MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó
Zártkörűen Működő Részvénytársaság

Szolgáltatási szabályzat fokozott biztonságú elektronikus aláíráshoz kapcsolódó hitelesítés-szolgáltatásokhoz és nem-minősített időbélyegzés szolgáltatáshoz (HSZSZ-F)

Verziószám	**6.0**
Objektum azonosító (OID)	**1.3.6.1.4.1.14868.1.1.6**
Hatósági nyilvántartásba vétel napja	**2008. 01. 01.**
Hatósági nyilvántartásba vétel száma	**HL-7691-2/2008f**
Hatálybalépés dátuma	**2008. 01. 01.**

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

HSZSZ verziók

Verzió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2002.09.30	A nem-minősített szolgáltatói regisztrálásra előkészített változat	Bodlaki Ákos		
1.1	2002.11.29	A HIF észrevételeivel javított változat	Bodlaki Ákos		
1.2	2003.03.31.	A nem-minősített szolgáltatás kezdeti gyakorlata alapján javított változat	Bodlaki Ákos		
1.3	2003.07.30	Formai és sajtóhibák javításával, szakértői észrevételek alapján felülvizsgált és javított változat	Néder Ferenc		
2.0	2005.08.19.	Felülvizsgált, átdolgozott változat	Néder Ferenc		
3.0	2007.01.22.	Felülvizsgált, az NHH észrevételei alapján javított, a 2004. évi CXL. törvény (a közigazgatási hatósági eljárás és szolgáltatás általános szabályai) előírásainak megfelelő változat	Néder Ferenc	Kovács Árpád	Hercegh Tamás
4.0	2007.05.29.	Az NHH észrevételei alapján javított változat	Néder Ferenc	Kovács Árpád	Hosszú Sándor István
5.0	2007.09. 04.	Időbélyegzés szolgáltatással bővített változat	Néder Ferenc	Kovács Árpád	Hosszú Sándor István
6.0	2008. 01. 01.	A Szolgáltató adatainak változásával korrigált változat	Néder Ferenc	Juhász György PKI SZE vezető	Hosszú Sándor István vezérigazgató

TARTALOMJEGYZÉK

1. Bevezetés

A MÁV INFORMATIKA Zrt. mint kereskedelmi hitelesítés-szolgáltató 2002. novemberétől nyújt fokozott biztonságú elektronikus aláíráshoz, 2003. áprilisától pedig minősített elektronikus aláíráshoz kapcsolódó hitelesítés-szolgáltatást. A minősített elektronikus aláírás hitelesítés-szolgáltatását 2003. augusztusától minősített időbélyegzés-szolgáltatással, majd 2005. júliusától valósidejű tanúsítványállapot protokoll (OCSP) szolgáltatással egészítette 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 INFORMATIKA Zrt. élve a törvény kínálta lehetőséggel, szolgáltatásai körét 2006. májusától kiterjesztette a Ket. hatálya alá tartozó hitelesítés-szolgáltatásokra.

E dokumentum a MÁV INFORMATIKA Zrt. (továbbiakban Szolgáltató) az [1] (Eat.) hatálya alá tartozó, az Eat. 2. § 15. pontja szerint meghatározott fokozott biztonságú elektronikus aláíráshoz kapcsolódó – nem-minősített – hitelesítés-szolgáltatására valamint a nem-minősített időbélyegzés szolgáltatására 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 jelen szolgáltatási szabályzat a Szolgáltató a következő szolgáltatásaira vonatkozik:

a. elektronikus aláírás hitelesítés-szolgáltatás,

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

c. nem-minősített időbélyegzés-szolgáltatás.

A HSZSZ-F további fejezeteiben a „*szolgáltatások*” kifejezés alatt a fenti részszolgáltatások közül bármelyik vagy azok tetszőleges kombinációja értendő.

1.1 Áttekintés

Jelen HSZSZ-F célja, hogy összefogja azokat a szabályokat, adatokat és információkat, melyeket a Szolgáltató jelen szolgáltatásával valamilyen módon kapcsolatba kerülő feleknek ismerni kell vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát, és lehetővé teszi a szolgáltatást igénybe vevők számára, hogy megállapítsák azt, hogy az ismertetett szolgáltatási gyakorlat, valamint a kibocsátott tanúsítványok és időbélyegek mennyiben felelnek meg az elvárásaiknak. A HSZSZ-F és egyéb, a HSZSZ-F-ben hivatkozott dokumentumok, ajánlások, szabványok tartalmának megismerése után, a tanúsítvány és az időbélyeg felhasználói közösségének (lásd: 1.3.3 pont) egyértelműen meg kell tudni állapítani a tanúsítvány és időbélyeg kezelésének módját, a tanúsítvány és időbélyeg által garantált hitelesség és biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügy garanciákat, jogi felelősségvállalásokat.

Jelen HSZSZ-F általában a [29] {Hitelesítési Rend nyilvános körben kibocsátott nem minősített tanúsítványokra (HR-NMT)} hatálya alá tartozó előfizetői tanúsítványokra vonatkozik.

A közigazgatásban alkalmazható előfizetői tanúsítványok esetében a szabályzat elfogadja a [10] – [16] alatt felsorolt hitelesítési rendeket, az ott rögzített követelményeket a Szolgáltató elfogadja, szolgáltatásaiban érvényesíti. A szabályzat a [10] – [16] alatt felsorolt hitelesítési rendeknek való megfelelőségét a Közigazgatási Gyökér Hitelesítés-szolgáltató a felülhitelesítéssel igazolja.

Jelen szabályzat vonatkozik még a [35] Időbélyegzési Rend követelményei szerint kiadott 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 fokozott biztonságú elektronikus aláíráshoz kapcsolódó hitelesítés-szolgáltatásokhoz és nem-minősített időbélyegzés szolgáltatáshoz*. A jelen dokumentumban és a kapcsolódó szabályzatokban HSZSZ-F-ként történik rá hivatkozás.

Azonosítója:	HSZSZ-F
OID:	1.3.6.1.4.1.14868.1.1.6
Első hatálybalépés időpontja	2002. november 6.

1.3 A szolgáltató és a felhasználói közösség

1.3.1 Szolgáltató adatai

Név: MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Zártkörűen Működő Részvénytársaság

Cégjegyzék szám: 01-10-045838

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

Levélcím: 1253 Budapest Pf. 28

Telefonszám: (36-1) 457-9300

Telefax szám: (36-1) 457-9500

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

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

Illetékes fogyasztóvédelmi felügyelőség:

Nemzeti Fogyasztóvédelmi Hatóság Közép-magyarországi Regionális Felügyelősége

1052 Budapest, Városház u. 7.

Telefon: 318-2681, telefax: 318-1639, Email: *fogyasztovedelem@pest.b-m.hu*

Fogyasztókapcsolati Iroda

1088 Budapest, József krt. 6.

Telefonszám: + 36 1 459 4999, +36 1 459 4836

Ingyenes zöldszám: +36 80 201 205, Telefax: +36 1 303 9075

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 Szolgáltatás honlapján teszi közzé.

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

A központi Ügyfélkapcsolati Iroda munkaidőben elérhető telefonon a +36-1-457-9578 és a +36-1-457-9507 előfizetői közvetlen számon, egyébként a +36 30 633-8666 (üzenetrögzítő is egyben) mobil számon, vagy telefaxon a +36-1-457-9510, vagy a +36 1 457-9509 számon, valamint elektronikus levélben a *hiteles@mavinformatika.hu* címen.

A területi ügyfélkapcsolati irodák címe és elérhetősége a Szolgáltatás 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

1.3.2 A Szolgáltató regiszráló és 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 a szolgáltatásokkal kapcsolatos egyes adminisztrációs feladatokat látják el.

1.3.2.2 Regisztrációs Iroda ("RA")

A Regisztrációs Iroda (rövidítve: RA) a szolgáltatások keretein belül biztosítja az előfizetők technikai regisztrációját, a tanúsítványok felfüggesztés és visszavonás kezelését és az aláírás-létrehozó adat adathordozó eszközre helyezését. Időbélyegzés szolgáltatás igénybe vétele esetén a szolgáltatás hozzáféréséhez biztosít jogosultságot (jellemzően authentikációs tanúsítványt ad ki előfizető részére).

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 a szolgáltatás-támogató informatikai rendszer erőforrásaiból, az ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Feladata az időbélyeget kérő jogosultság-ellenőrzése és az időbélyegek előállítása.

1.3.2.5 Viszontazonosító egység („VIAZ")

A viszontazonosító egység (rövidítve: VIAZ) a Hitelesítő Központ erőforrásaival szorosan együttműködve a viszontazonosítás szolgáltatást támogató informatikai rendszer központi erőforrásaiból, az ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető személyzetből áll. Feladata viszontazonosítás válaszok 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. az Előfizetők informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.),
d. a Ket. hatálya alá tartozó felhasználók, mint fokozott biztonságú aláírást alkalmazó személyek vagy eszközök
e. az érintett felek.

Szolgáltató által kibocsátott időbélyegek felhasználói közössége – a d) pont kivételével - megegyezik a fentiekkel.

1.3.3.1 Előfizető

Az 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 [30] Általános Szerződési Feltételek (továbbiakban: ÁSZF-PKI) tartalmazza.

Az Előfizető mint természetes személy egyben Aláíró is, amennyiben saját maga birtokolja és használja az aláírás-létrehozó adatot.

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

1.3.3.2 Előfizetők informatikai eszközei

Az Előfizetők informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.) rendelkezhetnek fokozott biztonságú aláíráshoz tartozó nem-minősített tanúsítvánnyal. Az informatikai eszköz ebben az esetben magánkulcs felhasználó. Eszközök estében a regisztráció során meg kell nevezni az eszköz üzemeltetéséért felelős személyt (rendszerint a rendszergazdát) is.

Az Előfizetők informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.) időbélyeget is kérhetnek (pl. tranzakciók időpontjának hitelesítése céljából). Az informatikai eszköz ebben az esetben az Előfizető részére kiadott hozzáférési jogosultság – jellemzően authentikációs tanúsítvány magánkulcs – felhasználója.

1.3.3.3 Közigazgatási szervek

A közigazgatási szervek az előfizetők azon csoportja, melyek a [2] Ket. hatálya alá tartoznak [lásd: Ket. 12. § (3) és (4) bekezdés].

1.3.3.4 Aláíró (alany)

Aláíró lehet:

a. bármely természetes személy, aki személyazonosságát a regisztráció során az általa igényelt tanúsítványnak megfelelően, a jelen szabályzat 3.2 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. tetszőleges, elektronikus aláírásra feljogosított informatikai eszköz,
d. a [2] Ket. hatálya alá tartozóan az elektronikus ügyintézésben közreműködő automatizmusok (eszközök)

e. az Aláíró (alany) definíciójára a közigazgatásban alkalmazható tanúsítványok esetében a Szolgáltató elfogadja és alkalmazza az [EHR_Ü], [EHR_ÜA], [EHR_K], [EHR_KA] 1.3.3 és az [EHR+_Ü], [EHR+_K], 1.3.3 pontokat.

1.3.3.5 Érintett fél

a. az Érintett fél (aláírás illetve időbélyeg ellenőrző) olyan természetes személy, aki saját maga vagy az őt megbízó jogi személy képviseletében egy tanúsítvánnyal hitelesített elektronikus aláírásra (illetve időbélyegre) hagyatkozva jár el.

b. az érintett fél definíciójára a Ket. hatálya alá tartozó tanúsítványok esetében a Szolgáltató elfogadja és alkalmazza az [EHR_Ü], [EHR_ÜA], [EHR_K], [EHR_KA] 1.3.4 és az [EHR+_Ü], [EHR+_K], 1.3.4 pontokat.

Az Érintett fél az aláírás ellenőrzése során az Aláíró nyilvános kulcsához tartozó tanúsítvány érvényességi ellenőrzésére hagyatkozva jár el.

Az Érintett fél az időbélyeg ellenőrzése során az időbélyeget aláíró szolgáltatói tanúsítvány érvényességi 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 szabályzatokat és a KGyHSz felügyeleti jogát.

1.4 Tanúsítvány- illetve időbélyeg használat

1.4.1 A szolgáltatás szintje

A Szolgáltató szolgáltatásait jelen szabályozás keretében az [1] Eat. 2.§. 15. pontjában meghatározott **fokozott biztonságú elektronikus aláírás** hitelesítéséhez nyújtja, az időbélyegeket pedig – jelen szabályzat keretében - nem-minősített időbélyegzés-szolgáltatás keretében adja ki.

1.4.2 Tanúsítványok alkalmazhatósága

A tanúsítványok alkalmazhatóságára a következő alapszabályok érvényesek:

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

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

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

Jelen szabályzat hatálya alatt kibocsátott tanúsítványok csak az 1.3.2.5 fejezetben meghatározott Szolgáltató és felhasználó közösség körében használhatók a [30] Általános Szerződési Feltételekben, illetve az előfizetői szerződésben rögzített összeghatárok szerinti korlátokkal.

A tanúsítvány használati lehetőségére vonatkozó fenti információk a tanúsítványban is rögzítésre kerülnek. A tanúsítvány elfogadása, a feltüntetett használati információktól eltérő bármely módú használata az Aláíró és az Érintett fél egyéni felelőssége és kockázata.

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 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 szolgáltatás nyújtásához.

1.4.3 Időbélyegek alkalmazhatósága

Szolgáltató által kiadott időbélyegek fokozott biztonságú elektronikus aláírásokhoz, elektronikus üzenetekhez, tetszőleges elektronikus dokumentumokhoz vagy állományokhoz kapcsolhatók hozzá.

1.5 A szolgáltatási szabályzat adminisztrációja

1.5.1 Szabályzat hatálya

A HSZSZ-F időbeli hatálya a hatálybalépés dátumával kezdődik és határozatlan időre szól. Időbeli hatálya megszűnik egy újabb szabályzat verzió hatályba lépésével vagy a szolgáltatási tevékenység beszüntetésekor.

A HSZSZ-F személyi hatálya a Szolgáltatóra, az előfizetőkre és az aláírókra terjed ki. A HSZSZ-F az érintett felekkel kapcsolatban ajánlásokat fogalmaz meg.

A HSZSZ-F tárgyi hatálya a következőkre terjed ki:

a. az 1. pontban meghatározott szolgáltatásokra,

b. a Szolgáltatónak a fenti szolgáltatásokkal kapcsolatban álló összes objektumára és tárgyi eszközére.

1.5.2 Kapcsolattartó személy

A Szolgáltató részéről a kapcsolattartó személy a PKI szolgáltató egység vezetője. Elérhetőségét a Szolgáltató 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-F karbantartásáért felelős. A szolgáltatási szabályzat hitelesítési rendeknek (illetve időbélyegzési rendnek) való megfeleléséért a Hitelesítési Rend és Szabályozási Csoport, illetve annak vezetője felel. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a változtatásokat életbe lépteti, az új szabályzat verziókat elektronikus aláírással hitelesíti.

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-F-vel kapcsolatos észrevételeket Szolgáltató az Ügyfélkapcsolati Iroda útján fogadja.

1.5.4 Közzétételi és tájékoztatási elvek

1.5.4.1 A HSZSZ-F-ben nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyeztetik: [29], [30]. A Szolgáltató több belső biztonsági és egyéb szabályzattal [24] – [28], operatív szintű előírással rendelkezik [31], [32], melyeket bizalmasan, üzleti titokként kezel.

1.5.4.2 A HSZSZ-F közzététele

A Szolgáltató a HSZSZ-F-t a szolgáltatás internetes honlapján teszi közzé.

1.5.5 Elfogadási eljárások

A jelen HSZSZ-F 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-F-t indokolt esetben, de legalább évente felülvizsgálja.

A szabályzat jogszabályoknak való megfelelőségét a Nemzeti Hírközlési Hatóság (NHH) vizsgálja a HSZSZ-F aktuális változatának hatálybalépését megelőzően.

Módosítás esetén a Szolgáltató a HSZSZ-F változtatásokkal egybeszerkesztett új verziójának tervezetét felülvizsgálat és nyilvántartásba vétel céljából átadja a Nemzeti Hírközlési Hatóság Hivatalának. A Szolgáltató alkalmanként ezt megelőzően is konzultál az NHH-val és/vagy a Közigazgatási Gyökér Hitelesítés-szolgáltatóval a tervezett változtatásairól. A HSZSZ-F új változat hatályba léptetésének feltétele, hogy azt a Nemzeti Hírközlési Hatóság nyilvántartásba vette. A közigazgatásban alkalmazható tanúsítványok kibocsátásának feltétele, hogy a Szolgáltató tanúsítványát a Közigazgatási Gyökér Hitelesítés-szolgáltató felülhitelesítette.

1.6 Meghatározások

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

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

Aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön (eszközellátás): az aláírás-létrehozó eszközök elkészítése és az előfizetők részére történő átadása.

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

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

Alany: egy tanúsítványban azonosított egyed, aki/amely a tanúsítványban szereplő nyilvános kulcsnak megfelelő magánkulcsot birtokolja.

Biztonságos környezet: Olyan fizikai környezet, mely védett illetéktelen hozzáféréstől, és bizonyos mértékig tűz, víz és egyéb katasztrófaeseményektől, egyéb erőszakos behatásoktól.

Címtár (Tanúsítványtár): X. 500 szabvány alapú címtár, amelyben a tanúsítványok, az állapotuk, a visszavonási listák (CRL) rendszeresen frissülnek. Tartalma nyilvánosan elérhető LDAP-al vagy web lapról.

Címtár szolgáltatások: A hitelesítő szervezet a regisztráló szervezeten keresztül fogadja és feldolgozza a Tanúsítványokkal kapcsolatos változások adatait, nyilvántartást vezet a Tanúsítványok aktuális helyzetéről, esetleges felfüggesztéséről, illetve visszavonásáról. Ezeket az információkat, valamint a Tanúsítványokhoz tartozó nyilvános kulcsokat, továbbá a visszavont Tanúsítványok nyilvántartását (CRL) Internet segítségével bárki számára hozzáférhető és folyamatosan elérhető módon közzéteszi a Tanúsítványtárban.

Egyed (entitás): a nyilvános kulcsú infrastruktúra (PKI) autonóm eleme, pl. egy tanúsítványkiadó, regisztrációs szervezet, végfelhasználó vagy eszköz.

Elektronikus aláírás: elektronikusan aláírt elektronikus dokumentumhoz azonosítási célból logikailag hozzárendelt, vagy ahhoz elválaszthatatlanul összekapcsolt elektronikus adat.

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes.

Előfizető: Az a személy vagy szervezet, amely Szolgáltatóval érvényes előfizetői szerződéssel rendelkezik szolgáltatás igénybe vételére, és így a Szolgáltató által kiadott tanúsítvány vagy időbélyeg tulajdonosának tekinthető.

Elsődleges (root) hitelesítő szervezet: az elsőnek létrehozott, fizikailag is működő hitelesítő szervezet, amely az alája rendelt másodlagos hitelesítő központokat hitelesíti,

Érvényességi lánc: az elektronikus dokumentum vagy annak lenyomata, és azon egymáshoz rendelhető információk sorozata, amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített aláírás, illetve időbélyeg, valamint az azokhoz kapcsolódó tanúsítvány az aláírás és időbélyeg elhelyezésének időpontjában érvényes volt.

Érintett fél: Az az entitás (személy/eszköz), aki/amely a magánkulcs felhasználó nyilvános kulcsához tartozó tanúsítvány ellenőrzése alapján egy adott tanúsítványon alapuló nyilvános kulcsú technikára (elektronikus aláírásra) hagyatkozva jár el.

Felhasználó (végfelhasználó): olyan egyed, aki/amely a szolgáltatások keretében előállított kulcsokat és tanúsítványokat és/vagy időbélyegeket rendeltetésüknek megfelelően használja. Felhasználó lehet előfizető, alany (aláíró) vagy érintett fél. Eszköz vagy alkalmazás is lehet felhasználó.

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

Hitelesítő szervezet (CA): a Szolgáltató azon egysége, amely a hitelesítés-szolgáltatás hitelesítő kulccsal folytatott tevékenységét végzi. A CA fizikailag egy telephelyre koncentráltan, védett, biztonságos körülmények között működik.

Hitelesítés-szolgáltatás: az Eat. 6.§ (2) szerint meghatározott szolgáltatás, melynek keretében a hitelesítés-szolgáltató azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat és a tanúsítvány aktuális állapotára (különösen esetleges felfüggesztésére vagy visszavonására) vonatkozó információkat.

Hitelesítés-szolgáltató: elektronikus aláírással kapcsolatos szolgáltatást nyújtó természetes személy, jogi személy vagy jogi személyiség nélküli szervezet. Lásd még: **Szolgáltató**

Igénylő: Az a személy vagy szervezet, amely Szolgáltatóhoz fordul a szolgáltatás igénybe vétele céljából. Az Igénylő előfizetői szerződés megkötése után válik Előfizetővé.

Időbélyegzés: az a folyamat, melynek során az elektronikus dokumentumhoz olyan igazolás (időbélyeg) 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.

Időbélyegzési rend (ISZR): olyan követelmény- és eljárásgyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) időbélyeg felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára.

Közigazgatási Gyökér Hitelesítés-szolgáltató: (KGyHSz): meghatározott feladatokkal és jogosultságokkal rendelkező hitelesítés-szolgáltató (a magyar közigazgatásban használható tanúsítványok hitelesítőinek felülhitelesítő szervezete). A KGyHSz az elektronikus aláírásával hitelesíti a tanúsítványt kibocsátó hitelesítés-szolgáltatók nyilvános kulcsát, és erről közigazgatási kiadói tanúsítványt bocsát ki, azaz a gyökér-tanúsítványkiadó a hierarchia csúcsán áll (aláíró kulcsának kompromittálódása esetén a teljes tanúsítvány lánc hitelességét veszti). A KGyHSz tanúsítvány kiadásával igazolja, hogy az adott hitelesítés-szolgáltató és a tanúsítvány adatai egyeznek, valamint azt, hogy ellenőrizte a megfelelő hitelesítési rend és szolgáltatási szabályzat előírásainak alkalmasságát. Egy felültanúsított hitelesítés-szolgáltató magára nézve kötelezőnek ismeri el a KGyHSz által kiadott szabályzatokat és a KGyHSz felügyeleti, ellenőrzési jogát a tanúsítvány elfogadásával.

Kompromittálódás: Az az eset, amikor a kulcshordozó eszköz használatára arra nem jogosított személy képessé válik.

Kriptográfiai modul: Hardver alapú biztonsági megoldás, amely alkalmas beépített eljárások segítségével biztonságos kulcsgenerálásra és tárolásra.

Kulcshordozó eszköz: Szoftver vagy hardver, melynek segítségével a magánkulcs felhasználó a magánkulcsának felhasználásával az elektronikus állományt aláírja.

Magánkulcs aktiválása: A magánkulcs aktiválása az a folyamat, melynek során a jogosult – különböző azonosító elemek pl. jelszó, PIN kód megadásával – engedélyezi, hogy a leolvasóba helyezett magánkulcs megkezdje üzemszerű működését. Az aktiválás általában a magánkulcsot igénylő környezetben (dokumentum kezelő, levelező rendszer) történik, és érvényes lehet a visszavonásig (deaktiválásig) illetve egyszeri használatra.

Magánkulcs deaktiválása: A magánkulcs deaktiválása az a folyamat, melynek során a magánkulcs üzemszerű működése megszüntetésre kerül. Ez olyan kulcshordozó eszköz esetén, amikor a kulcs üzemszerű működés során nem hagyja el a kulcshordozó eszközt, történhet a kulcshordozó eszköz olvasóból történő eltávolításával, más esetekben a kulcshordozó eszköznek az aláíró környezetből való eltávolításával, vagy az alkalmazásból való kilépéssel.

Nyilvános (publikus) kulcsú infrastruktúra (PKI): Az elektronikus aláírás vagy titkosítás létrehozására, ellenőrzésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.

Produktív hitelesítő szervezet: az elsődleges hitelesítő szervezet által létrehozott logikailag vagy fizikailag létező hitelesítő szervezet, amely egy adott alkalmazási, szervezeti, földrajzi stb. területre ad ki tanúsítványokat.

Regisztráló szervezet: A regisztráló szervezetek a Szolgáltató és a vele szerződése alapon együtt működő Társaságok azon szervezeti egységei, amelyek az előfizetők adatainak regisztrációját, ellenőrzését, az igénylő személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a hitelesítő szervezethez történő továbbítását, és egyéb azonosítási, Tanúsítványmenedzsment és adminisztrációs feladatokat látnak el.

Regisztrációs adatok: Azon információk, adatok összessége, amelyeket a Szolgáltató a Tanúsítványkiadás érdekében az Előfizetőről begyűjt.

Szolgáltatás: 1.) Elektronikus aláíró tanúsítvány hitelesítés-szolgáltatás (röviden: hitelesítés-szolgáltatás) és aláíró magánkulcs előállítása és elhelyezése a kulcshordozó eszközön. Tanúsítvány kibocsátás és publikálás. Tanúsítványkezelés (megújítás, visszavonás, felfüggesztés stb.)
2.) Időbélyegzés szolgáltatás

Szolgáltatási szabályzat: A Szolgáltató szolgáltatási tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.

Szolgáltató: elektronikus aláírással és/vagy időbélyegzéssel kapcsolatos szolgáltatást nyújtó természetes személy, jogi személy vagy jogi személyiség nélküli szervezet.

Tanúsítvány: A Szolgáltató által kibocsátott igazolás, amely a nyilvános kulcsot az elektronikus aláírásról szóló törvény szerint egy meghatározott személyéhez kapcsolja és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget.

Tanúsítványok osztályai: A tanúsítványok megbízhatósága szerinti megkülönböztetés. A kibocsátást megelőző ellenőrző lépések biztonságosságának jelzésére is szolgál (a jelenleg létező osztályok: minősített, nem-minősített, szolgáltatói, teszt).

Tanúsítványtár: lásd: címtár

Tanúsítvány visszavonási lista: Valamely okból visszavont vagy felfüggesztett, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, amelyet a hitelesítés szolgáltató bocsát ki.

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 (év, hó, nap, óra, másodpercben)

1.7 Hivatkozások

A Szolgáltató által nyújtott szolgáltatásokra elsősorban a következő jogszabályok és szabványok mérvadók:

[1] 2001. évi XXXV. törvény az elektronikus aláírásról (a továbbiakban: Eat.)

[2] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (a továbbiakban: Ket.)

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

[4] 194/2005. (IX. 22.) Korm. rendelet a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó követelményekről

[5] 9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról

[6] 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

[7] 4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról

[8] 7/2002 (IV.26) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről

[9] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára

[10] A Közigazgatási Gyökér Hitelesítés-szolgáltató Hitelesítési rendje
(azonosító: [KGyHSz_HR], OID: 0.2.216.1.100.42.1.200.1.0)

[11] Közigazgatási, ügyfélhez kapcsolódó, egységesített hitelesítési rend
(azonosító: [EHR_Ü], OID: 0.2.216.1.100.42.101.5.2.1)

[12] Közigazgatási, ügyfél által működtetett automatizmushoz kapcsolódó, egységesített hitelesítési rend
(azonosító: [EHR_ÜA], OID: 0.2.216.1.100.42.101.6.2.1)

[13] Közigazgatási, köztisztviselőhöz kapcsolódó, egységesített hitelesítési rend
(azonosító: [EHR_K], OID: 0.2.216.1.100.42.101.7.2.1)

[14] Közigazgatási, közigazgatást képviselő automatizmushoz kapcsolódó, egységesített hitelesítési rend
(azonosító: [EHR_KA], OID: 0.2.216.1.100.42.101.8.2.1)

[15] Közigazgatási, ügyfélhez kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend (azonosító: [EHR+_Ü], OID: 0.2.216.1.100.42.101.3.2.1)

[16] Közigazgatási, köztisztviselőhöz kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend (azonosító: [EHR+_K], OID: 0.2.216.1.100.42.101.4.2.1)

[33] 2/2002. (IV. 26) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

[34] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban
a hitelesítés-szolgáltatók által végzett viszontazonosítás protokolljának műszaki specifikációjára

Hivatkozott ajánlások, szabványok:

[17] ITU-T X.509 “Information technology - Open Systems Interconnection - The Directory: Public -key and attribute certificate frameworks” ajánlás 3. verziója

[18] Internet Közösség RFC 2459, RFC 3739, RFC 3161, RFC 3280 és RFC 3647 ajánlásai

[19] ETSI TS 101456, ETSI TS 101861, ETSI TS 101862, ETSI TS 102023 és ETSI TS 102042 szabványok

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

[21] American Bar Association (ABA) PKI Assessment Guidelines (PAG)

[22] a CWA 14167-1, és a CWA 14172-1,-2,-3,-4 CEN Workshop Agreement-ek

[23] MSZ ISO/EC 27001 szabvány

A Szolgáltató hivatkozott dokumentumai:

[24] A MÁV INFORMATIKA Zrt. Szervezeti és Működési Szabályzata

[25] A MÁV INFORMATIKA Zrt. Iratkezelési Szabályzata

[26] A MÁV INFORMATIKA Zrt. Titokvédelmi szabályzata

[27] A MÁV INFORMATIKA Zrt. Adatvédelmi és adatbiztonsági szabályzata
[28] A MÁV INFORMATIKA Zrt. Információbiztonsági szabályzata
[29] Hitelesítési Rend
nyilvános körben kibocsátott nem-minősített tanúsítványokra (HR-NMT)
[30] Általános Szerződési Feltételek a PKI szolgáltatásokhoz (ÁSZF-PKI)
[31] A PKI szolgáltatások biztonsági szabályzata
[32] A PKI szolgáltatások üzletmenet-folytonossági terve
[35] Időbélyegzési Rend nem-minősített időbélyegzés szolgáltatáshoz

Ezeken túlmenően a Szolgáltató az üzleti titkok vonatkozásában az 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról,
A személyes adatok vonatkozásban az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szerint jár el.

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

1.8 Tanúsítványok és időbélyegek jellemzői

A Szolgáltató által jelen szabályozás keretében kibocsátott nem minősített tanúsítványok jellemzőit az 1.7 pontban hivatkozott [10] - [16] és a [29] hitelesítési rendek írják le.

A Szolgáltató által jelen szabályozás keretében kibocsátott nem-minősített időbélyegek jellemzőit a [35] szerinti időbélyegzési rend írja le.

A nem minősített tanúsítvány a CWA 14167-1:2001 szerint az Európai Unió 1999/93. direktívájának (a továbbiakban: direktíva) 5.2 cikkelyével összhangban az aláíró és nyilvános kulcsának összetartozását tanúsítja. A direktíva 5.2 cikkelye kimondja, hogy az Európai Unió tagállamainak biztosítani kell, hogy egy elektronikus aláírás jogi eljárásban nem utasítható vissza, mint törvényesen hatályos és elfogadható bizonyíték csupán azon az alapon, mert az

a. elektronikus formában létezik, vagy mert az
b. nem minősített tanúsítványra alapozott, vagy mert az
c. nem egy akkreditált hitelesítés-szolgáltató által kibocsátott minősített tanúsítványra alapozott, vagy mert azt
d. nem ún. „biztonságos aláírás-létrehozó eszköz”-zel (BALE) hozták létre.

A Szolgáltató által kibocsátott tanúsítványok megfelelnek az Eat. előírásainak, nyilvános körben kerülnek kibocsátásra és olyan Szolgáltató adta ki, amely szerepel az NHH nyilvántartásában.

A tanúsítványok tartalmazzák:

- annak megjelölését, hogy a tanúsítvány nem-minősített tanúsítvány
- a tanúsítványt kibocsátó Szolgáltató és székhelyének (ország-) azonosítóját
- az aláíró nevét (vagy álnevét, 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,
- más személy (szervezet) képviseletére jogosító elektronikus aláírás tanúsítványa esetén a tanúsítvány ezen minőségét és a képviselt személy (szervezet) adatait.

A Szolgáltató által kibocsátott időbélyegek felépítése megfelel az IETF RFC 3161 szabványnak és a jelen szabályzatban meghatározott egyéb követelményeknek a következők szerint:

- tartalmazza a [35] időbélyegzési rend azonosítóját (OID-jét),
- tartalmazza az időbélyeg egyedi azonosítóját,
- tartalmazza a releváns időpontot év, hónap, nap, óra, perc, másodperc értékben
- tartalmazza a kérelmező által elküldött üzenetet (lenyomat)
- tartalmazza a Szolgáltató időbélyegzés céljára kiadott elektronikus aláírását
- az időbélyeg egy olyan névmegadást alkalmaz, amely tartalmazza:
- a Szolgáltató országának nevét (C), a Szolgáltató azonosítóját (CN) és az időbélyeget kibocsátó egység nevét (O, OU)

1.8.1 Tanúsítványok és időbélyegek fajtái, tulajdonságai

A tanúsítványok felhasználási területe és célja szerint megkülönböztetünk:

- előfizetői,
- szolgáltatói és
- teszt tanúsítványokat.

A felhasználási területen belül a következő tanúsítványokat különböztetjük meg:

- „személyes” tanúsítványokat
- „munkatársi” tanúsítványokat
- „szervezeti” tanúsítványokat
- „eszköz” tanúsítványokat.

Az időbélyegeket csak felhasználási területük és céljuk szerint különböztetjük meg:

- előfizetői,
- szolgáltatói és

- teszt időbélyegekre.

1.8.1.1 Előfizetői tanúsítvány, időbélyeg

Előfizetői tanúsítvány (időbélyeg) a Szolgáltatóval szerződéses viszonyban álló Előfizető számára kibocsátott tanúsítvány (időbélyeg).

A [29] szerinti előfizetői tanúsítványok hitelesítési rendjének objektum-azonosítója (OID):

1.3.6.1.4.1.14868.2.1.0

A közigazgatásban alkalmazható előfizetői tanúsítványok hitelesítési rendjeinek objektum-azonosítói:

0.2.216.1.100.42.101.5.2.1 [EHR_Ü]
0.2.216.1.100.42.101.6.2.1 [EHR_ÜA]
0.2.216.1.100.42.101.7.2.1 [EHR_K]
0.2.216.1.100.42.101.8.2.1 [EHR_KA]
0.2.216.1.100.42.101.3.2.1 [EHR+_Ü]
0.2.216.1.100.42.101.4.2.1 [EHR+_K]

Előfizetőknek a [35] szerint kiadott időbélyegek időbélyegzési rendjének objektum-azonosítója:

1.3.6.1.4.1.14868.3.1.1

1.8.1.2 Szolgáltatói tanúsítvány, időbélyeg

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

A szolgáltatói időbélyegeket Szolgáltató saját céljára bocsátja ki az informatikai rendszerének üzemeltetéséhez kapcsolódó egyes időpontok hitelességének biztosítására. Előfizető ezeket nem igényelheti.

A Szolgáltatói tanúsítványok objektum-azonosítója (OID): 1.3.6.1.4.1.14868.2.1.1

1.8.1.3 Teszt tanúsítvány, időbélyeg

A Szolgáltató teszt tanúsítványokat illetve időbélyegeket kizárólag tesztelési célokból ad ki.

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

A Teszt tanúsítványok azonosíthatók az alapján, hogy a tanúsítványok „Common Name" (CN) és „Title" mezőjében megtalálható a 'teszt' vagy 'Teszt' szövegrészlet.

A Teszt tanúsítványok objektum-azonosítója (OID): 1.3.6.1.4.1.14868.2.1.2

A tesztelési céllal kiadott időbélyegek nem különböznek a nem tesztelési célra kiadott időbélyegektől, a megkülönböztetés a felhasználói szinten történik: a teszt időbélyeget kérők azonosítása a számukra kiadott authentikációs tanúsítványuk alapján történik.

1.8.2 Tanúsítványtípusok

A Szolgáltató a Szolgáltatói és Teszt tanúsítványok tekintetében nem alkalmaz típus-megkötést.

A Szolgáltató a következő típusú Előfizetői tanúsítványokat adhatja ki:

1.8.2.1 „Személyes" tanúsítvány

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. A „SubjectAltName" 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 [9] az Informatikai és Hírközlési Minisztérium ajánlása szerinti követelményeknek és a [11] - [16] 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 adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

1.8.2.2 „Munkatársi" tanúsítvány

„Munkatársi" tanúsítványok jogi személy vagy jogi személyiség nélküli szervezet munkatársai, tisztségviselői számára kerülnek kibocsátásra. Az Előfizető ebben az esetben a jogi személy vagy szervezet, az Aláíró pedig a szervezet munkatársa, tisztségviselője.

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 a „SubjectAltName” 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 [9] az Informatikai és Hírközlési Minisztérium ajánlása szerinti követelményeknek és a [11] - [16] 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 adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

1.8.2.3 „Szervezeti” tanúsítvány

„Szervezeti” tanúsítványok jogi személy vagy jogi személyiség nélküli szervezet, illetve annak szervezeti egységei vagy szerepkörei számára kerülnek kibocsátásra. Az Aláíró (alany) ebben az esetben a szervezetet vagy szervezeti egység.

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

A tanúsítvány egyéb adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

Ez a tanúsítvány típus közigazgatási hatósági eljárásban nem alkalmazható.

1.8.2.4 Eszköz tanúsítvány

Eszköz tanúsítványok informatikai eszközök részére kerülnek kibocsátásra. Tipikus eszközök: web szerver, WAP szerver, VPN, stb.

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

Szerver tanúsítványok esetében a tanúsítvány Title mezője a ’szerver’ szöveget tartalmazza.

A tanúsítvány egyéb adatokat is tartalmazhat, különböző kiterjesztés mezőkben.

2. Általános rendelkezések

2.1 Feladatok és hatáskörök

2.1.1 A Szolgáltató feladatai és hatásköre

1. A Szolgáltató gondoskodik a szolgáltatásra vonatkozó valamennyi, a jelen HSZSZ-F-ben részletezett feltétel teljesüléséről, amennyiben azok az adott tanúsítványtípusra, időbélyegre alkalmazhatók.
2. A Szolgáltató szolgáltatásait nyilvánosan elérhetővé teszi.
3. A Szolgáltató jogi személy.
4. A Szolgáltató rendszeresen felülvizsgálja HSZSZ-F-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.
   Időbélyegeket az Előfizetők regisztrációja során a számukra kiosztott hozzáférés jogosultság (authentikációs tanúsítvány) vizsgálatát követően bocsát ki.
6. A Szolgáltató a Tanúsítványtárában teszi közzé az általa kibocsátott, visszavonási listákban a felfüggesztett és visszavont előfizetői tanúsítványokat. A Tanúsítványtár és a visszavonási listák elérhetőségét a Szolgáltató 99%-os rendelkezésre állással biztosítja úgy, hogy az elérhetőség kiesése esetenként nem lépheti túl a 24 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.
   Időbélyegzés szolgáltatás esetén a hozzáférés és az időbélyegek kiadása a szerződéskötést követően legkésőbb 30 naptári napon belül biztosított.
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 listái elérhetőségét, visszavonás kezelési, visszavonási állapot közzétételi szolgáltatását minden érdekelt fél számára. Ügyfélszolgálata útján folyamatos felügyeletet biztosít a tanúsítvány visszavonási és felfüggesztési igények 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 vagy más szabályozásban rögzített, a tanúsítvány felhasználhatóságával kapcsolatos korlátozásokat.
13. A Szolgáltató indokolt esetben felfüggeszti vagy visszavonja a tanúsítvány érvényességét és ezt a szolgáltatás 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 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. Szolgáltató tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel ellátott mentést készít. A mentett adatállományokat védi a jogosulatlan módosítástól, illetve biztosítja, hogy az adatállomány tartalmához jogosulatlan személyek ne férhessenek hozzá, valamint, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.
17. 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.
18. Ha a Szolgáltató ellen felszámolási vagy végelszámolási eljárás indult, a Szolgáltató haladéktalanul tájékoztatja a Hatóságot e tényről, megnevezve az eljárást lefolytató szervezetet.
19. Amennyiben szolgáltatásaihoz kapcsolódó egyes feladatait Szolgáltató kiadja alvállalkozóknak, úgy köteles ezen alvállalkozók ezirányú tevékenységét ellenőrizni. Ez esetben is Szolgáltató felelős elsődlegesen az alvállalkozók tevékenységéért.

2.1.1.1 Az Ügyfélkapcsolati Iroda feladatai és hatásköre

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 kérelmeket.
11. időbélyegzés-szolgáltatás esetén biztosítja az Előfizető részére a szolgáltatáshoz való hozzáférés jogosultságot (jellemzően authentikációs tanúsítványt).

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 igénybe vétele során. Ennek során:

1. az Előfizető a tanúsítvány igénylését és az aláíró eszközének felhasználását úgy végezni, hogy az harmadik fél jogait ne sértse,
2. az Előfizető a regisztráció során a tanúsítvány kiadásához (illetve az időbélyegzés hozzáféréshez) szükséges adatokat ellenőrizni,
3. az Aláíró saját érdekében biztosítani az aláírás-létrehozó eszközének és PIN kódjának védelmét,
4. az Előfizető saját érdekében biztosítani az időbélyegzés hozzáférés titkos adatait (jellemzően az authentikációs tanúsítvány magánkulcsát),
5. az Előfizető az Aláíró figyelmét külön felhívni arra, ha az Előfizetői Szerződés a tanúsítvány felhasználhatóságával kapcsolatban összeg, területi vagy egyéb korlátozásokat tartalmaz,
6. 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,
7. az Előfizető vagy az Aláíró azonnal intézkedni a tanúsítvány visszavonása, illetve felfüggesztése végett, amennyiben
   7.1. tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, tartalmában, a regisztrációs adatokban pontatlanság van, illetve azokban változás következett be,
   7.2. 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,
8. az Aláíró vagy az Előfizető az elektronikus aláírással, időbélyeggel ellátott elektronikus dokumentummal kapcsolatos jogvita megindulásáról köteles haladéktalanul tájékoztatni a Szolgáltatót.

Ezeken kívül:

1. az Aláíró jogosult arra, hogy a magánkulcsot birtokolja és a jogszabályokban meghatározott módon elektronikus aláíráshoz saját, illetve szervezete nevében 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-F-nek, valamint a hatályos jogszabályi rendelkezéseknek megfelelően használhatja.

2.1.3 Az Érintett félre vonatkozó ajánlások

2.1.3.1 Az Érintett fél számára ajánlott az aláírás ellenőrzése 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 (Szolgáltató) kilétéről;
   1.2. a 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.

2.1.3.2 Az Érintett fél számára ajánlott az időbélyeg ellenőrzése során

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

a. Azonosítani az aláíró szervert az időbélyeget aláíró kulcshoz tartozó tanúsítványban feltűntetett azonosító alapján; egyúttal ellenőrizni az aláíró szerver tanúsítványának érvényességét a tanúsítványban megadott adatok alapján.

Továbbá ajánlott elvégeznie a teljes tanúsítási lánc ellenőrzését az alábbiak szerint:

b. meggyőződni az aláíró szerver tanúsítványát kibocsátó szolgáltató kilétéről a kibocsátó szolgáltató azonosítója alapján

c. meggyőződni az aláíró szerver tanúsítványának integritásáról a kibocsátó szolgáltató szolgáltatói tanúsítványának segítségével

d. ellenőrizni az aláíró szerver tanúsítványának és szolgáltató szolgáltatói tanúsítványának állapotát a tanúsítvány visszavonási listák (CRL[1]) áttanulmányozásával

Nem szabad elfogadni az időbélyeget, ha az aláíró szerver tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata annak érvénytelenségére utal.

2.2 Felelősségek

2.2.1 A Szolgáltató felelőssége

A Szolgáltató azzal, hogy aláír egy, a jelen HSZSZ-F szerint meghatározott tanúsítványt – és ezzel jelzi a felhasználó közösség és az érintett felek felé ezen HSZSZ-F használatát – azért vállalja a felelősséget, hogy a tanúsítvány előállítása, kibocsátása, közzététele, visszavonása és a Visszavonási Lista közzététele tevékenységek a jelen HSZSZ-F-ben előírtaknak teljes mértékben megfelelnek, és a Szolgáltató megteszi a szükséges intézkedéseket ahhoz, hogy a Szolgáltató maga és az előfizetők is a jelen HSZSZ-F előírásainak megfelelően járjanak el.

Hasonlóan, a Szolgáltató azzal, hogy aláír illetve kiad egy időbélyeget, azért vállalja a felelősséget, hogy ezen tevékenysége a jelen HSZSZ-F ezirányú előírásainak és a kapcsolódó Időbélyegzési Rendnek megfelel, az időbélyegzés-szolgáltatása során a vonatkozó jogszabályi és szakmai előírásoknak valamint szabályzatoknak megfelelően jár el.

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 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-F-ben, az ÁSZF-PKI-ben 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 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, időbélyeg a jelen HSZSZ-F-ben előírtaktól eltérő módon kerül felhasználásra. Így a Szolgáltató nem felelős az olyan károkért, melyek abból adódtak, hogy az Érintett fél a tanúsítványok vagy időbélyegek ellenőrzése és felhasználása során nem a hatályos jogszabályok és Szolgáltató jelen HSZSZ-F-je 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 szolgáltatási tevékenysége vonatkozásában.

[1] **CRL:** Certificate Revocation List, magyarul: tanúsítvány visszavonási lista

2.2.2 Az Előfizető és az Aláíró felelőssége

Az Előfizetőnek felelőssége áll fenn Szolgáltatóval szemben, a regisztráció során megadott adatainak valódiságával kapcsolatban.

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

Az Előfizető vagy az Aláíró köteles haladéktalanul tájékoztatni a Szolgáltatót:

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 aláírás-létrehozó adatnak illetéktelen személy tudomására jutásáról vagy elvesztéséről;

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

d. a tanúsítvánnyal ellátott elektronikusan aláírt elektronikus dokumentummal kapcsolatos jogvita megindulásáról.

Az Előfizető és / vagy 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 magánkulcs hordozó elvesztéséből, vagy a kulcs biztonságának egyéb módon történő sérüléséből, elvesztéséből, illetve a PIN kód illetéktelen tudomásra jutásból származó károkért.

2.2.3 Az Érintett fél felelőssége

Érintett fél felelőssége fennáll a tanúsítvány vagy időbélyeg elfogadásából fakadó bármely következmény és kár esetén, ha a tanúsítvány vagy időbélyeg érvényességének ellenőrzése során nem az irányadó jogszabályok szerint és nem a tőle elvárható gondossággal jár el.

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

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

A HSZSZ-F csak a Szolgáltató részéről, írott és aláírással hitelesített formában módosítható.

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

2.3.2.2 Megszűnés

A HSZSZ-F a Szolgáltató fokozott biztonságú elektronikus aláíráshoz kapcsolódó nem-minősített hitelesítés-szolgáltatásának vagy nem-minősített időbélyegzés szolgáltatásának befejezésével tekintendő megszűntnek.

2.3.2.3 Értesítések

A Szolgáltató az Előfizetőket és Érintett feleket tipikusan a szolgáltatás Internetes honlapján történő közzététellel, illetve az ügyfélkapcsolati irodákban hozzáférhető 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 ügyfélfogadási időben személyesen vagy telefonon, postai úton írásban, e-mail-ben vagy faxon.

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 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 szolgáltatás internetes honlapján keresztül érheti el a Tanúsítványtár adatait.

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

2.4.1.2 Viszontazonosítás adatbázisa

A viszontazonosítás céljára kialakított adatbázis személyes adatokat tartalmaz, ezért annak védelmét a Szolgáltató az 1992. évi LXIII. törvény rendelkezései szerint biztosítja. Az adatbázisra vonatkozó védelmi intézkedéseket és szabályokat a [31] biztonsági szabályzata tartalmazza.

2.4.1.3 Naplók, regisztrációs adatok

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

2.4.1.4 Az adatbázisok elérésének szabályozása

A Szolgáltató minden Előfizető és érintett fél számára elérhetővé teszi a szolgáltatás 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 illetve időbélyegek és az azokhoz kapcsolódó kikötései és egyéb feltételei az előfizetők és az érintett felek rendelkezésére álljanak. Ezek közé tartoznak különösképpen:

a. a hitelesítési rendek
b. az időbélyegzési rend
c. a tanúsítványok illetve időbélyegek használatára vonatkozó ismertetők, szabályzatok, nyomtatványok
d. a kibocsátott előfizetői és szolgáltatói tanúsítványok
e. a felfüggesztett és visszavont előfizetői és szolgáltatói tanúsítványok
f. szolgáltatói közlemények

A Szolgáltató a szolgáltatói információkat elektronikus formában a szolgáltatás Internetes honlapján keresztül teszi elérhetővé. Hitelesnek csak a Szolgáltató saját elektronikus aláírásával ellátott dokumentumai tekinthetők.

Hiteles dokumentumaihoz a Szolgáltató az Ügyfélkapcsolati Irodáiban is hozzáférést biztosít.

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 illetve időbélyegző egységek 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 frissíti és teszi közzé, azaz két kibocsátás között legfeljebb 24 óra telhet el.

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

3. Azonosítási eljárások

3.1 Megnevezési konvenciók

3.1.1 Nevek típusa

A tanúsítványban szereplő név (betű-, szóköz- és ékezet-helyesen) megegyezik 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[2] 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 megegyezik 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 Szolgáltató a személyazonosság igazolására elfogadott hatósági személyazonosító igazolványban foglalt névtől eltérő nevet álnévként kezel és rögzít.

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 ([EHR_Ü], [EHR_ÜA], [EHR_K], [EHR_KA] 3.1.1 és az [EHR+_Ü], [EHR+_K], 3.1.1 pontok):

Természetes személy alany esetében a személyazonosság igazolására elfogadott hatósági igazolványban (személyi igazolvány, 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.

3.1.5 Álnevek használata

Az Előfizetőnek álnévre való igényét a regisztrációs űrlapon, az ott rendszeresített módon kell jeleznie.

Álnév használata esetén a CN mezőben található szöveg ’~’ (tilde) karakterrel kezdődik és végződik (pl. CN= „~LudasMatyi~”).

[2] „Information Technology - Open Systems Interconnection - The directory: Overview of concepts, models and services”

A közigazgatásban alkalmazható tanúsítványok DN mezőiben csak valós nevek szerepelhetnek, álnév használata kizárt.

3.1.6 Védjegyek elismerésének 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:

1. Az Előfizető kitölti vagy kitölteti a regisztrációs űrlapot és az Ügyfélkapcsolati Iroda részére átadja személyesen vagy megküldi (elektronikus) levélben,
2. a regisztrációs űrlap elfogadásával Szolgáltató gondoskodik az Előfizetői Szerződés előkészítéséről és intézkedik az előfizetői kulcspár és tanúsítvány elkészítésére,
3. 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.

3.2.1 Az aláírás-létrehozó adat birtoklás ellenőrzésének módszere

Ha az Aláíró számára az aláírás-létrehozó és aláírás-ellenőrző adat (kriptográfiai kulcspár) előállítása a Szolgáltatás keretében a Szolgáltató által történik, akkor a kulcspár generálása a Szolgáltató Hitelesítő Központjában, fokozott biztonságú környezetben történik.

A Szolgáltató a kriptográfiai kulcspárt kiemelt biztonságú környezetben állítja 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. Az aláírás-létrehozó eszköz személyes átvételénél az Előfizető aláírásával igazolja az aláírás-létrehozó eszköz és a PIN kód átvételét.

Előfizető vagy Aláíró által készített kulcspár használta esetén az Előfizető köteles az aláírás-ellenőrző adathoz tartozó aláírás-létrehozó adat birtoklását a regisztráció során a Szolgáltató számára hitelt érdemlően bizonyítani. Ennek hiányában a Szolgáltató a kért tanúsítvány kiállítását megtagadja.

3.2.2 Regisztráció „Személyes” tanúsítvány igénylése esetén

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

1. név,
2. álneve, amennyiben annak megjelölésére az Előfizető igényt tart,
3. személyazonosítására használt okmány száma (személyi igazolvány, jogosítvány vagy útlevél szám),
4. lakcím,
5. anyja neve,
6. születési hely és idő,
7. e-mail cím,
8. amennyiben az aláírás-létrehozó adatot az Előfizető hozta létre, úgy az ahhoz tartozó aláírás-ellenőrző adat azonosítója vagy lenyomata.

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.

A közigazgatási hatósági eljárásban használható tanúsítványok esetében a személyes megjelenés kötelező, az Aláíró természetes személyt az Ügyfélkapcsolati Iroda személyazonosító igazolvány (személyi igazolvány, jogosítvány vagy útlevél) személyes bemutatásával azonosítja.

Az Ügyfélkapcsolati Iroda a bemutatott személyazonosító igazolvány érvényességét és hitelességét ellenőrzi (lásd: 3.2.9. 1. pont).

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

3.2.3 Regisztráció „Munkatársi” tanúsítvány igénylése esetén

Jogi személy vagy jogi személyiség nélküli szervezet, mint Előfizető a regisztrációs űrlap kitöltésével igényelhet tanúsítványt. A regisztrációs űrlapon a következő adatokat lehet, illetve kell megadni:

1. Az Előfizető tekintetében:
   1.1. az Előfizető szervezet neve, székhelye
   1.2. az Aláíró(k) kijelölését engedélyező, a cég- vagy szervezet képviseletére jogosult személy neve, beosztása, munkahelyi telefonszáma, fax-száma, e-mail címe
2. A kapcsolattartó tekintetében:
   2.1. a kapcsolattartó neve, beosztása, telefonszáma és e-mail címe
3. Az Aláíró(k) tekintetében:
   3.1. annak a szervezeti egységnek a megnevezése, ahol az Aláíró dolgozik,
   3.2. annak a szervezeti egységnek a telephelye, ahol az Aláíró dolgozik
   3.3. Aláíró neve
   3.4. Aláíró álneve, ha annak megjelölésére az Aláíró igényt tart és azt számára az Előfizető engedélyezte
   3.5. az Aláíró beosztása
   3.6. az Aláíró azonosítására használt személyazonosító igazolvány száma
   3.7. az Aláíró anyja neve, születési helye és ideje,
   3.8. az Aláíró telefonszáma,
   3.9. az Aláíró e-mail címe
   3.10. ha az aláírás-létrehozó adatot az Aláíró hozta létre, úgy az ahhoz tartozó aláírás-ellenőrző adat azonosítója vagy lenyomata

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

Az Előfizető nevében eljáró, a cég- vagy szervezet képviseletére jogosult személy képviseleti jogát az Előfizetőnek a regisztráció során igazolnia kell.

A szolgáltatási szerződés megkötése során az Előfizető szervezet kapcsolattartót nevezhet meg a Szolgáltató részére, aki aláírási joggal rendelkezik a tanúsítványok kibocsátását illetően; a Szolgáltató később e személynek az aláírását fogadja el bármilyen kérelem vagy bejelentés esetén. A Szolgáltató ez esetben jogosult a kapcsolattartó azonosítás-hitelesítését személyazonosítói igazolvány személyes bemutatásával elvégezni.

Az Aláíró(k) azonosítása az Ügyfélkapcsolati Irodán a személyazonosító igazolvány bemutatásával személyesen történik. A Szolgáltató eltekint a személyes megjelenéstől és az aláíró azonosításától abban az esetben, ha az Előfizető a tanúsítványt cégszerűen aláírt megrendelőn kéri. A Szolgáltató az aláíró azonosításához kapcsolódó minden felelősséget ebben az esetben az Előfizető szervezetre hárítja. A Szolgáltató felelőssége ebben az esetben is az adatok teljeskörűségének ellenőrzése, illetve annak eldöntése, hogy a rendelkezésre álló adatok alapján a tanúsítvány kibocsátható.

A Szolgáltató a regisztrációs űrlapot minősített aláírással ellátott elektronikus dokumentumként is elfogadja abban az esetben, ha az Előfizetővel erről előzetesen megegyezett.

A közigazgatási hatósági eljárásban használható tanúsítványok esetében a személyes megjelenés kötelező, az Aláíró természetes személyt az Ügyfélkapcsolati Iroda személyazonosító igazolvány (személyi igazolvány, jogosítvány vagy útlevél) személyes bemutatásával azonosítja.

Az Ügyfélkapcsolati Iroda a bemutatott iratok és okmányok érvényessége és hitelessége, valamint az aláírási jogosultság ellenőrzése céljából adategyeztetést végez (lásd: 3.2.9. pont).

A Szolgáltató megtagadhatja a tanúsítvány kibocsátását, ha a bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel.

3.2.4 Regisztráció „Szervezeti" tanúsítvány igénylése esetén

Jogi személy vagy jogi személyiség nélküli szervezet, mint Előfizető a regisztrációs űrlap kitöltésével igényelhet tanúsítványt. A regisztrációs űrlapon a következő adatokat lehet, illetve kell megadni:

1. Az Előfizető tekintetében:
   1.1. az Előfizető szervezet neve, székhelye, e-mail címe
   1.2. az Előfizető szervezet képviseletére jogosult személy neve, beosztása, munkahelyi telefonszáma, fax-száma, e-mail címe
2. A kapcsolattartó tekintetében:
   2.1. a kapcsolattartó neve, beosztása, telefonszáma és e-mail címe
3. Az Aláíró (alany) tekintetében:
   3.1. a szervezeti egység megnevezése
   3.2. a szervezeti egység telephelye
   3.3. az aláíró szerepköre (beosztása)

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

Az aláíró azonosításának céljára a Szolgáltató elfogadja a cégszerűen aláírt tanúsítvány igénylési kérelmet.

A Szolgáltató az aláíró azonosításához kapcsolódó minden felelősséget ebben az esetben az Előfizető szervezetre hárítja. A Szolgáltató felelőssége ebben az esetben is az adatok teljeskörűségének ellenőrzése, illetve annak eldöntése, hogy a rendelkezésre álló adatok alapján a tanúsítvány kibocsátható.

A Szolgáltató a regisztrációs űrlapot minősített aláírással ellátott elektronikus dokumentumként is elfogadja abban az esetben, ha az Előfizetővel erről előzetesen megegyezett.

A Szolgáltató megtagadhatja a tanúsítvány kibocsátását, ha a bemutatott dokumentumok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel.

3.2.5 Regisztráció „Eszköz" tanúsítvány igénylése esetén

Eszköz tanúsítvány regisztrációs űrlap kitöltésével igényelhető. Az eszköz azonosításához a következőben megadott adatokat kéri az Ügyfélkapcsolati Iroda.

Természetes személy által igényelt eszköz-tanúsítvány esetén:

1. az Előfizető személyes adatai a 3.2.2 pont szerint,
2. az eszköz tanúsítványban feltüntetendő neve,
3. az Előfizető írásos nyilatkozata az eszköz birtoklásáról.

Jogi személy vagy jogi személyiség nélküli szervezet által igényelt eszköz-tanúsítvány esetén:

1. az Előfizető szervezet azonosításához szükséges adatok a 3.2.3 pont szerint,
2. az eszköz tanúsítványban feltüntetendő neve,
3. az Előfizető szervezet írásos nyilatkozata az eszköz birtoklásáról.

A regisztrációs űrlapon szereplő adatok ellenőrzése, az azonosítás rendje a 3.2.2 illetve 3.2.3 pontokban feltüntetett módon történik.

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

A Szolgáltató megtagadhatja a tanúsítvány kibocsátását, ha a regisztráció során kétsége merül fel az eszköznek az Előfizetőhöz tartozásával kapcsolatban.

3.2.6 Szervezet azonosítása közigazgatásban alkalmazható tanúsítványok igénylése esetén

a) Ha az ügyfél (Előfizető) 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.

b) Ha az ügyfél (Előfizető) által működtetett automatizmus tanúsítványában jelezni kívánják, hogy az egy adott szervezethez tartozik, akkor a regisztrációhoz az előfizető személynek, vagy az előfizető szervezetet képviselő igénylőnek 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.

c) 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 Szolgáltatónál előforduló ügyekben eljárjon, mely meghatalmazás egyúttal a szervezet azonosságát is hitelesíti. A természetes személynek külön is azonosítani kell magát a 3.2.7 pont szerint.

d) Egy közigazgatást képviselő automatizmus tanúsítványában szerepeltetni kell, hogy az automatizmus mely szervezethez tartozik. A regisztrációhoz az előfizető szervezetet képviselő igénylőnek 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.

3.2.7 Egyén azonosítása közigazgatásban alkalmazható tanúsítványok igénylése esetén

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.

j) Az ügyfelek által működtetett automatizmusok számára történő tanúsítvány kibocsátást megelőző regisztrációt az alábbiak kezdeményezhetik:

- maga az ügyfél, ha az automatizmus őt képviseli,
- ha az automatizmus egy szervezetet képvisel, a szervezetet képviselő természetes személy a Szolgáltató előtt, ha a regisztrációhoz magával viszi a szervezet által kiállított és közokiratba foglalt, a szervezet nevét tartalmazó, a szervezet képviseletére feljogosító meghatalmazást.

k) A közigazgatást képviselő automatizmusok számára történő tanúsítvány kibocsátást megelőző regisztrációt az alábbiak kezdeményezhetik:

- a hatóságot képviselő természetes személy a Szolgáltató előtt, ha a regisztrációhoz magával viszi a hatóság által kiállított és közokiratba foglalt, a közigazgatási szerv nevét tartalmazó, a hivatal képviseletére feljogosító meghatalmazást.

3.2.8 Regisztráció időbélyegzés szolgáltatás esetén

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. Időbélyegzés szolgáltatás esetén, a regisztráció során az Előfizető (igénylő) kezdeti azonosítását (személyes és/vagy céges adatainak ellenőrzését) kell elvégezni, személyazonosításra alkalmas igazolvány és/vagy céges hivatalos iratok alapján. Ennek célja a szerződésben foglalt adatok ellenőrzése, valamint igény esetén[3] az időbélyegzéshez kapcsolódó authentikációs tanúsítvány kiadásához szükséges adatok ellenőrzése.

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

Szervezeti előfizető azonosításához egy cégszerűen aláírt megrendelő bemutatása szükséges.

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 céges iratokból a szervezet kiléte nem állapítható meg minden kétséget kizáróan.

3.2.9 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.) Nem-minősített időbélyegzés szolgáltatás regisztrálásakor a Szolgáltató az adategyeztetéstől eltekinthet.

[3] Az időbélyegzés szolgáltatás hozzáféréséhez kliens authentikációs tanúsítvány szükséges az Előfizető oldalán, amivel Előfizető vagy már rendelkezik, és akkor ezt be kell mutassa Szolgáltató részére, vagy igény esetén Szolgáltató biztosít ingyenesen Előfizető részére a szolgáltatás keretében

3.2.10 Együttműködési képességek

a. A Szolgáltató eleget tesz a [10] 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 biztosít. A tesztek során felmerülő kérdések tisztázására a Szolgáltató partnereivel együttműködik.

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

3.2.11 Viszontazonosítás

Elektronikus aláírás közigazgatási felhasználása esetén a Szolgáltató az ***ügyintéző hatóság*** megkeresésére viszontazonosítást végez, melynek keretében:

- a hatóság a Szolgáltatónak megküldi:
  a) a megadott természetes személyazonosító adatokat (vagy azok egy részét)
  b) a viszontazonosítás alapjául szolgáló ellenőrző adatot (tanúsítványt vagy más, a viszontazonosítást végző szervezetnél az ügyfél azonosítására alkalmas adatot), és
  c) a viszontazonosítási kérést azonosító adatot.
- a Szolgáltató összeveti a megadott természetes személyazonosító adatokat az általa kezelt, beazonosított természetes személyazonosító adatokkal, és válaszként megküldi a viszontazonosítást kérő hatóságnak
  a) az adatok egyezőségének vagy annak hiányának tényét, valamint
  b) a viszontazonosítási kérést azonosító adatot.

A 193/2005. (IX. 22.) Korm. rendelet értelmében a közigazgatási hatósági ügyek elektronikus úton történő intézése során az ügyfél előzetes viszontazonosítása szükséges abban az esetben, ha az ügyfél személyes adathoz, illetve adó-, bank-, biztosítási-, vagy értékpapírtitokhoz kíván hozzáférni. A viszontazonosítás során a hatóság az ügyfélről jogszerűen rendelkezésére álló és a viszontazonosítást végző Szolgáltató által kibocsátott tanúsítvány kibocsátásakor ténylegesen rögzített személyazonosító adatok egyezőségét ellenőrzi.

A viszontazonosítási szolgáltatást a Szolgáltató automatikusan hajtja végre az Informatikai és Hírközlési Minisztérium ajánlása [34] szerinti eljárás alapján.

A kérelem szabványos formátumú elektronikusan aláírt üzenet formájában az arra jogosult célrendszer felől érkezik. A kérés fogadása után a Szolgáltató:

a. ellenőrzi a kérő fél jogosultságát, és a kérés elektronikus aláírását,

b. elvégzi az üzenet szintaktikai ellenőrzését,

c. ellenőrzi az ügyfél tanúsítványát,

d. nem jogosult kérő, nem értelmezhető kérés vagy nem megfelelő tanúsítvány-tartalom esetén visszaküldi a kapott üzenetet a megfelelő hibaválasszal,

e. elfogadható kérés esetében elvégzi az összehasonlításokat, saját adatbázisában a keresést, összeállítja a választ, ellátja elektronikus aláírásával, és visszaküldi a célrendszernek.

A Szolgáltató IGEN választ ad, ha a megadott természetes személyazonosító adatok és az ellenőrző által kezelt természetes személyazonosító adatok az alkalmazott tolerancia szabályok alapján megegyeznek.

Egyéb esetben a Szolgáltató NEM választ ad. NEM válasz esetén a kért szolgáltatás nem vehető igénybe, ha az viszontazonosításhoz kötött.

A szolgáltatást kérő célrendszernek a viszontazonosításhoz az alábbiak megadása kötelező:

a. viselt név vagy születési név (családi név, első utónév)

b. anyja születési neve (családi név, első utónév)

c. születési helye (születés település neve)

d. születési ideje

e. tanúsítvány adatok

A viszontazonosítást kérő célrendszer a viselt név helyett – amennyiben az rendelkezésére áll – a születési nevet is megadhatja a viszontazonosítás során.

Az összehasonlítás előtt a kérésben és a nyilvántartásban lévő adatokra az ellenőrzés algoritmusában az alábbi tolerancia elemek kerülnek alkalmazásra:

Nevek (viselt név, születési név, anyja neve) összehasonlításakor:

a. szóközök és egyéb speciális karakterek kivágása,

b. nagybetűkké konvertálás,

c. a doktorjelzők szűrése a családnevekből (dr, dr., Dr, Dr., DR, DR.),

d. az ékezetes betűk teljes körű helyettesítése ékezetmentes betűpárjaikkal (á-a, ä-a, é-e, í-i,

e. ó-o, ö-o, ő-o, ú-u, ü-u, ű-u, Á-A, Ä-A, É-E, Í-I, Ó-O, Ö-O, Ő-O, Ú-U, Ü-U, Ű-U).

A születés településnevének összehasonlításakor:

a. nagybetűkké konvertálás,

b. településnevek levágása balról az első szóköznél.

Az alkalmazott toleranciaszint így megegyezik az ügyfélkapun keresztül azonosított felhasználók viszontazonosításánál alkalmazott megoldással.

Az elektronikusan aláírt dokumentumok kezelése, az aláírás kezdeti és utólagos ellenőrzése, időbélyegzése a viszontazonosítástól függetlenül történik.

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 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 regisztrációs eljárást. Az űrlap nyomtatott vagy elektronikus formában igényelhető az Ügyfélkapcsolati Irodánál, vagy elektronikus formában letölthető a Szolgáltatás Internetes honlapjáról.

Az Előfizetői Szerződés aláírásával Előfizető egyúttal nyilatkozik arról is, hogy a Szolgáltató feltételei és kikötései, valamint saját kötelezettségei vonatkozásában tájékozódott, 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 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 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 (lásd: 6.1.3. pont), vagy
b. a Szolgáltató postai úton eljuttatja az Előfizető által megadott címre, vagy
c. az Előfizető letölti a Szolgáltató nyilvános Tanúsítványtárából
d. A közigazgatásban alkalmazható tanúsítványok esetében a 194/2005. (IX. 22.) Korm. rendelet 7. § (7) bekezdése értelmében, ha a regisztrációt végző szervezet az aláírás-létrehozó eszközt nem a regisztrációt követően azonnal, ugyanazon a helyszínen adja át az igénylőnek, - ideértve azt is, ha az átadást más elektronikus aláírással kapcsolatos szolgáltató végzi - az aláírás-létrehozó eszköz átadását megelőzően az átvételre jogosultságot a regisztrációnál szokásos eljárásnak megfelelően kell igazolni.

4.4 Tanúsítvány elfogadás

A tanúsítvány elfogadása az Előfizető részéről az átvétellel történik meg.

Az aláírás-létrehozó adat használatba vétele előtt az Előfizető (Aláíró) kötelessége ellenőrizni a tanúsítványban feltüntetett 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 jelen szolgáltatási szabályzat és az általános szerződési feltételek elfogadását is jelenti.

4.4.1 Tanúsítvány közzététele a 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.

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 megfelelő 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, ajánlott a kulcspár megfelelő használatát és a hozzá tartozó tanúsítványt az adott helyzetben tőle általában elvárható gondossággal ellenőriznie:

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 ellenőriznie 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 ellenőriznie azt a 2.1.3.2 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** Előfizetői tanúsítványok érvényességi ideje 1 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 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.

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 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 állomány megsérült

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 Tanúsítvány visszavonás és felfüggesztés

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 után (lásd: 4.9.7.1 pont) állapotát újra érvényesre kell állítani, vagy a tanúsítványt vissza kell vonni.

A felfüggesztési és visszavonási kérelmeket az Ügyfélkapcsolati irodák fogadják nyitvatartási időben. A 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/felfüggesztéshez vezető körülmények

1.) A Szolgáltató indokolt esetben felfüggeszti vagy visszavonja a tanúsítványt ha:

a. az Előfizető vagy az Aláíró ezt kéri
b. a Nemzeti 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

2.) 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.

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

3.) 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 hitelesítési szolgáltatás megszűnése
i. a Szolgáltató valamely szolgáltatói magánkulcsának kompromittálódása.

4.9.2 Visszavonás kérelmezése

Tanúsítvány visszavonását az előző pontban feltüntetett körülmények alapján az Aláíró, az Előfizető vagy azok képviselője, a Szolgáltató, a Nemzeti 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 a visszavonási igényét akadályoztatása miatt személyesen nem tudja bejelenteni vagy 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 bejelentőnek a felfüggesztett tanúsítvány visszavonására az ettől számított 5 napon belül kell intézkednie.

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 körülmények

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 igény 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).

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 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 tanúsítvány-

állapot 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 4.9.5.1 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. Amennyiben 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 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 ajánlott meggyőződniük a tanúsítvány visszavonási információ hitelességéről is.

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

4.9.9 Visszavonási listák (CRL) és kibocsátásuk gyakorisága

A visszavonási listákban 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 listák 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 leghosszabb idő

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

4.9.11 Visszavonási listák ellenőrzése

A visszavonási listák ellenőrzése az érintett felek felelőssége a tanúsítványok elfogadását megelőzően. A tanúsítványhoz tartozó visszavonási lista elérhetőségét a tanúsítvány tartalmazza. A lista ellenőrzésének arra kell vonatkozni, hogy a kérdéses tanúsítványt a lista tartalmazza-e (és ha igen, milyen időponttól), a lista hiteles és sértetlen, s a kérdéses tranzakció szempontjából időben releváns-e.

A tanúsítvány visszavonási listában a Szolgáltató által közzétett érvénytelen, vagy felfüggesztett tanúsítvány elfogadásából keletkező bárminemű kár Érintett felet terheli. (Lásd még a 2.2.3 pontot.)

4.9.12 Valósidejű tanúsítványállapot-ellenőrzés

A Szolgáltató valósidejű tanúsítványállapot-ellenőrzést (OCSP szolgáltatást) nem szolgáltat.

4.9.13 Visszavonási állapot közlés más formái

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

4.9.14 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 3.2.8 pontban leírt egyszerűsített eljárással kell elvégezni.

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

4.11.2 Az időbélyegzés szolgáltatás szintje

Az időbélyegben megadott idő 1 másodpercen belüli pontosságot biztosít az UTC[4] 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] **UTC:** Coordinated Universal Time, az ITU-R TF.460-5 ajánlás szerint definiált, másodperc felbontású időalap

4.11.3 Az időbélyegzés kérelmek teljesítés

Időbélyegzés iránti kérelmet (időbélyeg kérést) Előfizető erre feljogosított5 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.

Az időbélyeg kérés jóváhagyása vagy visszautasítása az Előfizetők regisztrációja során a számukra kiosztott hozzáférés jogosultság (authentikációs tanúsítvány) vizsgálata alapján 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 RFC3161 szerinti időbélyeg válasz elküldésével valósul meg

A kiadott időbélyegek kapcsán Szolgáltató biztosítja, hogy az időbélyegző válasz, az időbélyegzéssel összefüggésben hozzáadottaktól eltekintve, ugyanazokat az adatokat tartalmazza, amelyeket a kérelem tartalmazott

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 ellenőrzésezése

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

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

5. Fizikai, eljárásrendi és humán biztonsági szabályozások

A Szolgáltató az elfogadott szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések és az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazza. A Szolgáltató kockázat elemzést végzett üzleti kockázatainak felmérése, valamint a szükséges biztonsági követelmények és működési eljárások meghatározására. A Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja.

A biztonságkezelési szabályokat a Szolgáltató társasági szintű informatikai biztonságpolitikája [27] és biztonsági szabályzata [28] tartalmazza. A Szolgáltató szolgáltatást támogató informatikai rendszere vonatkozásában a PKI szolgáltatások biztonsági szabályzata [31] érvényesül. Ez a szabályzat szervezeti egység szinten és munkakörökre lebontva rögzíti a biztonságkezeléssel összefüggő feladatokat, felelősségeket és szabályokat, így többek között a bizalmi munkakörök felsorolását, a kinevezési feltételeket és az összeférhetetlenségi kritériumokat.

A MÁV INFORMATIKA Zrt. rendszeres belső és külső auditjai ezen dokumentumokat és a dokumentumokban a szolgáltatásokra vonatkozó előírások teljesülését a szolgáltatás évente esedékes ellenőrzései során vizsgálja.

A szolgáltatást támogató informatikai rendszer, annak személyi és fizikai környezete megfelel a 2/2002 MeHVM irányelvben rögzített követelményeknek, amely egyértelműen meghatározza a Hitelesítő Központok és a Regisztrációs Iroda informatikai rendszereinek, a szolgáltatás személyi és fizikai környezetének biztonsági követelményeit.

Szolgáltató gondoskodik az informatikai biztonság fenntartásáról azokban az esetekben is, amikor az elektronikus aláírással kapcsolatos szolgáltatások egyes funkcióira vonatkozó felelősség más szervezethez kerülnek kiadásra.

A Szolgáltató felelősséget vállal minden – jelen HSZSZ-F-ben tárgyalt – elektronikus aláírással kapcsolatos szolgáltatásért, még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki. Ilyen eset a nem-minősített időbélyegzés szolgáltatás esetén az időbélyegző egységek üzemeltetésének kiadása alvállalkozó vagy partner részére. Ebben az esetben az alábbiakban leírtakat értelemszerűen kell / lehet alkalmazni az alvállalkozóra.

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 elemeket tartalmazza. A Bizalmi Központban történik a kulcspárok és a tanúsítványok előállítása, a kulcspárok elhelyezése az aláírás-létrehozó eszközre és az aláírás-létrehozó eszközök megszemélyesítése.

5.2 Eljárásrendi szabályozások

A Szolgáltató eljárásrendi szabályait három szabályzat tartalmazza:

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 [31] 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 Szolgáltató a szolgáltatásokhoz a következő bizalmi munkaköröket kapcsolja:

a. a Szolgáltató informatikai rendszeréért általánosan felelős vezető,
b. biztonsági tisztségviselő,
c. rendszeradminisztrátor,
d. rendszerüzemeltető,
e. független rendszervizsgáló,
f. regisztrációs felelős.

Az alábbi táblázatban a szolgáltatásokhoz kapcsolódó munkakörök, azok feladat-, felelősség és hatáskörei kerülnek összefoglalásra.

Munkakör	Feladatkör	Felelősségi kör	Hatáskör
A PKI Szolgáltató Egység vezetője	A Szolgáltató szolgáltatási tevékenységének irányítása	Folyamatos és biztonságos szolgáltatás. A PKI Rendszer működtetésének egyszemélyi felelős vezetője	A Szolgáltató informatikai rendszeréért általánosan felelős vezető. A PKI Szolgáltató Egység 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 felügyelője (biztonsági tisztségviselő)	IB tevékenység irányítása, ellenőrzése a PKI Szolgáltató Egység területén	A szolgáltatás 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 és OCSP 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
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

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 Szolgáltató vezetője által kijelölt bizottság jelenlétében végezhetők az alábbi feladatok:

a. a PKI alkalmazás installálásához szükséges szolgáltatói kulcspárok generálása
b. a hitelesítő központok szolgáltatói tanúsítványaihoz tartozó kulcspárjainak generálása

c. a szolgáltatói nyilvános kulcsokat tartalmazó token Root CA-hoz való továbbítása, illetve a Root CA által kibocsátott tanúsítványok visszaszállítása
d. a Root CA nyilvános kulcsát tartalmazó tokennek a Produktív CA-hoz való továbbítása
e. Root CRL generálás

Továbbá csak két SO együttesen végezheti az alábbi feladatokat:

a. a szolgáltatói magánkulcsok biztonsági mentése
b. a szolgáltatói magánkulcsok mentésből történő visszaállítása
c. a szolgáltatói magánkulcsok (és másodpéldányainak) megsemmisítése
d. 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 csipkártya 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 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 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 kínált szolgáltatáshoz 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 kínált szolgáltatási 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 Szolgáltató Egység vezetője
b. A 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 szerepkörökhöz csak fokozott biztonsági ellenőrzéssel lehet személyt rendelni, amelyhez szükséges a szerepkörre kijelölt személy hozzájárulása, ugyanakkor a fokozott ellenőrzés a szerepkör betöltésének alapfeltétele.

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.

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

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

5.4 Naplózási eljárások

5.4.1 Naplózott esemény típusok

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.

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 A naplók feldolgozásának gyakorisága

A Szolgáltató a hitelesítő központok (CA-k) naplóit naponta, az egyéb napló fájlokat a [31] biztonsági szabályzatában rögzített gyakorisággal dolgozza fel.

5.4.4 Napló adatok tárolása

A napló adatok rendszeresen archiválásra kerülnek ellenőrzés, szükségessé váló visszakeresés és újbóli használat céljából.

5.4.5 A napló fájlok megőrzési időtartama

Lásd: 5.5 Adatok archiválása c. fejezetet.

5.5 Adatok archiválása

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

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 Előfizető által a regisztráció támogatása céljából benyújtott igazolványok és dokumentumok típusa, egyedi azonosító adatai (például a személyazonosító igazolvány száma)

b. az Előfizetői Szerződés másolata

c. a regisztrációs kérelmet elfogadó regisztrációs felügyelő (RO) azonosítója
d. Az 5.4.1 pontban felsorolt összes esemény, illetve napló típus.

5.5.2 Az archívum megőrzési időtartama

A Szolgáltató a tanúsítványokra vonatkozó archív adatokat 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 archívumában olyan fizikai védelmet biztosít, amely fenntartja az archivált adatok bizalmasságát és sértetlenségét.

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.

a. A Szolgáltató biztosítja, hogy mindaddig, amíg az archivált adatokat őrzi, az arra jogosult személyek számára hozzáférhetők és értelmezhetők lesznek.
b. A tanúsítványokra vonatkozó adatokat rendelkezésre bocsátja, ha azokra jogi eljárásokban bizonyíték nyújtása céljából szükség van.
c. Az alanynak, illetve az adatvédelmi követelmények korlátozásain belül az előfizetőnek hozzáférést biztosít az alanyra vonatkozó regisztrációs és egyéb információkhoz.

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 Hírközlési Hatóság a nyilvántartásba vételi eljárás keretében és azt követően – a jogszabályban előírt hatáskörrel – felügyeli többek között a jelen szolgáltatási szabályzat előírásainak a [11] – [16] hitelesítési rendeknek való megfelelőségét.

5.7 A Szolgáltató kulcscseréje

A Szolgáltató szolgáltatói kulcsának tervezett cseréje előtt fél évvel köteles tájékoztatni a Nemzeti 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 Katasztrófa elhárítás

5.8.1 A szolgáltatások azonnali felfüggesztése

A katasztrófa esemény bekövetkezése a szolgáltatások azonnali felfüggesztésével jár. Erről az eseményről Szolgáltató értesíti a Nemzeti Hírközlési Hatóságot és lehetőségei szerint a felhasználó Közösség tagjait.

5.8.2 Minimális szolgáltatás rendkívüli üzemeltetési helyzetben

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

Rendkívüli üzemeltetési helyzetben a Szolgáltató minden egyéb szolgáltatást szüneteltet.

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 [32] Üzletmenet-folytonossági Terve intézkedik. Az Üzletmenet-folytonossági Tervben az üzletmenetet veszélyeztető, sértő, illetve azt leállító események súlyossági osztályokba vannak sorolva. A Terv részletes intézkedési forgatókönyveket tartalmaz a súlyos üzemzavari, illetve katasztrófa események kezelésére és részletesen

szabályozza a Hitelesítő Központok szolgáltatói kulcsainak kompromittálódása esetén elvégzendő teendőket is. Ez a dokumentum biztonsági okokból nem nyilvános.

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

5.9 A szolgáltatási tevékenység megszüntetése

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

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

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

Ezzel egyidejűleg leállítja a visszavonás kezelési szolgáltatást.

A Szolgáltató gondoskodik a szolgáltatásainak megszüntetéséből fakadó zavarok minimalizálásáról. Különösképpen gondoskodik 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 Hírközlési Hatóságot és Internetes honlapján tájékoztatja a felhasználói közösség tagjait

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

c. 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 kibocsátás szolgáltatást (ezen belül a tanúsítvány megújítását)

b. a kulcshordozó eszközön a magánkulcs elhelyezése szolgáltatást.

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

Ezzel egyidejűleg leállítja a visszavonás kezelési szolgáltatást.

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

Időbélyegzés szolgáltatás leállása esetén a fentieket értelemszerűen kell alkalmazni.

6. Műszaki biztonsági óvintézkedések

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

Az informatikai rendszer neve: Trust&CA. V2.0,
Tanúsításának száma: HUNG-TJ-036-2007,
Érvényességi ideje: 2010 07. 24.

A Szolgáltató önkéntes akkreditációs rendszer keretében még nem lett tanúsítva, mert ilyen rendszer Magyarországon még nincs.

Szolgáltató a nem-minősített időbélyegzés szolgáltatása keretében egyes tevékenységeket alvállalkozóknak adhat ki; ilyen esetekben az alább leírtakat értelemszerűen kell alkalmazni.

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

A Szolgáltató maga generálja a szolgáltatói kriptográfiai kulcspárokat (az aláírás-létrehozó és az aláírás-ellenőrző adatokat) fizikailag védett környezetben, nagy biztonságú hardver modulban (HSM), kettős ellenőrzés mellett A kulcspárok generálását olyan algoritmusokkal valósítja meg amelyek szerepelnek a Nemzeti Hírközlési Hatóság HL-20336-7/2005. sz. határozatának 1. sz. mellékletében.

Az aláírás-létrehozó adat elhelyezésére a Szolgáltató csak tanúsítvány kibocsátással együtt vállalkozik.

6.1.2 Az aláírás-létrehozó eszköz megszemélyesítése

Az aláírás-létrehozó eszköz (alapvetően 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 kódot biztosít. A PIN kódot fizikailag védett környezetben állítja elő és a kódot tartalmazó PIN-borítékot az aláírás-létrehozó eszköztől elkülönítve tárolja.

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

A Szolgáltató:

a. az aláírás-létrehozó eszközt (a rajta lévő aláírás-létrehozó adattal, aláírás-ellenőrző adattal és tanúsítvánnyal) az Előfizető vagy az Aláíró által történő átvételig biztonságos módon tárolja,

b. az aláírás-létrehozó eszközt az Előfizetőnek vagy az Aláírónak úgy adja át, hogy az aláírás-létrehozó adat (magánkulcs) titkossága ne sérüljön,

c. az aláírás-létrehozó eszköz aktivizálási adatát (PIN kódját) biztonságosan, ún. PIN borítékban készíti el és tárolja.

Az Előfizetőnek az aláírás-létrehozó eszközt és a PIN kódot tartalmazó borítékot az átvétel írásos elismerésével kell átvennie.

A közigazgatásban alkalmazható tanúsítványok esetében a 194/2005. (IX. 22.) Korm. rendelet 7. § (7) bekezdése értelmében, ha a regisztrációt végző szervezet az aláírás-létrehozó eszközt nem a regisztrációt követően azonnal, ugyanazon a helyszínen adja át az igénylőnek, - ideértve azt is, ha az átadást más elektronikus aláírással kapcsolatos szolgáltató végzi - az aláírás-létrehozó eszköz átadását megelőzően az átvételre jogosultságot a regisztrációnál szokásos eljárásnak megfelelően kell igazolni.

6.1.4 Az Aláírók aláírás-ellenőrző adatának eljuttatása az érintett felekhez

A Szolgáltató az Aláírók aláírás-ellenőrző adatát (nyilvános kulcsát) Tanúsítványtárában teszi mindenki számára elérhetővé. Az Aláírók aláírás-ellenőrző adata az Előfizetői Tanúsítványba van foglalva.

6.1.5 A Szolgáltató aláírás-ellenőrző adatainak eljuttatása a felhasználói közösséghez

A Szolgáltató a hitelesítő központok (Root CA, Produktív CA) tanúsítványait és ezen keresztül aláírás-ellenőrző adatait (nyilvános kulcsait) a szolgáltatás internetes honlapján keresztül teszi mindenki számára elérhetővé.

A szolgáltatói tanúsítványok letölthetők és a felhasználók kliens-alkalmazásaiba installálhatók.

6.1.6 Kulcsméretek, használt algoritmusok

A Szolgáltató Hitelesítő Központja elektronikus aláírás létrehozására és időbélyegzés szolgáltatásához a Nemzeti Hírközlési Hatóság Hivatala HL-20336-7/2005. számú határozatának megfelelően az sha-1-with-rsa kriptográfiai algoritmuskészletet használja.

Az Előfizetői tanúsítványok az RSA[6] aláíró algoritmusokhoz használhatók.

A Hitelesítő Központ („Produktív CA") aláíró kulcsainak mérete:	legalább 2048 bit
Az időbélyegző egység aláíró kulcsának mérete:	legalább 2048 bit
Az Aláírók (Előfizetők) aláíró kulcsainak mérete:	legalább 1024 bit

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

6.1.7 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.

6.1.8 Kulcs felhasználási célok

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

Ennek érdekében a Szolgáltató az Előfizetői tanúsítványok egyes attribútumait a felhasználási területnek és célnak megfelelően állítja be.

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

6.2 Az aláírás-létrehozó adat védelme

6.2.1 Az aláírási termékre vonatkozó szabályok

Az aláírás-létrehozó adatot a Szolgáltató PIN kóddal védve bocsátja ki. Az aláírás-létrehozó adat átvétele után az Aláíró felelős az aláírás-létrehozó eszköz, az aláírás-létrehozó adat, valamint a PIN kód védelméért.

A Szolgáltató az aláírás-létrehozó adatot a szolgáltatás nyújtása során visszafejtésre alkalmas formában nem tárolja, az aláírás-létrehozó eszközre helyezést követően pedig biztosítja, hogy az aláírás-létrehozó adatról semmilyen másolat ne kerüljön tárolásra.

A 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.

6.2.2 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 NHH által regisztrált, illetve az Európai Unió valamely tagállamában nyilvántartásba vett tanúsításra jogosult szervezetek által erre a célra kiadott igazolással.

A nagy biztonságú hardver modul neve:	nChiper nShield 500 F3 (hardware version: nC4033P-500),
Tanúsításának száma:	ZP-004/2007

6.2.3 A többszereplős ("n-ből m") magánkulcs visszaállítás ellenőrzése

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

6.2.4 Aláírás-létrehozó adat letét, mentés, archiválás

Szolgáltató nem nyújt aláírás-létrehozó adat letét szolgáltatást. Szolgáltató az Előfizető aláírás-létrehozó adatát semmilyen formában nem menti vagy archiválja; annak előállítására, visszafejtésére alkalmas programot, adatot nem tárol.

6.2.5 Aláírás-létrehozó adat aktiválása

Az előfizetői aláírás-létrehozó adat aktiválása a felhasználó által történik a jelszó vagy PIN kód megadásával, azokban az esetekben, amikor az aláírás-létrehozó adat használatára szükség van.

[6] RSA Rsagen1 IETF RFC 3447 (2003) "PKCS #1: RSA Cryptography Specifications Version 2.1"

6.2.6 Aláírás-létrehozó adat deaktiválása

Az előfizetői aláírás-létrehozó adatok deaktiválását a felhasználó alkalmazása végzi az Aláíró kijelentkezésekor, vagy – pl. csipkártya esetén – amikor az Aláíró az aláírás-létrehozó eszközt eltávolítja az olvasóból.

6.2.7 Aláírás-létrehozó adat megsemmisítése

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

A szolgáltatói aláírás-létrehozó adatok megsemmisítése a Szolgáltató kötelessége.

6.3 Az előfizetői tanúsítványok megőrzése

Az előfizetői tanúsítványokat a Szolgáltató megőrzi az érvényesség lejáratától 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 archiválási szolgáltató igénybevételével is eleget tehet.

6.4 Aktiválási adatok (PIN kódok)

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

A Szolgáltató a PIN kódokat műszaki és szervezési intézkedésekkel védi és az Előfizető részére az aláírás-létrehozó eszköztől elkülönítve adja át. Az átvételt követően az Előfizetőnek saját felelősségi körében kell biztosítania PIN kód kizárólagos birtoklását.

Az Előfizető bármikor megváltoztathatja PIN kódját.

A PIN kódot a Szolgáltató nem tárolja és nem állítja újra elő 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.

6.5 Informatikai biztonsági előírások

6.5.1 Számítógép biztonsági követelmények

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

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

a. operációs rendszer,
b. PKI 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).

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 behatolás-detektáló 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),

6.5.2 Az informatikai biztonság értékelése

Az informatikai biztonsági értékelések rendszerét az 1. táblázat mutatja.

BIZTONSÁGI ELLENŐRZÉS TÍPUSA		VÉGZI	RENDSZERESSÉG
Operatív	PKI alkalmazás	Rendszer auditor	Naponta
	IT infrastruktúra	Informatikai biztonsági adminisztrátor	Havonta
Belső ellenőrzés	IT infrastruktúra	Informatikai biztonsági menedzser	Évente egyszer
	PKI szabályozási dokumentumok és alkalmazás	Hitelesítési Rend és Szabályozási Csoport	Évente egyszer

1. táblázat

6.6 Életciklusra vonatkozó műszaki előírások

6.6.1 Rendszerfejlesztési szabályok

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

6.6.2 Biztonságkezelési szabályok

A biztonságkezelési szabályokat a Szolgáltató társasági szintű informatikai biztonságpolitikája, a társasági és a rendszer szintű informatikai biztonsági szabályzatok tartalmazzák.

6.6.3 Életciklus biztonsági értékelések

A Szolgáltató által alkalmazott megbízható informatikai rendszerek megfelelnek a 2/2002 MeHVM irányelvben rögzített követelményeknek.

6.7 Hálózati biztonsági szabályok

a. A hálózati védelmi intézkedések megfelelnek a 2/2002 MeHVM irányelvben rögzített biztonsági szinteknek.

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

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

d. A Hitelesítő Központ nem folytat közvetlen külső kommunikációt a végfelhasználókkal.

6.8 Kriptográfiai modul ellenőrzése

A Szolgáltató a szolgáltatáshoz alkalmazott hardveres kriptográfiai modult rendszeresen ellenőrzi.

7. Tanúsítvány, időbélyeg és tanúsítvány-visszavonási profil

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

Szolgáltató által kiadott időbélyegek megfelelnek az RFC 3161 ajánlás előírásainak.

A Szolgáltató által alkalmazott tanúsítványprofilokat a Szolgáltató a szolgáltatás internetes honlapján teszi közzé.

7.1 Tanúsítvány profil

7.1.1 Alap mezők

A Szolgáltató az RFC 3280 bis 08-nak megfelelő tanúsítványokat bocsát ki.

7.1.2 Tanúsítvány kiterjesztések

A Szolgáltató az ITU X.509 szabvány 3. változatának 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 "Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára" előírásainak.

Az ajánlás 14 különböző tanúsítvány szerkezetre tesz javaslatot a magyar közigazgatás elektronikus kommunikációjához (2. fejezet, 1. sz. táblázat). A Szolgáltató elektronikus aláírás céljára a következő tanúsítványprofilokat alkalmazza:

a. közigazgatást képviselő automatizmusok (szerverek), értve ez alatt a web-es VPN (V1.0) szervert: 3-as profil
b. közigazgatást képviselő ügyintézők: 7-es profil
c. a közigazgatás ügyfelei: 11-es profil
d. a közigazgatással kapcsolatba kerülő ügyfelek által működtetett automatizmusok (szerverek): 15-ös profil

7.1.4 Időbélyegek

Az időbélyeg felépítése megfelel az IETF RFC 3161 szabványnak a következők szerint:

a. tartalmazza a vonatkozó időbélyegzési rend azonosítóját (OID-jét),
b. tartalmazza az időbélyeg egyedi azonosítóját,
c. tartalmazza a releváns időpontot év, hónap, nap, óra, perc, másodperc értékben
d. tartalmazza a kérelmező által elküldött üzenetet (lenyomat)
e. az időbélyeg egy olyan névmegadást alkalmaz, amely tartalmazza:
- a Szolgáltató országának nevét (C),
- a Szolgáltató azonosítóját (CN)[7],
- az időbélyeget kibocsátó egység nevét (O, OU)

Az időbélyegző egység belső órájának a pontossági tartományon belül maradását belső és külső szinkronizációs eljárás biztosítja.

A külső szinkronizálást több egymástól független UTC[8] időalap támogatja, amelyekkel nagy megbízhatósággal biztosítható az időbélyegzés belső órájának pontossága, valamint a külső órajelek redundancián alapuló ellenőrzésével annak hitelessége is.

Az időbélyegző egység belső órájának pontossága folyamatos ellenőrzés alatt áll. Amennyiben a nagy megbízhatóságú időszinkronizálás ellenére a belső óra pontossága az előírt 1 másodperces tartományból kiesne, az időbélyegzés szolgáltatás leáll, és a TSA a hiba kijavításáig minden további kérésre hiba üzenetet küld a kérelmezők felé.

A szolgáltatás az időbélyegző szerver belső órája által egymás után kétszer helyesen vett időszinkronnal indul.

[7] A CN és / vagy OU mezők jellemzően az időbélyegző egységet is azonosítják

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

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.

A Szolgáltató által alkalmazott tanúsítvány-visszavonási profilokat a Szolgáltató a szolgáltatás internetes honlapján teszi közzé.

8. A megfelelőség vizsgálata

8.1 Az ellenőrzések gyakorisága és körülményei

A megfelelőségi ellenőrzéseket évente meg kell ismételni. Ezek az ellenőrzések lehetnek belső auditok is. A nem minősített időbélyegzés szolgáltatás egyes tevékenységeinek kihelyezése esetén Szolgáltatónak rendszeresen ellenőrizni kell az alvállalkozó tevékenységét az időbélyegzéssel kapcsolatban. Az alvállalkozó köteles együttműködni az ellenőrzések során a Szolgáltató részéről kijelölt auditorral, és biztosítani az ellenőrzéshez szükséges feltételeket.

8.2 Az auditor és szükséges képesítése

A külső és belső auditálást végző személyeknek függetlennek kell lenniük a Szolgáltató üzemeltetését végző személyektől.
A külső és belső auditálást csak a megfelelő szakmai ismeretek birtokában lévő, tapasztalt szakemberek végezhetik.

8.3 Az auditor és az auditált rendszerelem függetlensége

Az auditornak függetlennek kell lennie az általa ellenőrzött rendszertől.

8.4 Az auditálás által lefedett területek

Az auditálásnak le kell fedni az alábbi területeket:

a. fizikai biztonság
b. dokumentálás és folyamatok biztonsága
c. a személyi állomány biztonsági ellenőrzése
d. adatvédelem
e. műszaki biztonság

8.5 A hiányosságok kezelése

A hiányosságok kezelése a [31] biztonsági szabályzat szerint történik.

8.6 Az eredmények közzététele

A külső és belső rendszervizsgáló csak a megbízójának adhat információt a szolgáltató tevékenységével kapcsolatban. Az audit és az ellenőrzés eredményei a szolgáltató bizalmas üzleti információi, ezért azokat [26] titokvédelmi szabályzat szerint kell kezelni.

9. Egyéb üzleti és jogi kérdések

9.1 Díjak

A mindenkor érvényes szolgáltatási díjakat a Szolgáltató a Szolgáltatás 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 alkalmazza a Szolgáltatások nyújtásakor.

9.1.1 Tanúsítvány kibocsátás és megújítás, időbélyegzés

Szolgáltató a kibocsátott illetőleg megújított tanúsítványokért éves fenntartási díjat számol fel az Előfizető felé, amely tartalmazza:

a. a tanúsítványok kibocsátásának illetőleg megújításának díját,
b. a tanúsítványtárban történő közzététel díját az érvényesség időtartamára,
c. a tanúsítvány felfüggesztésének illetve visszavonásának díját (amennyiben ilyen tevékenységre sor kerül),
d. a tanúsítványok lejárat utáni archiválásának a díját.

Időbélyegzés szolgáltatás esetén Szolgáltató fix havi díjat, valamint a kiadott időbélyegek mennyiségétől függő forgalmi díjat számol fel Előfizető részére.

9.1.2 Tanúsítvány hozzáférés

Szolgáltató a tanúsítványok közzétételéért, a közzétett tanúsítványok eléréséért nem számol fel díjat.

9.1.3 Visszavonás és állapot információ hozzáférés

Szolgáltató a közzétett visszavonási információ eléréséért nem számol fel díjat.

9.1.4 Egyéb szolgáltatásokra vonatkozó díjak

Szolgáltató – ha a felfüggesztést az Aláíró vagy az Előfizető kérte – a kibocsátott tanúsítványok újraérvényesítéséért eljárási díjat számol fel az Előfizető felé. Az eljárási díj tartalmazza a tanúsítvány megváltozott állapotának a tanúsítványtárban visszavonási lista formájában történő közzétételének díját is.

9.1.5 Visszatérítési elvek

Az Előfizető a számára kibocsátott tanúsítvány éves fenntartási díjának visszakérésére 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,[9]
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 írásban jeleznie a Szolgáltató részére. Az igényt a Szolgáltató 15 naptári napon belül köteles elbírálni. Az igény pozitív elbírálása esetén a Szolgáltató a tanúsítványt díjmentesen visszavonja és a fenntartási díjat az Előfizető által megjelölt bankszámlaszámra 20 naptári napon belül átutalja, 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.

Szolgáltató egyéb tevékenységeiért számlázott díjak esetében díjvisszafizetésre nem köteles.

9.2 Anyagi felelősség és annak korlátai

A Szolgáltató anyagi felelősségéről és annak korlátairól a [30] Általános Szerződési Feltételek (ÁSZF-PKI) rendelkezik.

[9] Pl. a kártya fizikai megszemélyesítése nem megfelelő.

9.3 Bizalmasság - Adatkezelési szabályzat

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 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[10] 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

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 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 lapon külön jelöli mindazon adatokat, melyek a Tanúsítványtárban hozzáférhető előfizetői tanúsítványban nyilvánosságra kerülnek.

9.3.3 Tanúsítvány visszavonási és felfüggesztési okok felfedése

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.

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 Feltárás bírósági meghatalmazással rendelkezők részére

A Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az aláíró személy-azonosságát 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 tájékoztatja az Előfizetőt.

[10] vagy nevükben az Előfizető

9.3.6 Feltárás tulajdonos kérésére

Szolgáltató a törvényi meghatalmazással rendelkezők részére történő adatszolgáltatáson és adategyeztetésen túl az Előfizetők és az Aláírók nem nyilvános személyes adatait csak az Előfizető írásos meghatalmazása alapján tárhatja fel harmadik fél részére.

9.3.7 Feltárás más esetekben

Szolgáltatónak tevékenysége befejezésekor az Eat. 16. § (2.) bek. szerint nyilvántartásait, a bizalmas adatokkal együtt, át kell adnia másik szolgáltató részére.

9.4 A személyes adatok védelme

a. A Szolgáltató gondoskodik az adatvédelem és az adatbiztonság területén a szabályszerű működésről, a jogok, kötelezettségek és felelősségek meghatározásáról

b. A Szolgáltató működése és szabályzatai megfelelnek a Személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992 évi XLIII. törvény követelményeinek.

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 és a 9.3.5 pontban meghatározott eseteket.

9.5 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 szolgáltatói felelősség és helytállás

A Szolgáltató felelősségét a jelen szolgáltatási szabályzat 2.2.1 fejezete, helytállására vonatkozó kötelezettségeit a [30] 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 [30] 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.