyegzés szolgáltatási szerződés megkötése során megtagadhatja a szerződés megkötését, ha

a. a bemutatott személyi okmányok személyhez tartozásával, valódiságával vagy érvényességével kapcsolatban kétsége merül fel

b. a megrendelőből a szervezet kiléte nem állapítható meg minden kétséget kizáróan

Az időbélyegzés szolgáltatás igénybe vételekor a Szolgáltató az igénybe vevőnél biztonságos csatornán keresztüli tanúsítvány alapú kliens azonosítást, vagy egyéb, az előfizető egyértelmű azonosítását lehetővé tevő megoldást alkalmaz.

3.2.6.1. Egyszerűsített regisztráció időbélyegzés szolgáltatáshoz

Magányszemély egyszerűsített előfizető azonosításához személyazonosító igazolvány (személyi igazolvány, útlevél vagy vezetői engedély) és a lakcím kártya bemutatása szükséges.

Szervezeti előfizető egyszerűsített azonosításához egy cégszerűen aláírt megrendelő bemutatása szükséges.

3.2.7. Adategyeztetés

1.) A Szolgáltató jogosult megállapítani az aláíró személyazonosságát a személyazonosításra alkalmas okmánya alapján. A Szolgáltató a regisztráció során az aláíró személyazonosságának ellenőrzése céljából - megnevezésének és az adatfelhasználás céljának feltüntetése mellett - adategyeztetést végez a következő nyilvántartások közül legalább eggyel:

a. személyi adat- és lakcímnyilvántartás,

b. úti okmány-nyilvántartás,

c. járművezetői engedély-nyilvántartás;

2.) A Szolgáltató a regisztráció során cég nevében történő aláírási jogosultság ellenőrzése céljából adategyeztetést végez a cégnyilvántartással.

3.2.8. Együttműködési képességek

a. A Szolgáltató eleget tesz a {J10} hitelesítési rend 3.2.6. a) pontjában rögzített együttműködési képességre vonatkozó követelménynek.

b. A Szolgáltató az együttműködő partnerek részére teszt célokat szolgáló tanúsítványokat és nyilvános körben hozzáférhető szolgáltatásaihoz teszt célú hozzáférést is biztosíthat. A tesztek során felmerülő kérdések tisztázására a Szolgáltató partnereivel együttműködik.

c. Az együttműködés eredményéről a Szolgáltató a szolgáltatások internetes honlapján esetenként tájékoztatást tehet közzé.

3.2.9. Viszontazonosítás

Szolgáltató nem végez viszontazonosítást.

4. A tanúsítvány-életciklusra vonatkozó szabályok

4.1. Tanúsítványigénylés

4.1.1. Ki nyújthat be tanúsítványkérelmet

Tanúsítványkérelmet azok az előfizetők nyújthatnak be, akik előzetesen a Szolgáltatóval szerződéses kapcsolatot létesítettek. A kérelmező lehet magánszemély vagy egy jogi szervezet képviselő személy, aki személyazonosságát a regisztráció során hitelt érdemlően igazolta (lásd: 3.2.1.-3.2.5. pontok)

A Szolgáltató azt megelőzően, hogy egy Előfizetővel szerződéses kapcsolatot létesít, tájékoztatja az Előfizetőt a tanúsítvány és/vagy az időbélyeg szolgáltatás használatával kapcsolatos kikötésekről és feltételekről. Ha az Aláíró (alany) nem azonos az Előfizetővel, úgy őt az Előfizető tájékoztatja kötelességeiről.

4.1.2. A tanúsítványigénylés folyamata és a résztvevők felelőssége

Tanúsítvány igényléséhez ki kell tölteni a regisztrációs űrlapot és le kell folytatni a 3.2 pontban meghatározott regisztrációs eljárást. Az űrlap nyomtatott vagy elektronikus formában igényelhető az Ügyfélkapcsolati Irodánál, vagy elektronikus formában letölthető a Szolgáltató internetes honlapjáról.

Az Előfizetői Szerződés aláírásával Előfizető egyúttal nyilatkozik arról is, hogy a Szolgáltató feltételei és kikötései, valamint saját kötelezettségei vonatkozásában tájékoztatást kapott, azokat elfogadja. Az Előfizető aláírása igazolja azt is, hogy:

a. vállalja az aláírás-létrehozó eszköz használatát, védelmét
b. garantálja feltüntetett adatainak valódiságát
c. megfizeti a szolgáltatások díját
d. az adatok későbbi változásairól a Szolgáltatót értesíti.

Az Előfizetőnek a Szolgáltató felkérésére írásban kell nyilatkozni arról, hogy hozzájárul a szolgáltatások során felhasznált személyes adatai Szolgáltató által történő nyilvántartásba vételéhez, tanúsítványa és az azzal kapcsolatos állapot információk szolgáltatói tanúsítványtárban való közzétételéhez, s ezen adatok harmadik félhez történő továbbításához a Szolgáltató szolgáltatásainak leállítása esetén, illetve egyéb, jogszabályok által meghatározott esetekben.

A regisztráció során az Ügyfélkapcsolati Iroda nyilvántartásba veszi az Aláíró azonosítására használt adatokat, beleértve az igazoláshoz használt dokumentumok regisztrációs számát és az azok érvényességével kapcsolatos esetleges korlátozásokat.

A Tájékoztató a szolgáltató internetes honlapján bárki számára elérhető.

4.2. A tanúsítvány kérelem feldolgozása

4.2.1. Azonosítási és hitelesítési funkciók megvalósítása

A Szolgáltató a regisztráció során az ott leírt módon ellenőrzi a tanúsítványkérelem érvényességét.

4.2.2. A tanúsítványkérelem jóváhagyása vagy visszautasítása

A Szolgáltató az előfizetői szerződés aláírásával hagyja jóvá a tanúsítványkérelmet.

A tanúsítványkérelem visszautasítása esetén a Szolgáltató az igénylővel előfizetői szerződést nem köt.

4.2.3. A tanúsítványigénylések feldolgozásának időtartama

A tanúsítványigénylések feldolgozásának időtartama legfeljebb 30 nap.

4.3. Tanúsítvány kibocsátás

Sikeres regisztráció után az Ügyfélkapcsolati Iroda a tanúsítvány igényt a Regisztrációs Iroda felé továbbítja. A Regisztrációs Iroda a hitelesítés szolgáltatást támogató informatikai rendszerben elindítja a tanúsítvány kibocsátást.

Az elkészült tanúsítvány a következő módon jut el az Előfizetőhöz:

a. az Előfizető, az Aláíró vagy azok képviselője személyesen átveszi az Ügyfélkapcsolati Irodán, vagy
b. az Előfizető letölti a Szolgáltató nyilvános Tanúsítványtárából

4.4. Tanúsítvány elfogadás

A tanúsítvány elfogadása az Előfizető részéről az átvétellel történik meg.

Az Előfizető (Aláíró) a tanúsítvány használatba vétele előtt köteles ellenőrizni a tanúsítvány adatainak helyességét.

Az aláírás-létrehozó adat használatba vétele előtt az Előfizető (Aláíró) köteles ellenőrizni a tanúsítvány adatainak helyességét és visszaigazolni a tanúsítvány átvételét. Amennyiben bármilyen rendellenességet talál, az aláírás-létrehozó adatot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonására.

A visszaigazolás egyben a hitelesítési rendek, a jeln szolgáltatási szabályzat és az általános szerződési feltételek elfogadását is jelenti.

4.4.1. Tanúsítvány közzététele a hitelesítés-szolgáltató által

Az Előfizető hozzájárulása esetén a Szolgáltató a kibocsátott tanúsítványokat Tanúsítványtárában teszi közzé.

4.4.2. A további szereplők értesítése a tanúsítvány kibocsátásáról

A közigazgatásban alkalmazható tanúsítványok esetében, - ha a hivatali aláíráshoz tartozó tanúsítvány kibocsátását megelőző regisztrációt a hatóságot képviselő természetes személy kezdeményezte - a Szolgáltató köteles a meghatalmazást kiállító hatóságot - a hivatali aláírást kiváltó személy adatainak megadása nélkül - a hivatali aláírás kiállításának tényéről és a hatóság által kiadott meghatalmazásban foglalt iktatószámról értesíteni.

További szereplőket a Szolgáltató a kibocsátott tanúsítványokról nem értesít. Időbélyeg kiadásáról Szolgáltató nem küld külön értesítést.

4.5. Kulcspár és tanúsítvány illetve időbélyeg használat

4.5.1. Az alany magánkulcs- és tanúsítvány használata

a. Az alany magánkulcsát és tanúsítványát csak az előfizetői szerződésben rögzített korlátozásnak megfelelően használhatja.

b. Az alany csak a tanúsítvány elfogadása után (lásd 4.4 pont) használhatja magánkulcsát.

c. Az alany a megfelelő tanúsítvány lejárta után nem használhatja tovább magánkulcsát.

d. Az alanynak az adott helyzetben általában elvárható gondosságot kell tanúsítania annak érdekében, hogy megelőzze magánkulcsának illetéktelen felhasználását.

e. Az alany magánkulcsait csak olyan célokra és olyan alkalmazásokkal használhatja, melyek összhangban vannak a tanúsítványok „kulcshasználat” és „kiterjesztett kulcshasználat” mezőinek tartalmával (lásd még 6.1.6, 7.1.2 és 7.1.3 pontok).

f. Időbélyeget Előfizető az 1.4.3 pontban megadott célokra használhat fel.

4.5.2. Az érintett felek nyilvános kulcs- és tanúsítvány használata

Annak érdekében, hogy az érintett fél megalapozottan hagyatkozhasson a tanúsítvánnyal igazolt kriptográfiai kulcspár használatával működő alkalmazásra, a kulcspár megfelelő használatát és a hozzá tartozó tanúsítványt az adott helyzetben tőle általában elvárható gondossággal ajánlott ellenőriznie. Ennek során többek között az alábbiakra ajánlott figyelemmel lennie:

a. Az érintett fél csak olyan célokra és olyan alkalmazásokkal fogadhat el nyilvános kulcsokat, melyek összhangban vannak a megfelelő tanúsítványok „kulcshasználat” és „kiterjesztett kulcshasználat” mezőinek tartalmával.

b. Mielőtt egy tanúsítványba foglalt nyilvános kulcsot felhasználna, az érintett félnek ajánlott ellenőrizni a tanúsítvány érvényességét, valamint azt, hogy a tanúsítvány nincs felfüggesztve, illetve visszavonva az érvényes visszavonási állapot információ alapján.

c. Amennyiben ésszerű módon egy tanúsítványra kíván hagyatkozni, az érintett félnek ajánlott figyelembe vennie a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, mely a tanúsítványban szerepel.

Amennyiben az érintett fél ésszerű módon egy időbélyegre kíván hagyatkozni, ajánlott azt ellenőriznie, a 2.1.3 pont szerint.

4.6. Tanúsítványok érvényessége, megújítása (tanúsítvány frissítése)

4.6.1. A tanúsítványok érvényessége

Szolgáltató által kibocsátott **Előfizetői tanúsítványok érvényességi ideje legfeljebb 2 év**. Az érvényesség kezdete (év, hónap, nap, óra, perc, másodperc) nem lehet korábbi, mint a kibocsátás napja. Az előfizetői tanúsítványok érvényessége az előfizető kérésére az érvényességi idő lejárata előtt legfeljebb egy alkalommal legfeljebb két évre meghosszabbítható.

Szolgáltató által kibocsátott **közigazgatásban alkalmazható tanúsítványok érvényességi ideje 1 év**. Az érvényesség kezdete (év, hónap, nap, óra, perc, másodperc) nem lehet korábbi, mint a kibocsátás napja. A tanúsítványok érvényessége az előfizető kérésére az érvényességi idő lejárata előtt legfeljebb egy alkalommal egy évre meghosszabbítható.

4.6.2. A tanúsítványok megújítása (tanúsítványok frissítése)

Tanúsítványfrissítés során a Szolgáltató a tanúsítványban az Aláíró változatlan nyilvános kulcsát és változatlan egyéb adatait hitelesíti új érvényességi időtartamra.

Tanúsítvány megújítása akkor lehetséges, ha:

a. a tanúsítvány nem szerepel a visszavonási listában

b. a tanúsítványban rögzített adatok érvényességéről és változatlanságáról az Előfizető írásban nyilatkozik.

A Szolgáltató az Előfizető nyilatkozata alapján adatai érvényességéről és változatlanságáról az illetékes hatóságokkal egyeztetést végezhet.

Ha a feltételek valamelyike nem teljesül, új tanúsítványt kell igényelni a regisztrációs eljárás újbóli végrehajtásával.

A Szolgáltató a tanúsítvány megújítás szükségességéről a lejárat előtt értesítést küldhet az Előfizetőnek.

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

4.6.3. Érvénytelen tanúsítványok megőrzése

A Szolgáltató a lejárt és a visszavont előfizetői tanúsítványokat a lejárattól, illetve a visszavonástól számított 10 évig, illetve a tanúsítványhoz tartozó privát kulccsal elektronikusan aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi. A Szolgáltató ugyanezen határidőig olyan eszközt biztosít, mellyel a kibocsátott tanúsítvány tartalma megállapítható. E megőrzési kötelezettségnek a Szolgáltató minősített archiválási szolgáltató igénybevételével is eleget tehet.

4.7. Kulcscsere

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

Kulcscserére a következő esetekben lehet szükség:

a. a tanúsítvány valamilyen okból visszavonásra került,

b. a tanúsítvány lejárt,

c. a magánkulcsot tartalmazó biztonságos aláírás-létrehozó eszköz megsérült és nem használható

A kulcscserét az Előfizető kezdeményezheti. Kulcscsere esetén a Szolgáltató lefolytatja a 3.2 pontban rögzített regisztrációs eljárást. A megújított tanúsítvány kibocsátása és publikálása megegyezik az új tanúsítványra vonatkozó eljárásokkal.

4.8. Tanúsítvány-módosítás

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

Tanúsítvány-módosításra akkor lehet szükség, ha a tanúsítvány alanyra vonatkozó adatai – a nyilvános kulcs kivételével – megváltoztak.

A tanúsítvány-módosítást az Előfizető kezdeményezheti.

A kérelem benyújtásakor a Szolgáltató ellenőrzi a tanúsítvány létezését és érvényességét, valamint az alany azonosságának és jellemzőinek igazolására használt információk érvényességét a 3.2 pontban rögzített regisztrációs eljárás szerint.

A módosított tanúsítvány kibocsátása és publikálása megegyezik az új tanúsítványra vonatkozó eljárásokkal.

A Szolgáltató a módosítandó tanúsítványt a módosított tanúsítvány kibocsátása előtt visszavonja.

A közigazgatásban alkalmazható tanúsítványok esetében tanúsítvány-módosítás nem engedélyezett.

4.9. Tanúsítványok visszavonása és felfüggesztése

A Szolgáltató a tanúsítványok érvényességének kezelésére mind tanúsítvány visszavonási, mind tanúsítvány felfüggesztési szolgáltatást nyújt. A tanúsítvány visszavonása a tanúsítvány állapotát végérvényesen érvénytelenre állítja. Felfüggesztés esetén a tanúsítvány csak rövid, átmeneti időszakra lesz érvénytelen. A tanúsítvány felfüggesztett állapotban csak ideiglenesen lehet, az engedélyezett időtartam (lásd 4.9.7.1 pont) után állapotát újra érvényesre kell állítani, vagy a tanúsítványt vissza kell vonni.

A felfüggesztési és visszavonási kérelmeket az Ügyfélkapcsolati irodák fogadják nyitvatartási időben. A visszavonási és felfüggesztési kérelmek fogadását és azoknak a sikeres ellenőrzés utáni végrehajtását a Szolgáltató Ügyfélszolgálatán keresztül is biztosítja, a nap 24 órájában, folyamatos rendelkezésre állással.

Visszavont/felfüggesztett tanúsítványt joghatályosan nem lehet felhasználni.

4.9.1. Visszavonáshoz vagy felfüggesztéshez vezető körülmények

A Szolgáltató felfüggeszti vagy visszavonja a tanúsítványt ha:

a. az Előfizető vagy az Aláíró ezt kéri

b. a Nemzeti Média- és Hírközlési Hatóság jogerős és végrehajtható határozatában így rendelkezik

c. harmadik személy bejelentése alapján, ha a csatolt bizonyítékok ezt alátámasztják

d. a Szolgáltató megalapozottan feltételezheti, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, azok használata jogszerűtlen, vagy az aláírás-létrehozó adat nem az Aláíró kizárólagos birtokában van

e. a Szolgáltató a szolgáltatással kapcsolatos rendellenességről vesz tudomást és a rendellenesség az érvényes szabályok szerint nem orvosolható

Az Előfizető vagy az Aláíró a következő körülmények fennállása esetén kezdeményezheti a visszavonást/felfüggesztést:

a. a magánkulcs kompromittálódása, vagy annak gyanúja

b. az aláírás-létrehozó eszköz elvesztése, eltulajdonítása, megrongálódása

c. az aláírás-létrehozó eszközt védő aktivizáló adat (PIN kód) kompromittálódása, vagy annak gyanúja

d. a tanúsítványban feltűntetett hibás adatok

e. az Előfizető tanúsítványban feltűntetett adatainak megváltozása

f. az Aláíró tanúsítványban feltűntetett adatainak megváltozása

g. a tanúsítványban feltűntetett Aláíró és szervezet kapcsolatának megváltozása vagy megszűnése[4].

A visszavonási/felfüggesztési kérelmet a Szolgáltató mérlegelés nélkül teljesíti, ha azt az Előfizető vagy az Aláíró kéri.

A Szolgáltató a következő esetekben kezdeményezheti a felfüggesztést vagy visszavonást:

a. jogszabály erre kötelezi

b. a tanúsítvány felfüggesztési ideje lejárt

c. az Előfizető és/vagy az Aláíró szerződés szegése esetén

d. az Előfizető és/vagy az Aláíró kötelezettségeinek be nem tartása

e. az Előfizetői szerződés megszűnése

f. a Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról

g. a tanúsítványban feltűntetett kibocsátó adatok megváltozása

h. a hitelesítés szolgáltatás megszűnése

i. a Szolgáltató valamely szolgáltatói magánkulcsának kompromittálódása.

[4] Eat. 10. § (3)

4.9.2. Visszavonás kérelmezése

Tanúsítvány visszavonását az előző pontban feltüntetett körülmények alapján az Aláíró, az Előfizető vagy azok képviselője, a Szolgáltató, a Nemzeti Média- és Hírközlési Hatóság vagy más harmadik fél kezdeményezheti. Az Előfizetőnek és a Szolgáltatónak kötelessége, harmadik félnek joga az előző (4.9.1.) pontban feltűntetett esetekben a visszavonás azonnali kezdeményezése.

A visszavonási kérelem benyújtható személyesen vagy írásban a Szolgáltató Ügyfélkapcsolati Irodájánál. Ha a bejelentő akadályoztatása miatt azonnali intézkedés szükséges, akkor a tanúsítvány felfüggesztése telefonon vagy elektronikusan aláírt e-mail-ben is kérhető az Ügyfélszolgálaton (a Szolgáltató Ügyfélszolgálata a nap 24 órájában, folyamatosan rendelkezésre áll). A tanúsítvány visszavonására az ettől számított 5 napon belül kell intézkedni.

A visszavonási kérelem teljesítéséhez a következő adatok szükségesek:

a. a tanúsítvány sorszáma, vagy egyéb olyan adatok, amely alapján a Szolgáltató rendszerében a tanúsítvány egyértelműen azonosítható

b. a visszavonást kérő azonosító adatai

c. a visszavonást kérő e-mail címe (ha van)

d. a visszavonáshoz vezető körülmény

4.9.3. Visszavonási kérelemre vonatkozó eljárás

A visszavonási igény bejelentése esetén a Szolgáltató a következők szerint jár el:

a. Személyesen az Ügyfélkapcsolati Irodánál az Iroda munkaidején belül lehet a visszavonási kérelmeket bejelenteni a bejelentő azonosítása-hitelesítése mellett.

b. Írásban történt bejelentés esetén a Szolgáltató a bejelentő adatai alapján azonosítja és hitelesíti a visszavonás kérelmezőjét.

c. Ha a kérelmező azonosítás-hitelesítése megtörtént, a visszavonási okok megalapozottak, az adatok egyeznek és a kérelmező jogosult a tanúsítvány visszavonását kezdeményezni, vagyis ha a Szolgáltató a visszavonási kérelem jogosságáról meggyőződött, akkor azonnal elvégzi a tanúsítvány visszavonását.

d. Ha a kérelmező azonosítás-hitelesítése sikertelen, a visszavonási okok nem megalapozottak, az adatok helytelenek, vagy a kérelmezőnek a Szolgáltató információi alapján nincs joga a tanúsítvány visszavonatására, akkor a Szolgáltató a visszavonási kérelmet visszautasítja.

e. E-mail-ben vagy telefonon történt bejelentés esetén a Szolgáltató bekéri a felfüggesztési jelszót és lefolytatja a 4.9.4.2. pont szerinti felfüggesztési eljárást. A visszavonási kérelem elbírálásához felkéri a bejelentőt, hogy jelenjen meg ügyfélkapcsolati irodájában személyes azonosítás-hitelesítésre. A bejelentő akadályoztatása esetén a tanúsítvány a felfüggesztés megengedett időtartamára (lásd: 4.9.7.1. pont) felfüggesztési állapotban marad, majd ennek lejártával a Szolgáltató a tanúsítványt visszavonja.

f. Szolgáltató a visszavonás megtörténtéről vagy annak visszautasításáról értesíti az Aláírót, az Előfizetőt és a visszavonás kérelmezőjét.

A visszavont tanúsítvány a visszavonási eljárás befejezése után haladéktalanul bekerül a visszavont tanúsítványok listájába.

4.9.4. A felfüggesztési kérelemre vonatkozó eljárás

4.9.4.1. Ki kérelmezheti a felfüggesztést

A felfüggesztést kérelmezheti az Aláíró vagy az Előfizető illetve annak képviselője; továbbá harmadik személy, ha azt a körülmények indokolják (lásd: 4.9.1. pont).

Felfüggesztést a következő körülmények fennállása esetén kell kezdeményezni:

a. a magánkulcs kompromittálódásának gyanúja,

b. a kulcshordozó eszközt védő aktivizáló adat (PIN kód) kompromittálódásának gyanúja,

A felfüggesztési kérelemben a visszavonási kérelemmel megegyező adatokat, illetve a Szolgáltató ügyfélszolgálatán keresztül történő bejelentés esetén azokon túlmenően a felfüggesztési jelszót kell megadni.

Szolgáltató a felfüggesztési kérelmet mérlegelés nélkül teljesíti, ha azt az Aláíró vagy az Előfizető kéri.

Tanúsítvány felfüggesztési igény telefonon is bejelenthető a Szolgáltató Ügyfélszolgálatán. Telefonon történt bejelentés esetén a Szolgáltató a személyes adatok bemondása után felfüggesztési jelszóval azonosítja a felfüggesztés kérelmezőjét, majd elvégzi a felfüggesztési kérelem formai és tartalmi ellenőrzését, illetve ezek sikeressége esetén a tanúsítvány felfüggesztését.

4.9.4.2. A felfüggesztési eljárás

a. A felfüggesztési eljárás első lépéseként a Szolgáltató azonosítja a bejelentőt, majd mérlegeli a felfüggesztési okokat. Ha a felfüggesztési kérelmet az Előfizető terjesztette be, az Előfizető azonosítása után a Szolgáltatónak nincs mérlegelési joga a felfüggesztés tekintetében

b. ha a felfüggesztési okok megalapozottak és az ellenőrzések sikeresek, vagyis ha a Szolgáltató a felfüggesztési kérelem jogosságáról meggyőződött, akkor azonnal elvégzi a tanúsítvány felfüggesztését

c. ha a felfüggesztési okok nem megalapozottak, az adatok helytelenek, vagy a kérelmező személye nem állapítható meg kellő bizonyossággal vagy a kérelmezőnek a Szolgáltató információi alapján nincs joga a tanúsítvány felfüggesztésére, akkor a Szolgáltató a felfüggesztési kérelmet visszautasítja

d. Szolgáltató a felfüggesztés megtörténtéről vagy visszautasításáról értesíti az Előfizetőt az Aláírót és a felfüggesztés kérelmezőjét.

e. A felfüggesztett tanúsítvány a felfüggesztési eljárás befejezése után azonnal bekerül a visszavont tanúsítványok listájába.

A felfüggesztett tanúsítványt a Szolgáltató az Előfizető vagy az Aláíró kérésére a felfüggesztési időn belül visszaállítja érvényesre.

4.9.4.3. A Szolgáltató függeszti fel a tanúsítványt

A Szolgáltató felfüggeszti a tanúsítványt, ha:

a. a Szolgáltató tudomására jutott alapos gyanú a regisztrációs adatok valótlanságáról,

b. az Előfizető vagy az Aláíró visszavonási kérelme kiegészítésre szorul.

A felfüggesztési idő lejárta után a Szolgáltató a tanúsítványt feltétel nélkül visszavonja.

4.9.5. Kivárási idő visszavonási/felfüggesztési kérelem esetén

A visszavonási/felfüggesztési kérelem esetén a Szolgáltató ennek végrehajtását soron kívül végrehajtja a kérelem elfogadása után. A Szolgáltató akkor tekinti a visszavonási/felfüggesztési kérelmet elfogadottnak, ha annak jogosságáról meggyőződött.

4.9.5.1. Kivárási idő felfüggesztési kérelem esetén

a. Felfüggesztési kérelem esetén a kérelem elfogadására a Szolgáltató nem alkalmaz kivárási időt. A felfüggesztési kérelem elfogadását követően azonnal intézkedik a tanúsítvány felfüggesztésére, a tanúsítványállapot megváltozását nyilvántartásában átvezeti és a felfüggesztési kérelem szerint módosított felfüggesztési állapotot 1 órán belül közzéteszi.

b. Ha a Szolgáltatónak a felfüggesztési kérelem hitelességéről kétségei merülnek fel, akkor a felfüggesztési kérelmet azonnal visszautasítja.

4.9.5.2. Kivárási idő visszavonási kérelem esetén

Visszavonási kérelem esetén a kérelem elfogadására a Szolgáltató kivárási időt alkalmaz:

a. A Szolgáltató a visszavonási kérelem fogadásától számított 3 órán belül dönt a kérelem érvényességéről (elbírálja a kérelmező jogosultságát), és érvényes kérelem esetén a visszavonási állapot megváltozását nyilvántartásában átvezeti.

b. Ha a Szolgáltató a visszavonási kérelem érvényességéről 3 órán belül nem tud kétséget kizáróan meggyőződni, akkor erről a kérelmezőt értesíti és a tanúsítványt nem visszavonja, hanem 4.9.4.2 pont szerint felfüggeszti. A visszavonást később – a kérelmező hiteles azonosítását követően végzi el.

c. A visszavonási kérelem elfogadását követően a Szolgáltató a visszavonási kérelem szerint módosított visszavonási állapotot 1 órán belül közzéteszi.

4.9.6. A Szolgáltatót és az Előfizetőt érintő felelősségi szabályok

a. A visszavonási/felfüggesztési kérelem bejelentésének a Szolgáltatóhoz történő megérkezéséig és elfogadásáig az ÁSZF-PKI-nek megfelelően az Előfizető felelős a felmerülő károkért.

b. A visszavonási/felfüggesztési kérelem elfogadásától a visszavonás/felfüggesztés tényének a visszavont tanúsítványok listájában való megjelenésig a Szolgáltató felelős a felmerülő károkért. Ez alól kivételt képez a bizonyíthatóan csalárd szándékkal történt visszavonás/felfüggesztés kérés, amely esetben a felmerülő károkért a Szolgáltató nem vállal felelősséget.

c. A felfüggesztett/visszavont tanúsítványnak a visszavont tanúsítványok listájában 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 Tanúsítványtárban megjelenő érvényességi adatokra.

4.9.7. Felfüggesztett állapotra vonatkozó korlátozások, újraérvényesítés

4.9.7.1. A felfüggesztés megengedett időtartama

Tanúsítvány felfüggesztett állapotban legfeljebb 5 naptári napig lehet.

Ha a felfüggesztést az Előfizető vagy az Aláíró 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.

Ha a felfüggesztésről a Szolgáltató határozott, akkor 5 napon belül dönt a tanúsítvány visszavonásáról is. Amenynyiben Szolgáltató nem képes ezen időszak alatt a körülmények kivizsgálására, akkor a tanúsítványt visszavonja, valamint az Előfizető igénye estén részére térítésmentesen új tanúsítványt bocsát ki.

4.9.7.2. A felfüggesztés megszüntetése

A felfüggesztés megszüntetésének, és ezzel a tanúsítvány újraérvényesítésének feltételei a következők:

a. Az újraérvényesítést csak az Előfizető vagy annak a regisztráció során nyilvántartásba vett képviselője kérheti,

b. Az újraérvényesítést kérő személyt azonosítani kell.

Az újraérvényesítés kéréséhez a következő adatokat kell megadni:

a. a felfüggesztett tanúsítvány sorszáma,

b. a felfüggesztés megszüntetését kérő személy azonosító adatai,

c. a felfüggesztés megszüntetésének oka.

A felfüggesztés megszüntetése csak a felfüggesztési időszak vége előtt kérhető. A felfüggesztés megszűntetésének eredménye a tanúsítvány újraérvényesítése vagy visszavonása.

4.9.8. A visszavonási információ ellenőrzése az érintett felek részéről

Ha az érintett felek kellő gondossággal kívánnak eljárni a tanúsítvány visszavonási állapotának ellenőrzésekor, akkor indokolt meggyőződniük a tanúsítvány visszavonási információ hitelességéről is.

Időbélyeg esetén értelemszerűen az időbélyeget aláíró szolgáltatói tanúsítványra vonatkozó visszavonási listát ajánlott ellenőrizni.

4.9.9. Visszavonási lista (CRL) és kibocsátásának gyakorisága

A visszavonási listában a visszavont és felfüggesztett tanúsítványok kerülnek feltüntetésre. A felfüggesztett tanúsítványok az újraérvényesítés hatására kerülhetnek ki a listából. Szolgáltató fenntartja a jogát arra vonatkozóan, hogy a lejárt tanúsítványokat kitörölje a listából.

A Szolgáltató által kezelt visszavonási listáják érvényességi ideje 24 óra. Szolgáltató legkésőbb a lista érvényességi idejének lejártakor új listát bocsát ki, új érvényességi idővel.

A Szolgáltató egy-egy tanúsítvány felfüggesztését, visszavonását illetve újraérvényesítését követően 1 órán belül új visszavonási listát tesz közzé.

4.9.10. A visszavonási lista előállítása és közzététele közötti közötti leghosszabb idő

A visszavonási lista előállítása és közzététele közötti közötti leghosszabb idő 1 óra.

4.9.11. A visszavonási listák ellenőrzése

A visszavonási listákat az érintett feleknek ajánlott ellenőrizni - saját felelősségükre - a tanúsítványok elfogadását megelőzően. A tanúsítványhoz tartozó visszavonási lista elérhetőségét a tanúsítvány tartalmazza. A lista ellenőrzése abból áll, hogy a kérdéses tanúsítványt a lista tartalmazza-e (és ha igen, milyen időponttól), a lista hiteles és sértetlen-e, s a kérdéses tranzakció szempontjából időben releváns-e.

A tanúsítvány visszavonási listában a Szolgáltató által közzétett visszavont, vagy felfüggesztett tanúsítvány elfogadásából keletkező bárminemű kár Érintett felet terheli.

4.9.12. Visszavonási állapot közlés más formái

A Szolgáltató a visszavonási listák mellett más visszavonási információs szolgáltatást nem nyújt.

4.9.13. Intézkedések magánkulcs kompromittálódás esetén

Az aláírás-létrehozó adat tényleges vagy vélelmezett kompromittálódása esetén a tanúsítvány visszavonásáról illetve felfüggesztéséről azonnal intézkedni kell. Alapos gyanú esetén az aláírás-létrehozó adat használatát azonnal be kell szüntetni.

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

4.10. Kulcsletét

A Szolgáltató kulcsletétet nem szolgáltat.

4.11. Időbélyegzés

4.11.1. Az időbélyegzés szolgáltatás igénylése

Időbélyegzés szolgáltatás igénylése esetén az Igénylőt tájékoztatni kell az időbélyeg használat módjáról, az azzal járó kötelezettségekről és felelősségről.

Az Igénylő azonosítását a 3.2.6 pontban leírt egyszerűsített eljárással kell elvégezni.

Az időbélyegzés szolgáltatást az Előfizető részére a szerződéskötést követő harmadik munkanaptól biztosítja a Szolgáltató.

4.11.2. Az időbélyegzés szolgáltatás szintje

Az időbélyegzés szolgáltatás elérhetőségét a Szolgáltató 99,9%-os rendelkezésre állással biztosítja úgy, hogy az elérhetőség kiesése esetenként nem lépheti túl a 3 órás időtartamot.

Az időbélyegben megadott idő 1 másodpercen belüli pontosságot biztosít az UTC[5] időalaphoz viszonyítva. Az időbélyegző egység órájának pontossága folyamatos ellenőrzés alatt áll. Ha ez túllépné a pontossági határt, akkor az ellenőrző program leállítja az időbélyegzés szolgáltatást, és minden további kérésre a hiba kijavításáig hibaüzenetet küld a felhasználók felé. A szolgáltatás akkor indul újra, ha az időszinkron helyreállt és az egy másodperces pontossági határ teljesül. Az időszinkron helyreállítását a Szolgáltató húsz percen belül biztosítja.

4.11.3. Az időbélyegzés kérelmek teljesítése

Időbélyegzés iránti kérelmet (időbélyeg kérést) Előfizető erre feljogosított[6] felhasználói nyújthatnak be, amennyiben Előfizető a Szolgáltatóval előzetesen szerződéses kapcsolatot létesített.

Az időbélyeg kérést az Előfizető erre feljogosított felhasználója az RFC 3161 szerinti szabványos formában kell elküldjön Szolgáltató időbélyegző egységének elektronikus úton, a Szolgáltató által megadott URL címre. Ehhez Előfizetőnek rendelkeznie kell megfelelő (az RFC 3161 szerinti kérés összeállítására alkalmas) alkalmazással.

Időbélyeg kérés esetén a kérelem jóváhagyása vagy visszautasítása az ellenőrzést követően automatikusan történik.

Az időbélyegzés kérelmek teljesítését (az időbélyeg válasz összeállítását) a Szolgáltató időbélyegző egysége automatikusan és haladéktalanul végzi:

a. a kérelmet egy olyan, a szolgáltatás igénybe vétele céljából megkötött szerződésben definiált kommunikációs csatornán keresztül fogadja, amelyen keresztül az időbélyeg kérőt a Szolgáltató rendszere azonosítani tudja,

b. Időbélyeg kiadása az időbélyegző egység által az RFC 3161 szerinti időbélyeg válasz elküldésével valósul meg

Időbélyeg fogadásához Előfizetőnek (illetve felhasználóinak) olyan alkalmazással kell rendelkezniük, mely az RFC 3161 szerinti időbélyeg választ fogadni és értelmezni képes.

4.11.4. Az időbélyeg érvényességének ellenőrzése

Az időbélyeg érvényességének ellenőrzése az időbélyeget aláíró szolgáltatói tanúsítvány érvényességének ellenőrzésére, illetve az időbélyeget aláíró szolgáltatói tanúsítványra vonatkozó visszavonási lista ellenőrzésére vonatkozik a jelen szabályzat 2.1.3.2 pontja szerint.

---

[5] **UTC:** Coordinated Universal Time, az ITU-R TF.460-5 ajánlás szerint definiált, másodperc felbontású időalap

[6] Feljogosítás általában a felhasználók gépére telepített authentikációs tanúsítványt jelent, melyet jellemzően Szolgáltató biztosít Előfizető részére

4.12. OCSP szolgáltatás

OCSP szolgáltatást a Szolgáltató nem szolgáltat.

5. Fizikai, eljárásrendi, és humán biztonsági szabályozások

A szolgáltatásokat támogató informatikai rendszer személyi és fizikai környezete megfelel a 2/2002 MeHVM irányelvben rögzített biztonsági követelményeknek.

A Szolgáltató az elfogadott szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket és az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazza. Ezen belül:

a. A Szolgáltató kockázat elemzést végzett üzleti kockázatainak felmérésére, valamint a szükséges biztonsági követelmények és működési eljárások meghatározására

b. A Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a Szolgáltató vezetősége hagy jóvá

c. A Szolgáltató megvalósította és folyamatosan fenntartja az aláírás-hitelesítési, időbélyegzési szolgáltatásokat nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait.

d. A Szolgáltató gondoskodik az informatikai biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással, időbélyegzéssel szolgáltatással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősségek más szervezethez kerülnek kiadásra.

A Szolgáltató biztonsági műveletei közé az alábbiak tartoznak:

a. üzemeltetési eljárások és felelősségek

b. ellenőrzési eljárások

c. biztonsági rendszerek és eljárások tervezése, elfogadása és működtetése

d. erőforrás gazdálkodás

e. hálózat menedzselés

f. a biztonsági naplók aktív felügyelete, eseményelemzések és nyomkövetések

g. adathordozó eszközök kezelése és biztonsága

h. rendszerkarbantartás

E felelősségeket a Szolgáltató biztonsági műveletei kezelik, és azokat a 3/2005. (III. 18) IHM rendelet 20.§-21.§-nak megfelelő, megbízható és 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 az elvégzett kockázat elemzéssel összhangban osztályokba sorolja és minősíti,.

A Szolgáltató fizikai, eljárásrendi (adminisztratív) és humán biztonsági szabályozásait a PKI Szolgáltatások Biztonsági Szabályzata tartalmazza részletesen. Ez a szabályzat biztonsági okokból nem nyilvános.

A szolgáltatásokat támogató informatikai rendszer, annak személyi és fizikai környezete megfelel a 2/2002 MeHVM irányelvben rögzített biztonsági követelményeknek.

A következő pontok csak a vonatkozó lényeges intézkedéseket tartalmazzák.

5.1. Fizikai biztonsági szabályozások

5.1.1. Hitelesítő Központok

A hitelesítő központok legmagasabb védelmi szintet képező objektuma a Bizalmi Központ, amely a biztonsági szempontból legkritikusabb hardver/szoftver egységeket tartalmazza. A Bizalmi Központban történik a kulcspárok és a tanúsítványok előállítása, a kulcspárok elhelyezése az aláírás-létrehozó eszközre és az aláírás-létrehozó eszközök megszemélyesítése.

5.1.2. Regisztrációs Iroda

A regisztrációs iroda a Bizalmi Központon belül van kialakítva, itt találhatók a regisztrációs munkahelyek és munkaállomások.

5.2. Eljárásrendi szabályozások

A Szolgáltató eljárásrendi szabályait a következő szabályzatok tartalmazzák:

a. a Szolgáltató Szervezeti és Működési Szabályzata, amely részletesen meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes munkaköröket és az azokhoz kapcsolt feladat-, felelősség és hatásköröket,

b. a jelen szolgáltatási szabályzat,

c. a PKI szolgáltatások biztonsági szabályzata, amely részletesen szabályozza az adatokhoz és az informatikai rendszerekhez, valamint a személyi és a fizikai környezethez kapcsolódó biztonsági szabályokat.

5.3. Humán szabályozások

5.3.1. Bizalmi munkakörök

A 3/2005. (III. 18.) IHM rendelet 2 § nevesíti a minősített hitelesítés-szolgáltatáshoz kapcsolódó bizalmi munkaköröket:

a. a Szolgáltató informatikai rendszeréért általánosan felelős vezető,

b. biztonsági tisztségviselő,

c. rendszeradminisztrátor,

d. rendszerüzemeltető,

e. független rendszervizsgáló,

f. regisztrációs felelős.

Jelen pont . táblázatában a szolgáltatásokhoz kapcsolódó munkakörök, azok feladat-, felelősség és hatáskörei kerülnek összefoglalásra.

Munkakör	Feladatkör	Felelősségi kör	Hatáskör
A PKI szolgáltatásokért kijelölt ill. megbízott aktuális vezető	A Szolgáltató PKI szolgáltatási tevékenységének irányítása.	Folyamatos és biztonságos szolgáltatás. A Szolgáltató informatikai rendszeréért általánosan felelős vezető	A Szolgáltató informatikai rendszeréért valamint a szolgáltatásokért általánosan felelős. A sajáti szervezeti szintjén dönt, intézkedik
Ügyfélkapcsolati Iroda vezetője	Az ügyfélkapcsolati tevékenység irányítása és ellenőrzése.	Az ügyfelek biztonságos azonosítása. Előfizetői szerződések előkészítése	Az ügyfélkapcsolati tevékenység ellenőrzése.
A Szolgáltató IB vezetője (biztonsági tisztségviselő)	IB tevékenység irányítása, ellenőrzése a Szolgáltató PKI szolgáltatásanak területén.	A szolgáltatások biztonságáért általánosan felelős személy	IB intézkedések, IB belső ellenőrzés.
Rendszerüzemeltető	Üzemeltetési adminisztráció, hibaelhárítás, karbantartás	A PKI Rendszer folyamatos üzemeltetése, mentése és helyreállítása	Operatív intézkedés az üzemeltetés területén
Rendszeradminisztrátor	Biztonsági beállítások, adminisztráció, karbantartás	A PKI Rendszer telepítése, konfigurálása, karbantartása	Operatív ellenőrzés, operatív intézkedés
Hitelesítő biztonsági felügyelő (Security Officer /SO/) (biztonsági felelős)	RO kulcsok, tanúsítványok létrehozása	Szolgáltatói kulcsok, PKI, Időbélyegzés alkalmazás és adatok biztonsága	Szolgáltatói (pl.: RO) kulcspárok, tanúsítványok létrehozása
Regisztrációs felügyelő (Registration Officer /RO/) (regisztrációs felelős)	Regisztrációs Iroda irányítása. Előfizető regisztráció, kulcs, tanúsítvány igénylése, kulcs megszemélyesítése	Regisztrációs Iroda folyamatos működtetése.	Regisztrációs Irodán intézkedési jog. SO hatásköre nem lehet.

Munkakör	Feladatkör	Felelősségi kör	Hatáskör
Rendszervizsgáló (auditor)	Operatív funkcionális és biztonsági ellenőrzések (naplózott, illetve archivált állományok vizsgálata).	Funkcionális és biztonsági hiányosságok, visszaélések felfedése. Kontroll intézkedések betartásának ellenőrzése.	Biztonsági és audit naplók ellenőrzése.

. táblázat

5.3.2. Az egyes feladatokhoz szükséges személyzeti létszámok

A PKI rendszerben minden rendszer-telepítési, hardver-konfigurálást és szoftver-frissítést igénylő beavatkozást csak két munkatárs egyidejű jelenlétében lehet elvégezni. A műveletek sikerességét auditorok ellenőrizik és hitelesítik.

A Szolgáltató vezetője által kijelölt bizottság jelenlétében végezhetők az alábbi feladatok:

a. Root CRL generálás

b. a szolgáltatói nyilvános kulcsokat tartalmazó token Root CA-hoz való továbbítása, illetve a Root CA által kibocsátott tanúsítványok visszaszállítása

c. a Root CA nyilvános kulcsát tartalmazó tokennek a Produktív CA-hoz való továbbítása

d. időbélyegző egység hitelesítése

Továbbá csak két bizalmi munkakört betöltő személy (SO) együttesen végezheti - fizikailag védett környezetben, más személyek jelenlétét kizárva - az alábbi feladatokat:

a. szolgáltatói magánkulcsok létrehozása

b. a szolgáltatói magánkulcsok biztonsági mentése

c. a szolgáltatói magánkulcsok mentésből történő visszaállítása

d. a szolgáltatói magánkulcsok (és másodpéldányainak) megsemmisítése

e. az RO szolgáltatói kulcspárok generálása, cseréje és megsemmisítése.

5.3.3. A bizalmi munkakörökben elvárt azonosítás és hitelesítés

A bizalmi munkakört betöltő munkatársak PKI alkalmazásokba erős azonosítás-hitelesítési eljárással, pl. szolgáltatói tanúsítvánnyal rendelkező chipkártya kártyaolvasóba helyezésével, majd az azt aktivizáló PIN kód megadásával lépnek be.

5.3.4. Egymást kizáró munkakörök

A bizalmi munkakörök közötti személyi átfedésekre az alábbi korlátozások vonatkoznak:

a. a biztonsági tisztviselő és a regisztrációs felelős nem töltheti be a független rendszervizsgáló munkakört,

b. a rendszeradminisztrátor nem töltheti be a biztonsági tisztviselő és a független rendszervizsgáló munkakört,

c. az informatikai rendszerért általánosan felelős vezető nem töltheti be a biztonsági tisztviselő és a független rendszervizsgáló munkakört,

d. törekedni kell a bizalmi munkakörök teljes személyi elválasztására.

5.3.5. Személyzetre vonatkozó előírások

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 munkatársai a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaköri leírásokkal 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 munkaköri leírások tartalmazzák a szakismeretre és a tapasztalatra vonatkozó követelményeket is.

5.3.6. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

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

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

5.3.7. Biztonsági háttér ellenőrzésekre vonatkozó eljárások

Az alább meghatározott szerepkörök betöltését az átlagosnál magasabb szintű biztonsági ellenőrzés előzi meg:

a. A PKI szolgáltatásokért általánosan felelős vezető
b. A Hitelesítési Rend és Szabályozási Csoport vezetője
c. Ügyfélkapcsolati Iroda vezetője
d. A Szolgáltató IB vezetője
e. IB adminisztrátor
f. Hitelesítő biztonsági felügyelő (Security Officer /SO/)
g. Regisztrációs felügyelő (Registration Officer /RO/)
h. rendszer auditor

A munkakörök betöltéséhez szükséges képzettség és gyakorlat:

A Szolgáltató informatikai rendszeréért általánosan felelős vezető kinevezéséhez szakirányú felsőfokú végzettség és legalább három év, az informatikai biztonsággal összefüggésben szerzett gyakorlat szükséges.

biztonsági tisztviselő (IB adminisztrátor, SO):

- szakirányú közép vagy felsőfokú végzettség,
- középfokú végzettség esetén legalább három, felsőfokú végzettség esetén legalább egy év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat,

regisztrációs biztonsági tisztviselő (RO):

- középfokú szakirányú végzettség,
- legalább egy év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat,

működtető adminisztrátor, rendszer auditor:

- középfokú szakirányú végzettség, valamint
- legalább egy év, hasonló munkakörben szerzett szakmai gyakorlat

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 szerepkörhöz történő hozzárendeléskor:

a. pontos és írásos munkaköri leírást kell átvennie a fölérendelt vezetőtől,
b. titoktartási nyilatkozatot kell a kijelölt személlyel aláíratni, amelyben 3 év titoktartási kötelezettség szerepel a Szolgáltatótól történő kilépés utáni időponttól számítva,
c. a szükséges mértékű oktatásban kell a kijelölt személyt részesíteni, annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és gyakorolni tudja.

Kilépéskor:

a. 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.
b. A kilépő személy számítógépes tevékenységét legalább két hétre visszamenőlegesen le kell ellenőrizni.
c. Vissza kell venni az aláírás-létrehozó eszközét, azonnal és dokumentáltan meg kell semmisíteni azt. A kapcsolódó tanúsítvány(oka)t azonnal vissza kell vonni.
d. 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, akinél a biztonsági ellenőrzés kockázatot tár fel.

5.3.8. Képzési követelmények

A Hitelesítő Központ, a Regisztrációs Iroda, az Ügyfélkapcsolati Iroda és az Ügyfélszolgálat területén dolgozó valamennyi munkatárs felvételét követően, illetve a szolgáltatások indítását megelőzően, a saját munkakörének betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt.

Rendszerüzemeltetői munkakörbe kinevezett munkatárs a kinevezést követő 3 hónapig, megfelelő gyakorlattal rendelkező kollégával közösen van beosztva.

Abban az esetben, amikor a szolgáltatásokban jelentős változás[7] következik be, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a számára szükséges dokumentációkat.[8]

Kisebb változások[9] bekövetkezése előtt a munkatársak írásos tájékoztatást kapnak a változásokról.

5.3.9. A felhatalmazás nélküli tevékenységek büntető következményei

Valamennyi bizalmi munkakört betöltő munkatárs a munkaköri kinevezéssel:

a. írásos tájékoztatást kap jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról

b. munkaköri leírása tartalmazza az őt érintő biztonsági feladatokat

c. titoktartási nyilatkozatot ír alá

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

5.3.10. A szerződéses alkalmazottakra vonatkozó követelmények

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

Az egyéb feladatok ellátására, vállalkozási vagy megbízásos szerződésben foglalkoztatott személyeket a Szolgáltató csak az „ellenőrzött beszállítók” listájáról választ. Az ellenőrzött beszállítókkal a Szolgáltató írásos megállapodást köt, amelyben rögzíti a biztonsági szabályokat.

Valamennyi szerződő fél titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során birtokába kerülő üzleti titkokat és bizalmas információkat illetéktelen személynek fel nem fedi, s egyéb módon sem hasznosítja. A titoktartási nyilatkozat záró része tartalmazza a megszegése esetén alkalmazandó szankciókat is.

5.4. Naplózási eljárások

A Szolgáltató gondoskodik arról, hogy az általa kibocsátott tanúsítványokra vonatkozó minden lényeges adat rögzítésre és megőrzésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében.

A Szolgáltató által végzett műveletek naplózásra kerülnek. A naplóbejegyzések többek között a regisztráció, az aláírás-létrehozó és ellenőrző kulcs-pár generálása, az aláírás-létrehozó eszköz megszemélyesítése, a tanúsítvány létrehozása, kibocsátása és kezelése, valamint egyéb Szolgáltatói tevékenységek során készülnek.

A naplózott adatállománynak tartalmazzák a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét vagy azonosítóját.

A Szolgáltató szolgáltatásait támogató informatikai rendszerének biztonsági naplózását és annak auditálását a jelen HSZSZ-M mellett a PKI szolgáltatások biztonsági szabályzata részletezi.

5.4.1. Naplózott esemény típusok

A tanúsítvány előállítással kapcsolatosan a Szolgáltató naplóz minden a rendszerrel és a szolgáltatás nyújtásával kapcsolatos eseményt, különösen:

a. a szolgáltatói tanúsítványok életciklusával kapcsolatos összes eseményt

b. az előfizetői tanúsítványokat aláíró infrastruktúrális és ellenőrző kulcsok tanúsítványainak életciklusával kapcsolatos összes eseményt, ezen belül különösen az előfizetői tanúsítványok előállítási és megújítási igény-benyújtási időpontját, valamint az igények teljesítésének időpontját

[7] Jelentős változásnak minősül a szervezeti biztonságpolitika módosulása, a szoftver vagy hardver rendszer változása (upgrade), valamint a kulcs kezelés és biztonság kezelési óvintézkedések változásai.

[8] Attól függően, hogy a bekövetkező jelentős változás előre tervezett volt, vagy váratlanul kellett sort keríteni rá, a továbbképzés illeszkedik az éves továbbképzési tervekbe, vagy rendkívüli módon, soron kívül iktatódik be.

[9] Kisebb változásnak minősül, pl. egy új, kevés tapasztalattal rendelkező munkatárs munkába állása, mely a vele dolgozóktól átmenetileg nagyobb figyelmet és óvatosságot igényel.

Az Előfizetők biztonságos aláírás-létrehozó eszközzel való ellátásával kapcsolatosan a Szolgáltató naplóz minden általa gondozott kulcs életciklusával kapcsolatos eseményt és a biztonságos aláírás-létrehozó eszközök megszemélyesítésével kapcsolatos valamennyi eseményt.

A visszavonás kezeléssel kapcsolatosan a Szolgáltató gondoskodik a kérések, valamint az ezek következtében előállt tevékenységek naplózásáról.

Az időbélyegzéssel kapcsolatosan naplóz minden a rendszerrel és a szolgáltatás nyújtásával kapcsolatos eseményt, különösen:

a. az időbélyegzés szolgáltatás fő lépései, a kérelemtől az időbélyeg válasz elküldésig

b. az időbélyeget aláíró kulcsok életciklusában bekövetkező eseményeket (generálás, használat, visszavonás, megsemmisítés)

c. az időbélyeget aláíró kulcsok tanúsítványa életciklusában bekövetkező eseményeket (kiadás, használat, visszavonás)

A hitelesítés-szolgáltatást támogató informatikai rendszer biztonságával kapcsolatosan naplózza:

a. a naplózási funkció elindításával és leállításával

b. a naplózási paraméterek megváltoztatásával

c. a naplózás tárolásával kapcsolatos hibákkal

d. a napló adatok integritásának megsértésével

e. a hitelesítés-szolgáltatást támogató informatikai rendszerhez történő bármely hozzáférési kísérlettel kapcsolatos eseményeket

A naplózott adatállománynak tartalmazzák a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét vagy azonosítóját.

A pontos időt a Szolgáltató időbélyegző egysége biztosítja.

A hitelesítés szolgáltatást támogató informatikai rendszer operációs rendszerére, illetve a rendszer többi elemére vonatkozóan a biztonsági szabályzatban meghatározott események kerülnek naplózásra.

5.4.2. Napló adatok védelme

A Szolgáltató a napló adatokat fokozott biztonságú fizikai környezetben menti el, a mentett állományokat időbélyeggel ellátott elektronikus aláírással hitelesíti és védett környezetben tárolja. A naplók olvasása hozzáférési jogosultsághoz kötött.

A Szolgáltató biztosítja naplóállományok bizalmasságát és sértetlenségét.

5.4.3. Naplók feldolgozásának gyakorisága

A Szolgáltató a hitelesítő központok (CA-k) naplóit naponta, az egyéb napló fájlokat a {Sz27} biztonsági szabályzatában rögzített gyakorisággal dolgozza fel.

A PKI alkalmazás, az időbélyegzés alkalmazás és az operációs rendszerek biztonsági esemény és audit naplóinak operatív ellenőrzését csak a rendszervizsgálók végezhetik és csak olvasási jogosultsággal. A rendszervizsgálók feladata az alkalmazásokon és operációs rendszereken kívüli, de a PKI rendszer részét képző szoftver elemek (hálózat, tűzfalak, betörés detektor) naplóinak ellenőrzése is.

5.4.4. Napló adatok tárolása

A napló adatokat a Szolgáltató archiválja (lásd: 5.5 pont).

5.4.5. A napló fájlok megőrzési időtartama

Lásd: 5.5 Adatok archiválása c. fejezetet.

5.5. Adatok archiválása

A Szolgáltató gondoskodik arról, hogy a tanúsítványokra és az időbélyegzésre vonatkozó minden lényeges információ megfelelő ideig rögzítésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében.

Az archivált adathordozók első példányai a Szolgáltató archívumában, a biztonsági példányai a Biztonsági Adattárban kerülnek elhelyezésre.

5.5.1. A tárolt adatok típusai

A Szolgáltató gondoskodik arról, hogy megőrzésre kerüljön a regisztráció során felvett összes információ, beleértve az alábbiakat is:

a. az Igénylő által a regisztráció támogatása céljából benyújtott dokumentum(ok) típusa

b. az azonosító dokumentumok egyedi azonosító adatai (például az Igénylő jogosítvány száma)

c. az Igénylő és azonosító dokumentumok (beleértve az aláírt, az Előfizetővel kötött megállapodást másolatainak tárolási helyszíne)

d. az Előfizetővel kötött megállapodás esetleges egyedi választásai

e. a kérelmet elfogadó regisztrációs felügyelő (RO) azonosítója

f. a fogadó Hitelesítő Központ és/vagy a küldő regisztrációs felügyelő (RO) azonosítója, amennyiben ez értelmezhető

A 5.4.1 pontban felsorolt összes esemény, illetve napló típus.

5.5.2. Az archívum megőrzési időtartama

A Szolgáltató az 5.4.1 pontban megnevezett naplókat az Eat. 9. § (7) bekezdése alapján és a 3/2005. (III. 18) IHM rendelettel összhangban a keletkezésüktől számított 10 évig, illetve jogi eljárásban a tanúsítványokon keresztül történő bizonyításhoz szükséges ideig megőrzi.

5.5.3. Az archívum védelme

A Szolgáltató az archívumában és a Biztonsági Adattárában olyan fizikai védelmet biztosít, amely fenntartja a tanúsítványokra és az időbélyegzésre vonatkozó aktuális és archivált adatok bizalmasságát és sértetlenségét. A Szolgáltató az archivált adatokat legalább fokozott biztonságú elektronikus aláírással és időbélyegzővel látja el.

5.5.4. Az archívum hozzáférését és ellenőrzését végző eljárások

A Szolgáltató az archívumhoz Ügyfélkapcsolati Irodáján keresztül biztosít hozzáférést és értelmezhetőséget. A jogosultságot és a hozzáférést a Szolgáltató minden esetben ellenőrzi és naplózza. A Szolgáltató biztosítja az archivált adatok megjelenítéséhez (olvasásához) szükséges eszközt.

5.6. Felülhitelesítés

A Szolgáltató közigazgatásban alkalmazható tanúsítványokat kibocsátó produktív hitelesítő központját (CA-t) a Közigazgatási Gyökér Hitelesítés-szolgáltató (KGyHSz) felülhitelesítette.

A KGyHSz tanúsítvány kiadásával igazolja a Szolgáltató és a szolgáltatói nyilvános kulcsok összetartozását, illetve a Szolgáltató a felültanúsított szolgáltatói tanúsítvány elfogadásával magára nézve kötelezőnek ismeri el a KGyHSz által kiadott szabályzatokat és a KGyHSz felügyeleti, ellenőrzési jogát.

A Nemzeti Média- és Hírközlési Hatóság a nyilvántartásba vételi eljárás keretében és azt követően – a jogszabályban előírt hatáskörrel – felügyeli többek között a jelen szolgáltatási szabályzat előírásainak a {J11} és {J12} hitelesítési rendeknek való megfelelőségét.

5.7. A Szolgáltató kulcscseréje

A Szolgáltató szolgáltatói kulcsának tervezett cseréje előtt fél évvel köteles tájékoztatni a Nemzeti Média- és Hírközlési Hatóságot és vele egyeztetni a szükséges feladatokról.

A Szolgáltató a közigazgatásban alkalmazható tanúsítványokat aláíró szolgáltatói kulcsának tervezett cseréje előtt fél évvel köteles tájékoztatni a Közigazgatási Gyökér Hitelesítés-szolgáltatót és vele egyeztetni a szükséges feladatokról.

A szolgáltatói kulcs kompromittálódása esetén az 5.8 pontban előírtak szerint kell eljárni.

5.8. A folyamatos üzemmenet biztosítása

A Szolgáltató olyan megbízható rendszert működtet, amely a rendszerben bekövetkezett hiba esetén is biztosítja a szolgáltatások elérhetőségét.

A Szolgáltató gondoskodik arról, hogy rendkívüli üzemeltetési helyzet esetén (pl.: súlyos üzemzavar vagy katasztrófa, beleértve a saját aláírás-létrehozó magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is) a rendszerüzemeltetés a lehető legrövidebb időn belül helyreálljon.

Rendkívüli üzemeltetési helyzet esetére a Szolgáltató rendelkezik a jogszabályban előírt minimális szolgáltatásokat biztosító (hideg) tartalék rendszerrel: a Szolgáltató rendkívüli üzemeltetési helyzet esetén is gondoskodik tanúsítványtára és nyilvános szabályzatai elérhetőségéről, a tanúsítvány felfüggesztés/visszavonás kezelésről és a tanúsítvány visszavonási listák közzétételéről, valamint az időbélyegzés szolgáltatás fenntartásáról (lásd: 2.1.1 fejezet 6. pont).

A rendkívüli üzemeltetési helyzetek kezelésére a Szolgáltató rendelkezik biztonsági mentésekkel, tartalékolt műszaki megoldásokkal és eljárásokkal. A megelőzőzésre és rendkívüli üzemeltetési helyzetekre érvényes intézkedéseket a Szolgáltató {Sz28} üzletmenet-folytonossági terve tartalmazza.

A rendkívüli üzemeltetési helyzetekben a Szolgáltató eseménynaplót vezet.

5.8.1. A szolgáltatások azonnali felfüggesztése

Rendkívüli üzemeltetési helyzet határidőn túli fennállása esetén a Szolgáltató haladéktalanul értesíti a Nemzeti Média- és Hírközlési Hatóságot a rendkívüli üzemeltetési helyzet bekövetkezéséről, annak hatásáról, várható időtartamáról, a rendkívüli üzemeltetési helyzet elhárítása érdekében tett és tervezett intézkedésekről, valamint a rendkívüli üzemeltetési helyzet megszűnéséről. A szolgáltató köteles a rendkívüli üzemeltetési helyzetről és annak hatásáról közvetlenül, illetve elektronikus levél formájában értesíteni a szolgáltatásokat igénybe vevő mindazon személyeket, akiket a rendkívüli üzemeltetési helyzet érint, valamint az erről szóló tájékoztatást az interneten elérhetővé tenni.

5.8.2. Biztonsági képesség rendkívüli üzemeltetési helyzetben

Rendkívüli üzemeltetési helyzetben a Szolgáltató életbe lépteti üzletmenet-folytonossági tervében megtervezett eljárásait annak érdekében, hogy az üzemeltetés helyreálljon az üzletmenet-folytonossági tervben megjelölt időn belül.

A visszaállítási időt alapvetően az esemény súlyossága, azaz az üzletmenet-folytonossági terv szerint értelmezett osztályba sorolása határozza meg. A súlyos üzemzavari és a katasztrófa esetet – többek között – az különbözteti meg egymástól, hogy katasztrófa esetén nagy valószínűséggel nem csak az informatikai rendszer, hanem annak fizikai környezete is megsemmisül részben vagy egészben. Ez utóbbi esetben az üzletmenet-folytonossági tervben meghatározott módon a Válságstáb intézkedik a tartalék helyszínre történő áttelepülésről és az informatikai rendszer szükséges mértékű visszaállításáról a tartalék helyszínen korábban elhelyezett mentések segítségével.

5.8.3. Rendkívüli eseményekről történő értesítés

A szolgáltatásokat támogató informatikai rendszerre, annak fizikai és személyi környezetére kiható súlyos üzemzavari és katasztrófa események megelőzéséről, kezeléséről, az érintettek értesítéséről és a rendszer visszaállításáról részletesen a Szolgáltató üzletmenet-folytonossági terve intézkedik. Az üzletmenet-folytonossági tervben az üzletmenetet veszélyeztető, sértő, illetve azt leállító események súlyossági osztályokba vannak sorolva. A terv részletesen szabályozza a Hitelesítő Központok saját aláírás-létrehozó adatainak, aktiváló adatainak és az időbélyegek aláíró kulcsának kompromittálódása esetén elvégzendő teendőket.

A Szolgáltató nem értesíti az eseményeket kiváltó alanyokat, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába.

5.8.4. Minimális szolgáltatás rendkívüli üzemeltetési helyzetben

A Szolgáltató rendkívüli üzemeltetési helyzetben is biztosítja az időbélyegzés szolgáltatást, Tanúsítványtárának elérhetőségét, a tanúsítványok felfüggesztésére és visszavonására vonatkozó kérelmek fogadását és teljesítését, valamint a visszavonási/felfüggesztési állapot közzétételét a visszavonási listákban.

Rendkívüli üzemeltetési helyzetben a Szolgáltató minden egyéb szolgáltatást szüneteltet.

5.8.5. Üzletmenet-folytonossági terv

A Szolgáltató rendelkezik üzletmenet-folytonossági tervvel (lásd: 1.7. pont), amely részletes intézkedési forgatókönyveket tartalmaz a súlyos üzemzavarok vagy katasztrófa események kezelésére. Ez a dokumentum biztonsági okokból nem nyilvános.

5.9. A szolgáltatási tevékenység megszüntetése

A Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezd más szolgáltatókkal a szolgáltatások átvételéről. A tárgyalások eredményéről tájékoztatja a felhasználói közösséget.

A Szolgáltató gondoskodik a szolgáltatásainak megszüntetéséből fakadó, a felhasználói közösséget érintő zavarok minimalizálásáról. Különösképpen gondoskodik az időbélyegzés, a tanúsítvány visszavonás kezelés és közzététel szolgáltatások folyamatos fenntartásáról.

Ennek érdekében a Szolgáltató mielőtt szolgáltatási tevékenységét leállítja:

a. legalább 60 nappal korábban értesíti a Nemzeti Média- és Hírközlési Hatóságot és internetes honlapján tájékoztatja a felhasználói közösség tagjait.

b. Az Aláíróknak illetve Előfizetőknek szóló értesítésben Szolgáltató tájékoztatást ad arról, hogy a tanúsítványok visszavonásra kerülnek, és ennek jogkövetkezményeként az aláíró kulcs nem használható fel a továbbiakban (visszavonás követően) elektronikusan történő aláírásra

c. megszűnteti a tanúsítványok kibocsátási folyamatában a nevében eljáró alvállalkozások összes felhatalmazását

d. megteszi a szükséges lépéseket, hogy a regisztrációs adatok és az eseménynapló archívumok fenntartására vonatkozó kötelezettségeket átruházza

A bejelentéssel egyidejűleg a Szolgáltató leállítja:

a. a tanúsítvány előállítás és kibocsátás szolgáltatást (ezen belül a tanúsítvány megújítását)

b. a biztonságos aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatást.

Szolgáltató a tervezett megszűnés előtt 20 nappal intézkedik az előfizetői tanúsítványok és szolgáltatói tanúsítványai visszavonásáról.

Ezzel egyidejűleg leállítja az időbélyegzést és a visszavonás kezelési szolgáltatását.

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

Eljárás Regisztrációs Iroda megszűnése esetén:

a. A Regisztrációs Iroda megszűnése előtt 60 nappal értesíti azon Előfizetőket, akik a megszűnő Regisztrációs Irodánál kötöttek szerződést és a Szolgáltató által kibocsátott érvényes tanúsítvánnyal rendelkeznek.

b. A Regisztrációs Iroda megszűnéséről a felhasználói közösség tagjait Szolgáltató a web oldalain történő közzététel útján tájékoztatja.

6. Műszaki biztonsági óvintézkedések

A Szolgáltató megbízható, információbiztonság szempontjából értékelt és minősített elemekből álló informatikai rendszert illetve elektronikus aláírási terméket használ szolgáltatásai nyújtásához. A hibák (különösen a telepítési és karbantartási hibák) elkerülése érdekében rendszer-telepítési, hardver-konfigurálást és szoftver-frissítést igénylő beavatkozást csak két munkatárs egyidejű jelenlétében lehet elvégezni. A műveletek sikerességét auditorok ellenőrizik és hitelesítik.

Az informatikai rendszer neve:	InfoCA V2.5
Tanúsításának száma:	HUNG-T-048-2009,
Érvényességi ideje:	2015. 08. 19.
A nagy biztonságú hardver modul neve:	nCipher nShield 500 F3
Hardware verzió:	nC4033P-500
Firmware verzió:	2.33.60-3
Tanúsításának száma:	HUNG-T-059-2011
Érvényességi ideje:	2014. 12. 15.

A Szolgáltató önkéntes akkreditációs rendszer keretében nem lett tanúsítva.

6.1. Kriptográfiai kulcspár előállítás és aláírás-létrehozó eszköz megszemélyesítés

6.1.1. Kulcspár előállítás

A Szolgáltató maga generálja a *szolgáltatói* kulcspárokat (az aláírás-létrehozó és az aláírás-ellenőrző adatokat) fizikailag védett környezetben, nagy biztonságú hardver modulban (HSM), kettős ellenőrzés mellett. A nagy biztonságú hardver modul hazai tanúsítvánnyal rendelkezik és szerepel a Nemzeti Hírközlési Hatóság által jóváhagyott minősített elektronikus aláírási termékek listájában. A kulcspárok generálását olyan algoritmussal végzi, amely szerepel a Nemzeti Média- és Hírközlési Hatóság EF/26838-11/2011. sz. határozatának 1. sz. mellékletében.

Az időbélyeget aláíró *szolgáltatói* kulcsot az időbélyegző egység szerves részét képező, tanúsított HSM modul generálja és tárolja. Az aláíró kulcs teljes életciklusa alatt ezen eszközben marad.

A Szolgáltató maga generálja az *előfizetői* kriptográfiai kulcspárokat és nem fogad el az Előfizető által generált kulcspárt.

Előfizetői kulcspárokhoz a Szolgáltató kizárólag biztonságos aláírás-létrehozó eszközt (BALE) alkalmaz, a kriptográfiai kulcspárt a Szolgáltató PKI alkalmazása magán a biztonságos aláírás-létrehozó eszközön generálja. Az aláíró kulcs teljes életciklusa alatt ezen eszközben marad.

6.1.2. Az aláírás-létrehozó eszköz megszemélyesítése

A biztonságos aláírás-létrehozó eszköz (*chip kártya*) megszemélyesítését a Szolgáltató maga végzi fizikailag védett környezetben üzemelő kártya-megszemélyesítő rendszeren.

A chip kártya megszemélyesítés szolgáltatáshoz vizuális megjelenítés, egy oldali nyomással történő grafikus megszemélyesítés is kapcsolódik az Előfizetői Szerződésben meghatározott adattartalommal.

A Szolgáltató az aláírás-létrehozó adat aktivizálásához (a chip kártyához) *PIN kód*ot biztosít. A PIN kódot fizikailag védett környezetben állítja elő és a kódot tartalmazó *PIN-boríték*ot az aláírás-létrehozó eszköztől elkülönítve tárolja.

6.1.3. Az aláírás-létrehozó adat eljuttatása az Aláíróhoz (Előfizetőhöz)

A Szolgáltató az aláírás-létrehozó adatot, illetve a megszemélyesített biztonságos aláírás-létrehozó eszközt az átvételig fizikailag védett környezetben tárolja és biztosítja, hogy az aláírás-létrehozó adat titkossága ne sérüljön.

A Szolgáltató a biztonságos aláírás-létrehozó eszközt és a PIN kódot tartalmazó borítékot személyesen adja át az Aláírónak (Előfizetőnek).

A biztonságos aláírás-létrehozó eszköz és a PIN boríték (kód) átvételét követően csak az Aláíró férhet hozzá saját magánkulcsához.

A biztonságos aláírás-létrehozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

6.1.4. Az Aláírók aláírás-ellenőrző adatának eljuttatása az érintett feklekhez

A Szolgáltató az Aláírók aláírás-ellenőrző adatát (nyilvános kulcsát) az előfizetői tanúsítványokon keresztül Tanúsítványtárában teszi mindenki számára elérhetővé. Az Aláírók aláírás-ellenőrző adatát az Aláírók előfizetői tanúsítványa tartalmazza.

6.1.5. A Szolgáltató aláírás-ellenőrző adatainak eljuttatása a felhasználói közösséghez

A Tanúsítványtárban közzétett tanúsítványok ellenőrzéséhez szükséges szolgáltatói nyilvános kulcsok (szolgáltatói tanúsítványok) és visszavonási listák a Szolgáltató szolgáltatásainak internetes honlapján keresztül közvetlenül elérhetők.

A tanúsítványok letölthetők és a felhasználók kliens-alkalmazásaiba installálhatók.

6.1.6. Kulcs méretek, algoritmosok

A Szolgáltató hitelesítő központjai elektronikus aláírás létrehozására az SHA256-2048-RSA[10] algoritmuskészletet használják.

A Hitelesítő Központok ("Root CA", „Produktív CA”) aláíró kulcsainak mérete:	2048 bit
Az időbélyegző egység aláíró kulcsának mérete:	2048 bit
Az Aláírók aláíró kulcsainak (aláírás-létrehozó adatának) mérete:	2048 bit

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

6.1.7. Előfizetői aláírás-ellenőrző adat előállításához használt paraméterek előállítása

Az előfizetői tanúsítványok az RSA aláíró algoritmusokhoz használhatók.

Az Előfizetői aláírás-ellenőrző adat előállításához használt paraméterek megfelelőségét a biztonságos aláírás létrehozó eszközt tanúsító szervezet és a gyártó tanúsítják. A kapcsolódó dokumentumok a Szolgáltatónál megtekinthetők.

6.1.8. Szolgáltatói kulcsgenerálás

A szolgáltatói tanúsítványokhoz a kulcsgenerálás nagy biztonságú hardver modulban (HSM-ben) vagy biztonságos aláírás-létrehozó eszközön történik.

A produktív hitelesítő központok és az időbélyeget aláíró kulcsok tanúsítványait a Szolgáltató 1. szintű hitelesítő központja (root CA-ja) hitelesíti.

A közigazgatásban alkalmazható tanúsítványokat kibocsátó produktív hitelesítő központ aláíró kulcsa tanúsítványát a KGYHSZ (felül) hitelesíti.

6.1.9. Kulcs felhasználási célok

A Szolgáltató Előfizetők részére tanúsítványt (kulcspárt) kizárólag elektronikus aláírási célra bocsát ki.

Az Előfizetők részére kibocsátott tanúsítványok bővítmény (Extension) részében található „KeyUsage” mezőbe elektronikus aláírás felhasználási célként a „nonRepudiation” kulcshasználati módnak megfelelő kijelölést kell alkalmazni.

Nem a közigazgatásban alkalmazható tanúsítványok bővítmény (Extension) részében található „*KeyUsage*” mezőbe elektronikus aláírás felhasználási célként – az NR mellett - a „*Content Commitment*” (CC) kulcshasználat is szerepeltethető.

6.2. Aláírás-létrehozó adat védelme

6.2.1. Az aláírási termékre vonatkozó szabályok

A Szolgáltató az Előfizetők aláírás-létrehozó adatának előállítására olyan eszközt használ, amely teljesíti a CC EAL4 követelményeket, rendelkezik az Európai Unió egyik tagállamában nyilvántartásba vett, eszköztanúsításra jogosult szervezet által erre a célra kiadott tanúsítvánnyal[11]. A Szolgáltató által az Előfizetők aláírás-létrehozó adatának előállítására használt biztonságos aláírás létrehozó termék a Gemalto S.A. által gyártott, Classic TPC IM CC v3 intelligens kártya, melynek neve és verziója (a megfelelőségi tanúsítvány szerint) MultiApp ID Citizen 72K (Generic configuration), IAS Classic v3.0 / MultiApp v1.1 T1003982 on S3CC91C rev.0.

[10] RSA Rsagen1 IETF RFC 3447 (2003) “PKCS #1: RSA Cryptography Specifications Version 2.1”

[11] A tanúsítási jelentés eredeti, francia nyelvű változatának elérhetősége: http://www.ssi.gouv.fr/IMG/certificat/dcssi_2009-07fr.pdf

6.2.2. A kriptográfiai modulra vonatkozó szabályok

A Szolgáltató saját szolgáltatói magánkulcsainak tárolására illetve használatára olyan biztonságos kriptográfiai modult (HSM) alkalmaz, amely teljesíti a vonatkozó (Eat. 7. § (5)-(6) bekezdéseiben foglalt) feltételeket, azaz rendelkezik az NMHH által regisztrált, illetve az Európai Unió valamely tagállamában nyilvántartásba vett tanúsításra jogosult szervezetek által kiadott igazolással.

6.2.3. A több-szereplős ("n-ből m") magánkulcs visszaállítás ellenőrzése

A Szolgáltatónál egyedül a Hitelesítő Központban alkalmazzák az „n-ből m" ellenőrzést a Root CA kulcsgondozási funkcióinak aktivizálásánál.

6.2.4. Aláírás-létrehozó adat letét, mentés, archiválás

A Szolgáltató nem nyújt magánkulcs letétszolgáltatást. Az előfizetői aláírás-létrehozó adatot, vagy annak előállítására, visszafejtésére alkalmas programot, adatot nem tárol.

A Szolgáltató az Előfizető aláírás-létrehozó adatot semmilyen formában nem menti vagy tárolja.

A Szolgáltatónál a Hitelesítő Központ aláíró magánkulcsai[12] biztonsági okokból duplikálásra kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik.

6.2.5. Aláírás-létrehozó adat védelme

Az előfizetői kulcspárokat a szolgáltató kizárólag a biztonságos aláírás-létrehozó eszközön generálja, így a magánkulcsok semmilyen körülmények között nem hagyják el azokat. A biztonságos aláírás-létrehozó eszközt a Szolgáltató PIN-kóddal védve adja át az Előfizetőnek.

A Szolgáltató munkatársai számára a PKI biztonsági felügyelő (SO) generálja a kulcspárokat a biztonságos aláírás-létrehozó eszközön, így a magánkulcsok semmilyen körülmények között nem hagyják el azokat. A biztonságos aláírás-létrehozó eszközt a Szolgáltató PIN-kóddal védve adja át munkatársainak.

HSM modulban generált szolgáltatói kulcspárok esetében a magánkulcs nyílt (titkosítatlan) formában semmilyen körülmények között sem hagyhatja el a modult. A szolgáltatói magánkulcsok csak a modul (token) mentésénél, duplikálásánál hagyják el a modult. A mentési (klón) modulba ilyen esetekben a magánkulcs rejtjeles védelem alatt másolódik át.

6.2.6. Aláírás-létrehozó adat aktiválása

Az előfizetői aláírás-létrehozó adat aktiválása az Aláíró által történik a PIN kód megadásával. A biztonságos aláírás-létrehozó eszköznél az aláírás-létrehozó adat az aktiváláskor sem hagyja el a chipkártyát, azt onnan leolvasni nem lehet.

6.2.7. Aláírás-létrehozó adat deaktiválása

Az előfizetői aláírás-létrehozó adatok deaktiválását az Aláíró alkalmazása végzi kijelentkezéskor vagy amikor az Aláíró a biztonságos aláírás-létrehozó eszközt (csipkártyát) eltávolítja az olvasóból.

6.2.8. Aláírás-létrehozó adat megsemmisítése

Az előfizetői aláírás-létrehozó adat tanúsítványának lejárta után a biztonságos aláírás-létrehozó eszköz fizikai megsemmisítését az Aláírónak 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. Kulcspár kezelés egyéb aspektusai

6.3.1. Aláírás-ellenőrző adat (az előfizetői tanúsítványok) megőrzése

Az aláírás-ellenőrző adatokat a tanúsítványok tartalmazzák. A Szolgáltató minden általa előállított és kibocsátott tanúsítványt megőriz az érvényesség lejártától számított 10 évig, illetve a tanúsítványhoz kapcsolódó privát kulccsal elektronikusan aláírt elektronikus dokumentummal kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig. A Szolgáltató ugyanezen határidőig olyan eszközt biztosít, amellyel a kibocsátott tanúsítvány tartalma megállapítható. E megőrzési kötelezettségnek a Szolgáltató minősített archiválási szolgáltató igénybevételével is eleget tehet.

12 A kriptográfiai hardver modul (tanúsítványokat, illetve visszavonási listákat aláíró) magánkulcsai.

Az archiválás biztonsági okokból 2 példányban történik.

6.3.2. Aláírás-létrehozó és aláírás-ellenőrző adatok felhasználási ideje

Az aláírás-létrehozó adat (aláíró kulcs) és az aláírás-ellenőrző adat (nyilvános kulcs) érvényességi ideje megegyezik a kulcsok hitelességét igazoló tanúsítvány érvényességi idejével:

Root CA aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 20 év
Időbélyegző egység aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 10 év
Produktív CA aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 20 év
RO kommunikációs kulcs és tanúsítvány érvényessége:	legfeljebb 3 év
Előfizetői aláíró kulcs és tanúsítvány érvényessége:	legfeljebb 2 év

A tanúsítványok és a benne foglalt aláírás-ellenőrző adatok (nyilvános kulcsok) érvényességének kezdete a kibocsátás időpontjával (év, hónap, nap, óra, perc, másodperc) egyezik meg.

6.4. Aktiválási adatok

6.4.1. Aktiválási adatok generálása és installációja

Az aláírás-létrehozó eszközök aktivizáló adatait (PIN kódjait) a Szolgáltató által használt PKI alkalmazás állítja elő.

A Szolgáltató az Aláíró hozzáférési jogosultságát ellenőrző adatot (PIN-kódot) csak abból a célból rögzítheti, hogy azt az Aláíró számára - másolat megőrzése nélkül - átadhassa[13].

6.4.2. Aktiválási adatok védelme

A Szolgáltató az aláírás-létrehozó eszközök PIN kódjait az alábbiak szerint védi az Előfizetőnek vagy az Aláírónak történő átadásig:

A Szolgáltató a PIN kódokat az előállítás során műszaki és szervezési intézkedésekkel védi.

Az Aláíró részére a PIN kódot tartalmazó borítékot az aláírás-létrehozó eszköztől elkülönítve adja át.

Az átvételt követően Aláírónak saját felelősségi körében kell biztosítania PIN kódja kizárólagos birtoklását.

Az Aláírónak rendelkeznie kell megfelelő PIN-kód módosító kliens alkalmazással, amelyet a Szolgáltató biztosít számára.

Az aláírás-létrehozó eszköz első használatakor –- jellemzően az Aláíró saját munkaállomásán –- az alkalmazás kikényszeríti a PIN-kód megváltoztatását.

Az Aláíró a későbbiekben is bármikor megváltoztathatja a PIN kódját.

Az Előfizető és Aláíró személye „munkatársi” tanúsítvány esetén jellemzően szétválik, de az aláírás-létrehozó adat felhasználása az Aláíró felelőssége. Mivel az aláírás-létrehozó adat felhasználása szempontjából a PIN-kód kritikus biztonsági elem, ezért a PIN-kódokat Szolgáltató az Aláírónak adja át. Előfizetői szempontból az aláírás-létrehozó adatnak az Aláíró által történő kizárólagos birtoklása az alapvető feltétel az elektronikusan aláírt adat, dokumentum hitelességének biztosítására. Emiatt az Előfizetőnek saját felelősségi körében kell biztosítania azt, hogy az aktivizáló adatot kizárólag az Aláíró birtokolja. Amennyiben a PIN-kód sérül vagy elveszik, illetve ennek alapos gyanúja fennáll, akkor az Aláírónak ezt haladéktalanul jelentenie kell az Ügyfélkapcsolati Irodánál vagy az Ügyfélszolgálatnál, amely azonnal intézkedik a tanúsítvány felfüggesztéséről.

A PIN kódot a Szolgáltató nem tárolja és nem állítja újra elő sem az Aláíró, sem az Előfizető, sem 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, amely esetenként új aláírás létrehozó adat illetve tanúsítvány előállítását is feltételezi.

6.4.3. Aktiválási adatok egyéb aspektusai

Az aláírás-létrehozó eszközök aktiválási adatait Szolgáltató nem tárolja, és nem állítja újra elő az Aláíró, Előfizető, harmadik fél, vagy hatóság kifejezett kérése esetén sem.

[13] 3/2005. (III. 18.) IHM rendelet 40. §, 4. bek. szerint.

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

6.5. Az időszinkronizálás megvalósítása

A Szolgáltató által adott időbélyeg felépítése megfelel az RFC 3161 szabványnak és a Szolgáltató {Sz26} Időbélyegzés Szolgáltatási Rendjében (ISZR) meghatározott további követelményeknek.

Az időszinkronizáció menetét a Szolgáltató Időbélyegzés Szoltáltatási Rendje 7.3. pontja illetve jelen szabályzat 4.11 pontja írja le.

A Szolgáltató által alkalmazott referencia időforrások:

server 148.6.0.1	ubul.kfki.hu
server 129.132.2.21	swisstime.ee.ethz.ch
server 192.53.103.103	ptbtime1.ptb.de
server 145.238.110.49	ntp-p1.obspm.fr
server 192.168.6.90	gps time

A referencia időforrások pontossága századmásodpercen belül van.

6.6. Számítógép biztonsági szabályok

6.6.1. Számítógép biztonság technikai követelményei

A Számítógép biztonság technikai követelményeit a 2/2002 MeHVM ajánlás határozza meg.

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

a. operációs rendszer,
b. PKI alkalmazás, időbélyegzés alkalmazás,
c. kriptográfiai hardver modulok,
d. tűzfalak, behatolás detektorok.

Az operációs rendszerek által megvalósított biztonsági funkciók az alábbiak:

a. biztonsági naplózás (a biztonsági napló védelme, az ahhoz való hozzáférés korlátozása),
b. a felhasználói adatok védelme (a felhasználói adatok csak alkalmazáson keresztüli elérésének biztosítása),
c. azonosítás és hitelesítés (a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
d. a biztonsági funkciók védelme (a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása).

A PKI alkalmazás által megvalósított biztonsági funkciók az alábbiak:

a. biztonsági naplózás (a rendszerüzemeltetői hozzáférések és tevékenységek rögzítése),
b. kommunikáció (a Hitelesítő Központ és a Regisztrációs Iroda közötti kommunikáció bizalmasságának, sértetlenségének és hitelességének biztosítása),
c. a felhasználói adatok védelme (az elindított alkalmazások csak a jogosultságnak megfelelő funkciók elérhetőségét biztosítják),
d. azonosítás és hitelesítés (a rendszerüzemeltetők azonosítása, hitelesítése, az alkalmazások által biztosított funkciók elérésének sikeres hitelesítéshez kötése).

Az időbélyegzésre szolgáltatásra vonatkozó biztonsági funkciók az alábbiak:

a. Az időbélyeget aláíró kulcsok tárolása a tanúsítással rendelkező HSM egység(ek)ben történik. Az időbélyegző szerverek külön biztonsági zónában történő üzemeltetése.
b. Az időbélyegző szerverek belső órájának pontossága folyamatos ellenőrzés alatt áll. A pontossági tartományból történő kilépés esetén az időbélyegző szolgáltatás leáll és a hiba kijavításáig minden további kérésre hibaüzenet kerül kiküldésre.
c. A szinkronizáló órajelek hitelességét az időbélyegző informatikai rendszer indításakor egy erre a célra létrehozott bizottság tanúsította.
d. biztonsági naplózás,
e. Az időbélyeget választ kibocsátó szervereket többszörös tűzfal rendszer védi a külső hálózatokról érkező fenyegetésektől.
f. Az időbélyegzés szolgáltatás rendelkezésre állási szintje 99,9%. Ez a szint meleg tartalékolt időbélyegző szerver architektúrával, és a szervereknek a hitelesítés szolgáltató informatikai rendszer magas rendelkezésre állást felügyelő és vezérlő rendszerébe történő integrálásával biztosított

A kriptográfiai hardver modulok által megvalósított biztonsági funkciók az alábbiak:

a. biztonsági naplózás,

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

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

d. azonosítás és hitelesítés,

e. biztonságkezelés (a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),

f. a biztonsági funkciók megbízható védelme (a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása),

g. 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:

a. biztonsági naplózás (a hálózati kommunikáció naplózása, a biztonsági napló védelme, a napló folyamatos elemzése: biztonsági riasztások és automatikus válaszok megvalósítása),

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

c. azonosítás és hitelesítés,

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

6.6.2. Számítógép biztonsági értékelések

A számítógép biztonsági értékelések rendszerét a . táblázat mutatja.

BIZTONSÁGI ELLENŐRZÉS TÍPUSA		VÉGZI	RENDSZERESSÉG
Operatív	IT infrastruktúra	Rendszerüzemeltető	Naponta
	PKI alkalmazás	Rendszervizsgáló (auditor)	Naponta
	Szerverek biztonsági beállításai	Rendszervizsgáló (auditor)	Negyedévente
Belső ellenőrzés	IT infrastruktúra	Információbiztonsági vezető	Évente egyszer
	PKI alkalmazás	Hitelesítési Rend és Szabályozási Csoport	Évente egyszer
Külső ellenőrzés	IT infrastruktúra	Külső auditor	Évente egyszer
	PKI alkalmazás	Külső auditor	Évente egyszer

. táblázat

6.7. Életciklus technikai szabályok

6.7.1. Rendszerfejlesztési szabályok

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató {Sz23} társasági szintű információbiztonsági szabályzat tartalmazza, amelyek pontosan meghatározzák az előkészítés, a projekt, a működtetés, a menedzselés és a visszavonás/rekonstrukció ciklus időszakok feladatait és az alkalmazott módszertanokat.

6.7.2. Biztonságkezelési szabályok

A biztonságkezelési szabályokat a Szolgáltató {Sz23} társasági és a {Sz27} rendszer szintű információi biztonsági szabályzatai tartalmazzák.

6.7.3. Életciklus biztonsági értékelések

A Szolgáltató által alkalmazott megbízható informatikai rendszerek megfelelnek a 2/2002 MeHVM ajánlásban rögzített követelményeknek, mely megfelel az {Sz14} Common Criteria EAL4 szintnek.

Az életciklus biztonsági értékelések a . táblázat szerinti rendszerben történnek.

6.8. Hálózati biztonsági szabályok

A hálózati védelmi intézkedések a 2/2002 MeHVM ajánlásnak felelnek meg.

A Hitelesítő Központ és a Regisztrációs Iroda közötti kommunikációt biztosító belső hálózat PKIX kapcsolattal védett a sértetlenség és letagadhatatlanság érdekében, illetve bizalmasság elvesztése ellen.

A Szolgáltató szolgáltatásait támogató informatikai rendszerénél a védett belső és a külső hálózatok biztonságos elválasztását tűzfal és behatolás érzékelő rendszer (IDS) biztosítja.

A Hitelesítő Központ nem folytat közvetlen külső kommunikációt a végfelhasználókkal.

6.9. Kriptográfiai (HSM) modul ellenőrzése

A kriptográfiai modulok ellenőrzik az illetéktelen beavatkozási kísérleteket. Ha egy modul ilyet detektál, akkor:

a. a memóriájában levő magánkulcsot törli

b. a modul saját tanúsítványa is törlésre kerül és ezzel a modul használhatatlanná válik

7. Tanúsítvány és tanúsítvány-visszavonási profil

A Szolgáltató által kibocsátott minősített tanúsítvány profilok és tanúsítvány-visszavonási profilok megfelelnek a 2/2002 (IV.26.) MeHVM irányelvnek, az ITU-T X.509 szabvány 3. változatának, az EU ETSI TS 101 862 (*Minősített tanúsítvány profil*) szabványnak és az RFC 3739 (*Internet X.509 Nyilvános kulcsú infrastruktúra – Minősített tanúsítvány profil*) Internet szabványnak. Az alkalmazott minősített tanúsítványtípus mezői és azok értelmezése e szabványokat követi.

7.1. Tanúsítvány profil

7.1.1. Alap mezők

A Szolgáltató az RFC 3280 ajánlásnak megfelelő tanúsítványokat bocsát ki.

7.1.2. Tanúsítvány kiterjesztések

A Szolgáltató az ITU X.509 szabvány 3. változatának, az EU ETSI TS 101 862 és az RFC 3739 szabványoknak megfelelő tanúsítvány kiterjesztéseket támogatja.

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.

7.1.3. Közigazgatásban alkalmazható tanúsítványok

A közigazgatásban alkalmazható tanúsítványok megfelelnek a Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára előírásainak.

7.2. Tanúsítvány-visszavonási profil

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

Szolgáltató a kiterjesztéseket nem köteles kitölteni.

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.

7.3. Időbélyeg profil

A Szolgáltató által kibocsátott időbélyegek szerkezete követi az RFC 3161 szabványt és az ETSI ET 102 023 szabvány 7.3.1 pontjában előírtakat.

8. A megfelelőség vizsgálata

A Szolgáltatót a Nemzeti Média- és Hírközlési Hatóság jogelődje, a Hírközlési Felügyelet minősített hitelesítés-szolgáltatóként 2003. április 3.-án nyilvántartásba vette.

A Nemzeti Média- és Hírközlési Hatóság a Szolgáltató bejelentése alapján a jelen dokumentumban megnevezett biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő minősített tanúsítványokra vonatkozó hitelesítési rendet {Sz24}, és a jelen dokumentumban megnevezett időbélyegzés szolgáltatási rendet {Sz26} nyilvántartásába felvette.

A Szolgáltató minősített hitelesítés-szolgáltatásához olyan biztonságos elektronikus aláírási termékeket használ, amelyek szerepelnek a Nemzeti Média- és Hírközlési Hatóság „Tanúsított elektronikus aláírási termékek" listáján.

A Szolgáltató az időbélyegzés szolgáltatásához olyan biztonságos aláírás létrehozó eszközt használ, mely szerepel a Nemzeti Média- és Hírközlési Hatóság „Tanúsított elektronikus aláírási termékek" listáján.

A Szolgáltató a szolgáltatásaihoz kapcsolódó tevékenységét, a szolgáltatásait támogató informatikai rendszert, valamint annak személyi és fizikai környezetének biztonságát auditáltatja, illetve tanúsíttatja:

a. a saját szervezetén belüli belső auditor szervezettel

b. független külső auditor céggel

A Szolgáltató a szolgáltatási rendszerének következő elemeit auditáltatja:

a. Az előfizetői és szolgáltatói minősített tanúsítványok kezeléshez és az időbélyegzéshez felhasznált elektronikus aláírási termékeit

b. Az előfizetői és szolgáltatói minősített tanúsítványok kezeléshez, az időbélyegzéshez használt rendszereit és módszereit

A Szolgáltató a magánkulcsainak tárolására használt aláírás-létrehozó eszközeit tanúsíttatja. A tanúsításhoz a Szolgáltató külső szervezetet vesz igénybe.

A Szolgáltató az Eat. 8/b § szerint önkéntes akkreditációs rendszer keretében nem lett tanúsítva.

8.1.1. Vizsgálatok gyakorisága

A Szolgáltató aláírás-létrehozó eszközözének tanúsítására a használatba vételt megelőzően egyszer került sor.

A Szolgáltató az Előfizetők számára tanúsított biztonságos aláírás-létrehozó eszközöket (BALE) biztosít.

A Nemzeti Média- és Hírközlési Hatóság a jogszabályoknak megfelelően évente átfogó helyszíni ellenőrzést végez.

A Szolgáltató a külső, illetve a saját ellenőrző szervezete által végzett belső vizsgálatokat a {Sz27} PKI szolgáltatások biztonsági szabályzatában megjelölt rendszerességgel végezteti, illetve végzi.

8.1.2. 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 hitelesítés szolgáltatás minősítési kérelmének beadása előtt az EDIPORT Kft. végezte el. Az auditálás folyamatát és eredményét a Nemzeti Média- és Hírközlési Hatóság szakértői listájában szereplő Erdősi Péter Máté ellenőrizte, aki a Szolgáltató részére kötelezően előírt külső elektronikus aláírás szakértői vizsgálatokat is elvégzi évi rendszerességgel.

8.1.3. Hiányosságok kezelése

Az üzemszerű ellenőrzések, a belső és külső auditok, valamint a szakértői elemzések során feltárt hiányosságokat, hibás gyakorlatokat a Szolgáltató késlekedés nélkül megszünteti, intézkedéseit naplózza.

A Nemzeti Média- és Hírközlési Hatóság által végzett rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltató késlekedés nélkül megszünteti a vizsgálatot végző Nemzeti Média- és Hírközlési Hatóságtól kapott információk és ajánlások alapján.

8.1.4. Eredmény kommunikációja

A hiányosságok felszámolásáról a Szolgáltató Nemzeti Média- és Hírközlési Hatóságot tájékoztatja.

A Szolgáltató nem köteles a feltárt konkrét hiányosságokat nyilvánosságra hozni.

9. Egyéb üzleti és jogi kérdések

9.1. Díjak

A mindenkor érvényes szolgáltatási díjakat a Szolgáltató internetes honlapján keresztül teszi közzé. A Szolgáltató jogosult az árlistát egyoldalúan módosítani.

Az Előfizetőkre vonatkozó hatályos szolgáltatási díjak az Előfizetői Szerződésben kerülnek rögzítésre.

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

9.1.1. Tanúsítvány kibocsátás

Szolgáltató a kibocsátott és megújított tanúsítványokért éves fenntartási díjat számol fel az Előfizető felé, amely tartalmazza a tanúsítványok kibocsátásának (illetve megújítás esetén megújításának) és Tanúsítványtárban történő közzétételének díját az érvényesség időtartamára, valamint a tanúsítványok lejárat utáni archiválásának a díját.

9.1.2. Tanúsítvány hozzáférés

Szolgáltató a közzétett tanúsítványok eléréséért nem számol fel díjat.

9.1.3. Visszavonási lista hozzáférés

A Szolgáltató a közzétett visszavonási lista eléréséért nem számol fel díjat.

9.1.4. Időbélyegzés

A Szolgáltató az időbélyegek kibocsátásáért az erre vonatkozó szerződés keretében meghatározott díjat számol fel.

9.1.5. Egyéb szolgáltatásokra vonatkozó díjak

Szolgáltató a kibocsátott tanúsítványok újraérvényesítéséért eljárási díjat számol fel az Előfizető felé, mely tartalmazza a tanúsítvány megváltozott állapotának a tanúsítványtárban 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.

9.1.6. Visszatérítési elvek

Az Előfizető a számára kibocsátott tanúsítvány éves fenntartási díjának visszatérítésére a következő esetekben jogosult:

a. a kibocsátott tanúsítvány valamely adata a Szolgáltató hibájából fakadóan nem megfelelő,

b. a kibocsátott tanúsítvány, magánkulcs és aktivizáló adat nem összetartozó,

c. a kibocsátott aláírás-létrehozó eszközön szereplő adatok a Szolgáltató hibájából fakadóan nem megfelelők,

d. a kibocsátott aláírás-létrehozó eszköz, az aktivizáló kód és a kulcsok nem összetartozók,

e. a Szolgáltató bizonyítottan nem tartja be valamely kötelezettségét Előfizető tanúsítványának kezelésekor.

A díj visszatérítésére vonatkozó igényt Előfizetőnek a tanúsítvány kibocsátását, illetve megújítását követő 30 naptári napon belül a regisztrációt végző ügyfélkapcsolati irodánál kell beadnia Szolgáltató részére. A kérvény pozitív elbírálása esetén a Szolgáltató a tanúsítványt díjmentesen visszavonja és a fenntartási díjat az Előfizető számára a megjelölt bankszámlaszámra 20 naptári napon belül visszautalja, vagy részére új tanúsítványt bocsát ki.

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

A Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

9.2. Anyagi felelősség és annak korlátai

A Szolgáltató anyagi felelősségéről és annak korlátairól a {Sz25} Általános Szerződési Feltételek (ÁSZF-PKI) rendelkezik.

9.3. Bizalmasság – Adatkezelési szabályok

9.3.1. Bizalmas információk

Szolgáltató az előfizetői adatokat csakis és kizárólag a szolgáltatásokkal összefüggésben használja fel.

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

a. A fontos bejegyzéseket védi az elveszéstől, tönkretételtől és hamisítástól

b. megfelelő technikai és szervezeti intézkedéseket hoz a személyes adatok felhatalmazás nélküli, illetve törvénysértő kezelése ellen

c. nyilvántartásba veszi az Előfizetővel aláírt szerződést, beleértve az Előfizető hozzájárulását az alábbiakhoz:

- hozzájárulás a szolgáltatások során felhasznált adatok hitelesítés-szolgáltató által történő nyilvántartásba vételéhez
- hozzájárulás a nyilvántartásba vett adatok harmadik félhez történő továbbításához, a Szolgáltató szolgáltatásainak leállítása esetén
- a tanúsítvány közzétételéhez

d. csak annyi bizonyítékot követel meg az azonosításhoz, mely elégséges a tanúsítvány tervezett felhasználásához

e. gondoskodik az Előfizetőre és az Aláíróra vonatkozó adatok bizalmas kezeléséről, kivéve, ha felfedésükhöz ők maguk[14] hozzájárulnak, vagy ha bíróság, illetve egyéb jogi követelmény ezt előírja,

f. védi a regisztrációs adatok bizalmasságát (és sértetlenségét) az Előfizetővel folytatott adatcsere során is

A bizalmasság szempontjából legmagasabb érzékenységi szintet képviselő Aláírók aláírás-létrehozó adatait és a szolgáltatói aláírás-létrehozó adatokat, illetve az ezeket hordozó eszközöket, aktiváló kódokat fokozott biztonsággal kezeli.

A Szolgáltató tevékenysége során a következő bizalmas adatköröket kezeli:

a. a Szolgáltató üzleti titkai

b. az Előfizető Társaságok által a Szolgáltatónak átadott üzleti titkok

c. az Előfizetők és az Aláírók személyes adatai

Az 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 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 9.3.4 pontban meghatározott eseteket.

A Szolgáltató által kezelt adatok egy része a nyilvános kulcs tulajdonosának azonosítása céljából a tanúsítványba foglalva a Szolgáltató tanúsítványtárán keresztül – Előfizető és Szolgáltató ilyen irányú megállapodása esetén - nyilvánosságra kerül, másik részét a Szolgáltató védett módon tárolja az Előfizető és az Aláíró azonosságának igazolása és egyéb adatszolgáltatási kötelezettségei céljából.

9.3.2. Nem bizalmas információk

A Szolgáltató a regisztrációs űrlapon külön jelöli mindazon adatokat, melyek a Tanúsítványtárban hozzáférhető előfizetői tanúsítványban nyilvánosságra kerülnek.

9.3.3. Tanúsítvány visszavonási és felfüggesztési okok felfedése

A Szolgáltató az általa kibocsátott tanúsítványok felfüggesztését és visszavonását tanúsítvány-visszavonási listákban teszi közzé.

A Szolgáltató a tanúsítvány visszavonás okát a vonatkozó szabványok által támogatott módon feltünteti a visszavonási listában. Ezen kívül a visszavonással kapcsolatos minden egyéb adatot bizalmasan kezel.

[14] vagy nevükben az Előfizető

9.3.4. 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 – az Eat. 11.§ paragrafusa alapján adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak.

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

9.3.5. Információszolgáltatás polgári eljárás keretében

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 az Eat. 11.§ paragrafusa alapján.

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

9.3.6. 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 meghatalmazása alapján tárhatja fel harmadik fél részére.

9.3.7. Feltárás más esetekben

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

9.4. 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 Szolgáltató tulajdonát képezik:

a. a visszavonási információk

b. a Szolgáltató által az Aláíró részére kibocsátott egyedi azonosító

c. a Szolgáltató szabályzatai, szerződéses feltételei

d. a tanúsítványban szereplő hitelesítő azonosító

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

A tanúsítványban szereplő megkülönböztető név használatára az Előfizető jogosult.

10. Tevékenységért viselt felelősség és helytállás

10.1. A hitelesítés-szolgáltatói felelősség és helytállás

A Szolgáltató felelősségét a jelen szolgáltatási szabályzat 2.2.1 fejezete, helytállására vonatkozó kötelezettségeit a {Sz25} Általános Szerződési Feltételek (ÁSZF-PKI) tartalmazza.

10.2. Az előfizetői felelősség és helytállás

Az előfizetői felelősség és helytállás mértékére a jelen szolgáltatási szabályzat 2.2.2 fejezete, az előfizetői szerződés és a {Sz25} Általános Szerződési Feltételek (ÁSZF-PKI) előírásai érvényesek.

10.3. Az érintett fél felelőssége

Az érintett fél felelősségét a jelen szolgáltatási szabályzat 2.2.3 fejezete tartalmazza

10.4. Érvényességi időtartam

Jelen szabályzat visszavonásig, illetve egy újabb verzió hatályba lépéséig érvényes.

10.5. Irányadó jog

A Szolgáltató működésére a Magyar Köztársaság törvényei az irányadók.