INFORMATIKAI ÉS HÍRKÖZLÉSI MINISZTÉRIUM
1077 BUDAPEST, DOB U. 75-81. KÖZPONTI TELEFON: (06-1) 342 0520, (06-1) 461 3300 WWW.IHM.HU
Informatikai és Hírközlési Minisztérium

A hitelesítési rendet jóváhagyom.

Ikt. szám: / /2006.

Kovács Kálmán
informatikai és hírközlési miniszter

KÖZIGAZGATÁSI GYÖKÉR HITELESÍTÉS-SZOLGÁLTATÓ IRODA

# HITELESÍTÉSI REND

[KGyHSz rendszer]

A hitelesítési rendben foglaltakkal egyetértek:

Pataki Dániel
a Nemzeti Hírközlési Hatóság elnöke

Verzió: v1.0

Kibocsátás dátuma: 2006-03-01

OID: 0.2.216.1.100.42.1.200.2.0

# DOKUMENTUMKÍSÉRŐ LAP

| Változat | Dátum | A változás leírása | Szerző, kiadó |
|---|---|---|---|
| v0.1 | 2005-11-30 | Első verzió | KFKI-LNX Hálózatintegrációs „zrt.” |
| v0.2 | 2005-12-14 | Szerkesztett és javított változat | Sillye Ferenc |
| v0.32 | 2006-02-09 | Észrevételek szerinti javítások | Dr. Rényi István, Sillye Ferenc |
| v0.5 | 2006-02-15 | Észrevételek szerinti javítások | Endrődi Zs., Gerencsér A., Sillye F. |
| v1.0 | 2006-03-01 | Az első nyilvános változat | Dr. Rényi István, Sillye Ferenc |
| | | | |
| | | | |
| | | | |
| | | | |

# TARTALOMJEGYZÉK

# 1. BEVEZETÉS

Az Informatikai és Hírközlési Minisztérium (IHM) és a Nemzeti Hírközlési Hatóság (NHH) a Közigazgatási Gyökér Hitelesítés-szolgáltató (KGyHSz) létrehozásával és működtetésével megteremti az alapját az elektronikus aláírás jogszabályoknak megfelelő, nemzetközi szinten is együttműködni képes alkalmazhatóságának a teljes magyar közigazgatásban.

A nyilvános kulcsú infrastruktúrán (PKI) alapuló biztonságos elektronikus ügyintézés és kommunikáció feltétele a tanúsítványok hitelessége iránti bizalom. A bizalmi hierarchia legfelső elemét a Közigazgatási Gyökér Hitelesítés-szolgáltató hivatott betölteni.

A Közigazgatási Gyökér Hitelesítés-szolgáltató elsősorban a közigazgatási szervek első szintű tanúsítványkiadóit hitelesíti. Végfelhasználók számára nem bocsát ki tanúsítványt. Magáncég, kereskedelmi szolgáltató tanúsítványkiadóit abban az esetben hitelesítheti, amennyiben azok közigazgatási alkalmazásokhoz adnak ki tanúsítványt, vagy valamely közigazgatási szerv nevében szolgáltatnak a magyar közigazgatási nyilvános kulcsú infrastruktúra előírásai szerint.

Jelen dokumentum a Közigazgatási Gyökér Hitelesítés-szolgáltató Hitelesítési rendje (röviden: Hitelesítési rend), amely a KGyHSz létesítési, működési előírásait határozza meg, és tartalmazza azokat a feltételeket, amelyek betartása esetén a KGyHSz (a dokumentumban foglaltak szerint) szolgáltathat.

## 1.1. Áttekintés

A magyar közigazgatási nyilvános kulcsú infrastruktúra (MK-PKI) hierarchikus felépítésű, melynek csúcsán a KGyHSz áll. A hierarchia a legegyszerűbb bizalmi architektúra, melyben egyetlen olyan biztonsági pont található, amely tanúsítja minden belső kommunikáció hitelességét.

A magyar közigazgatási nyilvános kulcsú infrastruktúra esetében az informatikai és hírközlési miniszter (ebben a dokumentumban: miniszter) látja el a szabályozási-felügyeleti feladatokat, míg az előírások érvényre juttatását az Informatikai és Hírközlési Minisztérium és a hitelesítés-szolgáltatók felügyeletét ellátó Nemzeti Hírközlési Hatóság (NHH) szervezeti keretében működtetett Közigazgatási Gyökér Hitelesítés-szolgáltató (KGyHSz) biztosítja.

Az IHM a magyar közigazgatási PKI valamennyi résztvevő szervezetének, intézményének érdekeit képviseli a szabályozási tevékenység során. A szabályozás egyik fő feladata a közigazgatás belső és az állampolgárokkal, privát partnerekkel folytatott külső kommunikációban használatos hitelesítési irányelvek meghatározása, karbantartása, illetve különböző mintaszabályzatok kiadása. Az IHM és a KGyHSz tevékenysége alapvetően hozzájárul a PKI alkalmazások országos és közösségi szintű együttműködő képességének biztosításához.

Közigazgatási Gyökér Hitelesítés-szolgáltató tanúsítványt ad ki a közigazgatás csatlakozni kívánó első szintű tanúsítványkiadóinak és a kereskedelmi hitelesítés-szolgáltatóknak a magyar közigazgatási nyilvános kulcsú infrastruktúrán belül.

A KGyHSz kiépítése és üzemeltetése a legmagasabb nemzetbiztonsági követelmények szerint történik. A tanúsítványkiadó off-line üzemű, így elektronikus módon nem támadható. Elhelyezésére egy megfelelően védett objektum szolgál, melynek fizikai környezete az előírások szerinti további biztonsági intézkedésekkel biztosított. A KGyHSz saját szolgáltatói kulcspárja elkülönítetten, külön biztonsági hardver modulban kerül létrehozásra és tárolásra. A biztonsági hardver modul őrzése a fizikai biztonsági követelmények szerint történik. A KGyHSz a teljes magyar közigazgatási nyilvános kulcsú infrastruktúra biztonságát erősíti a sebezhetőségek minimalizálásával.

A KGyHSz saját tanúsítványát, a kiadott tanúsítványokat és a visszavonási listákat az MK-PKI központi tanúsítványtárában teszi hozzáférhetővé.

A Hitelesítési rend a [9] szerinti struktúrát követi az áttekinthetőség és a könnyebb auditálhatóság érdekében. Mivel jelen esetben nem általános, végfelhasználóknak hitelesítést biztosító szolgáltatóról van szó, hanem a más hitelesítés-szolgáltatókat hitelesítőről, így a [9] számos pontja nem értelmezhető a KGyHSz esetében.

A Közigazgatási Gyökér Hitelesítés-szolgáltató működését a hitelesítési rend (jelen esetben: Hitelesítési rend) és szolgáltatási szabályzat (jelen esetben: Szolgáltatási szabályzat) dokumentumok alapvetően meghatározzák.

A Hitelesítési rend az alábbi hitelesítés-szolgáltatásokat várja el:

- Regisztráció,
- Tanúsítvány-előállítás,
- Tanúsítvány-kibocsátás,
- Tanúsítvány-visszavonáskezelés és
- Tanúsítványállapot-információszolgáltatás.

## 1.2. A dokumentum neve és azonosítója

A jelen dokumentumban meghatározott Hitelesítési rend teljes címe és azonosítói az alábbiak:

Cím: A Közigazgatási Gyökér Hitelesítés-szolgáltató Hitelesítési rendje

Azonosító: [KGyHSz_HR]

OID: **0.2.216.1.100.42.1.200.2.0**[1]

Azzal, hogy a Közigazgatási Gyökér Hitelesítés-szolgáltató (röviden: KGyHSz) egy tanúsítványban a fenti objektumazonosítót szerepelteti, azt állítja, hogy megfelel a Hitelesítési rendnek.

A Közigazgatási Gyökér Hitelesítés-szolgáltatónak a támogatott hitelesítési rend azonosítóit (OID, cím, verziószám, kibocsátás dátuma stb.) szerepeltetnie kell az előfizetők és érintett felek rendelkezésére bocsátott szabályzataiban[2], utalva a megfelelőség állítására.

[1] Ez az X.509 – X.660 előírások szerinti X.208-ASN.1 objektumazonosító.
[2] A szabályzatokba beleértendők a szerződéses feltételek is.

## 1.3. A magyar közigazgatási nyilvános kulcsú infrastruktúra (MK-PKI) szereplői

A magyar közigazgatási nyilvános kulcsú infrastruktúra (MK-PKI) keretében működő KGyHSz rendszerhez kapcsolódó, meghatározó szereplők az alábbiak:

a) A miniszter, aki a Tanácsadó testületére támaszkodva, szabályozási és felügyeleti jogkört gyakorol a magyar közigazgatási nyilvános kulcsú infrastruktúra szereplői felett,

b) A Nemzeti Hírközlési Hatóság (NHH) Hivatala (röviden: Hivatal), amely biztosítja KGyHSz és a Közigazgatási Gyökér Hitelesítés-szolgáltató Iroda (KGyHSzI) működtetésének feltételeit, és egyéb (hatósági) feladatokat lát el a KGyHSz szolgáltatásaihoz kapcsolódóan,

c) A Közigazgatási Gyökér Hitelesítés-szolgáltató (KGyHSz), amely hitelesítés-szolgáltatást nyújt a magyar közigazgatási nyilvános kulcsú infrastruktúra szereplői számára (lásd az 1.1 pontot),

d) A Biztonsági Hitelesítés-szolgáltató (BHSz), amely szorosan együttműködik a KGyHSz-szel a szolgáltatások ellátásában a köztük lévő Együttműködési megállapodás alapján,

e) Első szintű elektronikus aláírás hitelesítés-szolgáltatók és az elektronikus aláírás törvény hatálya alá nem tartozó hitelesítés-szolgáltatók (a továbbiakban: hitelesítés-szolgáltatók), amelyek előfizetők a KGyHSz szempontjából a PKI fogalomkörben, azaz egy közigazgatási szerv által működtetett első szintű és a kereskedelmi hitelesítés-szolgáltatók tanúsítványkiadói.

f) Érintett felek – azon végfelhasználók, amelyek a KGyHSz aláírás ellenőrző tanúsítványával kapcsolatba kerülnek, pl. tanúsítvány hitelességének vizsgálatakor, a hitelesítési lánc ellenőrzése során.

A KGyHSz a magyar közigazgatási nyilvános kulcsú infrastruktúra (MK-PKI) szereplőivel és feladataikkal kapcsolatos további információkat a dokumentum további részében, illetve a Szolgáltatási szabályzatban teszi közzé.

### 1.3.1. Hitelesítés-szolgáltatók

A magyar közigazgatási nyilvános kulcsú infrastruktúra (MK-PKI) keretében az alábbi hitelesítés-szolgáltatók működnek együtt (lásd még az 1.3 pontot):

- Közigazgatási Gyökér Hitelesítés-szolgáltató (KGyHSz),
- Biztonsági Hitelesítés-szolgáltató (BHSz) és alárendelt hitelesítés-szolgáltatói (sub HSz-ek)
- Kereskedelmi és közigazgatási szervek által működtetett hitelesítés-szolgáltatók,

E dokumentumban meghatározott Hitelesítési rend a KGyHSz-re vonatkozik. A KGyHSz a szolgáltatásait a BHSz-szel szorosan együttműködve biztosítja.

A hitelesítés-szolgáltatók – KGyHSz-szel kapcsolatos – feladataival összefüggő további információkat a Szolgáltatási szabályzat tartalmazza.

### 1.3.2. Regisztrációs szervezet

A KGyHSz nem rendelkezik külön regisztrációs szervezettel, hanem a Hivatal végzi a regisztrációval kapcsolatos feladatokat.

A regisztrációs szervezettel kapcsolatos további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

### 1.3.3. Előfizetők

A KGyHSz ügyfelei, illetve a PKI fogalomkörében az „előfizetők" (akik számára a KGyHSz tanúsítványt bocsát ki) a Hitelesítési rendben meghatározottak szerinti első szintű hitelesítés-szolgáltatók tanúsítványkiadói. A KGyHSz végfelhasználók részére nem bocsáthat ki tanúsítványt.

### 1.3.4. Érintett felek

Az érintett fél olyan egyed (entitás), aki egy adott tanúsítványon alapuló nyilvános kulcsú infrastruktúrára hagyatkozva jár el.

Minden felhasználó érintett fél a KGyHSz vonatkozásában, aki a magyar közigazgatási nyilvános kulcsú infrastruktúra keretében kibocsátott tanúsítványokat ellenőrzi, alkalmazza.

A magyar közigazgatási nyilvános kulcsú infrastruktúrában érintett felek jogait és az ellenőrzésekkel kapcsolatos ajánlásokat a dokumentum további része tartalmazza.

### 1.3.5. Egyéb szereplők

A magyar közigazgatási nyilvános kulcsú infrastruktúra (MK-PKI) egyéb szereplői az alábbiak (lásd még az 1.3 pontot):

- Az informatikai és hírközlési miniszter, aki szabályozási és felügyeleti jogkört gyakorol a magyar közigazgatási nyilvános kulcsú infrastruktúra szereplői felett,
- Nemzeti Hírközlési Hatóság (NHH) Hivatala (röviden: Hivatal), amely biztosítja a KGyHSz és a KGyHSzI működtetésének feltételeit, és egyéb feladatokat lát el a KGyHSz szolgáltatásaival kapcsolatban.
- Az informatikai és hírközlési miniszter mellett működő Tanácsadó testület, amelynek feladata a miniszter támogatása szabályozási és felügyeleti jogkörében, a döntések előkészítése a kereskedelmi hitelesítés-szolgáltatók esetében a közigazgatási követelményeknek való megfelelés vizsgálatával, valamint általában a Hivatal hatáskörébe nem tartozó feladatok ellátásában a nem az elektronikus aláírás törvény hatálya alá tartozó hitelesítés-szolgáltatások kapcsán.

## 1.4. Tanúsítványhasználat

A KGyHSz csak az első szintű szolgáltatók tanúsítvány és CRL kibocsátására használható tanúsítványait hitelesíti felül a funkciójából adódóan.

Ez alól csak a KGyHSz belső működéséhez és működtetéséhez szükséges adminisztrátori tanúsítványok kezelése (előállítása, tárolása, felhasználása stb.) jelent kivételt, amely nem tartozik a Hitelesítési rend hatálya alá.

### 1.4.1. Megfelelő tanúsítványhasználat

a) A Hitelesítési rend megfelel a közigazgatási felhasználásra vonatkozó követelményeknek.

b) A Hitelesítési rend szerepel a Hivatal hatósági nyilvántartásában.

c) Egy tanúsítványt csak a tanúsítványhoz tartozó Hitelesítési rendben meghatározott célokra és csak az ott közölt módon (lásd e dokumentum 4.4, 4.5.1, 6.1.7 és 7.1.2 pontjait) használhatják fel az arra feljogosítottak.

A megfelelő tanúsítványhasználattal kapcsolatos további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

### 1.4.2. Tiltott tanúsítványhasználat

Egy tanúsítványt csak az arra jogosítottak, és csak a tanúsítványhoz tartozó hitelesítési rendben (jelen esetben: a Hitelesítési rendben) meghatározott célra használhatják fel (lásd e dokumentum 4.5.1 és 6.1.7 pontjait). A tanúsítvány minden más célú használata tilos! Az előírás megszegését az Eat. hatálya alá tartozó hitelesítés-szolgáltatók esetében a Nemzeti Hírközlési Hatóság (NHH) Hivatala, az Eat. hatálya alá nem tartozó hitelesítés-szolgáltató esetében a Tanácsadó Testület kivizsgálja, és végső esetben a működés felfüggesztésével is szankcionálhatja. A vele kötött Együttműködési megállapodást súlyosan megszegő első szintű hitelesítés-szolgáltató tanúsítványát a KGyHSz visszavonhatja.

## 1.5. A Hitelesítési rend adminisztrálása

A PKI technológia használatának közigazgatáson belüli koordinálásáért és felügyeletéért az informatikai és hírközlési miniszter a felelős. A miniszter felelős a magyar közigazgatási nyilvános kulcsú infrastruktúrában (MK-PKI-ban) alkalmazott valamennyi biztonsági szintnek megfelelő típusú és osztályú hitelesítési rendért és a szolgáltatási mintaszabályzatért is. Az MK-PKI-ban részt vevő hitelesítés-szolgáltatók dokumentációinak és működésének ellenőrzése az NHH hatásköre.

### 1.5.1. A hitelesítési rend adminisztrációs szervezete

A Hitelesítési rend adminisztrációját a Közigazgatási Gyökér Hitelesítés-szolgáltató Iroda látja el. A Hitelesítési rend és változásainak jóváhagyása a miniszter hatáskörébe tartozik, amelyhez szükséges az NHH elnökének előzetes egyetértése.

Az adminisztrációt ellátó szervezet adatai az alábbi táblázatban találhatók.

| A szervezet adatai | |
|---|---|
| Szervezet neve | **Közigazgatási Gyökér Hitelesítés-szolgáltató Iroda** |
| Szervezet címe | **1015 Budapest, Ostrom u. 23-25.** |
| Levelezési címe | **1525 Budapest, Pf. 75.** |
| Telefonszáma | **+36 1 457-7420** |
| Faxszáma | **+36 1 457-7210** |
| E-levél címe | **kgyhsz@nhh.hu** |

### 1.5.2. Kapcsolattartó személy

a) A szabályzatokkal, illetve a KGyHSz működésével kapcsolatos értesítéseket a Közigazgatási Gyökér Hitelesítés-szolgáltató Iroda vezetőjének kell címezni.

b) A Közigazgatási Gyökér Hitelesítés-szolgáltató a fenti levelezési címeken biztosít kapcsolattartási lehetőséget az előfizetők és érintett felek számára.

### 1.5.3. A Szolgáltatási szabályzat Hitelesítési rendnek való megfelelőségéért felelős személy/szervezet

A Szolgáltatási szabályzatot kibocsátó Közigazgatási Gyökér Hitelesítés-szolgáltató Iroda felelős a Szolgáltatási szabályzat Hitelesítési rendnek való megfelelőségéért, felelős továbbá e dokumentumokban foglaltak szerinti szolgáltatásért.

### 1.5.4. A Szolgáltatási szabályzat elfogadási eljárása

A miniszter szakértők segítségével vizsgálja meg a Hitelesítési rend és Szolgáltatási szabályzat megfelelőségét, továbbá a szolgáltatás feltételeinek meglétét. A Szolgáltatási szabályzatot a miniszter hagyja jóvá az NHH elnökének egyetértését követően.

## 1.6. Meghatározások

| | |
|---|---|
| Nyilvános kulcsú kriptográfiai módszer | Olyan kriptográfiai módszer, mely arra épít, hogy minden felhasználónak két összetartozó kulcs áll a rendelkezésére, melyekkel kriptográfiai műveleteket hajthat végre. Az egyik kulcs az ún. magánkulcs, melyet csak az azt birtokló felhasználó ismerhet. A másik kulcs nyilvános. A két kulcs bármelyikével kódolt adat a másik kulcs segítségével visszafejthető. |
| Nyilvános kulcsú infrastruktúra (PKI) | A tanúsítványok és kulcsok kezelését biztosító jogszabályok, irányelvek, eljárások, szervezetek, hardverek és szoftverek összessége. |
| Tanúsítvány | Hitelesítés-szolgáltató által kibocsátott igazolás, amely a nyilvános kulcsot egy meghatározott entitáshoz kapcsolja. |
| Hitelesítés-szolgáltató (HSz) | Az elektronikus aláírási célú és a nem az Eat. hatálya alá tartozó hitelesítés-szolgáltató által kibocsátott tanúsítványon lévő nyilvános kulcs és a tulajdonos azonosító adatainak hiteles összekapcsolásáért felelős, a kommunikációban résztvevő felek mindegyike által hitelesnek tartott szervezet. |
| Hitelesítési rend | Olyan szabálygyűjtemény, amely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára. |
| Közigazgatási Gyökér Hitelesítés-szolgáltató (KGyHSz) | A magyar közigazgatásban használható tanúsítványok hitelesítőinek felülhitelesítő szervezete. |
| Közigazgatási Gyökér Hitelesítés-szolgáltató Iroda (KGyHSzI) | A Nemzeti Hírközlési Hatóság önálló jogi személyiséggel nem rendelkező szervezeti egysége |

| | |
|---|---|
| Biztonsági Hitelesítés-szolgáltató (BHSz) | Az eSzignó/eTár program keretében megvalósuló hitelesítési szolgáltatásokat, ill. a hozzá kapcsolódó PKI-alapú szolgáltatásokat biztosító szervezet, amely szorosan együttműködik a KGyHSz-szel. |
| Elektronikus aláírás | Elektronikus adat, amely egy elektronikus dokumentumhoz azonosítási célból logikailag hozzárendelt, vagy ahhoz elválaszthatatlanul kapcsolódik. |
| Időbélyegzés | Az a folyamat, melynek során elektronikus dokumentumhoz olyan igazolás rendelődik, amely tartalmazza a bélyegzés nagy pontosságú, hiteles időpontját, és amely a dokumentumhoz oly módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető. |
| NHH Hivatala (Hivatal) | A közigazgatási követelményeknek megfelelő elektronikus aláírás tanúsítványokat kibocsátani kívánó hitelesítés-szolgáltatók és a közigazgatási követelményeknek megfelelő hitelesítési rendek nyilvántartását végző hatóság, amely a KGyHSz regisztrációs tevékenységét is ellátja. |
| Előfizető | Az első szintű hitelesítés-szolgáltatók tanúsítványkiadói, akik számára a KGyHSz tanúsítványt bocsát ki |
| Elektronikus aláírás törvény hatálya alá nem tartozó hitelesítés-szolgáltató | Titkosítási és azonosítási célú kulcspárok és az azokat használó egyedek (entitások) hiteles összetartozását igazoló tanúsítványokat kibocsátó PKI szolgáltató, amelynek hitelességét a kommunikációban résztvevő valamennyi fél elfogadja.. |
| Érintett fél | Olyan egyed (entitás), aki egy adott tanúsítványon alapuló nyilvános kulcsú technikára (elektronikus aláírásra, titkosításra vagy hitelesítésre) hagyatkozva jár el |
| Szolgáltatási szabályzat | A hitelesítés-szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat. |
| Tanúsítvány | Hitelesítés-szolgáltató által kibocsátott digitális igazolás, amely a belefoglalt nyilvános kulcsot egy meghatározott entitáshoz kapcsolja. |
| Kulcsőr | A KGyHSz bizalmi tisztségviselője, aki a KGyHSz szolgáltatói aláíró kulcsának aktivizálásához, valamint előállításához, mentéséhez, visszaállításához és kriptográfiai modulban történő installálásához szükséges, „m az n-ből” titokmegosztással részekre osztott aktivizáló adat egy részletét birtokolja és őrzi. |
| Tanúsítvány visszavonási lista (CRL) | Valamely okból visszavont, vagy felfüggesztett, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a hitelesítés-szolgáltató bocsát ki, s aláírásával hitelesít. |

## 1.7. Rövidítések

| | | |
|---|---|---|
| BHSz | Biztonsági Hitelesítés-szolgáltató | - |
| CN | - | Common Name |
| CRL | tanúsítvány visszavonási lista | Certificate Revocation List |
| DIT | - | Directory Information Tree |
| DN | megkülönböztetett név | Distinguished Name |
| Eat. | Az elektronikus aláírásról szóló 2001. évi XXXV. törvény | - |
| HSz | Hitelesítés-szolgáltató | - |
| Ket. | A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól 2004. évi CXL. törvény | - |
| KGyHSz | Közigazgatási Gyökér Hitelesítés-szolgáltató | - |
| KGyHSzI | Közigazgatási Gyökér Hitelesítés-szolgáltató Iroda | |
| NHH | Nemzeti Hírközlési Hatóság | National Communications Authority |
| OCSP | valósidejű tanúsítványállapot protokoll | On-line Certificate Status Protocol |
| OID | objektumazonosító | Object Identifier |
| OU | - | Organisation Unit |
| PCA | - | Primary Certification Authority |
| PKI | nyilvános kulcsú infrastruktúra | Public Key Infrastructure |
| URI | egységes forrás azonosító | Uniform Resource Identifier |
| URL | egységes forrás meghatározó | Uniform Resource Locator |
| UTF | egységes átalakítás formátum | Unicode Transformation Format |

## 1.8. Hivatkozások

[1] 2001. évi XXXV. törvény az elektronikus aláírásról

[2] FIPS PUB 140-2: Kriptográfiai modulok biztonsági követelményei

[3] MSZ/ISO/IEC 15408 1999: Informatika - Biztonságtechnika - Az informatikai biztonságértékelés közös szempontjai (1-3 részek)

[4] CEN CWA 14167-2: Védelmi profil hitelesítés-szolgáltató aláírási műveletét végző, mentési funkcióval rendelkező kriptográfiai moduljára

[5] ETSI TS 101 456 Szabályozási követelmények a minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatók számára (Műszaki specifikáció)

[6] RFC 3280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile

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

[8] 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

[9] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[10] ITU-T X.501 /ISO/IEC 9594-2:1997

[11] Az Informatikai és Hírközlési Minisztérium közigazgatási nyilvános kulcsú infrastruktúrára vonatkozó ajánlásai

# 2. KÖZZÉTÉTELRE ÉS TÁROLÁSRA VONATKOZÓ FELELŐSSÉGEK

## 2.1. Adatbázisok

a) A KGyHSz működése folyamán keletkező naplófájlokat, a regisztrációs adatokat, tanúsítványokat saját belső adatbázisban kell tárolni.

b) Az adatbázis nem rendelkezhet külső kapcsolattal, fizikailag és logikailag izoláltnak kell lennie.

## 2.2. A tanúsítványokra vonatkozó információk közzététele

a) A KGyHSz által kiadott tanúsítványok és visszavonási állapot információk listájának kézi úton kell a Biztonsági Hitelesítés-szolgáltató (BHSz) tanúsítványtárába kerülniük a belső adatbázisból, a biztonsági szabályok betartásával, a köztük lévő Együttműködési megállapodás alapján.

A tanúsítványokra vonatkozó információk közzétételével kapcsolatos további információkat a KGyHSz a Szolgáltatási szabályzatban ismerteti.

## 2.3. A közzététel gyakorisága

A publikációs szerver frissítésének a következő rendszerességgel kell megtörténnie:

a) A tanúsítványokra vonatkozóan a KGyHSz tanúsítványtárában történt változáskor,

b) A visszavonási listára vonatkozóan a 4.9.7 pontban foglaltak szerint, továbbá

c) A Hitelesítési rend, a Szolgáltatási szabályzat, vagy a KGyHSz nyilvános dokumentumainak megváltozásakor.

## 2.4. Az adatbázisok elérésének szabályozása

a) Gondoskodni kell róla, hogy a belső adatbázist elektronikusan csak magáról a KGyHSz gépről lehessen elérni.

b) A géphez való fizikai hozzáférés-védelemről gondoskodni kell (lásd 5.1.2).

c) A rendszerbe való belépéskor a rendszernek azonosítási és jogosultságvizsgálati eljárást kell folytatnia.

Az adatbázisok elérésére vonatkozó további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

# 3. AZONOSÍTÁS ÉS HITELESÍTÉS

## 3.1. Megnevezési konvenciók

### 3.1.1. Név típusok

A KGyHSz által kiállított elektronikus tanúsítványokra a következő névkonvenció érvényes:

- X.500 formátum ([6] és [9]) az azonosító okmányok adataival megegyezően és
- A tanúsítvány *SubjectAltname* mezejében szereplő elektronikus levelezési cím struktúrája feleljen meg az RFC 822 előírásainak.

### 3.1.2. Igény a nevek értelmezhetőségére

a) A KGyHSz-nek be kell tartania a nevek értelmezhetőségére vonatkozó szabályokat, amelyeket a [7] szerinti 8. táblázat (a különböző tanúsítványok *Subject* mezejének elvárt adattartalma) tartalmaz.

### 3.1.3. Álnevek használata

a) A tanúsítványok DN mezőiben valós neveknek kell szerepelniük. Álnév használata nem megengedett a hitelesítés-szolgáltatók kiadói tanúsítványában.

### 3.1.4. A különböző elnevezési formák értelmezési szabályai

A különböző elnevezési formák értelmezési szabályait a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

### 3.1.5. A nevek egyedisége

a) A KGyHSz-nek gondoskodnia kell arról, hogy az általa kiadott tanúsítványokban használt megkülönböztetett nevet (DN) sohasem fogja másik entitáshoz rendelni.

b) A neveket érkezési sorrendben kell kiadni.

### 3.1.6. Márkanevek elismerése, azonosításuk és szerepük

A tanúsítványkérelemmel az igénylő szerv kifejezi, hogy a benne foglalt nevek, védjegyek, egyéb adatok nem sértik harmadik fél jogait.

a) A KGyHSz-nek jogában áll visszavonni a kérdéses tanúsítványt jogszerűtlen név- vagy adathasználat miatt, amennyiben erre bíróság kötelezi, vagy másik fél megalapozott módon bizonyítani tudja a kérelme jogosultságát a KGyHSz felé.

A márkanevek elismerésével, azonosításával és szerepével kapcsolatos további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

## 3.2. Kezdeti regisztrálás / személyazonosság megállapítása

A Közigazgatási Gyökér Hitelesítés-szolgáltató regisztrációs szervezete az NHH Hivatala (röviden: Hivatal).

### 3.2.1. A magánkulcs birtoklásának igazolása

a) A tanúsítványt igénylő hitelesítés-szolgáltatónak igazolnia kell, hogy birtokában van-e a tanúsítványkérelemben lévő nyilvános kulcshoz tartozó magánkulcs.

b) A KGyHSz-nek a tanúsítvány generálása előtt meg kell győződnie arról, hogy az igénylő szolgáltató valóban birtokolja-e a tanúsítványba foglalandó nyilvános kulcsnak megfelelő magánkulcsot.

A magánkulcs birtoklásának igazolásával kapcsolatban a Szolgáltatási szabályzat további információkat tartalmaz.

### 3.2.2. Szervezet azonosságának hitelesítése

a) A felültanúsítást igénylő hitelesítés-szolgáltatót képviselő természetes személynek a kérelemhez csatolnia kell mindazon dokumentumokat, amelyek alapján a szervezetet egyértelműen azonosítani lehet.

### 3.2.3. Egyén azonosságának hitelesítése

A Hivatal hitelesíti az igénylő azonosságát a felültanúsítás kérelmezése során. Ennek során eleget tesz az alábbi követelményeknek, illetve az együttműködő féltől elvárja a következőket:

a) A tanúsítványkiadást kérelmező hitelesítés-szolgáltató szervezet képviselőinek személyesen kell megjelenniük a Hivatalnál a kérelem benyújtásához.

b) Be kell mutatniuk megbízólevelüket és kétféle személyi azonosításra alkalmas hatósági igazolványukat, melyek közül az egyik (közigazgatási szerv megbízása esetén) a szolgálati igazolvány is lehet.

c) A megbízólevelet közigazgatási szerv megbízása esetén a szerv által kiállított közokiratba, egyéb esetben teljes bizonyító erejű magánokiratba kell foglalni.

d) A hitelesítés-szolgáltató és a képviseletében eljáró személy azonosságának igazolására szolgáló adatok helyességét az igénylő szolgáltató képviseletére jogosultnak írásban, saját kezű aláírásával, vagy minősített elektronikus aláírással ellátott elektronikus dokumentumban kell igazolnia.

e) A hitelesítés-szolgáltatót képviselő személyek azonosságának és eljárási jogosultságának ellenőrzésére szolgáló hatósági igazolványok azonosító adatait, a megadott adatok egyezését és a hatósági igazolványok érvényességét a kérelem vizsgálata során a Hivatalnak közhiteles nyilvántartásban kell ellenőriznie.

f) Amennyiben az adott hatósági igazolvány vonatkozásában ez megvalósítható, a hatósági igazolványt folyamatosan elérhető elektronikus nyilvántartásban kell ellenőrizni.

g) A közigazgatási szervek által kibocsátott szolgálati igazolványok érvényességét a kibocsátónál szintén ellenőrizni kell.

h) Amennyiben a Hivatalnál korábban regisztrált adatokban nincs változás és a személyazonosítás más hitelt érdemlő módon elvégezhető, a Hivatal a korábbi adatokat is felhasználhatja.

### 3.2.4. Nem ellenőrzött előfizetői információk

a) A tanúsítványban csak ellenőrzött információk szerepelhetnek.

b) Regisztrációhoz csak felültanúsítási kérelemhez előírt információk szükségesek a Hivatalnál.

### 3.2.5. Jogok, felhatalmazások ellenőrzése

A tanúsítványkiadást kérelmező szolgáltató nevében eljáró személyek felhatalmazását, jogait megbízólevelük tartalmazza, amellyel kapcsoltban a következők érvényesek:

a) A Hivatal köteles ellenőrizni a regisztrációs adatokat a kérelem benyújtásakor,

b) A KGyHSz Iroda köteles megőrizni a regisztrációs adatok egy példányát a kérelem vizsgálata során a felhasznált többi szervezeti és személyazonosságot igazoló információval együtt.

### 3.2.6. Az együttműködési képességre vonatkozó követelmények

a) A regisztráció során a tanúsítványkiadást kérelmező szolgáltatónak egyértelműen bizonyítania kell, hogy a rendszere(i) kielégíti(k) a jogszabályokban és a miniszter által kibocsátott ajánlásokban megfogalmazott közigazgatási követelményeket.

b) A rendszerekre vonatkozó közigazgatási követelményeket a Hivatal, illetve az informatikai és hírközlési miniszter mellett működő Tanácsadó testület független külső szakértő bevonásával ellenőrizheti a kérelem vizsgálat során.

c) A regisztrációs kérelem nem kötelezi a KGyHSz-t a tanúsítvány kibocsátására.

## 3.3. Azonosítás és hitelesítés kulcs megújítás kérelem esetén

### 3.3.1. Azonosítás és hitelesítés szokványos kulcsmegújítás esetén

a) A KGyHSz által kiadott tanúsítványokra nem megengedett a kulcscsere (kulcsmegújítás).

b) A KGyHSz nem végez kulcsmegújítás szolgáltatást.

### 3.3.2. Azonosítás és hitelesítés visszavonást követő kulcsmegújítás esetén

a) Tilos egy kulcsot megújítani a visszavonását követően.

## 3.4. Azonosítás és hitelesítés tanúsítvány-visszavonási kérelem esetén

a) A kérelmező hitelesítés-szolgáltató, a Hivatal, vagy a miniszter erre felhatalmazott képviselője személyesen vagy minősített elektronikus aláírással ellátott dokumentumban kezdeményezi a tanúsítvány visszavonást a KGyHSz Iroda vezetőjénél.

b) Csak hiteles és érvényes tanúsítvány-visszavonási kérelem esetén vonható vissza tanúsítvány (lásd még a 4.9 pontot).

# 4. A TANÚSÍTVÁNY-ÉLETCIKLUSRA VONATKOZÓ KÖVETELMÉNYEK

## 4.1. Tanúsítványkérelem

a) A KGyHSz csak az alábbi kiadói tanúsítványokat hitelesíti felül:

- Minősített elektronikus aláírás szolgáltatások kiadói tanúsítványai,
- Nem minősített elektronikus aláírás szolgáltatások kiadói tanúsítványai,
- Az elektronikus aláírás törvény hatálya alá nem tartozó hitelesítés-szolgáltatások kiadói tanúsítványai.

b) Minden felültanúsítási kérelmet a Hivatalhoz kell benyújtani.

### 4.1.1. Ki nyújthat be tanúsítványkérelmet

A magyar közigazgatási alkalmazások számára az elektronikus ügyintézéshez szükséges elektronikus aláírás hitelesítés-szolgáltatások nyújtásához a szolgáltatói tanúsítvány felülhitelesítésére és a közigazgatási követelményeknek megfelelő hitelesítési rend nyilvántartásba vételére vonatkozó igényt csak az Eat-nak és a kapcsolódó végrehajtási rendeleteknek eleget tevő, továbbá a [8] szerinti közigazgatási követelményeknek megfelelő hitelesítés-szolgáltató nyújthat be.

Amennyiben a kérelmező hitelesítés-szolgáltató a Hivatal nyilvántartásában az adott szolgáltatás tekintetében még nem szerepel, akkor a felülhitelesítő tanúsítvány kibocsátására vonatkozó kérelem a külön jogszabályok szerinti nyilvántartásba vételre vonatkozó kérelemmel együttesen is benyújtható.

Az elektronikus aláírás törvény hatálya alá nem tartozó hitelesítés-szolgáltatás esetén a felültanúsítási kérelmet a szolgáltatást működtető szervnek, vagy személynek kell előterjesztenie. A felülhitelesítő tanúsítvány iránti kérelem csak akkor terjeszthető elő, ha a szolgáltatás az informatikai és hírközlési miniszter által kibocsátott ajánlásokban [11] megfogalmazott közigazgatási követelményeknek is eleget tesz.

A tanúsítványkérelmet a tanúsítandó hitelesítés-szolgáltató aláírási jogosultságú képviselőinek kell személyesen a Hivatalhoz benyújtania. Elektronikus aláírási célú (az Eat. hatálya alá tartozó) hitelesítés-szolgáltatás esetében a kérelemhez csatolni kell a kérelmet benyújtó szolgáltató által a közigazgatási hatósági eljárásban felhasználható tanúsítványok kibocsátásához felhasználni kívánt, a közigazgatási követelményeknek megfelelő hitelesítési rendek nyilvántartásába felvenni kért hitelesítési rendet (illetve amennyiben a kérdéses hitelesítési rend a Hivatal nyilvántartásában már szerepel, akkor annak azonosítóját), az annak megfelelő szolgáltatási szabályzatot és Általános szerződési feltételeket.

Csatolni kell továbbá a [8] szerinti közigazgatási követelményeknek való megfelelésre vonatkozó, független elektronikus aláírás szolgáltatási szakértő által elkészített igazoló szakvéleményt.

Az elektronikus aláírás törvény hatálya alá nem tartozó hitelesítés-szolgáltatás esetében a tanúsítványkérelemhez a miniszter által kibocsátott ajánlásoknak való megfelelésről szóló, külső, független szakértő által készített szakvéleményt is csatolni kell.

### 4.1.2. Tanúsítványigénylés folyamata és a résztvevők felelőssége

A Hivatal az elektronikus aláírás hitelesítés-szolgáltatók által hozzá benyújtott kérelmeket megvizsgálja a jogszabályban és az MK-PKI körbe eső hitelesítés-szolgáltatókra vonatkozó hitelesítési rendekben előírt követelmények teljesülése szempontjából. Ennek során különös figyelemmel van a közigazgatási felhasználásra vonatkozó követelményeknek megfelelő hitelesítési rend(ek) előírásaira.

Az elektronikus aláírás törvény hatálya alá nem tartozó hitelesítés-szolgáltatás esetén a Hivatal a kérelem benyújtásakor annak teljességét ellenőrzi. A benyújtott és formailag és tartalmilag teljes kérelmeket a Hivatal az informatikai és hírközlési miniszter mellett működő Tanácsadó testülethez továbbítja, amely a kérelmeket megvizsgálja a jogszabályokban és a miniszter által kibocsátott ajánlásokban foglalt közigazgatási követelményeknek való megfelelés szempontjából.

A hitelesítési rendeknek megfelelő egyedi követelményeket és eljárásokat a megfelelő szolgáltatási szabályzat(ok) írja(k) elő.

a) Minden tanúsítványkérelemben dokumentálni kell a következőket:
   - A kérelmező első szintű hitelesítés-szolgáltatónak és meghatalmazottjainak azonosítását;
   - Jogosultság-igazolást a tanúsítvány attribútumaiként szolgáló adatok használatára vonatkozóan;
   - A külön jogszabályok szerinti közigazgatási követelmények teljesítését és az együttműködési képességet az MK-PKI-ban (hatósági nyilvántartásba vett elektronikus aláírás szakértő szakvéleményének benyújtásával);
   - Kötelezettség-vállalást az adott hitelesítési rend és az MK-PKI szabályainak elfogadására vonatkozóan.

   Az adatok helyességéért a tanúsítványkérelmező a felelős.

b) Amennyiben a bejelentésben szereplő hitelesítési rend megfelel a közigazgatási követelményeknek, a Hivatal bejegyzi azt a közigazgatási követelményeket kielégítő hitelesítési rendek nyilvántartásába. Amennyiben a hitelesítés-szolgáltató teljesíti a jogszabályban és a [8] szerinti közigazgatási követelményekben előírt feltételeket, a Hivatal határozatában felhatalmazza a KGyHSz-t, hogy megindítsa a szolgáltató számára a tanúsítvány kibocsátási eljárást. A nem az elektronikus aláírás törvény hatálya alá tartozó hitelesítés-szolgáltatások esetében a miniszter a mellette működő Tanácsadó testület vizsgálatának eredménye alapján a közigazgatási követelményeket teljesítő szolgáltató vonatkozásában felhatalmazza a KGyHSz-t a szolgáltató számára a tanúsítvány kibocsátási eljárás megindítására.

c) A felhatalmazás a KGyHSz-t nem kötelezi a tanúsítvány kibocsátására.

A tanúsítványkérelem elfogadására vonatkozó további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

## 4.2. A tanúsítvány kérelem feldolgozása

a) A Hivatal feladata a tanúsítvány kérelem tartalmi és formai teljességének ellenőrzése, a benyújtott dokumentumok, okmányok alapján a kérelmező regisztrációja. valamint a nem az elektronikus aláírás törvény hatálya alá tartozó hitelesítés-szolgáltatók tanúsítványkérelmeinek továbbítása az informatikai és hírközlési miniszter mellett működő Tanácsadó testülethez. Elektronikus aláírás hitelesítés-szolgáltatók esetében a Hivatal végzi a külön jogszabály szerinti közigazgatási követelményeknek való megfelelés ellenőrzését, a kérelmező által felhasználni kívánt, közigazgatási követelményeknek megfelelő hitelesítési rend nyilvántartásba vételét, valamint határozatban felhatalmazza a KGyHSz-t a tanúsítvány kibocsátási eljárás megindítására.

b) Az informatikai és hírközlési miniszter mellett működő Tanácsadó testület feladata a nem az elektronikus aláírás törvény hatálya alá tartozó hitelesítés-szolgáltatók esetén a tanúsítványkérelmek fogadása a Hivataltól, a jogszabályokban és a miniszter által kibocsátott ajánlásokban megfogalmazott közigazgatási követelményeknek való megfelelés ellenőrzése, valamint a vizsgálat eredménye alapján javaslattétel a miniszter számára.

c) Az informatikai és hírközlési miniszter feladata a Tanácsadó testület támogató javaslata alapján a KGyHSz felhatalmazása a nem az elektronikus aláírás törvény hatálya alá tartozó hitelesítés-szolgáltató felültanúsításának elvégzésére. A Tanácsadó testület javaslata a miniszterre nem kötelező.

d) A KGyHSz feladata a tanúsítvány kérelem teljességének, tartalmi és formai megfelelőségének és hitelességének, a hitelesítés-szolgáltató által benyújtott nyilvános kulcshoz tartozó magánkulcs meglétének ellenőrzése, a hiteles, teljes és tartalmilag, valamint formailag megfelelő kérelmek alapján a felülhitelesítő tanúsítvány kibocsátása és közzététele a Hivatal, illetve az informatikai és hírközlési miniszter megfelelő felhatalmazása alapján.

e) A KGyHSz Iroda gondoskodik a benyújtott dokumentumok, és a regisztráció, valamint a tanúsítvány kibocsátás során keletkezett adatok megőrzéséről.

### 4.2.1. Az azonosítási és hitelesítési funkciók megvalósítása

a) A KGyHSz a tanúsítvány előállítása előtt a Szolgáltatási szabályzatában meghatározott azonosítási és hitelesítési funkciókkal ellenőrzi a tanúsítványkérelem érvényességét.

b) Amennyiben a kérelmező szolgáltató a közigazgatási követelményeket teljesíti, a KGyHSz előállítja, majd közzé teszi a felülhitelesített tanúsítványt.

### 4.2.2. A tanúsítványkérelem elfogadása vagy visszautasítása

a) Amennyiben a tanúsítványkérelem nem felel meg mindenben a Hitelesítési rendben és a Szolgáltatási szabályzatban meghatározottaknak, a Hivatal hiánypótlásra szólítja fel az igénylőt.

b) Eredménytelen hiánypótlás esetén a Hivatal visszautasíthatja a kérelmet.

c) A tanúsítvány kérelem elfogadásának feltétele a KGyHSz-szel kötendő Együttműködési megállapodás aláírása.

### 4.2.3. A tanúsítványigénylések feldolgozási időtartama

a) A tanúsítványigénylések feldolgozásának időtartama legfeljebb 30 nap.

## 4.3. Tanúsítvány kibocsátás

a) A tanúsítványigénylés feltételeinek teljesülése esetén a KGyHSz kibocsátja felülhitelesítő tanúsítványát az igénylő hitelesítés-szolgáltató számára.

b) A felülhitelesítő tanúsítvány a BHSz tanúsítványtárába kerül a KGyHSz-szel kötött Együttműködési megállapodás alapján.

c) A felülhitelesítő tanúsítvány kibocsátása a Hatóság határozathozatalától, illetve a miniszter felhatalmazásától számítva legkésőbb a 15. napon megtörténik.

### 4.3.1. A hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során

A Szolgáltatási szabályzatban meghatározott.

### 4.3.2. Az előfizető értesítése a tanúsítvány kibocsátásról

A Szolgáltatási szabályzatban meghatározott.

## 4.4. A tanúsítvány elfogadása

### 4.4.1. A tanúsítvány elfogadás jelzése

a) A tanúsítványt igénylő köteles visszaigazolni a felülhitelesítő tanúsítvány átvételét és a tanúsítvány adatainak helyességét a tanúsítvány aktivizálása előtt. A visszaigazolás egyben a Hitelesítési rend és a Szolgáltatási szabályzat összes előírásának elfogadását is jelenti a részéről.

### 4.4.2. A tanúsítvány közzététele a hitelesítés-szolgáltató által

a) A KGyHSz által kibocsátott felülhitelesítő tanúsítvány a BHSz tanúsítványtárából kerül közzétételre a köztük lévő Együttműködési megállapodás alapján.

### 4.4.3. A további szereplők értesítése a tanúsítvány kibocsátásról

a) A KGyHSz hivatalosan értesíti a Hivatalt a felülhitelesítő tanúsítvány kibocsátásáról.

## 4.5. Kulcspár- és tanúsítványhasználat

a) A KGyHSz a saját szolgáltatói aláíró tanúsítványát 20 éves lejárati idővel adja ki.

b) A KGyHSz által hitelesített tanúsítványok kizárólag szolgáltatói aláíró tanúsítványként használhatók fel (tanúsítványok és tanúsítvány-visszavonási listák aláírására).

c) Az érintett feleknek a KGyHSz által hitelesített tanúsítványokat, valamint a KGyHSz saját tanúsítványát is szolgáltatói tanúsítványként kell kezelniük.

### 4.5.1. Az előfizetői magánkulcs és tanúsítvány használata

A közigazgatási hitelesítés-szolgáltatókra vonatkozó rendelkezések:

a) Az első szintű, közigazgatási hitelesítés-szolgáltató – a miniszter felhatalmazása alapján – a KGyHSz jóváhagyásával hitelesíthet felül egy neki alárendelt hitelesítés-szolgáltatót.

b) Az első szintű, közigazgatási hitelesítés-szolgáltatók felülhitelesített szolgáltatói aláíró tanúsítványai 15 (tizenöt) éves lejárati idővel kerülnek kiadásra.

A kereskedelmi hitelesítés-szolgáltatókra vonatkozó rendelkezések:

c) A KGyHSz által felülhitelesített kereskedelmi hitelesítés-szolgáltató nem tanúsíthat felül neki alárendelt hitelesítés-szolgáltatót a közigazgatási felhasználásra vonatkozó követelményeknek való megfelelőség szempontjából.

d) A kereskedelmi hitelesítés-szolgáltatók felülhitelesített aláíró tanúsítványai legfeljebb 15 (tizenöt) éves lejárati idővel kerülhetnek kiadásra.

### 4.5.2. Az érintett fél nyilvános kulcs és tanúsítvány használata

Annak érdekében, hogy az érintett fél megalapozottan hagyatkozhasson a tanúsítvánnyal igazolt kriptográfiai kulcspár használatával működő alkalmazásra, többek között az alábbiakra kell figyelemmel lennie:

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

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

c) Figyelembe kell venni a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, mely a tanúsítványban és a tanúsítványt kibocsátó szolgáltató szabályzataiban szerepel.

## 4.6. Tanúsítványmegújítás

a) A KGyHSz által kiadott tanúsítványokra a megújítás nem megengedett.

## 4.7. Tanúsítvány kulcscsere

a) A KGyHSz által kiadott tanúsítványokra a kulcscsere nem megengedett.

## 4.8. Tanúsítványmódosítás

a) A KGyHSz rendszerben tanúsítványmódosítás[3] nem megengedett.

b) Amennyiben az adatokban (pl. az első szintű hitelesítés-szolgáltató neve) változás történik, a tanúsítványt vissza kell vonni, és új tanúsítványt kell hitelesíttetni a kezdeti tanúsítványhitelesítésre vonatkozó eljárás szerint.

## 4.9. Tanúsítványvisszavonás és -felfüggesztés

a) A KGyHSz által kiadott szolgáltatói tanúsítványokat nem lehet felfüggeszteni.

b) A KGyHSz-nek gondoskodnia kell arról, hogy hiteles és érvényes tanúsítvány-visszavonási kérelmek esetén a tanúsítványok haladéktalanul visszavonásra kerüljenek, s erről az alanyok, illetve az érintett felek hiteles és megbízható információt kapjanak.

[3] Tanúsítványmódosítás olyan eljárás, amely során a tanúsítványban szereplő alanyra vonatkozó adatok – a nyilvános kulcs kivételével – megváltoznak, és a tanúsítvány az új adatokkal, a régi kulccsal kerül kiadásra.

### 4.9.1. A visszavonás körülményei

Az első szintű hitelesítés-szolgáltató tanúsítványa visszavonásának lehetséges okai:

a) A tanúsítványhoz tartozó magánkulcs kompromittálódott,

b) A KGyHSz magánkulcsa kompromittálódott,

c) Megváltozott a tanúsítvány információtartalma,

d) A tanúsítvány lecserélésre került,

e) Az első szintű hitelesítés-szolgáltató súlyosan megsérti a KGyHSz-szel kötött megállapodás szerinti szabályokat,

f) A visszavonást jogszabály teszi kötelezővé,

g) A Hivatal törli a közigazgatási követelményeknek megfelelő tanúsítványokat kibocsátó hitelesítés-szolgáltatót az adott szolgáltatásra vonatkozó szolgáltatói nyilvántartásából, vagy a hitelesítés-szolgáltató valamennyi hitelesítési rendjét törli a közigazgatási követelményeknek megfelelő hitelesítési rendek nyilvántartásából, illetve a szolgáltató befejezi működését.

### 4.9.2. Ki kérelmezheti a visszavonást

a) Ezt az eljárást az első szintű hitelesítés-szolgáltató részéről az a személy (illetve személyek) kezdeményezheti(k), aki(k) a kezdeti regisztrálásra (a felülhitelesítés kérvényezésére) is jogosult(ak).

b) Az NHH kérelmezheti a visszavonást.

c) A miniszter kérelmezheti a visszavonást.

d) A KGyHSz Iroda kérelmezheti a visszavonást.

### 4.9.3. A visszavonási kérelemre vonatkozó eljárás

a) A KGyHSz Szolgáltatási szabályzatának dokumentálnia kell a tanúsítvány visszavonásának eljárásait, beleértve az alábbiakat:

- A visszavonási kérelmek benyújtásának módja,
- A visszavonási kérelmek megerősítésére vonatkozó követelmények;

b) A visszavonásra vonatkozó kérelmeket ellenőrizni kell, hogy hiteles forrásból származnak-e.

c) A visszavont tanúsítvány alanyát tájékoztatni kell tanúsítványa állapotának megváltozásáról.

d) A Hivatalt tájékoztatni kell a hitelesítés-szolgáltató tanúsítványa állapotának megváltozásáról.

e) Ha egy tanúsítvány visszavonásra került, azt nem szabad érvényesre visszaállítani.

### 4.9.4. A visszavonási kérelem benyújtására vonatkozó kivárási idő

a) Amennyiben az első szintű hitelesítés-szolgáltatónak tudomása van arról, hogy aláíró magánkulcsa kompromittálódott, a visszavonási kérelmet a lehető leghamarabb be kell nyújtania a KGyHSz Iroda felé.

### 4.9.5. A visszavonási eljárás maximális hossza

a) A visszavonási eljárás időtartama legfeljebb 24 óra lehet.

### 4.9.6. Az érintett felek kötelezettsége a visszavonási információ ellenőrzésére

a) Amennyiben az érintett felek kellő gondossággal kívánnak eljárni a tanúsítvány visszavonási állapotának ellenőrzésekor, a tanúsítvány visszavonási információ hitelességéről és sértetlenségéről is meg kell győződniük.

### 4.9.7. A visszavonási lista kibocsátás gyakorisága

a) A KGyHSz által kibocsátott CRL érvényességi ideje legfeljebb 35 (harmincöt) nap.

b) A KGyHSz-nek új CRL-t kell kibocsátania minden tanúsítványállapot-változáskor, de legkésőbb az utoljára kiadott CRL lejárata előtt.

### 4.9.8. A visszavonási lista előállítása és közzététele közötti idő maximális hossza

a) A KGyHSz új CRL-jének generálása és annak elérhetővé tétele (közzététele) között legfeljebb 1 (egy) óra telhet el.

### 4.9.9. Valósidejű tanúsítványállapot-ellenőrzés elérhetősége

a) Amennyiben a KGyHSz valósidejű tanúsítványállapot-szolgáltatást is biztosít, a Szolgáltatási szabályzatnak kell meghatároznia a tanúsítványállapot-ellenőrzés elérhetőségét.

b) A KGyHSz jelenleg nem végez valósidejű tanúsítvány állapot szolgáltatást.

### 4.9.10. A valósidejű tanúsítványállapot-ellenőrzésre vonatkozó követelmények

a) Amennyiben a KGyHSz valósidejű tanúsítványállapot szolgáltatást is biztosít, a Szolgáltatási szabályzatnak kell meghatároznia a tanúsítványállapot-ellenőrzésre vonatkozó követelményeket.

b) A KGyHSz jelenleg nem végez valósidejű tanúsítvány állapot szolgáltatást.

### 4.9.11. A visszavonási hirdetmények egyéb elérhető formái

A Szolgáltatási szabályzatban meghatározott.

## 4.9.12. Speciális követelmények magánkulcs kompromittálódásakor

a) Az első szintű hitelesítés-szolgáltató köteles a KGyHSz Irodát azonnal értesíteni, amennyiben a kulcskompromittálódás gyanúja felmerül. A KGyHSz a visszavonási eljárás megindításával egy időben külső auditot kezdeményez az adott szolgáltatónál, jelentést küld a miniszternek és értesíti a Hivatalt.

b) Amennyiben a KGyHSz szolgáltatói aláíró kulcsa kompromittálódásának gyanúja felmerül, akkor a KGyHSz köteles azonnal jelentést küldeni a miniszternek, értesíteni a Hivatalt, és az összes általa felültanúsított szolgáltatót.

c) A KGyHSz szolgáltatói aláíró magánkulcsának kompromittálódása esetén az MK-PKI minden felültanúsított tanúsítványát vissza kell vonni, és igény esetén új tanúsítványokat kell kiadni.

d) A KGyHSz szolgáltatói aláíró kulcsa kompromittálódása esetén az új tanúsítványok kibocsátását megelőzően elő kell állítani a KGyHSz új, szolgáltatói aláíró kulcspárját.

## 4.9.13. A felfüggesztés körülményei

a) A KGyHSz által kiadott, felülhitelesített tanúsítványok nem függeszthetők fel.

## 4.10. Tanúsítványállapot-szolgáltatások

a) A KGyHSz a visszavont tanúsítványok listáját az aláíró tanúsítványában definiált URL-en teszi elérhetővé.

b) A KGyHSz valósidejű tanúsítvány állapot szolgáltatást jelenleg nem biztosít.

## 4.10.1. A működés jellemzői

Nincs megkötés.

## 4.10.2. A szolgáltatás rendelkezésre állása

a) A KGyHSz közzétételi kötelezettségeit teljesítő Biztonsági Hitelesítés-szolgáltatónak biztosítania kell a tanúsítványtár folyamatos elérhetőségét 99,9 %-os rendelkezésre állás mellett, ahol az eseti szolgáltatás-kiesések nem haladhatják meg a 3 órát.

## 4.10.3. Nem kötelező szolgáltatások

A tanúsítvány állapot szolgáltatásokra vonatkozó további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

## 4.11. A tanúsítvány előfizetés vége

a) A felültanúsított első szintű szolgáltató köteles értesíteni a Hivatalt, a minisztert és a KGyHSz Irodát működésének várható befejezését megelőzően legalább 60 nappal.

b) A KGyHSz a továbbiakban az Eat-ban előírtak és az előfizetőivel kötött Felülhitelesítési megállapodásban foglaltak szerint jár el.

## 4.12. Kulcs letétbe helyezése és visszaállítása

A KGyHSz nem végez kulcs letétbe helyezés és visszaállítás szolgáltatást.

# 5. ELHELYEZÉSI, IRÁNYÍTÁSI ÉS MŰKÖDTETÉSI RENDSZABÁLYOK

A biztonsági előírásokról általában:

A Közigazgatási Gyökér Hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy kellő, az elismert szabványoknak megfelelő adminisztratív és irányítási eljárások kerüljenek alkalmazásra. Különösképpen:

a) A KGyHSz-nek kockázatelemzést kell végeznie a kockázatainak felmérése, valamint a szükséges biztonsági követelmények és védelmi intézkedések meghatározása érdekében.

b) A KGyHSz-nek felelősséget kell vállalnia minden hitelesítési szolgáltatásáért, még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki. A KGyHSz-nek egyértelműen meg kell határoznia a harmadik felek felelősségét, és biztosítania kell azt, hogy a harmadik felek a KGyHSz által megkövetelt összes (a KGyHSz-nél igényelt szolgáltatással összefüggő) ellenőrzésre rákényszerüljenek.

c) A KGyHSz általánosan felelős vezetőjének útmutatást kell adnia az adatok biztonságára vonatkozóan.

d) A biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenn kell tartani a KGyHSz-nél. A biztonságra hatást gyakorló bárminemű változtatást a KGyHSz vezetőjének kell jóváhagynia.

e) A hitelesítés-szolgáltatást nyújtó teljes rendszer és az összes informatikai vagyontárgy biztonságkezelési (ellenőrzési és üzemeltetési) eljárásait[4] létre kell hozni, rendszer biztonsági szabályzataiban dokumentálni kell, és fenn is kell tartani a KGyHSz-nél.

f) A KGyHSz-nek gondoskodnia kell az informatikai biztonság fenntartásáról akkor is, ha egyes funkciói más szervezeti egységnél kerülnek megvalósításra.

g) A KGyHSz vezetője felelős a megfelelő gyakorlat megvalósításáért.

h) A KGyHSz biztonsági műveleteit el kell különíteni az egyéb (pl. szolgáltatási) műveletektől.

A KGyHSz biztonságkezelési eljárásaival kapcsolatos felelősségek közé az alábbiak tartoznak:

- üzemeltetési eljárások és felelősségek,
- biztonsági rendszerek tervezése, kivitelezése és átvétele,
- a káros szoftver elleni védelem,

[4] Ajánlott, hogy a rendszer biztonsági szabályzatai azonosítsák a szolgáltatásokkal kapcsolatos valamennyi fontos célt és potenciális veszélyt, valamint az ezen veszélyek hatásainak elkerülése, illetve korlátozása érdekében szükséges védelmi intézkedéseket. Ajánlott leírni a szabályzatokban az arra vonatkozó szabályokat, irányelveket és eljárásokat is, hogy a meghatározott szolgáltatásokat és az ezekkel kapcsolatos biztonsági garanciákat hogyan biztosítják.

- információs erőforrás-gazdálkodás,
- a biztonsági napló aktív felügyelete, eseményelemzések és nyomkövetések,
- az adathordozó eszközök kezelése és biztonsága,
- adat és szoftver csere (változásmenedzsment keretében),
- a folyamatos működés és vállalt rendelkezésre állás biztosítása,
- a kockázatok kezelése,
- fizikai biztonság.

E felelősségeket a KGyHSz biztonsági eljárásai határozzák meg, amelyeket az üzemeltető személyzet csak megfelelő felügyelet és (a felelősségre vonhatóságot biztosító) ellenőrzési rend mellett hajthatja végre.

Az értékek osztályozása, minősítése és kezelése

A Közigazgatási Gyökér Hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy eszközei és informatikai vagyontárgyai megfelelő szintű védelemben részesüljenek. Különösképpen:

i) Valamennyi informatikai vagyontárgyról leltárt kell vezetnie, és azokat (a védelmi követelmények osztályai alapján) minősítenie kell biztonsági szempontból a kockázatelemzés [lásd az 5. a) pontot] eredményével összhangban.

A biztonsági előírásokra vonatkozó további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

## 5.1. Fizikai rendszabályok

a) A KGyHSz-nek gondoskodnia kell arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen, és a kritikus szolgáltatások eszközeinek fizikai kockázatát minimalizálják.

b) A fizikai rendszabályok kapcsán különösen az alábbi követelményekre kell tekintettel lenni (lásd a következő alpontokat).

### 5.1.1. A telephely elhelyezése és szerkezeti felépítése

A KGyHSz általános tevékenységével kapcsolatosan:

a) Biztosítani kell, hogy elkerülhető legyen az értékek elvesztése, sérülése, és kompromittálódása, valamint a működési tevékenységek megzavarása.

b) Előírásokat kell érvényre juttatni az információ és az információ feldolgozó berendezések kompromittálódásának, illetve ellopásának elkerülése érdekében.

Tanúsítvány-előállítással, visszavonás-kezeléssel kapcsolatosan:

c) A KGyHSz szolgáltatásaihoz szükséges fizikai védelmet biztosítani kell, első sorban egyértelműen meghatározott biztonsági körletek létrehozásával. Bármely más szervezettel megosztott résznek e körleten kívül kell esnie.

d) Fizikai és környezeti biztonsági előírásokat érvényre kell juttatni a rendszer erőforrásokat tartalmazó berendezéseknek, maguknak a rendszer erőforrásoknak, illetve a működésük támogatására használt berendezések megvédése érdekében. A KGyHSz rendszerei előírás szerinti működéséhez szükséges fizikai környezet biztonsága érdekében tekintettel kell lenni az alábbiakra:

- A fizikai hozzáférés szabályozása,
- Természeti katasztrófa elleni védelem,
- Villámvédelem,
- Tűzbiztonság,
- A támogató infrastruktúra (például áram, telekommunikáció, klíma berendezés) meghibásodása,
- Az építmény összeomlása,
- Vízvezeték szivárgás, talajvíz elleni védelem,
- Lopás, betörés és behatolás elleni védelem,
- Katasztrófa utáni helyreállítás[5].

e) Előírásokat kell érvényre juttatni annak megakadályozása érdekében, hogy a KGyHSz által nyújtott szolgáltatásokkal kapcsolatos berendezéseket, (adatokat és információt tartalmazó) adathordozókat, szoftvereket stb. jogosulatlanul ne vihessék el a helyszínről.

### 5.1.2. Fizikai hozzáférés

a) A szolgáltatás nyújtásával összefüggésben használt elektronikus aláírási termékeket, illetve azokat a helyiségeket, amelyekben a szolgáltató ilyen termékeket helyez el, fizikailag is védeni kell a jogosulatlan hozzáféréstől a jogosulatlan személyek bejutását kizárva.

b) A Közigazgatási Gyökér Hitelesítés-szolgáltatónak meg kell akadályoznia, hogy az a) pontban említett helyiségekbe olyan személyek jussanak be, akik erre nem jogosultak.

c) A belépésre jogosultak nevét, a belépésének időpontját, tartózkodásának célját, kilépésének időpontját naplóban kell rögzíteni.

### 5.1.3. Áramellátás, légkondicionálás

Áramellátás tekintetében a KGyHSz-nek olyan tartalék rendszerekkel kell rendelkeznie, amelyek biztosítják a folyamatos szolgáltatáshoz szükséges villamos energiát. Légkondicionálás tekintetében az eseti szolgáltatás-kiesések időtartama nem haladhatja meg a 3 órát (Lásd a 5. d) pontot).

[5] A fizikai és környezeti biztonsággal kapcsolatban útmutatóként lásd az MSZ/ISO/IEC 17799 dokumentumot.

### 5.1.4. Beázás és elárasztódás veszély kezelése

Lásd az 5.1.1. d) pontot.

### 5.1.5. Tűzmegelőzés és tűzvédelem

Lásd az 5.1.1. d) pontot.

### 5.1.6. Adathordozók tárolása

a) Az adathordozókat biztonságosan kell kezelni azok sérülése, ellopása, és a jogosulatlan hozzáférés elleni védelem érdekében.

b) Az adathordozókat biztonságosan kell kezelni az adatminősítési követelményeknek megfelelően (lásd 5. i) pont).

### 5.1.7. Hulladék megsemmisítése

a) Érzékeny adatokat tartalmazó adathordozó eszközt - amennyiben azokra már nincs szükség - biztonságosan kell megsemmisíteni. A megsemmisítésről jegyzőkönyvet kell felvenni.

b) Az érzékeny adatokat tartalmazó adathordozók megsemmisítéséről a Szolgáltatási szabályzat további információkat tartalmaz.

### 5.1.8. A mentési példányok fizikai elkülönítése

a) A rendszer biztonsági mentéseit, amelyekkel hiba esetén visszaállítható a rendszer működése, a Szolgáltatási szabályzatban előírt módon, rendszeresen el kell készíteni.

b) A biztonsági mentéseket legalább 2 (két) példányban, fizikailag védett helyen kell tárolni.

c) Legalább 1 (egy) biztonsági másolatot külső, a KGyHSz rendszertől távol eső biztonságos helyszínen kell tárolni.

d) A fizikai és eljárásbeli biztonsági intézkedések a biztonsági mentéseket tároló helyen legyenek összhangban az üzemi KGyHSz számára előírtakkal.

A fizikai biztonsági előírásokra vonatkozó további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

## 5.2. Eljárásbeli rendszabályok

a) A KGyHSz-nek gondoskodnia kell arról, hogy rendszereit az előírásoknak megfelelően, biztonságosan, szabályszerűen, a legalacsonyabb meghibásodási kockázat mellett üzemeltesse.

b) A KGyHSz eljárásbeli előírásainak meg kell felelniük a személyes adatok védelmére és a minősített adatok, valamint a jogszabályban nevesített, vagy a szolgáltatásban közreműködőkkel (Hivatal, BHSz, előfizető) kötött megállapodásokban ismertetett titokfajták kezelésére vonatkozó, jogszabályi és mértékadó dokumentumokban meghatározott, a legjobb gyakorlatot tükröző műszaki-szervezési előírásoknak (lásd 9.15 a).

c) A munkakörök ellátásához szükséges létszámot operatív, adminisztratív és felügyeleti jellegük és az összeférhetetlenségi elvek alapján kell megtervezni a KGyHSz-nél.

d) A személyzetnek olyan adminisztratív és kezelési eljárások szerint kell tevékenykednie, amelyek megfelelnek a KGyHSz informatika biztonságkezelési (ellenőrzési és üzemeltetési) eljárásainak (lásd az 5. e) pontot).

### 5.2.1. Bizalmi munkakörök

a) A KGyHSz-nél egyértelműen azonosítani kell azokat a bizalmi munkaköröket, amelyektől a működésének biztonsága függ.

b) A szervezeti, szolgáltatási és biztonsági szabályzataiban meghatározott bizalmi munkaköröket ellátó személyzet feladatait, jogosultságait és felelősségeit a munkaköri leírásokban (is) dokumentálni kell.

c) A KGyHSz-nél az alábbiak tartoznak a bizalmi munkakörök közé:

- Általánosan felelős vezető,
- Biztonsági tisztviselő: a szolgáltatás biztonságáért, a biztonsági irányelvek és szabályzatok érvényre juttatásáért általánosan felelős személy,
- Rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy,
- Független rendszervizsgáló: a KGyHSz naplózott, illetve archivált adatállományát vizsgáló, a Szolgáltató által (a biztonságos működés érdekében) megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos felülvizsgálatáért felelős személy,
- Kulcsőr: olyan bizalmi tisztségviselő, aki a KGyHSz szolgáltatói aláíró kulcsának aktivizálásában, előállításában, mentésében, visszaállításában és kriptográfiai modulban történő elhelyezésében vesz részt, és az „m az n-ből” titokmegosztással részekre osztott aktivizáló adat egy részletét birtokolja, őrzi.

d) Az általánosan felelős vezetőt az NHH elnöke nevezi ki. A további bizalmi munkakörök ellátásával az általánosan felelős vezetőnek kell formálisan megbíznia a KGyHSz munkatársait.

e) Üzemeltetési eljárásokat kell kidolgozni valamennyi olyan bizalmi és adminisztratív feladatra, amely hatást gyakorol a hitelesítési szolgáltatásokra, s ezeket az eljárásokat be kell tartani.

f) Általánosan felelős vezető, kulcsőr és biztonsági tisztviselő csak köztisztviselő lehet.

A bizalmi munkakörökkel kapcsolatos további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

### 5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

a) A munkaköri leírásoknak (lásd 5.2.4 pont) támogatniuk kell a feladatok szétválasztásának és a legkisebb jogosultság megadásának szempontjait a KGyHSz-nél. A leírásoknak tartalmazniuk kell a feladatokhoz szükséges létszámot is.

b) Csak bizalmi munkakört betöltő személyzet (lásd 5.2.1 pont) végezheti az alábbi feladatokat – 5 (öt) kulcsőr közül 3 (három) jelenléte mellett:

- a KGyHSz saját (szolgáltatói) aláíró kulcsainak (összetartozó magán és nyilvános kulcsok) előállítása (lásd 6.1.1),
- a KGyHSz szolgáltatói aláíró kulcsainak kriptográfiai hardverben történő elhelyezése (lásd 6.2.4),
- a KGyHSz szolgáltatói aláíró kulcsainak másolása, visszaállítása (lásd 6.2.2),
- a KGyHSz szolgáltatói magánkulcsának megsemmisítése (lásd 6.2.10).

A személyzeti létszámokkal kapcsolatos további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

### 5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés

a) A KGyHSz személyzetét megfelelően azonosítani és hitelesíteni kell a biztonsági zónákba lépéskor és az információs rendszerek hozzáférés engedélyezéséhez, mielőtt a tanúsítványkezeléssel kapcsolatos kritikus alkalmazásokat használnák.

b) A hitelesítés-szolgáltatáshoz tartozó informatikai tevékenységet naplózni kell a rendszeradatok, időpontok stb. feltüntetésével.

### 5.2.4. Egymást kizáró munkakörök

a) Meg kell határozni azokat a szerepköröket, amelyeket nem tölthet be egyazon személy.

b) A bizalmi munkakörök közötti személyi átfedésekre az alábbi korlátozások vonatkoznak:

- A független rendszervizsgáló munkakört betöltő személy nem tölthet be más (lásd a 5.2.1 alatt felsorolt) bizalmi munkakört és
- a rendszerüzemeltető nem láthatja el a biztonsági tisztviselő feladatait.

Az egymást kizáró munkakörökre vonatkozó további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

## 5.3. Személyzetre vonatkozó rendszabályok

A Közigazgatási Gyökér Hitelesítés-szolgáltatónak gondoskodnia kell arról, hogy személyzeti gyakorlata támogassa a biztonságot. Különös tekintettel kell lenni az alábbiakra:

a) A KGyHSz-nek kellő számú, a hitelesítési szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező személyzetet kell alkalmaznia.

b) A KGyHSz valamennyi bizalmi munkakört betöltő munkatársának függetlennek kell lennie minden olyan ütköző érdektől, ami hátrányosan érinthetné a tevékenysége semlegességét, illetve a KGyHSz szolgáltatásainak megbízhatóságát és biztonságát.

c) A KGyHSz (ideiglenes és állandó) munkatársainak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai szerint meghatározott munkaleírásokkal kell rendelkezniük. A munkaleírásoknak tartalmazniuk kell a beosztás érzékenységét, a feladatok elvégzéséhez szükséges hozzáférési jogosultságok alapján. Ahol erre szükség van, meg kell különböztetni az általános funkciókat és a KGyHSz specifikus funkcióit. A munkaleírásoknak meg kell határozniuk az egyes feladatokhoz szükséges létszámot is. Ajánlott, hogy a munkaleírások tartalmazzák a szakismeretre és a tapasztalatra vonatkozó követelményeket.

### 5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

a) A KGyHSz-nek olyan személyzetet kell alkalmaznia, amely rendelkezik a kínált szolgáltatáshoz szükséges szakértői tudással, tapasztalattal és minősítésekkel.

b) Csak olyan személy tölthet be a KGyHSz üzemeltetésével kapcsolatos munkakört, akinél a „C” típusú nemzetbiztonsági ellenőrzés kockázati tényezőt nem tárt fel.

c) A KGyHSz-nek olyan általánosan felelős vezetőt kell alkalmaznia, aki tapasztalattal rendelkezik az elektronikus aláírási technológia terén, ismeri a biztonsági felelősséggel tartozó munkatársakra vonatkozó biztonsági eljárásokat, valamint gyakorlattal rendelkezik az informatikai biztonság területén, valamint megfelel a jogszabályban előírt képesítési és szakmai gyakorlatra vonatkozó előírásoknak.

### 5.3.2. Előélet vizsgálatára vonatkozó eljárások

A személyzet előéletének vizsgálatához az alábbi követelmények betartása szükséges:

a) A KGyHSz semmilyen munkakörbe nem helyezhet olyan személyt, aki bűncselekményért, illetve más olyan vétségért el lett ítélve, amely befolyásolhatja az illető alkalmasságát a várható beosztásban.

b) A munkatársaknak nem szabad hozzáférniük biztonsági funkciókhoz mindaddig, amíg a szükséges, személyükre és alkalmasságukra vonatkozó ellenőrzések végrehajtása meg nem történik.

c) Minden háttérellenőrzést a kormányzati nemzetbiztonsági előírások szerint kell végezni.

### 5.3.3. Kiképzési követelmények

a) Az üzemeltető személyzetet a rendszer használatba vétele előtt ki kell képezni a következőkre, illetve meg kell győződni az alábbi ismereteikről:
   - PKI elméleti ismeretek,
   - A Hitelesítési rend és Szolgáltatási szabályzat alkalmazása,
   - A rendszer használata,
   - A regisztrációs, tanúsítási és visszavonási eljárásrendek,
   - Az informatikai biztonsági követelmények és szabályok,
   - A tevékenységek (jogi és egyéb) következményei.

b) Az oktatást meg kell ismételni minden, a rendszerben történő változás után (a változás által érintett területen). Legalább 6 (hat) havonta utóképzések szükségesek a személyzet számára a szakmai ismeretek és a gyakorlati készség hosszabb idő alatt bekövetkező halványodására való tekintettel.

A Szolgáltatási szabályzatban további információk találhatóak a kiképzésre vonatkozóan.

### 5.3.4. Továbbképzési gyakoriság és követelmények

Alkalmazkodva a KGyHSz informatikai rendszer szükségszerű változásaihoz az alábbi követelmények szerint kell eljárni a személyzet továbbképzése kapcsán az 5.3.3 pontban meghatározott követelmények szerinti ismeretek naprakészen tartása céljából:

a) Minden jelentős üzemeltetési változ(tat)áshoz oktatási tervet is kell készíteni (Ilyen változás lehet a KGyHSz szoftver vagy hardver eszközeinek frissítése, vagy változtatás a biztonsági rendszerben stb.).

b) Az oktatási terv végrehajtását dokumentálni kell.

c) Az ismereteket felfrissítő oktatásokat meg kell tartani az előírások szerint (az előírásokat a miniszter rendszeresen felülvizsgálja).

### 5.3.5. Munkabeosztás körforgásának gyakorisága és sorrendje

Nincs megkötés.

### 5.3.6. A felhatalmazás nélküli tevékenységek büntető következményei

Nincs megkötés.

### 5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

A szerződés keretében munkát végző személyeknek:

a) rendelkezniük kell a megfelelő nemzetbiztonsági bevizsgálással,

b) titoktartási nyilatkozatot kell tenniük a megbízás előtt,

c) betekintési engedéllyel kell rendelkezniük a minősített dokumentumokhoz való hozzáférés előtt.

### 5.3.8. A személyzet számára biztosított dokumentációk

A személyzet számára biztosított dokumentumok az alábbiak lehetnek:

- Szolgáltatói nyilvános dokumentumok – amelyek a szolgáltatásokhoz közvetlenül kapcsolódnak, és első sorban az előfizetők, együttműködők, érintett felek stb. számára készültek (pl. Hitelesítési rend, Szolgáltatási szabályzat);
- Szolgáltatói korlátozott hozzáférésű dokumentumok, amelyek a szolgáltatásban együttműködő felek (KGyHSz, KGyHSzI, BHSz, Hivatal, első szintű hitelesítés-szolgáltatók) feladatait és felelősségeit tartalmazzák;
- A szolgáltatást és üzemeltetést támogató dokumentációk. Ezek olyan belső használatra szánt (szolgálati titokkörbe eső) leírások, útmutatók, amelyek részletesen tartalmazzák a szolgáltatásokkal kapcsolatos szakmai és biztonsági ismerteteket (követelményeket, adatokat, beállítási paramétereket, folyamatokat, szereplőket stb.);
- Hardver és szoftver dokumentációk, amelyeket a rendszer beszállítói és integrátorai a termékekhez biztosítanak (ezek részben szolgálati titokkörbe tartoznak);
- Biztonsági dokumentumok (ezek mind szolgálati titokkörbe tartoznak) – lásd még az 5. e) pontot.

## 5.4. Naplózási eljárások

A Szolgáltatási szabályzatban kell meghatározni, hogy a KGyHSz milyen eseménynaplózó és ellenőrző rendszereket valósít meg (az 5.4.1-5.4.8 pontok szempontrendszere alapján) a biztonság fenntartása érdekében.

A Hitelesítési rend a biztonságos környezet fenntartásához szükséges esemény és audit naplózás követelményeit határozza meg. Különösen a következőket:

a) A munkafolyamatokat, eseményeket az időpont és a résztvevők azonosíthatóságával kell naplózni.

b) A KGyHSz környezeti eseményeihez, a kulcsgondozáshoz és a tanúsítványgondozáshoz használt óra szinkronizálására vonatkozó fontosabb események pontos időpontját rögzíteni kell.

c) Biztosítani kell a KGyHSz személyzetének felelősségre vonhatóságát a tevékenységéért, például az eseménynapló utólagos felhasználásával.

d) Az eseménynapló biztonságos megőrzéséről gondoskodni kell.

### 5.4.1. A tárolt események típusai

A naplózandó speciális események és adatok körét a Szolgáltatási szabályzatban kell meghatározni. A tárolt eseményekkel kapcsolatban az alábbi követelményeket fegyelembe kell venni.

A KGyHSz általános tevékenységével kapcsolatosan:

a) A naplózandó speciális események és adatok körét dokumentálni kell a Szolgáltatási szabályzatban.

b) A következő események naplózása feltétlenül szükséges:

- a működtető rendszerek környezetében bekövetkező, illetve a kulcsok és tanúsítványok kezelésével kapcsolatos események,
- a naplózási funkció elindítása és leállítása,
- a naplózási paraméterek megváltoztatása,
- a naplózás tárolási hibája miatt elvégzett tevékenységek.

A regisztrációval kapcsolatosan:

c) A KGyHSz Irodának gondoskodnia kell arról, hogy naplózásra kerüljön valamennyi regisztrációval kapcsolatos esemény és a kérelmek jóváhagyásával kapcsolatos események. Ennek érdekében a Hivatal köteles a hitelesítés-szolgáltatók regisztrációja során keletkezett adatokat a KGyHSz Iroda részére továbbítani.

A tanúsítvány előállítással kapcsolatosan:

d) A KGyHSz-nek naplóznia kell a KGyHSz saját kulcsainak életciklusával kapcsolatos összes eseményt.

e) A KGyHSz-nek naplóznia kell a KGyHSz saját tanúsítványainak életciklusával kapcsolatos összes eseményt.

f) A KGyHSz-nek naplóznia kell az általa kibocsátott tanúsítványok életciklusával kapcsolatos összes eseményt.

A visszavonás-kezeléssel kapcsolatosan:

g) A KGyHSz-nek gondoskodnia kell arról, hogy a visszavonással és az annak eredményét képező tevékenységgel kapcsolatos összes kérés és jelentés naplózva legyen.

### 5.4.2. A napló fájl feldolgozásának gyakorisága

a) A KGyHSz-nek biztosítania kell a rendszeres naplófájl kiértékeléseket.

### 5.4.3. A napló fájl megőrzési időtartama

a) A naplóadatokat archiválni szükséges,

b) Az archívum megőrzési idejét illetően lásd az 5.5.2 pontot.

### 5.4.4. A napló fájl védelme

a) A naplózott adatállománynak tartalmaznia kell a naplózott esemény bekövetkezésének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az események kiváltásában közreműködő felhasználó vagy más érintett személy nevét.

b) A naplózott adatállomány minden bejegyzését védeni kell a módosítástól, illetve biztosítani kell, hogy a napló tartalmához csak arra feljogosított személy, elsősorban a független rendszervizsgáló férhessen hozzá.

c) A napló kezelését olyan módon kell megoldani, hogy kizárható legyen a napló megsemmisítése, a napló bejegyzéseinek törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása.

### 5.4.5. A napló fájl mentési eljárásai

a) A naplóállományokról és az ellenőrzési jelentésekről eseményhez kötötten mentést és egy biztonsági másolat-párt kell készíteni.

b) A biztonsági másolat egyik példányát fizikailag elkülönített tároló helyre kell küldeni (lásd még az 5.1.8 pontot).

c) Gondoskodni kell a mentések biztonságos kezeléséről és nyilvántartásáról.

### 5.4.6. A naplózás adatgyűjtési rendszere (belső vagy külső)

A naplók gyűjtési rendszerét a Szolgáltatási szabályzat ismerteti.

### 5.4.7. Az eseményeket kiváltó alanyok értesítése

Nincs megkötés.

### 5.4.8. A sebezhetőség felmérése

a) A biztonsági eseményeket automatikus naplózással kell rögzíteni.

b) A rendszervizsgálónak ellenőrizni kell a naplózás folyamatosságát.

c) Elemezni kell a rendszer sebezhetőségét a naplóadatok feldolgozása során, és javaslatokat kell tenni a kockázatkezelés további módjára.

A sebezhetőség felmérésére végzett tevékenységeket a Szolgáltatási szabályzat ismerteti.

## 5.5. Az adatok archiválása

a) A KGyHSz-nek gondoskodnia kell arról, hogy a felülhitelesített tanúsítványokra vonatkozó minden lényeges adat rögzítésre és megfelelő ideig tárolásra kerüljön, különös tekintettel a jogi eljárásokhoz szükséges bizonyítékok alátámasztására.

### 5.5.1. Az archivált adatok típusai

Az archivált adatok típusai a következők lehetnek:

a) Audit és eseménynaplók,

b) A regisztráció során a Hivatalnál és a KGyHSz Irodában keletkezett valamennyi regisztrációs információ (az első szintű hitelesítés-szolgáltató adatai, kérelme, a kérelmezők személyi adatai),

c) A tanúsítványokra vonatkozó valamennyi naplóbejegyzés,

d) Tanúsítványok, CRL-ek,

e) A KGyHSz Iroda hivatalos levelezése,

f) A KGyHSz Iroda elektronikus levelezésének naplóadatai,

g) A (teljes körű) biztonsági mentések.

### 5.5.2. Az archívum megőrzési időtartama

Az archívum megőrzési időtartamára vonatkozóan az alábbiak érvényesek:

a) A regisztrációs adatokat tartalmazó nyilvántartásokat a KGyHSz szolgáltatásait igénybe vevő első szintű hitelesítés-szolgáltatók tanúsítványai esetében az érvényességi idejüket követő 15 (tizenöt) évig meg kell őrizni.

b) A tanúsítványok életciklus menedzsmentjével kapcsolatos naplóadatokat, tanúsítványokat és CRL-eket legalább a KGyHSz saját tanúsítvány érvényességének lejártától számított 10 (tíz) évig kell megőrizni.

c) A biztonságos informatikai környezet fenntartásának utólagos ellenőrizhetősége és bizonyíthatósága érdekében az 5.5.1 pont a) és e) alpontjai szerinti archivált egyéb naplóbejegyzéseket a keletkezésüktől, a Szolgáltatási szabályzatot és annak módosításait pedig hatályon kívül helyezésétől számított 10 (tíz) évig meg kell őrizni.

### 5.5.3. Az archívum védelme

A KGyHSz archív állományait a BHSz elektronikus archiválási szolgáltatása kezeli a köztük lévő Együttműködési megállapodás alapján.

a) A hitelesség biztosítása érdekében az archivált állományokat az archiváló személy legalább fokozott biztonságú elektronikus aláírásával kell ellátni.

b) A bizalmasság biztosítását, az archivált állomány törlésének, megsemmisülésének, a tároló média, szoftver és hardver elévülésével járó problémák megakadályozásának kötelezettségeit a BHSz elektronikus archiválási szolgáltatásánál biztosítani kell a KGyHSz és BHSz közötti Együttműködési megállapodásban rögzítettek szerint, amely összhangban van a KGyHSz és a BHSz hitelesítési rend és szolgáltatási szabályzat dokumentumaiban foglaltakkal.

### 5.5.4. Az archívum mentési folyamatai

Az archívum mentési folyamatait a Szolgáltatási szabályzat határozza meg.

### 5.5.5. A naplóadatok időpont megjelölésére vonatkozó követelmények

a) Biztosítani kell a naplózott bejegyzések és az archiválás időpontjának megállapíthatóságát.

b) Az archivált adatállományt legalább fokozott biztonságú aláírással kell ellátni.

c) Az archivált adatállományt időbélyegzővel kell ellátni.

### 5.5.6. Az archívum gyűjtési rendszere (belső vagy külső)

A KGyHSz külső archiválást végeztet: a BHSz elektronikus archiválási szolgáltatását veszi igénybe a köztük lévő Együttműködési megállapodás alapján.

Az archívum gyűjtési rendszerét a Szolgáltatási szabályzat határozza meg.

### 5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

Az archivált adatokhoz történő hozzáférés során (ami pl. az archivált adatok ellenőrzéséhez kell) az alábbi követelmények betartása szükséges:

a) A BHSz archiválási szolgáltatásának biztosítania kell, hogy mindaddig, amíg az archivált adatokat őrzi, azok az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek a fennálló rendelkezések és a KGyHSz-szel kötött Együttműködési megállapodás alapján.

b) A tanúsítványokra vonatkozó adatokat rendelkezésre kell bocsátani, ha azokra jogi eljárásokban bizonyíték nyújtása céljából szükség van a fennálló rendelkezések és a KGyHSz-szel kötött Együttműködési megállapodás alapján.

Az adatok archiválására vonatkozó további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

## 5.6. A tanúsítványkiadó kulcscseréje

a) A KGyHSz szolgáltatói aláíró kulcs párjának tervezett cseréje előtt 1 (egy) évvel köteles:

- jelentést küldeni a miniszternek,
- értesíteni a Hivatalt,
- értesíteni a BHSz-t és
- értesíteni a szolgáltatásait igénybe vevő többi első szintű hitelesítés-szolgáltatót.

A KGyHSz szolgáltatói aláíró kulcs kompromittálódása esetén a 4.9.12 pontban előírtak szerint kell eljárni.

## 5.7. Kompromittálódást és / vagy katasztrófát követő helyreállítás

a) A KGyHSz működést amilyen hamar csak lehet, helyre kell állítani az után, hogy a KGyHSz berendezései, eszközei, programjai stb. megsérülnek vagy működésképtelenné váltak, de a szolgáltatói aláíró kulcsai rendelkezésre állnak.

b) A helyreállítás sorrendjében elsőbbséget kell adni a visszavonás-kezelésnek és a tanúsítványállapot-szolgáltatásnak.

c) A KGyHSz szolgáltatói aláíró kulcs kompromittálódása esetén a 4.9.12 pontban előírtak szerint kell eljárni.

d) A KGyHSz köteles jelentést küldeni a miniszternek, értesíteni a Hivatalt, a BHSz-t és a szolgáltatásait igénybe vevő hitelesítés-szolgáltatókat a kompromittálódásról és / vagy a katasztrófát követő helyreállításról.

### 5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások

A váratlan események bekövetkezése és kompromittálódás esetén az alábbi követelmények betartása szükséges:

a) A Közigazgatási Gyökér Hitelesítés-szolgáltatónak a rendkívüli üzemeltetési helyzetek esetére (különösen a kompromittálódás és a katasztrófa bekövetkezésére) olyan eljárást kell kidolgoznia, amely lehetővé teszi a megbízható szolgáltatás mielőbbi helyreállítását.

b) A rendkívüli üzemeltetési helyzet bekövetkezése esetén a visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását meg kell, hogy előzze.

c) Rendkívüli üzemeltetési helyzet bekövetkezése esetén a KGyHSz köteles haladéktalanul értesíteni

- A minisztert;
- A Hivatalt a rendkívüli üzemeltetési helyzet bekövetkezéséről, annak hatásáról, várható időtartamáról, a rendkívüli üzemeltetési helyzet elhárítása érdekében tett és tervezett intézkedésekről, valamint a rendkívüli üzemeltetési helyzet megszűnéséről;
- A BHSz-t a köztük lévő Együttműködési megállapodás szerint;
- A szolgáltatásait igénybe vevő első szintű hitelesítés-szolgáltatókat, akiket a rendkívüli üzemeltetési helyzet érint, valamint az erről szóló tájékoztatást az interneten elérhetővé tenni és
- Az üzemeltetés-folytonossági tervben meghatározott személyeket.

d) A szolgáltatások folytonosságának fenntartását megelőző és visszaállítási eljárások összehangolt bevezetésével kell elérni.

e) Fel kell mérni a bekövetkezett katasztrófa közvetlen hatásait (az életvédelem, vagyonvédelem, adatvédelem stb. szempontjai szerint), és meg kell vizsgálni a szolgáltatások kiesését és a biztonság sérülését.

f) Biztosítani kell, hogy a működés szempontjából kritikus szolgáltatások visszaállíthatóak legyenek egy meghatározott időn belül az Üzletmenet-folytonossági terv szerint.

g) A biztonságkezelési dokumentumok elkészítésével, bevezetésével, tesztelésével és folyamatos fejlesztésével támogatni kell a vállalt rendelkezésre állást és adatbiztonságot.

h) A működés folyamatos fenntartásába bele kell érteni a kockázati tényezők ellenőrzését, a katasztrófa következményeinek azonosítását és a válaszlépéseket, valamint a legszükségesebb alkalmazások meghatározott időn belül történő visszaállítását.

i) A személyzet minden tagja felelős a zavartalan működés és a vele kapcsolatos gyakorlatok megtervezéséért, valamint a szabályzatok maradéktalan betartásáért.

### 5.7.2. Meghibásodott informatikai erőforrások, szoftverek, és/vagy adatok

Az információs erőforrások (hardverek, szoftverek, adatok stb.) meghibásodása esetén az alábbi követelmények betartása szükséges:

a) A KGyHSz Üzletmenet-folytonossági tervének a kritikus szoftver/hardver komponensek meghibásodásával, mint katasztrófahelyzettel kell foglalkoznia. Ilyen esetekben a tervezett eljárásokat végre kell hajtani annak érdekében, hogy az üzemeltetés helyreálljon, amint csak lehetséges.

b) A biztonsági események és hibás működések által okozott kárt eseményjelentés és válaszadás eljárások használatán keresztül minimalizálni kell.

c) A KGyHSz-nek időben és összehangoltan kell fellépnie annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Az esemény bekövetkezése után a legrövidebb időn belül jelenteni kell az esetet a miniszternek, továbbá tájékozatnia kell a Hivatalt és a BHSz-t a szolgáltatások kieséséről és a várható következményekről.

### 5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások

A magánkulcs kompromittálódása esetén az alábbi követelmények betartása szükséges a KGyHSz részéről:

a) A KGyHSz szolgáltatói aláíró magánkulcsának kompromittálódása esetén tájékoztatnia kell a minisztert, a Hivatalt, a BHSz-t és a szolgáltatásait igénybe vevő összes első szintű hitelesítés-szolgáltatót, illetve érintett felet a kompromittálódásról, és a KGyHSz alá tartozó összes tanúsítványt vissza kell vonnia.

b) Ha egy, a szolgáltatásait igénybe vevő első szintű hitelesítés-szolgáltató kulcsa kompromittálódik, és erről a KGyHSz egyértelmű tudomást szerez, az adott kulcshoz tartozó tanúsítványt haladéktalanul vissza kell vonnia.

### 5.7.4. Működés folyamatosságának biztosítása katasztrófát követően

A szolgáltatás folyamatosságának biztosításához az alábbi követelmények betartása szükséges a katasztrófát követően:

a) Természeti vagy más egyéb katasztrófát követően a KGyHSz Üzletmenet-folytonossági terve által megtervezett eljárásokat kell életbe léptetni annak érdekében, hogy az üzemeltetés mielőbb helyreálljon.

b) A KGyHSz-nek lépéseket kell tennie a katasztrófa ismételt bekövetkezésének megakadályozására a katasztrófát követően (amikor ez észszerű).

A kompromittálódás elkerülésére és katasztrófát követő helyreállításra vonatkozó további információkat a KGyHSz a Szolgáltatási szabályzatban teszi közzé.

## 5.8. Hitelesítés-szolgáltató leállítása

A KGyHSz-nek gondoskodnia kell a szolgáltatásainak megszüntetéséből származó, az előfizetőket és az érintett feleket érintő potenciális zavarok minimalizálásáról.

A KGyHSz-re vonatkozó követelmények a következők:

a) A tevékenysége tervezett megszüntetése előtt engedélyt kell kérnie a minisztertől a megszüntetéshez a megfelelő időben[6], feltüntetve ezen a megszűnés tervezett időpontját. Ugyanakkor értesítenie kell erről a Hivatalt is.

b) A megszüntetésre vonatkozó miniszteri engedély birtokában azonnal értesítenie kell a Hivatalt a megszüntetés várható időpontjáról. Ezzel egy időben hivatalosan értesítenie kell a BHSz-t is erről a köztük lévő Együttműködési megállapodásban foglaltak szerint.

c) A KGyHSz tevékenységének megszüntetése előtt legalább 180 nappal értesíteni kell a szolgáltatásait igénybe vevő első szintű szolgáltatókat a megszüntetés várható időpontjáról. Ettől az időponttól a KGyHSz-nek meg kell szüntetnie az új tanúsítványok kibocsátását.

d) A megszüntetéskor a KGyHSz által kiadott, még érvényben lévő tanúsítványokat vissza kell vonni.

e) A megszüntetést követő 10 (tíz) évig biztosítani kell a visszavont tanúsítványok listájának (CRL) vállalt rendelkezésre állású elérhetőségét a BHSz-en keresztül a fennálló rendelkezések és a köztük lévő Együttműködési megállapodás alapján.

[6] Ennek annyi idővel korábban kell megtörténnie, hogy biztosítható legyen a HSz-ek felé annak a 180 napnak a betartása, amelyet a szolgáltatások megszűnésével kapcsolatban az előírások szerint teljesítenie kell.

# 6. MŰSZAKI BIZTONSÁGI INTÉZKEDÉSEK

A Közigazgatási Gyökér Hitelesítés-szolgáltatónak módosítás ellen védett megbízható rendszereket és termékeket[7] kell használnia[8] a biztonsági osztályba sorolás szintjével arányosan (lásd az [1] dokumentum 3. mellékletének f) pontját).

## 6.1. Kulcspár előállítása és telepítése

A KGyHSz szolgáltatói aláíró kulcspárjára az alábbi követelmények érvényesek:

a) Hardveres biztonsági modulban (HSM) kell előállítani és tárolni a kulcspárt az 5.1.8-pontban meghatározott fizikailag védett környezetben, és a 6.2 szerint készült szabályzatokban leírt eljárásrend alapján, az 5.2.1 pontban rögzített szerepköröket betöltő személyek jelenlétében.

b) A kulcshossz nem lehet rövidebb az Eat-ban és a hozzá kapcsolódó rendeletekben - a minősített hitelesítés-szolgáltatóra vonatkozó követelményekben - megfogalmazottnál.

A KGyHSz aláíró tanúsítványa kizárólag off-line módon kerülhet át a BHSz publikációs szerverébe.

### 6.1.1. Kulcspár előállítás

A KGyHSz a saját kulcspár előállítása során az alábbi követelmények szerint jár el:

a) A KGyHSz a saját kulcspárjának előállítását fizikailag védett környezetben (lásd 5.1 pont), bizalmi munkakört betöltő (lásd 5.2.1 pont) személyzettel, 5 (öt) erre feljogosított kulcsőr közül 3 (három) jelenléte mellett kell, hogy elvégezze.

b) A KGyHSz-nek a kulcspár előállítását olyan hardveres biztonsági modulon (HSM) belül kell végrehajtania, amely megfelel a [2] szerinti 3-as, illetve annál magasabb szintű követelményeknek, vagy megfelel a [4] szerinti követelményeknek.

c) A KGyHSz által történő kulcspár előállítását egy, az Eat. 18.§ alapján kiadott NHH határozat[9] szerinti algoritmussal kell megvalósítani.

### 6.1.2. Magánkulcs eljuttatása az előfizetőhöz

A KGyHSz nem nyújt ilyen szolgáltatást.

[7] A megbízható rendszerek követelményei biztosíthatóak például olyan rendszerek használatával, amelyek kielégítik egy megfelelő, a [3], illetve azzal egyenértékű dokumentum alapján meghatározott védelmi profilt (vagy védelmi profilokat).
[8] A KGyHSz szolgáltatásaira vonatkozóan végrehajtott kockázat elemzésnek (lásd 5. a) azonosítania kell azokat a kritikus szolgáltatásokat, amelyekhez megbízható rendszerek kellenek, illetve a szükséges garanciális szinteket.
[9] HL-20336/2005

### 6.1.3. A nyilvános kulcs eljuttatása a tanúsítvány kibocsátójához

a) Az első szintű hitelesítés-szolgáltatótól az ott (HSM modulban) generált kulcspár nyilvános kulcs részét olyan módon kell a KGyHSz-hez eljuttatni, ami biztosítja a továbbított adat sértetlenségét, valamint a feladó hitelességét.

### 6.1.4. A tanúsítványkiadó nyilvános kulcsának közzététele az érintett felek számára

a) A KGyHSz-nek elérhetővé kell tennie a saját aláírás-ellenőrző (nyilvános) kulcsait az érintett felek részére olymódon, amely biztosítja a nyilvános kulcs sértetlenségét és hitelességét, lásd 2.2 pont.

### 6.1.5. Kulcsméretek

A KGyHSz szolgáltatói aláíró kulcsa 2048 bites RSA kulcs.

### 6.1.6. Nyilvánoskulcs-paraméterek előállítása, a paraméterek ellenőrzése

Nincs előírás.

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

A KGyHSz a tanúsítványok aláírásához használja a magánkulcsát, és ezen kívül csak a tanúsítvány visszavonási lista (CRL) aláírására szabad felhasználnia.

A KGyHSz olyan tanúsítványokat bocsáthat ki, melyekre teljesülnek az alábbiak:

a) A tanúsítvány kulcshasználat bitje kritikus és

b) Csak a *KeyCertSign* és a *CRLSign* bitek vannak beállítva „true” értékre.

## 6.2. A szolgáltatói magánkulcs védelme és a kriptográfiai modullal kapcsolatos műszaki előírások

a) A KGyHSz-nek gondoskodnia kell a szolgáltatói aláíró magánkulcsának titkosságáról és sértetlenségéről.

b) A KGyHSz szolgáltatói aláíró magánkulcsát csak fizikailag biztonságos helyszínen, 2 (két) bizalmi munkatárs (a kulcsőrök) egyidejű jelenléte mellett szabad használni.

### 6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

A KGyHSz szolgáltatói aláíró magánkulcsának tárolására, felhasználására vonatkozó szabványok és előírások:

a) A KGyHSz magán aláíró kulcsát olyan biztonságos kriptográfiai hardver eszközben kell tartani, illetve használni, amely megfelel a [2] előírás 3-as szintű követelményeinek vagy megfelel a [4] szerinti követelményeknek.

### 6.2.2. Magánkulcs többszereplős (“n-ből m”) használatának szabályozása

a) A KGyHSz szolgáltatói aláíró magánkulcsához történő hozzáférést biztosító kulcsok „n-ből m” titokmegosztásúak, ahol az n=5 és m=2.

b) A kulcsrészekről másolatot kell készíteni, és azt az elsődleges kulcsoktól fizikailag elkülönített helyen, kiemelt biztonsági intézkedések betartása mellett kell őrizni.

### 6.2.3. Magánkulcs letétbe helyezése

a) A KGyHSz nem nyújthat magánkulcs letétbe helyezése szolgáltatást.

b) A KGyHSz a szolgáltatói aláíró magánkulcsát nem helyezheti letétbe.

### 6.2.4. Magánkulcs mentése

a) A katasztrófaállóság biztosítása érdekében (a KGyHSz esetében) létre kell hozni a szolgáltatói aláíró kulcspár másolatát a magánkulcs tárolására szolgáló hardveres biztonsági modul (HSM) által támogatott módon.

b) A KGyHSz szolgáltatói aláíró magánkulcsának biztonsági célú lemásolása 5 (öt) erre feljogosított kulcsőr közül 3 (három) jelenléte mellett, fizikailag biztonságos környezetben történik.

c) A KGyHSz magánkulcsának másolati példányát elkülönített helyszínen kell tárolni.

d) A KGyHSz szolgáltatói aláíró magánkulcsának másolatára ugyanolyan szintű biztonsági rendszabályoknak kell vonatkozni, mint a használatban levő kulcsokra.

### 6.2.5. Magánkulcs archiválása

A KGyHSz szolgáltatói aláíró magánkulcsát nem szabad archiválni.

### 6.2.6. Magánkulcs bejuttatása kriptográfiai modulba, vagy onnan történő exportja

a) A Közigazgatási Gyökér Hitelesítés-szolgáltató szolgáltatói magánkulcsait a kriptográfiai modulban kell előállítani, így azt kívülről nem szükséges bejuttatni.

b) A szolgáltatói magánkulcsok kriptográfiai modulba kívülről történő bejuttatására egyedül a magánkulcs véletlen megsérülése, megsemmisülése esetén lehet szükség. Az ilyen esetekre a 6.2.2 pont elvárása vonatkozik.

c) A szolgáltatói magánkulcsok kriptográfiai modulból történő exportálására kizárólag biztonsági másolat elkészítése céljából kerülhet sor. Az ilyen esetekre a 6.2.4 pont elvárásai vonatkoznak.

### 6.2.7. Magánkulcs tárolása a kriptográfiai modulban

A KGyHSz szolgáltatói aláíró magánkulcsait hardveres biztonsági modulban kell tárolni. Hozzáférés-ellenőrzést és más biztonsági intézkedéseket kell alkalmazni annak biztosítása érdekében, hogy a kulcsok a hardveres biztonsági modulon kívül ne legyenek hozzáférhetőek.

### 6.2.8. A magánkulcs aktiválásának módja

a) A KGyHSz szolgáltatói aláíró magánkulcsának aktiválása többszereplős ("n-ből m") felügyelet mellett történhet, 5 (öt) erre feljogosított kulcsőr közül legalább 2 (kettő) a jelenlétében.

b) A kulcsőrök csak sikeres belépési (login) eljárást követően aktiválhatják a kulcsot.

### 6.2.9. A magánkulcs deaktiválásának módja

A KGyHSz szolgáltatói aláíró magánkulcsa automatikus deaktiválásának módjára vonatkozóan a Szolgáltatási szabályzatban leírtak érvényesek.

### 6.2.10. A magánkulcs megsemmisítésének módja

A KGyHSz-nek gondoskodnia kell arról, hogy szolgáltatói aláíró magánkulcsai ne legyenek felhasználhatók az életciklusuk vége után. Különösképpen:

a) A KGyHSz kriptográfiai hardverében tárolt magán aláíró kulcsot az eszköz visszavonásakor meg kell semmisíteni. A megsemmisítést fizikailag védett környezetben bizalmi munkakört betöltő személyzet végzi, 5 (öt) erre feljogosított kulcsőr közül 3 (három) jelenléte mellett.

b) A KGyHSz szolgáltatói aláíró magánkulcsainak összes másolatát meg kell semmisíteni az életciklusuk vége után úgy, hogy a magánkulcsok ne legyenek helyreállíthatók.

### 6.2.11. A kriptográfiai modul értékelése

Összhangban a 6.2.1 elvárásaival, a szolgáltatói magánkulcsokat tartalmazó és aktivizáló kriptográfiai moduloknak az alábbi értékelési eredmények valamelyikével kell rendelkezniük:

a) A [2] szerint, legalább 3-as szinten,

b) A [3] szerint, legalább 4-es szintű értékelési garancia szinten,

c) A tanúsítványok előállításához csak olyan kriptográfiai modul használható, mely rendelkezik a Hivatal által nyilvántartásba vett, tanúsításra jogosult szervezetek által erre a célra kiállított (az a) pontban szereplő értékelési eredményeken alapuló), vagy azzal egyenértékű igazolással.

## 6.3. A kulcspár kezelésének egyéb szempontjai

### 6.3.1. Nyilvános kulcs archiválása

A KGyHSz az 5.5 pontban leírtak szerint archiválja nyilvános kulcsát.

### 6.3.2. A tanúsítvány működési időtartama és a kulcspár használatának periódusa

a) A KGyHSz magánkulcsának használati periódusa nem haladhatja meg annak érvényességi idejét.

b) A KGyHSz-nek gondoskodnia kell arról, hogy aláíró magánkulcsai ne legyenek felhasználhatók életciklusuk vége után, összhangban a 6.2.5 pont elvárásával.

c) A KGyHSz magán aláíró kulcsát nem szabad archiválni!

## 6.4. Aktivizáló adatok

A Szolgáltatási szabályzatban meghatározott.

## 6.5. Informatikai biztonsági intézkedések

### 6.5.1. Speciális informatikai biztonsági műszaki követelmények

A KGyHSz-nek gondoskodnia kell arról, hogy az informatikai rendszeréhez való hozzáférés kellően felhatalmazott személyekre legyen korlátozva. Különösképpen:

a) A KGyHSz rendszereinek és információinak a sértetlenségét védeni kell vírusok, káros és engedély nélküli szoftverek ellen.

b) Az adathordozó eszközöket biztonságosan kell kezelni azok sérülése, ellopása és jogosulatlan hozzáférése elleni védelem érdekében.

c) A KGyHSz-nek gondoskodnia kell a felhasználói[10] hozzáférés hatékony nyilvántartásáról a rendszerbiztonság fenntartása érdekében, beleértve a felhasználói hozzáférések naplózását, illetve a hozzáférési jogosultságok kellő időben történő módosítását, áthelyezését.

d) A KGyHSz-nek gondoskodnia kell arról, hogy az információkhoz és az alkalmazói rendszerfunkciókhoz történő hozzáférés, a szabályzatainak megfelelően korlátozott legyen, és hogy a KGyHSz rendszere megfelelő biztonsági funkciókkal rendelkezzen a KGyHSz szabályzatában azonosított bizalmi munkakörök elkülönítése érdekében.

e) A KGyHSz személyzetét sikeresen azonosítani és hitelesíteni kell, mielőtt a tanúsítványkezeléssel kapcsolatos kritikus alkalmazásokat használnák.

f) A KGyHSz bizalmi és adminisztratív munkaköreire vonatkozó tételes előírásokat kell meghatározni a biztonsági szabályozás során.

[10] A felhasználó fogalma itt felöleli a rendszerüzemeltetőket, rendszeradminisztrátorokat és bármely olyan felhasználót, akinek közvetlen hozzáférése van a rendszerhez.

g) A KGyHSz időben és összehangoltan lépjen fel annak érdekében, hogy gyorsan válaszolni tudjon a váratlan eseményekre, és korlátozza a biztonság megsértésének hatásait. Valamennyi eseményt jelenteni kell az esemény bekövetkezte után, amint lehetséges.

h) A BHSz által működtetett nyilvánosságra hozatal (közzététel) alkalmazásnak hozzáférés ellenőrzést kell érvényesítenie a tanúsítványok hozzáadására és törlésére, illetve a kiegészítő információk módosítására irányuló kísérletekre vonatkozóan.

i) A BHSz által működtetett visszavonásállapot-alkalmazásnak hozzáférés ellenőrzést kell érvényesítenie a visszavonás állapot információ módosítására irányuló próbálkozások esetében.

j) Az érzékeny adatokat védeni kell az újra felhasználható, jogosulatlan felhasználók által is elérhető tároló egységeken (például törölt adatállományokon) keresztüli felfedés ellen.

k) Biztosítani kell a KGyHSz személyzet felelősségre vonhatóságát a tevékenységekért, például az eseménynapló megőrzésének segítségével.

### 6.5.2. Az informatika biztonság értékelése

a) A KGyHSz csak megbízható rendszereket és termékeket használhat szolgáltatásainak biztosításához.

b) A KGyHSz értékelését informatika biztonsági szempontból nemzetközileg elfogadott módszertanok szerint kell tervezni és végrehajtani.

## 6.6. Életciklusra vonatkozó műszaki előírások

a) A KGyHSz rendszer hardver és szoftver eszközei csak egyetlen feladatra használhatók: a KGyHSz szolgáltatások megvalósítására. Nem lehet semmi olyan alkalmazás, hardver eszköz, hálózati kapcsolat vagy szoftver komponens a KGyHSz-nél, amely nem része a KGyHSz rendszernek.

b) Megkülönböztetett figyelmet kell fordítani a rosszindulatú szoftverek telepítésének megakadályozására a KGyHSz berendezések esetében. Csak a KGyHSz rendszer működését biztosító alkalmazások szerezhetők be a vonatkozó szabályok és előírások betartásával.

c) Az újonnan beszerzett szoftvereket, programokat elkülönített konfiguráción kell először üzembe helyezni és az informatikai műszaki tudományok pillanatnyi állása szerinti összes biztonsági vizsgálatot végre kell hajtani ellenőrzött, naplózott körülmények között.

d) Informatikai és informatikai biztonsági auditoroknak kell figyelemmel kísérni az üzembe helyezést és a kísérleti üzemeltetést. Az előírt karantén időszak lejárta után helyezhetők üzembe az üzemi környezetben az ellenőrzött adathordozókról a szoftverek és programok.

### 6.6.1. Rendszerfejlesztési előírások

a) Elemezni kell a biztonsági követelményeket a KGyHSz, illetve a KGyHSz nevében végzett minden egyes rendszerfejlesztési projekt tervezési és követelmény meghatározási fázisában, annak biztosítása érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.

b) Változáskezelési eljárásokat kell alkalmazni valamennyi működő szoftver esetében a kibocsátásokra, a módosításokra és a sürgős szoftverjavításokra vonatkozóan.

c) Üzembe helyezés előtt kötelező a mindenre kiterjedő tesztelés.

### 6.6.2. Biztonságkezelési előírások

A KGyHSz-szel kapcsolatban általában:

a) A KGyHSz-nek kockázatelemzést kell végrehajtania működési kockázatainak felmérése, valamint a szükséges biztonsági követelmények és működési eljárások meghatározása érdekében.

A rendszer tervezésével kapcsolatban:

b) A KGyHSz rendszert úgy kell megtervezni, hogy a megfelelő informatikai erőforrások rendelkezésre álljanak a szolgáltatáshoz funkcionális és biztonsági szempontból.

A tanúsítványok aláírására használt hardver biztonsági modul kezelésével kapcsolatban:

A KGyHSz-nek gondoskodnia kell a kriptográfiai hardver biztonságáról annak teljes élettartama alatt. Különösképpen:

c) A tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert nem manipulálják szállítás közben;

d) A tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardvert nem manipulálják tárolás közben;

e) A KGyHSz szolgáltatói aláíró kulcsainak kriptográfiai hardverben történő installálása, mentése, visszaállítása és megsemmisítése 3 (három) kulcsőr együttes jelenlétét kívánja meg;

f) A tanúsítványt és a visszavonási állapotot aláíró kriptográfiai hardver helyesen működik;

g) A KGyHSz kriptográfiai hardverén tárolt magánkulcsokat az eszköz visszavonásakor megsemmisítik.

### 6.6.3. Életciklusra vonatkozó biztonsági előírások

Nincs előírás.

## 6.7. Hálózati biztonsági előírások

a) A KGyHSz-nek fizikailag és logikailag szeparált környezetben kell működnie, hálózati kapcsolata nem lehet.

b) A kibocsátott tanúsítványoknak és a visszavonási listáknak off-line médián kell a tűzfallal védett BHSz adattárba, illetve a publikációs szerverre kerülnie a BHSz-szel kötött Együttműködési megállapodás szerint.

c) A BHSz-nek gondoskodnia kell arról, hogy informatikai rendszerében megfelelő hálózatbiztonsági ellenőrzésekre kerüljön sor a saját hitelesítési rend és szolgáltatási szabályzataiban foglaltak szerint, illetve a KGyHSz-szel kötött Együttműködési megállapodás alapján.

d) A BHSz által megvalósított nyilvánosságra hozatal és visszavonásállapot-szolgáltatásokkal kapcsolatosan: az alkalmazásoknak hozzáférés ellenőrzést kell érvényesíteniük a tanúsítványok hozzáadására és törlésére, a kiegészítő információk módosítására, illetve a visszavonás állapot információ (hálózati) módosítására irányuló kísérletekre vonatkozóan a saját hitelesítési rend és szolgáltatási szabályzataiban foglaltak szerint, illetve a KGyHSz-szel kötött Együttműködési megállapodás alapján.

## 6.8. Időbélyegzés

A KGyHSz nem nyújt időbélyegzés-szolgáltatást.

# 7. TANÚSÍTVÁNY, TANÚSÍTVÁNY VISSZAVONÁSI LISTA ÉS OCSP PROFILOK

## 7.1. Tanúsítványprofilok

A kibocsátott tanúsítványok feleljenek meg a [6]-ban leírt X.509 3-as verziójú tanúsítványoknak, ezen belül különösen az alábbiaknak:

### 7.1.1. Verzió szám(ok)

A [6]-ban leírt X.509 3-as verziójú tanúsítvány verziójának értékszáma: 2

### 7.1.2. Tanúsítvány kiterjesztések

A kiterjesztések részletes leírását [7] tartalmazza.

### 7.1.3. Az algoritmus objektumazonosítója

a) A KGyHSz-nek az alábbi objektumazonosítót (OID-t) kell használnia a tanúsítványok és a visszavonási listák (CRL) aláíró algoritmusának meghatározásához:

- sha-1WithRSAEncryption OBJECT IDENTIFIER::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha-1(5)

### 7.1.4. Névformák

a) A KGyHSz-nek egy megkülönböztetett nevet (DN-t) kell belefoglalnia a tanúsítványba a Hitelesítési rend alapján kibocsátott tanúsítványok alanyaként. E név formájának az X.520 szerinti részletes meghatározását a 3.1.1 pont ismerteti ebben a dokumentumban.

### 7.1.5. Névhasználati megkötöttségek

a) A *Subject* (alany) és *Issuer* (kibocsátó) megkülönböztetett neveket minden tanúsítványban meg kell adni, és ezeknek meg kell felelni a [7]-ban előírtaknak.

b) Minden névnek meg kell felelni a 3.1. alatt előírtaknak is.

### 7.1.6. A Hitelesítési rend objektum azonosítója

a) A KGyHSz minden (a Hitelesítési rend szerint kibocsátott) tanúsítványába köteles felvenni „nem kritikus” megjelöléssel a *Certificate Policies* kiterjesztést. Ez a kiterjesztés tartalmazza az 1.2 pontban meghatározott objektumazonosítót.

b) Amennyiben a KGyHSz eltér ezen előírásoktól, akkor más OID-t kell azonosítóként feltüntetnie.

### 7.1.7. A „hitelesítési rend megkötöttségek” kiterjesztés használata

Nincs megkötés.

### 7.1.8. A „hitelesítési rend jellemzők” szintaktikája és szemantikája

a) A KGyHSz-nek együtt kell telepítenie a *PolicyQualifiers* kiterjesztést a Hitelesítési rend URI-jével.

### 7.1.9. A kritikus hitelesítési rend kiterjesztések feldolgozási szemantikája

a) A kritikus kiterjesztéseket a [6]-ban meghatározottak szerint kell értelmezni.

## 7.2. Tanúsítvány visszavonási lista profil

A kibocsátott tanúsítvány visszavonási listák feleljenek meg a [6]-ban leírt X.509 2-es verziójú visszavonási listáknak, ezen belül különösen az alábbiaknak.

### 7.2.1. Verzió szám

a) A [6]-ban leírt X.509 2-as verziójú tanúsítvány visszavonási lista verziójának értékszáma: 1

### 7.2.2. Tanúsítvány visszavonási lista kiterjesztések

A Szolgáltatási szabályzatban meghatározott.

## 7.3. Az OCSP-profil

a) Amennyiben a KGyHSz valós idejű tanúsítvány állapot protokoll (OCSP) szolgáltatást biztosít, akkor az abban alkalmazott OCSP profilt a Szolgáltatási szabályzatban kell meghatároznia.

# 8. MEGFELELŐSÉGI AUDIT ÉS EGYÉB ELLENŐRZÉSEK

## 8.1. Az ellenőrzések gyakorisága és körülményei

a) A megfelelőségi vizsgálatok gyakoriságát a miniszter határozza meg. A miniszter jogosult auditot végezni annak megállapítására, hogy a KGyHSz működése megfelel-e a Hitelesítési rendben és a Szolgáltatási szabályzatban lefektetett elveknek és az egyéb előírásoknak.

b) A megfelelőségi vizsgálatok gyakorisága típusonként a következő lehet:

- Független rendszervizsgáló összefoglaló auditja: legalább félévente;
- Független külső auditálás: 1 (egy) évente.

## 8.2. Az auditor és szükséges képesítése

a) Az auditálást végző személynek függetlennek kell lennie a KGyHSz üzemeltetését végző személyektől.

b) Auditálást csak a megfelelő szakmai végzettség és ismeretek birtokában lévő, tapasztalt szakember végezhet a KGyHSz-nél.

## 8.3. Az auditor és az auditált rendszerelem függetlensége

a) Az auditornak függetlennek kell lennie az általa ellenőrzött rendszer összes elemétől.

## 8.4. Az auditálás által lefedett területek

Az auditálás által lefedett területek a KGyHSz esetében a következők:

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 Szolgáltatási szabályzat szerint történik a KGyHSz-nél.

## 8.6. Az eredmények közzététele

A külső és belső rendszervizsgáló csak a megbízójának adhat információt a KGyHSz-nél végzett tevékenységével kapcsolatban. Az audit és ellenőrzés eredményei, amennyiben nem is tartalmaznak minősített adatot, üzleti/nem nyilvános információnak tekintendők, és így a 9.3 és 9.4 pontok szerint védendők.

# 9. EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

## 9.1. Díjak

Nincs megkötés.

## 9.2. Anyagi felelősségvállalás

A KGyHSz a tevékenységéért anyagi felelősséget nem vállal.

## 9.3. Az üzleti információk bizalmassága

Nincs megkötés.

### 9.3.1. Felelősség a bizalmas információk védelméért

Nincs megkötés.

## 9.4. A személyes adatok védelme

A KGyHSz működése és szabályzatai megfelelnek a Személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvénynek.

Az első szintű hitelesítés-szolgáltató aláírásra jogosult képviselője nyilatkozatban ad engedélyt arra, hogy a személyes adatait a Hivatal és a KGyHSz Iroda ellenőrizze és kezelje.

Az adatvédelemmel kapcsolatos elveket és szabályokat külön dokumentum tartalmazza.

## 9.5. Szellemi tulajdonjogok

Nincs megkötés.

## 9.6. Tevékenységért viselt felelősség és helytállás

### 9.6.1. A hitelesítés-szolgáltatói felelősség és helytállás

A KGyHSz elsődleges feladata, hogy a magyar közigazgatási nyilvános kulcsú infrastruktúra keretében történő felhasználások legfelsőbb hitelességi forrása legyen.

A KGyHSz-nek gondoskodnia kell arról, hogy a rá vonatkozó valamennyi, e dokumentumban részletezett követelmény teljesüljön.

A KGyHSz hitelesítés-szolgáltatói funkcióit önállóan végzi, de közzétételi kötelezettségét a BHSz útján teljesíti a közöttük lévő Együttműködési megállapodás alapján.

Az első szintű hitelesítés-szolgáltatók kötelezettségeit a saját hitelesítési rend és szolgáltatási szabályzat dokumentumaik tartalmazzák. Ezeknek a nyilvánosan elérhető dokumentumoknak meg kell felelniük a vonatkozó rendelkezéseknek, és a KGyHSz-től igénybevett szolgáltatások tekintetében pedig e Hitelesítési rendnek és a Szolgáltatási szabályzatnak.

### 9.6.2. A regisztrációs szervezet felelőssége és helytállása

Nincs előírás.

### 9.6.3. Az előfizetői felelősség és helytállás

Nincs előírás.

### 9.6.4. Az érintett fél felelőssége

Az érintett felek számára rendelkezésre bocsátott kikötéseknek és feltételeknek tartalmazniuk kell egy megjegyzést, miszerint: „Ha ésszerű módon egy tanúsítványra kívánnak hagyatkozni, az alábbiakat kell tenniük:

a) Ellenőrizzék a tanúsítvány érvényességét, azt, hogy a tanúsítvány nincs felfüggesztve, illetve visszavonva az érvényes visszavonási állapot információ szerint a Hitelesítési rendnek és a Szolgáltatási szabályzatnak megfelelően;

b) Vegyék figyelembe a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, mely a tanúsítványban, a Hitelesítési rendben és a Szolgáltatási szabályzatban szerepel;

c) Tegyenek meg minden, a megállapodásokban vagy máshol előírt, illetve az adott helyzetben általában elvárható egyéb óvintézkedést.”

### 9.6.5. Egyéb szereplők felelőssége és helytállása

Nincs előírás.

## 9.7. A helytállás érvénytelenségi köre

Nincs előírás.

## 9.8. Felelősségi korlátozások

Nincs előírás.

## 9.9. Kártérítési kötelezettségek

Nincs előírás.

## 9.10. Érvényesség időtartama és vége

Jelen Hitelesítési rend visszavonásig érvényes.

### 9.10.1. Időtartam

Nincs megkötés.

### 9.10.2. Befejezés

Nincs megkötés.

### 9.10.3. A befejezés hatása és az érvényben maradó intézkedések

A Hitelesítési rend 2. fejezetében, valamint az 5.4. és az 5.5. pontokban – az adatok megőrzésére vonatkozó – kötelezettségek a szolgáltatás befejezését követően is érvényben maradnak a megőrzési időre vonatkozó előírások szerint.

## 9.11. A felek közötti kommunikációra vonatkozó előírások

Nincs megkötés.

## 9.12. Kiegészítések

Nincs megkötés.

## 9.13. Vitás kérdések megoldása

Amennyiben eredménytelenek a KGyHSz tevékenységével kapcsolatos vitás eseteket megszüntető egyezető tárgyalások az érintettekkel, akkor a kérdésben a KGyHSz székhelye szerint illetékes bíróság dönt.

## 9.14. Irányadó jog

A KGyHSz működésének jogi vonatkozásaira a Magyar Köztársaság törvényei az irányadók.

## 9.15. Az érvényben lévő jogszabályoknak való megfelelőség

A jelen dokumentumban megfogalmazott Hitelesítési rend az alábbi törvényeknek, rendeleteknek és irányelveknek való megfelelőséget tűzi célul:

a) Személyes adatok védelméről és a közhasznú adatok nyilvánosságáról szóló 1992 évi XLIII. Tv.

b) Az elektronikus aláírásról szóló 2001:XXXV. törvény

c) 9/2005 (VII.21.) IHM rendelet

d) 45/2005 (III. 11.) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

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

f) 20/2001 (XI. 15.) MeHVM rendelet a Hírközlési Főfelügyeletnek az elektronikus aláírással összefüggő minősítéssel és nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról

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

h) 2/2002 (IV. 26.) MeHVM irányelv A minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.

i) Az Európai Parlament és a Tanács 1999/93/EK számú irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről

j) A közigazgatási hatósági eljárás és szolgáltatás szabályairól szóló 2004. évi CXL. törvény és az elektronikus ügyintézéshez kapcsolódó végrehajtási rendeletek, azaz a 193/2005 (IX.22.), 194/2005 (IX.22.) és 195/2005 (IX.22.) számú kormányrendeletek.

## 9.16. Vegyes rendelkezések

Nincs előírás.

## 9.17. Egyéb rendelkezések

Nincs megkötés.