



**GIRO Zrt.**

**nem minősített**

**Elektronikus Aláírás Hitelesítés Szolgáltatásának**

**HITELESÍTÉSI RENDJE**

**(HR)**

**NHH regisztrációs szám: FA 7717-1/2001**

**Verzió: 1.1**

**Biztonsági besorolás: Nyilvános**

**Jóváhagyta: Giesz István**

**Jóváhagyás dátuma: 2007. július 31.**

**Hatályba lépés: 2007. augusztus 31.**

**OID: 1.3.6.1.4.1.11526.2.1.1.3.1.1**

**Verziókövetési információk:**

Verzió	Készítette	Ellenőrizte	Hatálybalépés	Módosítások leírása
1.1	Egey Attila, Hradzky Gabriella	Dr. Gyarmati János, Kovács Orsolya	2007. augusztus 31.	Első változat

# Tartalomjegyzék

<b>1</b>	<b>BEVEZETÉS</b>	<b>5</b>
1.1	ÖSSZEFOGLALÁS	5
1.1.1	Szabályzat célja	5
1.1.2	Szabályzat tartalma	5
1.1.3	Alkalmazott szabványok	6
1.2	AZONOSÍTÁS	6
1.3	KÖZÖSSÉG ÉS ALKALMAZHATÓSÁG	6
1.4	TANÚSÍTVÁNYOK OSZTÁLYAI ÉS TÍPUSAI	6
1.5	SZOLGÁLTATÓ ADATAI	7
1.5.1	Cím, cégjegyzékszám, kontaktinformációk	7
1.5.2	Ügyfélszolgálat	7
1.5.3	Szabályzat kibocsátó adatok	8
<b>2</b>	<b>ÁLTALÁNOS RENDELKEZÉSEK</b>	<b>8</b>
2.1	PÉNZÜGYI FELELŐSSÉG KORLÁTJAI	8
2.2	BIZALMASSÁG - ADATKEZELÉSI SZABÁLYZAT	8
<b>3</b>	<b>AZONOSÍTÁS ÉS HITELESÍTÉS</b>	<b>9</b>
3.1	KEZDETI REGISZTRÁCIÓ	9
3.1.1	Nevek típusa	9
3.1.2	Név szemantika	9
3.1.3	Különböző névformátumok értelmezése	9
3.1.4	Nevek egyedisége	10
3.1.5	Név igénylési viták feloldása	10
3.1.6	Védjegyek elismerésének és hitelesítésének módszere	10
3.1.7	Privát kulcs birtoklás ellenőrzésének módszere	10
3.1.8	Szervezeti identitás hitelesítése	11
3.1.9	Személyes identitás hitelesítése	12
3.2	TANÚSÍTVÁNY MEGÚJÍTÁS	14
<b>4</b>	<b>ÜZEMELTETÉSI KÖVETELMÉNYEK</b>	<b>15</b>
4.1	TANÚSÍTVÁNYIGÉNYLÉS	15
4.3	TANÚSÍTVÁNY ELFOGADÁS	16
4.4	TANÚSÍTVÁNY VISSZAVONÁS ÉS FELFÜGGESZTÉS	16
<b>5</b>	<b>A HITELESÍTÉSI SZERVEZETRE VONATKOZÓ FIZIKAI, ELJÁRÁSRENDI, ÉS HUMÁN BIZTONSÁGI SZABÁLYOZÁSOK</b>	<b>16</b>
<b>6</b>	<b>TECHNIKAI SZABÁLYOZÁSOK</b>	<b>17</b>
<b>7</b>	<b>TANÚSÍTVÁNY ÉS KULCS-VISSZAVONÁSI PROFIL</b>	<b>19</b>
7.1	TANÚSÍTVÁNY PROFIL	19
7.1.2	Alap mezők	20
7.1.12	Egyéb kiterjesztések	20
7.2	KULCS-VISSZAVONÁSI PROFIL	20
<b>8</b>	<b>SPECIFIKÁCIÓ ADMINISZTRÁCIÓ</b>	<b>21</b>
8.1	SPECIFIKÁCIÓ VÁLTOZÁSKEZELÉSI ELJÁRÁSAI	21

8.2 PUBLIKÁCIÓS ÉS ÉRTESÍTÉSI SZABÁLYOK.....	21
8.3 HITELESÍTÉSI REND ELFOGADÁSI ELJÁRÁSOK .....	21
<b>MELLÉKLET –SZEMÉLYES TANÚSÍTVÁNY IGÉNYLŐ ADATLAP .....</b>	<b>22</b>
<b>MELLÉKLET –SZERVEZETI TANÚSÍTVÁNY IGÉNYLŐ ADATLAP .....</b>	<b>23</b>
<b>MELLÉKLET – ESZKÖZ TANÚSÍTVÁNYTÍPUS IGÉNYLŐ ADATLAP .....</b>	<b>24</b>

# 1 Bevezetés

## 1.1 Összefoglalás

### 1.1.1 Szabályzat célja

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

Jelen Hitelesítési Rend célja, hogy szabálygyűjteményként, a Hitelesítés Szolgáltató által kibocsátott "Személyes", "Szervezeti" és "Eszköz" tanúsítványtípus felhasználhatóságát határozza meg a Közösség számára. A Szabályzat a Szolgáltató nyilvános Hitelesítési Szolgáltatási Szabályzatával együtt értelmezendő.

### 1.1.2 Szabályzat tartalma

Jelen szabályzat a GIRO Zrt. hitelesítési szolgáltatásának Hitelesítési Rendjét tartalmazza.

A Bevezetés fejezetben ismerteti a Szolgáltatóval kapcsolatos adminisztratív adatokat; eligazítást ad a dokumentum szerepét és a szolgáltatás mibenlétét illetően; megnevezi azon szabványokat, ajánlásokat és előírásokat, melyeket a szabályzat formai megjelenésében és tartalmilag követ.

Az Általános rendelkezések fejezet tájékoztat Szolgáltató pénzügyi felelősségének korlátjairól és felvilágosítást ad a Szolgáltató által kezelt adatokról.

Az Azonosítás és hitelesítés fejezet a tanúsítvány igényléséhez kapcsolódó előfizetői regisztráció menetét ismerteti, leírja a tanúsítvány megújításának kérelmezését, hitelesítését, és elbírálását, s a megújítás menetét; valamint kifejti a tanúsítvány visszavonásának kérelmezését, hitelesítését, elbírálását, és végrehajtását.

Az Üzemeltetési követelmények fejezet leírja a szolgáltató által követendő gyakorlatot és támasztott követelményeket a tanúsítványok igénylése, elfogadása, felfüggesztése és visszavonása kapcsán.

A Tanúsítvány és kulcsvisszavonási profil fejezet ismerteti a tanúsítványok alap és opcionális mezőit, a tanúsítvány felépítését, az egyes mezők tartalmát, a tanúsítványban alkalmazott névformátumokat, ezekre vonatkozó kötöttségeket.

A Specifikáció adminisztráció fejezet ismerteti a szolgáltatást meghatározó kapcsolódó dokumentumok változtatásának, elfogadtatásának és publikálásának szabályait.

A Szabályzat végül Személyes, Szervezeti, illetve Eszköz tanúsítvány Igénylő Adatlap mintákat tartalmaz.

### 1.1.3 Alkalmazott szabványok

A Szabályzat az IETF RFC 2527 szabvány egyes fejezeteinek részletes kidolgozásával készült, és felhasználja a következő szabványokat: ETSI TS 101-456, az ITU X.509, RFC 3039, RFC 2527, RFC 3647, RFC 3280, ETSI TS 102 042, ETSI TS 102 280, ETSI TS 101 456 .

## 1.2 Azonosítás

Jelen dokumentum teljes neve: GIRO Zrt. nem minősített Elektronikus Aláírás Hitelesítés Szolgáltatásának Hitelesítési Rendje. Szolgáltató egyes dokumentumaiban Hitelesítési Rendként vagy HR-ként, e dokumentumon belül Szabályzatként történik rá hivatkozás.

Verzió: 1.1

[http://www.giro.hu/szolgáltatások\\_hiteles\\_szabalyzatok.php](http://www.giro.hu/szolgáltatások_hiteles_szabalyzatok.php)

Szabályzat hatályba lépése: 2007. augusztus 31.

## 1.3 Közösség és alkalmazhatóság

A Regisztrációs Szervezet Regisztrációs Egységeken keresztül nyújtja a szolgáltatásait az Előfizetők részére. Ezen Regisztrációs Egységek listáját a Regisztrációs Szervezet teszi közzé, illetve a lista elérhető a [www.giro.hu/szolq-hiteles-tajek-szerv](http://www.giro.hu/szolq-hiteles-tajek-szerv) weboldalon.

Előfizető Hitelesítés Szolgáltató tanúsítványpublikálási szolgáltatását közvetlenül veheti igénybe, egyéb - pl. ügyfélszolgálati, tanúsítványkezelési - szolgáltatásait csak azon Regisztrációs Szervezet Regisztrációs Egységein keresztül veheti igénybe, amely Regisztrációs Szervezet számára a tanúsítvány igénylése kapcsán a regisztrációt végezte.

## 1.4 Tanúsítványok osztályai és típusai

Hitelesítés Szolgáltató Előfizetők részére több tanúsítványosztályt és tanúsítványtípust kínál.

Jelen Szabályzat a nem minősített osztályba tartozó Személyes, Szervezeti és Eszköz tanúsítványtípust tárgyalja.

### Személyes tanúsítványtípus

A Személyes tanúsítványtípus esetében Aláíró és Előfizető megegyezik, egy és ugyanaz a természetes személy.

A Személyes tanúsítványtípus főbb jellemzői:

Előfizető:	kizárólag természetes személy részére (magánszemély minőségében) kiadható tanúsítvány
Osztálya:	nem minősített
Aláírás-létrehozó eszköz:	intelligens kártya
Kulcs jellemzők:	1024 bit RSA
Kulcs-használat:	Digitális aláírásra
Érvényesség:	365 nap
Felhasználása:	elsődlegesen home-banking, levelezés aláírására

### Szervezeti tanúsítványtípus

A Szervezeti tanúsítvány kizárólag természetes személy részére (szervezethez tartozásának minőségében) adható ki. A tanúsítványtípus esetében Aláíró és Előfizető szétválik: Előfizetőnek

a tanúsítványt igénylő szervezet számít, Aláírónak az a természetes személy (szervezet képviselője) számít, aki számára a szervezet a tanúsítványt igényelte. A tanúsítványban Aláíró az Előfizető azonosító név (*common name*) mezőjében megnevezésre kerül. Előfizető kötelezettségei egyetemlegesen érvényesek az Aláíró személyre.

A Szervezeti tanúsítványtípus főbb jellemzői:

Előfizető:	Valamilyen szervezet (cég, alapítvány, hivatal, kamara, stb.)
Aláíró:	természetes személy (szervezethez tartozó)
Osztálya:	nem minősített
Aláírás-létrehozó eszköz:	intelligens kártya
Kulcs jellemzők:	1024 bit RSA
Kulcs-használat:	digitális aláírásra
Érvényesség:	365 nap
Felhasználása:	elsődlegesen home-banking, levelezés aláírására

### **Eszköz tanúsítványtípus**

Az Eszköz tanúsítványtípus esetében Aláíró és Előfizető szétválik: Előfizetőnek a tanúsítványt igénylő szervezet vagy magánszemély számít, Aláírónak pedig az Előfizető által megnevezett eszköz, amely számára a tanúsítvány igénylése történik. A tanúsítványban Aláíró az Előfizető azonosító név (*common name*) mezőjében megnevezésre kerül. Előfizető kötelezettségei egyetemlegesen érvényesek az Aláíró entitásra.

## **1.5 Szolgáltató adatai**

### **1.5.1 Cím, cégjegyzékszám, kontaktinformációk**

A Szolgáltató teljes neve:	GIRO Elszámolásforgalmi Zártkörűen Működő Részvénytársaság, röviden: GIRO Zrt.
Cégjegyzékszám:	01-10-041159
Székhelye:	1054 Budapest, Vadász u. 31.
Telephelye:	1205 Budapest, Mártonffy u. 25-27.
Postacím:	1054 Budapest, Vadász u. 31.
Telefonszám:	428-5600
Fax:	269-5458
Honlap:	<a href="http://www.giro.hu/szolg-hiteles">www.giro.hu/szolg-hiteles</a>
E-mail cím:	<a href="mailto:hiteles@hiteles.giro.hu">hiteles@hiteles.giro.hu</a>

### **1.5.2 Ügyfélszolgálat**

A szolgáltatással kapcsolatos kérdésekkel, problémákkal Előfizető a tanúsítványának kiadását végző Regisztrációs Szervezet ügyfélszolgálatához fordulhat, melynek elérhetőségét és nyitva tartását az Előfizetői Szerződés tartalmazza, illetve a Regisztrációs Szervezetek listája és elérhetőségük megtekinthető a [www.giro.hu/szolg-hiteles-tajek-szerv](http://www.giro.hu/szolg-hiteles-tajek-szerv) címen.

A szolgáltatással kapcsolatos kérdésekkel, amennyiben a Regisztrációs Szervezet ügyfélszolgálati irodájában nem tudta megoldani, vagy annak működésére van panasa, a Hitelesítő Központ a következő címen kereshető meg: [kerdes@hiteles.giro.hu](mailto:kerdes@hiteles.giro.hu).

### 1.5.3 Szabályzat kibocsátó adatok

A Szabályzatot kibocsátó és karbantartó szervezet a Szolgáltató Szabályozó Szervezete. A szabályzattal kapcsolatos kérdésekkel e szervezet kereshető fel.

Postacím: 1054 Budapest, Vadász u. 31.

Telefonszám: 36-1-428-5600

Fax: 36-1-269-5458

E-mail cím: [szabalyzat@hiteles.giro.hu](mailto:szabalyzat@hiteles.giro.hu)

## 2 Általános rendelkezések

### 2.1 Pénzügyi felelősség korlátjai

Szolgáltató felelősségének korlátjai (a kártérítés felső határa) tanúsítványosztályonként és tanúsítványtípusonként eltérőek. A felelősségvállalás pontos mértéke megtalálható Szolgáltató Általános Szerződési Feltételeiben.

### 2.2 Bizalmasság - Adatkezelési szabályzat

Szolgáltató által kezelt előfizetői adatok:

Mezőnév	Megjegyzés	Cert <sup>1</sup>
Előfizető neve	Elő és utótagokkal együtt	x
Regisztráló szervezet	A regisztrációt végző Intézmény rövid neve	x
Aláíró e-mail	Előfizető egyéni e-mail címe	x
Születési hely, idő	Előfizető születési helye és a születési dátuma	
Anyja neve	Előfizető anyjának leánykori neve	
Leánykori név	Előfizető leánykori neve	
Állandó lakcím	Előfizető állandó lakcíme (ország csak akkor, ha az nem Magyarország, postai irányítószám, város, utca/közterület, házszám, emelet ajtó, hrsz).	
Állampolgárság	Előfizető állampolgársága (ország megnevezése)	
Értesítési cím	Előfizető értesítési címe	
Telefonszám 1	Előfizető napközbeni elérhetősége (mhely/mobil)	
Telefonszám 2	Előfizető egyéb elérhetősége (Otthoni / Mobil)	
Igazolvány 1	Előfizető által bemutatott azonosító okmány (okmány típusa, azonosítója, kibocsátó ország, lejárat ideje)	
Igazolvány 2	Előfizető által bemutatott azonosító okmány (okmány típusa, azonosítója, kibocsátó ország, lejárat ideje)	
Igazolvány 3	Előfizető által bemutatott azonosító okmány (okmány típusa, azonosítója, kibocsátó ország, lejárat ideje)	
Visszavonási jelszó	Előfizető visszavonási jelszava (kódolt formában tárolódik kizárólag a Hitelesítés Szolgáltató rendszerében)	
Nyilvános kulcs	Előfizető nyilvános kulcsa	
Felhasználó azonosító	Előfizető Intézménybeli azonosítója az Intézmény által kezelt azonosító adat, mely nem titkos vagy bizalmas, és nem biztosít hozzáférést ilyen információkhoz harmadik fél számára	x

<sup>1</sup> Az „x”-szel jelölt adatok a tanúsítványba kerülnek.

Fontos megjegyzés, hogy a tanúsítványba kerülő „Aláíró e-mail” mező valóságát és érvényességét Szolgáltató nem ellenőrzi.



### 3 Azonosítás és hitelesítés

A Hitelesítési Rend ezen fejezete a Kezdeti regisztráció, valamint a Tanúsítvány megújítás esetén alkalmazandó azonosítási és hitelesítési eljárásokkal szemben támasztott követelményeket tárgyalja.

#### 3.1 Kezdeti regisztráció

##### 3.1.1 Nevek típusa

Az Előfizető tanúsítványba foglalt azonosítója (Subject) ITU-T X.500 ajánlása egyedi névformátum előírásainak felel meg.

Előfizető azonosítója a következő kötelező mezőkből épül fel, melyeket az itt leírt módon kell kitölteni és értelmezni:

Név: ( <i>Common Name</i> )	Aláíró entitás megnevezése azon a módon, ahogy a regisztrációs úrlapon szerepel
Szervezet: ( <i>Organization</i> )	A regisztrációt végző Intézmény rövid neve, azon a módon, ahogy az együttműködési szerződésben szerepel
Szervezeti egység: ( <i>Organization unit</i> )	Előfizető személy / szervezet neve azon a módon, ahogy a regisztrációs úrlapon szerepel
Ország: ( <i>Country</i> )	HU – Magyarország kétkarakteres kódja az ISO 3166 szabvány szerint
Email cím: ( <i>Email</i> )	Előfizető email címe
Felhasználó azonosító: ( <i>Locality</i> )	Aláíró egyedi azonosítója Intézmény saját azonosító rendszere alapján

##### 3.1.2 Név szemantika

Magyar állampolgárok esetében a személyazonosító igazolványban szereplő írásmódot kell használni, akkor is, ha rendelkeznek más személyazonosító okmánnal.

Nem latin karakterkészlettel (cirill, arab, görög, írásjelek, stb.) íródó nevek esetében a magyar személyazonosító okmányban szereplő írásmódot kell használni. Előfizető azonosító mezői esetében az angol ABC betűi használatosak.

##### 3.1.3 Különböző névformátumok értelmezése

**Személyes tanúsítványtípus** esetében az Előfizető azonosító a "Nevék típusa" fejezetben ismertetett formátumban kerül kiosztásra.

A mezők értelmezése a következő: A tanúsítvány a „Név” nevű természetes személyé, amely „Szervezet” Intézmény ügyfele, „Felhasználó azonosító” azonosítószámmal. A személy e-mail címe „E-mail cím”.

A Felhasználó azonosító mezőnek nem célja, hogy tartalma Intézményen és Előfizetőn túl harmadik fél által értelmezhető legyen.

**Szervezeti tanúsítványtípus** esetében az Előfizető azonosító a "Nevék típusa" fejezetben ismertetett formátumban kerül kiosztásra.

A mezők értelmezése a következő: A tanúsítvány a „Név” nevű természetes személyé, „Szervezeti egység” szervezettel összefüggésben, amely „Szervezet” Intézmény ügyfele. A személy e-mail címe „E-mail cím”, Intézménybeli azonosítószáma „Felhasználó azonosító”.

A Felhasználó azonosító mezőnek nem célja, hogy tartalma Intézményen és Előfizetőn túl harmadik fél által értelmezhető legyen.

**Eszköz tanúsítványtípus** esetében az Előfizető azonosító a "Nevék típusa" fejezetben ismertetett formátumban kerül kiosztásra.

A mezők értelmezése a következő: A tanúsítvány a „Név” megnevezésű (címmel / azonosítóval rendelkező) eszköze, amely „Szervezeti egység” szervezet / személy fennhatósága alatt áll, aki „Szervezet” Intézmény ügyfele. Az eszköz Intézménybeli azonosítószáma „Felhasználó azonosító”, az üzemeltető szervezet / személy email címe „Email cím”.

A Felhasználó azonosító mezőnek célja, hogy a Név mezőben feltüntetett érték összehasonlítható legyen az eszköz tényleges azonosítójával.

### **3.1.4 Nevek egyedisége**

Előfizető azonosítójának egyediségéről egyrészt az Intézmény nevének szerepeltetése másrészt felhasználó intézménybeli egyedi azonosítója, illetve az eszköz azonosítója gondoskodik. A felhasználó azonosító olyan Intézmény által kezelt azonosító adat, mely egyedi és egyértelműen az Előfizetőhöz (Aláíróhoz) kapcsolódik.

### **3.1.5 Név igénylési viták feloldása**

Előfizető azonosítójának kiosztása a Nevek típusa és Név szemantika fejezetekben leírtak alapján történik.

### **3.1.6 Védjegyek elismerésének és hitelesítésének módszere**

Személyes tanúsítvány védjegyre való utalást (kivéve a regisztrációt végző Intézmény védjegyét) nem tartalmazhat. Ezért személyes tanúsítvánnyal összefüggésben a védjegyek hitelesítésére nincs szükség.

Szervezeti tanúsítvány védjegyre való utalást (kivéve a regisztrációt végző Intézmény, valamint Előfizető szervezet nevét) nem tartalmazhat. Szolgáltató Előfizető szervezeti identitását hitelesíti (ld. 3.1.8 Szervezeti identitás hitelesítése).

Eszköz tanúsítvány védjegyre való utalást (kivéve a regisztrációt végző Intézmény megnevezését, valamint Előfizető szervezet nevét és domain nevét) nem tartalmazhat. Szolgáltató Előfizető szervezeti identitását, valamint a domain név használatának jogosságát hitelesíti (ld. 3.1.2 Név szemantika és 3.1.8 Szervezeti identitás hitelesítése).

### **3.1.7 Privát kulcs birtoklás ellenőrzésének módszere**

Személyes és Szervezeti tanúsítvány típus esetén a Szolgáltató maga generálja a felhasználói kulcs-párt, s nem fogad el az Előfizető által generált magánkulcsot, ezért minden esetben biztosított a tanúsítvány kérelemben szereplő nyilvános kulcs és a magánkulcs összetartozása.

Eszköz tanúsítványtípus esetén az Előfizető generálja a kulcs-párt, amelyet kizárólag személyesen nyújthat be a Szolgáltatóhoz. Szolgáltató az eljáró személy személyazonosságát és jogosultságát ellenőrzi.

### 3.1.8 Szervezeti identitás hitelesítése

#### **Személyes tanúsítványtípus**

Személyes tanúsítvány szervezetre való utalást (kivéve a regisztrációt végző Intézményt, vagyis a Regisztrációs Egységet) nem tartalmazhat, ezért személyes tanúsítvánnyal összefüggésben szervezeti identitás hitelesítése nem történik.

#### **Szervezeti tanúsítványtípus**

A Szervezeti tanúsítványban feltüntetésre kerül az Igénylő szervezet neve, valamint a szervezet képviselőjének (Aláírónak) a neve. A regisztráció során a Szolgáltató (Regisztrációs Egység) csak akkor adja ki a szervezeti tanúsítványt, ha a Hitelesítési Szolgáltatási Szabályzatban megfogalmazott feltételeknek az igénylés eleget tesz.

Ennek teljesítésére két módszer kínálkozik az Aláíró részére:

1. Az Igényléshez csatolni kell a szervezet egyértelmű felhatalmazását a tanúsítvány kiadására, az adott Aláíró részére, a szervezet képviselőre jogosult vezető tisztségviselőinek aláírásával és aláírási címpéldánnyal (amennyiben ezzel a Regisztrációs Egység rendelkezik újbóli benyújtásra nincs szükség).
2. A tanúsítványt igénylő Szervezet és a Regisztrációs Szervezet megállapodhat abban, hogy a Regisztrációs Egység a szervezet képviselői részére tanúsítványokat bocsát ki, és azt milyen, az 1. ponttól eltérő, azonosítás mellett teszi. Az azonosítási módszernek olyannak kell lennie, hogy az alapján egyértelműen megállapítható legyen az Aláírónak a szervezethez való tartozása, és biztosítania kell a jogosultság egyértelmű igazolását. Ez a módszer nagyobb mennyiségű tanúsítvány igénylése esetén egyszerűsíti szervezet számára az adminisztrációt.

Az igénylésnek vagy a megállapodásnak tartalmaznia kell egy e-mail címet, mely a Hitelesítési Szervezettel való kapcsolattartására szolgál. Hitelesítés Szolgáltató ezen az e-mail címen értesíti az Igénylés során megjelölt Szervezetet a tanúsítvány kibocsátásáról, vagy annak megtagadásáról.

A Regisztrációs Egység a regisztrációs eljárás során a felhatalmazásról, az aláírási címpéldányról (amennyiben be lett nyújtva), illetve a szervezeti identitás igazolására használt egyéb dokumentumról fénymásolatot készít.

A Regisztrációs Egység a regisztráció során ellenőrzi a bemutatott iratok és okmányok érvényességét és hitelességét. Az azonosítás során felhasznált szervezeti dokumentumokért, a dokumentumok kiállítására, visszavonására, és kezelésére alkalmazott módszer hiányosságaiért a szervezet felelős. Regisztrációs Egység az aláírási jogosultság ellenőrzése céljából adategyeztetést végez a cégnyilvántartással.

Regisztrációs Egység a tanúsítvány kibocsátását megtagadja, amennyiben az okmányok személyhez vagy szervezethez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel.

A Szolgáltató visszautasíthatja a tanúsítvány kiadását, ha:

- a személy szervezethez tartozása nem egyértelmű;
- a szervezet kiléte nem állapítható meg minden kétséget kizáróan;
- nem egyértelmű a szervezet felhatalmazása a tanúsítvány kiadására.

### **Eszköz tanúsítványtípus**

Eszköz tanúsítványban feltüntetésre kerül az Igénylő személy vagy szervezet neve. Szolgáltató csak akkor adja ki az Eszköz tanúsítványt, ha a Hitelesítési Szolgáltatási Szabályzatban megfogalmazott feltételeknek az igénylés eleget tesz.

Amennyiben az igénylés egy szervezet nevében történik, ahhoz csatolni kell a szervezet egyértelmű felhatalmazását a tanúsítvány kiadására, adott Aláíró (eszköz) részére, és az igénylést lefolytató személy meghatalmazásával a szervezet nevében történő eljárásra, a szervezet képviselőre jogosult vezető tisztségviselőinek aláírásával és aláírási címpéldánnyal (amennyiben ezzel Intézmény rendelkezik újbóli benyújtásra nincs szükség).

Az igénylésnek vagy a megállapodásnak tartalmaznia kell egy email címet, mely Szolgáltató Előfizetővel való kapcsolattartására szolgál. Szolgáltató ezen az email címen értesíti az Igénylés során megjelölt Szervezetet a tanúsítvány kibocsátásáról, vagy annak megtagadásáról.

Szolgáltató a Regisztrációs eljárás során a felhatalmazásról, az aláírási címpéldányról (amennyiben be lett nyújtva), és domain név / internet cím felhasználásának jogosságát igazoló dokumentumról fénymásolatot készít.

Szolgáltató a regisztráció során ellenőrzi a bemutatott iratok és okmányok érvényességét és hitelességét. Szolgáltató az aláírási jogosultság ellenőrzése céljából adategyeztetést végez a cégnyilvántartással.

Szolgáltató a tanúsítvány kibocsátását megtagadja, amennyiben az okmányok személyhez vagy szervezethez tartozásával, eredetiségével, valódiságával vagy érvényességével kapcsolatban kétsége merül fel.

A Szolgáltató visszautasíthatja a tanúsítvány kiadását, ha:

- A domain név / internet cím szervezethez tartozása nem egyértelmű
- A szervezet kiléte nem állapítható meg minden kétséget kizáróan
- Nem egyértelmű a szervezet felhatalmazása a tanúsítvány kiadására
- Igénylő személy jogosultsága nem egyértelmű

### **3.1.9 Személyes identitás hitelesítése**

A Regisztrációs Egység az Aláíró személyazonosságáról az elsődleges személyazonosító okmánya alapján győződik meg. A Regisztrációs Egység az elsődleges személyazonosító okmányon túl további másodlagos azonosító dokumentumokat is igényel a biztonság fokozása végett.

#### **Személyes tanúsítványtípus**

A Személyes tanúsítványtípus kibocsátásához egy elsődleges és két másodlagos azonosító dokumentum bemutatása szükséges. A két másodlagos azonosító dokumentum helyettesíthető egy további elsődleges személyazonosító okmány bemutatásával. Az elsődleges személyazonosító okmányok esetében a fénykép és az aláírás alapján, Aláírónak egyértelműen felismerhetőnek kell lennie. A bemutatott dokumentumok mindegyikében az Aláíró nevének, címének, születési dátumának és anyja nevének meg kell egyeznie, amennyiben ilyen adatok szerepelnek rajta (a név esetében a vezetéknev és keresztnév egyezősége elegendő, az elő- és utótagok figyelmen kívül hagyásával; lakcím esetében az értelemszerű egyezés elegendő az emelet és ajtószám hiánya esetén is).

A bemutatott dokumentumok mindegyikének eredetinek és érvényesnek kell lennie. Szolgáltató ennek ellenőrzésére, a bemutatott dokumentumoktól függően, adategyeztetést végez a személyi adat- és lakcímnnyilvántartással, az úti-okmány nyilvántartással, és a gépjárművezetői nyilvántartással. Szolgáltató az Előfizető/Aláíró hozzájárulásával jogosult emellett a bemutatott dokumentumokról fénymásolatot készíteni.

Amennyiben az Aláíró nem képes a kért dokumentumokat bemutatni, nem engedélyezi azokról a másolat elkészítését, vagy a dokumentumok nem a személyhez tartoznak, nem hitelesek, nem érvényesek, a bennük szereplő adatok nem konzisztensek, vagy ezek valamelyikére alapos gyanú áll fenn, a Szolgáltató a tanúsítvány kibocsátását megtagadja.

Elsődleges személyazonosító okmányok	Személyazonosító igazolvány <sup>1</sup> Útleveél Új kiadású (kártya formájú) vezetői engedély
Másodlagos azonosító dokumentumok	Vezetői engedély („régí”) Adóigazolvány Egyéb, a hatóságok által elfogadott dokumentumok (pl. külföldi állampolgárok esetén tartózkodási engedély)

<sup>1</sup> Amennyiben a személyazonosító igazolvány nem tartalmaz érvényes lakcímbegyegyzést, akkor lakcím igazoló kártyával együtt.

### Szervezeti tanúsítványtípus

A Szervezeti tanúsítványtípus kibocsátásához egy elsődleges és két másodlagos azonosító dokumentum bemutatása szükséges. A két másodlagos azonosító dokumentum helyettesíthető egy további elsődleges személyazonosító okmány bemutatásával. Az elsődleges személyazonosító okmányok esetében a fénykép és az aláírás alapján az Aláírónak egyértelműen felismerhetőnek kell lennie. A bemutatott dokumentumok mindegyikében az Aláíró nevének, címének, születési dátumának és anyja nevének meg kell egyeznie, amennyiben ilyen adatok szerepelnek rajta (a név esetében a vezetéknev és keresztnév egyezősége elegendő, az elő- és utótagok figyelmen kívül hagyásával; lakcím esetében az értelemszerű egyezés elegendő az emelet és ajtószám hiánya esetén is).

A bemutatott dokumentumok mindegyikének eredetinek és érvényesnek kell lennie. Regisztrációs Egység ennek ellenőrzésére, a bemutatott dokumentumoktól függően, adategyeztetést végez a személyi adat- és lakcímnnyilvántartással, az úti-okmány nyilvántartással, és a gépjárművezetői nyilvántartással, cégnyilvántartással. Regisztrációs Egység Előfizető/Aláíró hozzájárulásával jogosult emellett a bemutatott dokumentumokról fénymásolatot készíteni.

Amennyiben az Aláíró nem képes a kért dokumentumokat bemutatni, nem engedélyezi azokról a másolat elkészítését, vagy a dokumentumok nem a személyhez tartoznak, nem hitelesek, nem érvényesek, a bennük szereplő adatok nem konzisztensek, vagy ezek valamelyikére alapos gyanú áll fenn, Szolgáltató a tanúsítvány kibocsátását megtagadja.

Elsődleges személyazonosító okmányok	Személyazonosító igazolvány <sup>1</sup> Útleveél Új kiadású (kártya formájú) vezetői engedély
Másodlagos azonosító dokumentumok	Vezetői engedély („régí”) Adóigazolvány Egyéb, a hatóságok által elfogadott dokumentumok (pl. külföldi állampolgárok esetén tartózkodási engedély)

<sup>1</sup> Amennyiben a személyazonosító igazolvány nem tartalmaz érvényes lakcímbegyegyzést, akkor lakcím igazoló kártyával együtt.

### **Eszköz tanúsítványtípus**

Az Eszköz tanúsítványtípus kibocsátásához egy elsődleges és két másodlagos azonosító dokumentum bemutatása szükséges. A két másodlagos azonosító dokumentum helyettesíthető egy további elsődleges személyazonosító okmány bemutatásával. Az elsődleges személyazonosító okmányok esetében a fénykép és az aláírás alapján Igénylőnek egyértelműen felismerhetőnek kell lennie. A bemutatott dokumentumok mindegyikében az Igénylő nevének, címének, születési dátumának és anyja nevének meg kell egyeznie, amennyiben ilyen adatok szerepelnek rajta (a név esetében a vezetéknév és keresztnév egyezősége elegendő, elő és utótagok figyelmen kívül hagyásával; lakcím esetében az értelemszerű egyezés megfelelő az írásmód eltérései ellenére, emelet és ajtószám hiánya esetén is).

A bemutatott dokumentumok mindegyikének eredetinek és érvényesnek kell lennie. Szolgáltató ennek ellenőrzésére, a bemutatott dokumentumoktól függően, adategyeztetést végez a személyi adat- és lakcímnnyilvántartással, az úti-okmány nyilvántartással, és a gépjárművezetői nyilvántartással, cégnnyilvántartással. Szolgáltató jogosult Előfizető/Aláíró hozzájárulásával emellett a bemutatott dokumentumokról fénymásolatot készíteni.

Amennyiben Igénylő nem képes a kért dokumentumokat bemutatni, nem engedélyezi azokról a másolat elkészítését, vagy a dokumentumok nem a személyhez tartoznak, nem hitelesek, érvényesek, a bennük szereplő adatok nem konzisztensek, vagy ezek valamelyikére alapos gyanú áll fenn, Szolgáltató a tanúsítvány kibocsátását megtagadja.

Elsődleges személyazonosító okmányok	Személyi igazolvány <sup>1</sup> Útleve Új kiadású (kártya formájú) vezetői engedély
Másodlagos azonosító dokumentumok	Gépjárművezetői engedély („régí”) Adóigazolvány TAJ kártya

<sup>1</sup> Amennyiben a személyi igazolvány nem tartalmaz érvényes lakcímberegyszítést, akkor lakcím igazoló kártyával együtt.

## **3.2 Tanúsítvány megújítás**

Hitelesítés Szolgáltató a tanúsítvány lejáratá előtti 30 nappal, e-mail üzenetben figyelmezteti az Előfizetőt (Aláíró) a tanúsítványának lejáratára a lejárat dátumának megjelölésével. Megújítás esetén az Előfizetőnek abban az esetben nem szükséges a Regisztrációs Szervezetnél a tanúsítvány igénylése (hasonlóan, mint a kezdeti regisztrációkor), ha nyilatkozik arról, hogy a tanúsítványban megjelenő adatai, valamint a kezdeti regisztrációkor magadott összes adata, továbbra is érvényes, azóta nem változott, és a tanúsítványt megújítani szándékozik.

A Szolgáltató által kibocsátott új tanúsítvány megjelenik a tanúsítványtárban.

## 4 Üzemeltetési követelmények

A Hitelesítési Rend ezen fejezete a Tanúsítványigénylés, Tanúsítvány elfogadás, valamint a Tanúsítvány visszavonás és felfüggesztés esetén alkalmazandó eljárásokkal szemben támasztott követelményeket tárgyalja.

### 4.1 Tanúsítványigénylés

#### **Személyes tanúsítványtípus**

Személyes tanúsítványt csak Előfizető igényelhet a saját nevében a Személyes tanúsítvány Igénylő Adatlap kitöltésével és/vagy aláírásával. A Személyes tanúsítvány Igénylő Adatlap (lásd 1. sz. melléklet) megjelenhet Előfizető által kitöltendő formanyomtatványként, vagy a Regisztrációs Szervezet által kinyomtatott (és kitöltött) nyomtatványként is.

Új tanúsítvány nem igényelhető elektronikus úton, továbbá a Regisztrációs Szervezet a hagyományos aláírás helyett nem fogad el elektronikus aláírást.

A magánkulcs védelmére szolgáló aktiválási adatot a Hitelesítés Szolgáltató generálja vagy az Aláíró adja meg. Aláírónak kötelessége a kód biztonságos módon történő tárolása, illetve a PIN kód megváltoztatása. Az adatlap tartalmazza a visszavonáshoz szükséges jelszót is.

#### **Szervezeti tanúsítványtípus**

Szervezeti tanúsítvány igénylése a Szervezeti tanúsítvány Igénylő Adatlap az Igénylő természetes személy (majdani Aláíró) általi kitöltésével és/vagy aláírásával történik. A Szervezeti tanúsítvány Igénylő Adatlap (lásd 1. sz. melléklet) megjelenhet Előfizető által kitöltendő formanyomtatványként, vagy a Regisztrációs Szervezet által kinyomtatott (és kitöltött) nyomtatványként is.

Új tanúsítvány nem igényelhető elektronikus úton, továbbá a Regisztrációs Szervezet a hagyományos aláírás helyett nem fogad el elektronikus aláírást.

A magánkulcs védelmére szolgáló aktiválási adatot a Hitelesítés Szolgáltató generálja vagy az Aláíró adja meg. Aláírónak kötelessége a kód biztonságos módon történő tárolása, illetve a PIN kód megváltoztatása. Az adatlap tartalmazza a visszavonáshoz szükséges jelszót is.

#### **Eszköz tanúsítványtípus**

Eszköz tanúsítvány igénylése az Eszköz tanúsítványtípus regisztrációs űrlapjának az Igénylő természetes személy általi kitöltésével és/vagy aláírásával történik. A regisztrációs űrlap (lásd 1. sz. Melléklet) megjelenhet Előfizető által kitöltendő formanyomtatványként, vagy a Regisztrációs Szervezet által kinyomtatott (és kitöltött) nyomtatványként is..

Új tanúsítvány nem igényelhető elektronikus úton, és Szolgáltató a hagyományos aláírás helyett nem fogad el elektronikus aláírást.

A magánkulcs védelmére szolgáló aktiválási adatot Szolgáltató generálja vagy Igénylő adja meg. Igénylőnek kötelessége a kód biztonságos módon történő tárolása. Az űrlap tartalmazza a visszavonáshoz szükséges jelszót is.

Amennyiben Előfizető egy szervezet, az igényléshez be kell nyújtani a regisztráció során eljáró természetes személyre vonatkozó hivatalos meghatalmazást is a regisztráció lefolytatására. Az Igénylés során eljáró magánszemély alapadatai a regisztrációs kérelem magánszemélyre vonatkozó részében kerül felvételre.

### **4.3 Tanúsítvány elfogadás**

Személyes tanúsítványt és magánkulcsot, valamint az aláírás-létrehozó eszközt kizárólag az Aláíróként megjelölt Előfizető veheti át személyesen.

Szervezeti tanúsítványt és magánkulcsot, valamint az aláírás-létrehozó eszközt kizárólag az Aláíróként megjelölt természetes személy veheti át.

Eszköz tanúsítványt és magánkulcsot, valamint a kulcshordozó eszközt kizárólag az Igénylés lefolytatására jogosult természetes személy veheti át.

### **4.4 Tanúsítvány visszavonás és felfüggesztés**

Személyes tanúsítvány visszavonását csak Előfizető kérelmezheti. A tanúsítvány visszavonható és felfüggeszthető a Hitelesítés Szolgáltató és annak Felügyeletének kezdeményezése alapján is.

Szervezeti tanúsítvány visszavonását Aláíró és az Előfizető szervezet kérelmezheti. A tanúsítvány visszavonható és felfüggeszthető Hitelesítés Szolgáltató és annak Felügyeletének kezdeményezése alapján is.

Eszköz tanúsítvány visszavonását Előfizető kérelmezheti. A tanúsítvány visszavonható és felfüggeszthető Szolgáltató és annak Felügyeletének kezdeményezése alapján is.

## **5 A Hitelesítési Szervezetre vonatkozó fizikai, eljárásrendi, és humán biztonsági szabályozások**

### **Fizikai biztonsági szabályok:**

A szolgáltatói környezetet a vonatkozó magyar szabványok figyelembe vételével kell kialakítani. A szolgáltatás céljára használt helyiségei fizikai behatolás elleni védelemre felkészítetteknek kell lenniük, a számítástechnikai berendezések üzemeltetéséhez megfelelő környezetet kell biztosítaniuk.

A fizikai védelmi megoldásokban preventív – közvetlen beavatkozást megakadályozó -, és az utólagos visszakereshetőséget biztosító elemeket kell alkalmazni. A biztonsági eseményekről azonnali értesítést kell tudni küldeni az elhárításban, kezelésben érintett személyzetnek.

A szolgáltatás céljaira használt helyiségekbe történő bejutást a szűk üzemeltetői és kiszolgáló személyzet számára kell korlátozni.

A folyamatos működés biztosítása érdekében el kell látni szünetmentes áramforrással.

A folyamatos működés biztosítása érdekében a megfelelő hőmérsékletet és páratartalmat kell biztosítani az üzemi helyiségekben.

Megfelelő tűzvédelmi berendezésekkel kell rendelkezni az eszközök és a kezelő személyzet védelme érdekében.

Az adathordozók tárolása külön, a keletkezési helytől fizikailag elkülönítve oldandó meg.

A keletkezett hulladékok kezelése szabályozottan történjen.



### **Eljárásrendi biztonsági szabályok:**

Szolgáltatás bizalmi jellegű tevékenységeinek ellátása olyan szabályok szerint történik, amelyek biztosítják azt, hogy a feladatokat csak az ellátásához szükséges képzettséggel és felhatalmazással rendelkező, az előírt létszámban egyidejűleg jelen levő és azonosított munkatársak végezhessék.

A szolgáltatást érintő műszaki-technikai változásokat, változtatásokat a Szolgáltató köteles előzetes vizsgálatnak alávetni, és csak sikeres tesztelési eredmény után vezetheti be.

Az eljárásrendi szabályozásnak kiterjed a szorosan értelmezett szolgáltatás, valamint a vele kapcsolatban álló összes kiszolgáló folyamat azonosítására, leírására, feladat és szerepkör leírására.

### **Humán biztonsági szabályok:**

Szolgáltató hitelesítési szolgáltatást nyújtó személyzete megfelelő képzettséggel rendelkezik feladata ellátásához, és rendszeres továbbképzésben részesül.

A szolgáltatás által érintett folyamatokban részt vevő dolgozók a szerepkörönkénti elkülönítése folyamatos ellenőrzés és az ú.n. összeférhetetlenségi táblázat alapján folyamatosan ellenőrzés alatt áll. A kritikus rendszerekhez történő hozzáférés önállóan nem történhet egyetlen személy által sem.

A kezelő-személyzet megfelelő tagjai naprakész ismeretekkel rendelkeznek mind az alapfunkciók, mind a kiszolgáló egységek működésének biztosítása érdekében. A szállítói és gyártói hardver és szoftvertámogatási szerződések biztosítják a vállalt kereteken belüli rendelkezésre állást.

## **6 Technikai szabályozások**

### **Kulcs kezelés:**

A magán kulcsok és kulcs-párok kezelése a Szolgáltató és az Előfizető/Aláíró együttes felelősége. Az alkalmazott algoritmus: RSA – SHA1. A kulcshosszúságok a kibocsátott tanúsítványokban 1024 bit hosszúságúak. A Szolgáltató a hitelesítő központban 2048 bit hosszúságú kulcsokat használ.

A kulcskezelés biztonságos úton valósítja meg a következőket:

- Kulcspár generálás
- Magán kulcs biztonságos továbbítása
- Nyilvános kulcsok és tanúsítványok publikálása
- Aktiválási és visszavonási eljárások

Szolgáltató nem biztosítja a következőket:

- Előfizetői/Aláírói magán kulcsok mentése, archiválása kezelése.

### **Biztonságos környezet biztosítása:**

A szolgáltatás bizalmas jellegének megtartása érdekében a Szolgáltató a fizikai biztonsági védelmi intézkedéseken túl biztosítja a logikai biztonságot is. A szolgáltatás nyújtása közben csak az érintett felek számára megismerhető módon zajlik a kommunikáció. Az informatikai rendszer rosszindulatú vagy illetéktelen hozzáférés ellen védett. Szolgáltató biztosítja továbbá a hitelesítő központ és kapcsolódó elemei magánkulcsainak védelmét.

### **Fizikai biztonság:**

Szolgáltató a pénzügyi szervezetek számára általánosan és kötelezően előírt biztonságos környezetben üzemelteti a szolgáltatáshoz kapcsolódó technikai eszközeit, mellyel a Szolgáltató megakadályozza az illetéktelen hozzáférést, behatolást, károkozást, illetve az információk eltulajdonítását. Zsilipekkel elhatárolt zárt területen, belépés és hozzáférés menedzsmentet alkalmaz, folyamatos (7/24/365) ügyeletben levő biztonságtechnikai személyzettel.

### **Logikai biztonság:**

Szolgáltató a kapcsolódó hardver és szoftver eszközeit kizárólag a szolgáltatás nyújtásához használja, azokon más alkalmazások nem találhatóak. A hitelesítő központok határvédelmi eszközökkel szeparáltan több zónás biztonsági rendszert alkotnak és a hozzáférés az egyszilárdság biztosítása érdekében nem megkerülhető módon biztosított, amely minden esetben csak a következő zónáig terjed.

A határvédelmi megoldások tartalmaznak tűzfalakat, behatolás detektáló és elhárító berendezéseket, vírusvédelmi eszközöket.

Szolgáltató saját időszerverével biztosítja rendszereiben az egységes időt, és ezáltal a naplófájlok konzisztenciáját. Az időszerver két független időforrásra szinkronizált, napi eltérése kevesebb, mint 1/1000 s/nap (nem időpecsét szolgáltatás).

Rendelkezésre állás biztosítása érdekében Szolgáltató rendelkezik Üzletmenet Folytonossági Tervvel, mely tartalmazza az incidenskezelési-, katasztrófa elhárítási és helyreállítási eljárásokat is.

Szolgáltató a visszakereshetőség és bizonyíthatóság érdekében folyamatos üzemeltetési- és külön biztonsági naplózást végez, melyek modulonként és zónánként elkülönítetten keletkeznek és tárolódnak.

Szolgáltató a logikai és fizikai biztonságot, illetve az alkalmazott technológiát, megoldások napra készségét rendszeresen ellenőrzi és ellenőriztetni független auditor céggel.

Szolgáltató olyan operációs rendszereket alkalmaz, amely a biztonságpolitikát legalább a következő területeken támogatja:

- Account-politika, amely meghatározza a felhasználó által karbantartott jelszavakkal kapcsolatos követelményeket,
- Felhasználói jog politika, amely meghatározza, hogy a felhasználókat (felhasználói csoportokat) milyen jogok illethetik meg, felülvizsgálatuk gyakoriságát,
- Audit-politika, amely meghatározza azt, hogy milyen informatikai eseményekről készüljön napló.

A felhasználói, az üzemeltetői, rendszertámogatói és a fejlesztői jogosultságok elhatároltak. A rendszergazdák, rendszeradminisztrátorok, biztonsági adminisztrátorok, továbbá a széles körű hozzáférései jogokat nyert felhasználók neveit és jelszavait kiemelt biztonsággal kezeli; esetükben az azonosítás és a hitelesítés kötelező.

A Hitelesítő központ és a Regisztrációs Szervezet közti kommunikáció védett csatornán keresztül bonyolódik.

### **Életciklus:**

Szolgáltató a magas biztonsági követelményeket a rendszer teljes életciklusára kiterjedően biztosítja.

## 7 Tanúsítvány és kulcs-visszavonási profil

### 7.1 Tanúsítvány profil

A Hitelesítési Rend ezen fejezete a 7.1.2 Alap mezőkkel, valamint a 7.1.12 Egyéb kiterjesztések mezőkkel szemben támasztott követelményeket tárgyalja.

Mezőnév	Érték	Kritikus <sup>1</sup>
Verzió	V3	
Sorozatszám	<i>Szolgáltató által kiadott egyedi sorozatszám</i>	
Algoritmusazonosító	RSA - SHA1	
Kibocsátó	c=hu/o=giro/ou=hiteles/cn=fokozott	
Érvényesség	<i>A tanúsítvány érvényességének kezdő és végdátuma</i>	
Előfizető	<i>c=hu/ o=Regisztrációs Szervezet neve/ L=Előfizető intézményi azonosítója/ cn=Előfizető neve/e-mail=Előfizető e-mail címe</i>	
Előfizető nyilvános kulcsának algoritmus azonosítója	RSA – SHA1	
Előfizető nyilvános kulcsa	<i>Előfizető nyilvános kulcsa</i>	
Aláírás	<i>Szolgáltató tanúsítványt hitelesítő elektronikus aláírása</i>	
Kibocsátó egyedi azonosító	Üres	
Előfizető egyedi azonosító	Üres	
Tanúsítási szabályzat	PolicyIdentifier = <b>1.3.6.1.4.1.11526.2.1.1.2.2</b> PolicyQualifier = <a href="http://www.giro.hu/szolg-hiteles-szabaly">http://www.giro.hu/szolg-hiteles-szabaly</a> UserNotice = "A tanúsítvány értelmezéséhez és elfogadásához a Szolgáltató Hitelesítési Szabályzatában és Hitelesítési Szolgáltatási Szabályzatában foglaltak szerint kell eljárni, melyek megtalálhatók a következő címen: <a href="http://www.giro.hu/szolg-hiteles-szabaly">http://www.giro.hu/szolg-hiteles-szabaly</a> "	Nem
Alapvető megkötések	Subject type = End Entity Path Length Constraint = None	Nem
Kulcshasználat	Key Usage = Non-Repudiation	Nem
Kiterjesztett kulcshasználat	<i>Nem kitöltött</i>	Nem
CRL szétosztási pont	URL=ldap://tar.giro.hu:389/cn%3dgirootcr,ou%3droot,o%3dgiro,c%3dhu?certificateRevocationList?base?objectClass=cRLDistributionPoint	Nem
Netscape típus	SSL Client és S/MIME Client	Nem

<sup>1</sup> A kritikus azt jelenti, hogy az alkalmazás a tanúsítványban ellenőrzi, ezen mező kitöltését, és csak akkor fogadja el, ha értelmezni tudja, és az ott lévő érték számára megfelelő.

### **7.1.2 Alap mezők**

Szolgáltató által kibocsátott Személyes tanúsítványok Subject mezőjébe Előfizető egyedi azonosítója kerül a Nevek típusa fejezetben tárgyaltnak megfelelően.

Szolgáltató által kibocsátott Szervezeti tanúsítványok Subject mezőjébe Előfizető egyedi azonosítója kerül a Nevek típusa fejezetben tárgyaltnak megfelelően.

Szolgáltató által kibocsátott Eszköz tanúsítványok Subject mezőjébe Előfizető egyedi azonosítója kerül a Nevek típusa fejezetben tárgyaltnak megfelelően.

### **7.1.12 Egyéb kiterjesztések**

#### **7.1.12.1 Alapvető megkötések**

Szolgáltató a kibocsátott tanúsítványok Basic Constraints kiterjesztésének "Subject Type " mezőjébe az „End Entity” értéket írja.

#### **7.1.12.2 Kulcshasználat**

Szolgáltató a kibocsátott tanúsítványok Key Usage kiterjesztésébe a Non-Repudiation értéket írja.

#### **7.1.12.3 Kiterjesztett kulcshasználat**

Szolgáltató a kibocsátott tanúsítványok Extended Key Usage kiterjesztését nem tölti ki.

#### **7.1.12.5 CRL szétosztási pont**

Szolgáltató a kibocsátott tanúsítványok CRL Distribution Point kiterjesztésébe a tanúsítványtár címét írja.

#### **7.1.12.6 Netscape típus**

Szolgáltató a kibocsátott tanúsítványok Netscape Type kiterjesztésébe az SSL Client és S/MIME Client értéket írja.

## **7.2 Kulcs-visszavonási profil**

Szolgáltató az International Telecommunication Union által kiadott ITU-T X.509 "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks" ajánlás (továbbiakban X.509) 2. verziója szerinti Tanúsítvány Visszavonási Listákat bocsát ki.

Szolgáltató az X.509 2. verziója szerinti tanúsítvány visszavonási kiterjesztéseket támogatja. A kritikus visszavonási lista kiterjesztés és visszavonás bejegyzési kiterjesztések feldolgozásáért Előfizető és Érintett fél alkalmazása és eljárása felelős. Szolgáltató semmilyen körülmények között nem hibáztatható a kiterjesztések figyelmen kívül hagyása vagy téves értelmezése miatt.

## **8 Specifikáció adminisztráció**

A Hitelesítési Rend specifikáció adminisztrációját a Szolgáltató Szabályozó Szervezete végzi. Elérhetősége a Szabályzat 1.5.3 pontjában található.

### **8.1 Specifikáció változáskezelési eljárásai**

Szolgáltató saját döntése alapján jogosult a Hitelesítési Rend módosítására. A módosított Szabályzatot új verziószámmal hozza létre.

### **8.2 Publikációs és értesítési szabályok**

Jelen szabályzatot érintő változás bejelentéséről az értesítést GIRO Zrt. az Interneten, a következő címen: [http://www.giro.hu/szolgáltatások\\_hiteles\\_szabalyzatok.php](http://www.giro.hu/szolgáltatások_hiteles_szabalyzatok.php) teszi közzé.

### **8.3 Hitelesítési Rend elfogadási eljárások**

A Hitelesítési Rend bármely módosítását a Szolgáltató Szabályozó Szervezete hagyja jóvá.

Iktatószám: .....

## Melléklet –Személyes tanúsítvány Igénylő Adatlap

Igényazonosító:				...../200 .
-----------------	--	--	--	-------------

<b>Tanúsítványba kerülő (nyilvános) adatok</b>					
Aláíró neve <sup>1,5</sup> :				e-mail cím <sup>5</sup> :	
<b>Szolgáltató által nyilvántartott (bizalmasan kezelt) adatok</b>					
<b>Aláíró személyes adatai</b>					
Születési hely <sup>6</sup> :				Születési idő <sup>2</sup> :	
Leánykori név:				Anyja neve:	
Állampolgárság					
Telefon <sup>7</sup> :				Fax:	
<b>Állandó lakcím</b>					
Ország:				Város:	
Irányítószám:	Utca, hsz., em., ajtó:				
<b>Levelezési cím</b>					
Ország:				Város:	
Irányítószám:	Utca, hsz., em., ajtó:				
<b>Azonosító dokumentumok adatai<sup>3</sup></b>					
<b>Elsődleges személyazonosító okmány 1</b>					
Okmány típusa <sup>4</sup> :	Szem. ig.	Útlevel	Egyéb:	Azonosító:	
Kibocsátó ország:				Lejárat <sup>2</sup> :	
<b>Elsődleges személyazonosító okmány 2</b>					
Okmány típusa <sup>4</sup> :	Szem. ig.	Útlevel	Egyéb:	Azonosító:	
Kibocsátó ország:				Lejárat <sup>2</sup> :	
<b>Másodlagos azonosító dokumentum 1</b>					
Okmány típusa <sup>4</sup> :	Adóigazolvány	Lakcímgazoló	Egyéb:	Azonosító:	
	Vezetői engedély				
Kibocsátó ország:				Lejárat <sup>2</sup> :	
<b>Másodlagos azonosító dokumentum 2</b>					
Okmány típusa <sup>4</sup> :	Adóigazolvány	Lakcímgazoló	Egyéb:	Azonosító:	
	Vezetői engedély				
Kibocsátó ország:				Lejárat <sup>2</sup> :	

Kijelentem, hogy a tanúsítványigényléssel kapcsolatos tájékoztatást megkaptam, Szolgáltató szerződéses feltételeit, valamint szabályzatait megértettem, azokat elfogadom és hozzájárulok tanúsítványom Szolgáltató által történő publikálásához.

Dátum: \_\_\_\_\_

Aláíró aláírása: \_\_\_\_\_

<sup>1</sup> Ahogy az a személyazonosító igazolványban szerepel

<sup>2</sup> ÉÉÉÉ HH NN

<sup>3</sup> Két elsődleges vagy egy elsődleges és két másodlagos dokumentum szükséges az igényléshez

<sup>4</sup> X-elje be a megfelelőt.

<sup>5</sup> Tanúsítványban megjelenik.

<sup>6</sup> Város, ország

<sup>7</sup> Napközbeni elérhetőség (Mhely / Mobil), egyéb elérhetőség (Otthoni / Mobil)

<sup>8</sup> Magánkulcs védelmére szolgáltató aktiválási adat

<sup>9</sup> Tanúsítvány visszavonásához szükséges adat



### Aláíró titkosan kezelendő adatai (szolgáltató által nem tárolt)

Magánkulcs jelszó / PIN kód <sup>9</sup> :		Visszavonási jelszó <sup>9</sup> :	
--	--	------------------------------------	--

Iktatószám: .....

## Melléklet – Szervezeti tanúsítvány Igénylő Adatlap



Igényazonosító: \_\_\_\_\_

...../200 .

Tanúsítványba kerülő (nyilvános) adatok					
Aláíró személy neve <sup>1,5</sup> :			e-mail cím <sup>5</sup> :		
Előfizető szervezet neve <sup>5</sup> :					
Szolgáltató által nyilvántartott (bizalmasan kezelt) adatok					
Aláíró személyes adatai					
Születési hely <sup>6</sup> :		Születési idő <sup>2</sup> :			
Leánykori név:		Anyja neve:			
Állampolgárság					
Telefon <sup>7</sup> :		Fax:			
Állandó lakcím					
Ország:		Város:			
Irányítószám:		Utca, hsz., em., ajtó:			
Előfizető szervezet adatai					
Cím, Székhely					
Ország:		Város:			
Irányítószám:		Utca, hsz., em., ajtó:			
Telefon, Fax <sup>7</sup> :		e-mail cím <sup>7</sup> :			
Azonosító dokumentumok adatai <sup>3</sup>					
Elsődleges személyazonosító okmány 1					
Okmány típusa <sup>4</sup> :		Szem. ig.		Útlevel	
Kibocsátó ország:		Egyéb:		Azonosító:	
				Lejárat <sup>2</sup> :	
Elsődleges személyazonosító okmány 2					
Okmány típusa <sup>4</sup> :		Szem. ig.		Útlevel	
Kibocsátó ország:		Egyéb:		Azonosító:	
				Lejárat <sup>2</sup> :	
Másodlagos azonosító dokumentum 1					
Okmány típusa <sup>4</sup> :		Adóigazolvány		Lakcímgazoló	
		Vezetői engedély		Egyéb:	
Kibocsátó ország:		Azonosító:			
		Lejárat <sup>2</sup> :			
Másodlagos azonosító dokumentum 2					
Okmány típusa <sup>4</sup> :		Adóigazolvány		Lakcímgazoló	
		Vezetői engedély		Egyéb:	
Kibocsátó ország:		Azonosító:			
		Lejárat <sup>2</sup> :			
Szervezeti identitás hitelesítésére alkalmazott dokumentum					
Dokumentum <sup>11</sup> :		Felhatalmazás		Más:	
		Aláírási címpéldány		Azonosító:	
				Lejárat:	

Kijelentem, hogy a tanúsítvány igényléssel kapcsolatos tájékoztatást megkaptam, Szolgáltató szerződéses feltételeit, valamint szabályzatait megértettem, azokat elfogadom és hozzájárulok tanúsítványom Szolgáltató által történő publikálásához.

Dátum: \_\_\_\_\_

Aláíró aláírása: \_\_\_\_\_

<sup>1</sup> Ahogy az a személyazonosító igazolványban szerepel

<sup>2</sup> ÉÉÉÉ.HH.NN alakban

<sup>3</sup> Két elsődleges vagy egy elsődleges és két másodlagos dokumentum szükséges az igényléshez

<sup>4</sup> X-elje be a megfelelőt.

<sup>5</sup> Tanúsítványban megjelenik.

<sup>6</sup> Város, ország

<sup>7</sup> Napközbeni elérhetőség (mhely / mobil), egyéb elérhetőség (otthoni / mobil)

<sup>8</sup> Magánkulcs védelmére szolgáló aktiválási adat

<sup>9</sup> Tanúsítvány visszavonásához szükséges adat

<sup>10</sup> Szervezet központi telefon és fax elérhetősége és e-mail címe

<sup>11</sup> A felhatalmazás aláírási címpéldánnyal és a nélkül is érvényes lehet



### Aláíró titkosan kezelendő adatai (szolgáltató által nem tárolt)

Magánkulcs jelszó / PIN kód<sup>9</sup>:Visszavonási jelszó<sup>9</sup>:

Iktatószám: .....

## Melléklet – Eszköz tanúsítványtípus Igénylő Adatlap



Igény azonosító:				...../200 .
------------------	--	--	--	-------------

Tanúsítványba kerülő (nyilvános) adatok					
Aláíró megnevezése <sup>1,5</sup> :					
Előfizető neve <sup>5,12</sup> :		E-mail cím <sup>5</sup> :			
Szolgáltató által nyilvántartott (bizalmasan kezelt) adatok					
Igénylő <sup>12</sup> (és meghatalmazottja) adatai <sup>13</sup>					
Születési hely <sup>6</sup> :				Születési idő <sup>2</sup> :	
Leánykori név:				Anyja neve:	
Állampolgárság					
Telefon <sup>7, 13</sup> :				Fax:	
Cím, Székhely <sup>13</sup>					
Ország:				Város:	
Irányítószám:				Utca, hsz., em., ajtó:	
Azonosító dokumentumok adatai <sup>3</sup>					
Elsődleges személyazonosító okmány 1					
Okmány típusa <sup>4</sup> :		Személyi lg.		Azonosító:	
Kibocsátó ország:		Útleve		Lejárat <sup>2</sup> :	
Okmány típusa <sup>4</sup> :		Személyi lg.		Azonosító:	
Kibocsátó ország:		Útleve		Lejárat <sup>2</sup> :	
Másodlagos azonosító dokumentum 1					
Okmány típusa <sup>4</sup> :		Jogosítvány		Azonosító:	
Kibocsátó ország:		Adóigazolvány		Lejárat <sup>2</sup> :	
		TAJ kártya			
		Lakcímgazoló			
Másodlagos azonosító dokumentum 2					
Okmány típusa <sup>4</sup> :		Jogosítvány		Azonosító:	
Kibocsátó ország:		Adóigazolvány		Lejárat <sup>2</sup> :	
		TAJ kártya			
		Lakcímgazoló			
Szervezeti identitás hitelesítésére alkalmazott dokumentum Domain név és Internet cím használatának jogossága					
Dokumentum <sup>11</sup> :		Felhatalmazás		Más:	
		Aláírási címpéldány		Internet szolgáltatási szerződés	

Kijelentem, hogy a tanúsítványigényléssel kapcsolatos tájékoztatást megkaptam, Szolgáltató szerződéses feltételeit, valamint szabályzatait megértettem, azokat elfogadom és hozzájárulok tanúsítványom Szolgáltató által történő publikálásához.

Dátum: \_\_\_\_\_

Aláírás: \_\_\_\_\_

<sup>1</sup> Aláíró eszköz web címe vagy domain néve

<sup>2</sup> ÉÉÉÉ.HH.NN alakban

<sup>3</sup> Két elsődleges vagy egy elsődleges és két másodlagos dokumentum szükséges az igényléshez

<sup>4</sup> X-elje be a megfelelőt.

<sup>5</sup> Tanúsítványban megjelenik.

<sup>6</sup> Város, ország (ha nem Magyarország)

<sup>7</sup> Magánszemélynél: Napközbeni elérhetőség (Mhely / Mobil), egyéb elérhetőség (Otthoni / Mobil), Szervezetnél: Szervezet telefonszámai

<sup>8</sup> Magánkulcs védelmére szolgáló aktiválási adat

<sup>9</sup> Tanúsítvány visszavonásához, felfüggesztéséhez és újraterjesztéséhez szükséges adat

<sup>11</sup> A felhatalmazás aláírási címpéldánnyal és a nélkül is érvényes lehet

<sup>12</sup> Magánszemély vagy szervezet

<sup>13</sup> Amennyiben Igénylő magánszemély az összes adat rá vonatkozik, ha Igénylő egy szervezet, akkor a „Telefon”, „Fax”, „Székhely” és „Szervezeti identitás hitelesítésére alkalmazott dokumentum” mezők a szervezetre, többi mező a meghatalmazásával eljáró magánszemélyre vonatkozik



Aláíró titkosan kezelendő adatai (szolgáltató által nem tárolt)

Magánkulcs jelszó / PIN kód <sup>8</sup> :		Visszavonási jelszó <sup>9</sup> :	
--	--	------------------------------------	--