GIRO Rt.

Hitelesítési Szolgáltatási Szabályzata

1.0 változat

HIF regisztrációs szám: FA 7717-1/2001

Verzió: 1.0

Szabályzat hatályba lépése: 2001. december 20.

Tartalomjegyzék

1 Bevezetés

A Giro Rt szerződéses partnereivel Hitelesítés Szolgáltatást nyújt. Ennek keretében

- A regisztráció során hitelt érdemlően azonosítja az igénylőket.
- A regisztrált ügyfelek részére elektronikus aláírás készítésére alkalmas kulcsokat és az ezek ügyfélhez tartozását igazoló tanúsítványt készít és helyez el egy intelligens kártyán.
- A kiadott tanúsítványokról nyilvántartást vezet, melynek elérhetőségét biztosítja annak érdekében, hogy az aláírt dokumentumot elfogadó azt ellenőrizni tudja.
- Amennyiben az ügyfél ezt kéri, vagy vélelmezhető, hogy a tanúsítványon szereplő kulcs kompromitálódott, a tanúsítvány érvényességét felfüggeszti, illetve visszavonja. A felfüggesztés kérését több módon is lehetővé teszi.
- A visszavont tanúsítványok listáját rendszeresen publikálja.
- A lejárati időn belül lehetőséget biztosít a megváltozott adatok módosítására, illetve a lejárat végén annak meghosszabítására.
- Működését nyilvános szabályzatokban írja le, hogy minden fél meggyőződhessen arról, hogy milyen mértékben bízhat meg a tanúsítványban szereplő adatokban.
- Ezen lehetőségeket magánszemélyek és szervezetek számára is biztosítja annak érdekében, hogy azok saját maguk, illetve eszközeik adatait is tanúsíttatni tudják.

1.1 Összefoglalás

1.1.1 Szabályzat célja

Jelen dokumentum célja, hogy összefogja azokat az előírásokat és információkat, melyeket a Szolgáltatással valamilyen módon kapcsolatba kerülő feleknek tudni érdemes. Biztosítja a Szolgáltató működésének átláthatóságát, s lehetővé teszi a felhasználók számára, hogy megállapítsák azt, hogy az ismertetett gyakorlat, valamint a kibocsátott tanúsítványok mennyiben felelnek meg az elvárásaiknak. A Szabályzat, az Általános Szolgáltatási Feltételek és egyéb, a Szabályzatban hivatkozott dokumentumok tartalmának megismerése után, a tanúsítvány elfogadóinak egyértelműen meg kell tudni állapítani a tanúsítvány kezelésének módját, az általa garantált biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügy garanciákat, jogi felelősség vállalásokat.

1.1.2 Szabályzat tartalma

A Hitelesítési Szolgáltatási Szabályzat 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; felsorolja a szabályzat alapján kibocsátható tanúsítvány osztályokat és típusokat; ismerteti a szabályzat egyéb dokumentumokhoz való viszonyát, tájékoztatást ad a Szolgáltató által nyújtott szolgáltatásokról, és ezek alkalmazói közösségéről.

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

Az Azonosítás és hitelesítés fejezet a tanúsítványok igényléséhez kapcsolódó előfizetői regisztráció menetét ismerteti, a regisztrációval kapcsolatos tájékoztatással, a regisztrációs adatok összegyűjtésével, és egyéb részletekkel. A kezdeti regisztráció kapcsán felsorolja az elnevezés során követett szabványokat és szabályokat, a különböző név formátumok értelmezését, a nevek egyediségének biztosítását, a név igénylési viták feloldását; 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 követett gyakorlatot és támasztott követelményeket a tanúsítványok igénylése, kibocsátása, elfogadása, felfüggesztése és visszavonása, és kezelése kapcsán; tájékoztat a szolgáltatás megszűnésének körülményeiről, a felek ez esetre vonatkozó jogairól és kötelességeiről, a tanúsítványok kezeléséről, az előfizetők értesítéséről, és az archív adatok kezelésére vonatkozó eljárásokról; valamint ismerteti Szolgáltató naplózási, archiválási és katasztrófa elhárítási eljárásait.

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

A Technikai szabályozások fejezet ismerteti a kulcs-párok generálásának, a privát kulcs címzetthez juttatásának, a Hitelesítő Szervezet nyilvános kulcsának a felhasználókhoz való eljuttatásának szabályait, s a kulcsokkal kapcsolatos technikai követelményeket. Megadja a Szolgáltató és az előfizetők privát kulcsának védelmére vonatkozó előírásokat, a privát kulcs kriptográfiai modulba helyezésének módját, aktiválását, deaktiválását és megsemmisítését. Tájékoztatást ad a kulcs-párok kezelésének egyéb aspektusairól, mint például a nyilvános kulcs archiválására vonatkozó előírásokról, vagy a nyilvános és privát kulcs felhasználási idejéről; leírja a privát kulcsok védelmére szolgáló aktiválási adatok generálását, installációját, s védelmét; valamint IT és hálózati biztonsági, életciklus technikai eljárásokat ismertet.

A Tanúsítvány és kulcsvisszavonási profil fejezet ismerteti a kiadott 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 változatásának, elfogadtatásának és publikálásának szabályait.

A Meghatározások fejezet a jelen szabályzatban használt, kifejezések értelmezését, magyarázatát tartalmazza.

1.1.3 Szabványok

A Szabályzat, az IETF RFC 2527 szabvány egyes fejezeteinek részletes kidolgozásával készült, tartalmi vonatkozásokban eleget tesz a 2001. évi XXXV. sz. elektronikus aláírásról szóló törvény előírásainak. Ezen túl felhasználja az ETSI TS 101-456, az ITU X.509, valamint az ABA és a CARAT Guidelines egyes ajánlásait.

1.2 Azonosítás

Jelen dokumentum teljes neve: GIRO Rt. Hitelesítési Szolgáltatási Szabályzata. A Szolgáltató egyes dokumentumaiban Hitelesítési Szolgáltatási Szabályzatként vagy HSZSZ-ként, e dokumentumon belül Szabályzatként történik rá hivatkozás.

HIF regisztrációs szám: FA 7717-1/2001

Verzió: 1.0

Szabályzat hatályba lépése: várhatóan 2001. december 20.

1.3 Közösség és alkalmazhatóság

A Szabályzat keretei között a Szolgáltató által kibocsátott tanúsítványok alkalmazó közössége a GIRO Rt., a GIRO Rt.-vel szerződést kötött Pénzügyi Intézmények, a Magyar Nemzeti Bank, a Magyar Államkincstár és a KELER Rt. (továbbiakban együttesen Intézmény, illetve Intézmények), ezen Intézmények ügyfelei (Előfizetők) és az Érintett felek (1.3.4.2 pont).

1.3.1 Hitelesítő Szervezet

A Hitelesítő Szervezet a Szolgáltató központi eleme, amely tanúsítvány-létrehozás és egyéb tanúsítvány-menedzsment feladatokat lát el. A Hitelesítő Szervezetet a Szolgáltató jelen Szabályzat, és egyéb nyilvános előírások, és eljárásrendek szerint üzemelteti.

1.3.2 Regisztrációs Szervezetek

A Regisztrációs Szervezet a szolgáltatás Giro Rt., illetve a vele együtt működő Intézmények azon eleme, amely az Előfizetők adatainak regisztrációját, ellenőrzését, az igénylő azonosságának megállapítását, a tanúsítvány kérelmek összeállítását, Hitelesítő Szervezethez továbbítását, és egyéb azonosítási és tanúsítványmenedzsment feladatokat látnak el. A Regisztrációs Szervezeteket a Szolgáltató jelen Szabályzat és egyéb előírások (Általános Szerződési Feltételek, Előfizetői Szerződés) és eljárásrendek szerint üzemelteti. Egy regisztrációs szervezethez tartozó Előfizetők önálló közösséget alkothatnak, melyre a regisztrációs szervezet további szabályokat is alkalmazhat. A további szabályok nem tartalmazhatnak olyan kikötést, amely ellentétben áll a Szabályzattal vagy az Általános Szerződési Feltételekkel.

1.3.3 Szabályozó Szervezet

A Szabályozó Szervezet a Szolgáltató által létrehozott szervezet, amely a Szolgáltatással kapcsolatos szabályzatok kialakításáért, elfogadásáért, adminisztrációjáért felelős.

A Regisztrációs Szervezet által létrehozott szabályokat Szabályozó Szervezet ellenőrzi a Szolgáltató szabályzatainak, szerződésének és üzletpolitikájának való megfelelőség szempontjából.

1.3.4 Végfelhasználók

1.3.4.1 Előfizető

Előfizető a Szolgáltatóval, az Általános Szerződési Feltételekben foglaltak szerint szerződéses viszonyban álló felhasználó, aki számára a Szolgáltató tanúsítványt bocsát ki.

1.3.4.2 Érintett fél

Az Érintett fél a Szolgáltatóval - ezen minőségében - szerződéses viszonyban nem álló személy, vagy szervezet, amely az elektronikus dokumentum fogadója, és egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el.

1.3.5 Alkalmazhatóság

1.3.5.1 Szabályzat hatálya

A Szabályzat időbeli hatálya: A Hitelesítési Szolgáltatási Szabályzat hatályba lépése várhatóan 2001. december 21. napja a Hírközlési Főfelügyelet nyilvántartásba vételétől függően. A Szabályzat hatálya megszűnik, amennyiben a Szolgáltató új szabályzatot bocsát ki, és abban így rendelkezik, ha visszavonja azt, vagy ha beszűnteti tevékenységét.

A Szabályzat személyi hatálya: A Hitelesítési Szolgáltatási Szabályzat személyi hatálya az alkalmazó Közösségre terjed ki.

1.3.5.2 Szolgáltatás szintje

A Szolgáltató jelen Szabályzatot és egyéb dokumentumokat 2001. november 21. napján átadta a Hírközlési Főfelügyelet részére fokozott biztonságú hitelesítési szolgáltatóként történő nyilvántartásba vétel céljából.

A Szolgáltató a 2001. évi XXXV. sz. elektronikus aláírásról szóló törvény szerinti fokozott biztonságú (nem minősített) szolgáltatást nyújt.

A Szolgáltatást a 2.7 pontnak megfelelően független auditor cég tanúsítja.

1.3.5.3 Tanúsítványok alkalmazhatósága

A Szolgáltató által kibocsátott tanúsítványok és magánkulcsok az Előfizető és az Intézmény között az elektronikus adatcsere során használt üzenetek, dokumentumok hitelesítésére kerültek kibocsátásra, de Intézmények a tanúsítványok alkalmazhatóságára vonatkozóan további szabályokat határozhatnak meg a Hitelesítő Központtal egyetértésben. A Szolgáltató által kibocsátott előfizetői tanúsítványok jogszerűen kizárólag a Szolgáltató által meghatározott célra használhatóak az Általános Szerződési Feltételek, a Hitelesítési Szolgáltatási Szabályzat illetve az Előfizetői Szerződés feltételeinek elfogadása után.

1.4 Tanúsítványok osztályai és típusai

Szolgáltató az Előfizetők részére tanúsítványokat bocsát ki. Ezen kibocsátott tanúsítványok az 1.3.5.3 Tanúsítványok alkalmazhatósága fejezetben meghatározott célokra használhatók. A kibocsátott Előfizetői tanúsítványok 1 évig érvényesek. Az érvényesség kezdete a tanúsítvány elhelyezésének napja a Szolgáltató Tanúsítványtárában, lejárata az ezt követő 365. nap 24.00 óra. Ezen időszak alatt az Előfizető kérésére, illetve egyéb okok miatt a tanúsítványok ideiglenesen felfüggeszthetők, illetve véglegesen visszavonhatók a Regisztrációs Szervezeten keresztül. A tanúsítványokat és a visszavont tanúsítványok listáját a Szolgáltató tanúsítványtár szolgáltatáson keresztül elérhetővé teszi, mind az Előfizető, mind az Érintett Fél részére.

Szolgáltatónál három hitelesítési osztály működik. Az egyes hitelesítési osztályok – többek között - az azonosítás menetében, és ezáltal a tanúsítvány és az Aláíró közötti egyértelmű megfeleltethetőség szintjében térnek el. Előfizető egyéni mérlegelési joga, hogy meghatározza, melyik osztályba tartozó tanúsítványt alkalmaz egy adott célra.

Az egyes tanúsítványtípusoknál alkalmazott azonosítási eljárást, felelősségvállalást, kötelezettségeket és díjakat részletesen, illetve specifikusan a Hitelesítési Szabályzat, illetve az Előfizetői Szerződés tartalmazza.

1.4.1 Tanúsítványok osztályai és tulajdonságaik

Szolgáltató fokozott biztonságú, szolgáltatói és teszt osztályú tanúsítványokat bocsát ki. A szolgáltatói és teszt osztályú tanúsítványok kibocsátását és kezelését Szolgáltató nem nyilvános szolgáltatás keretében végzi. Jelen Szabályzat a fokozott osztályú tanúsítványok kezelését írja le.

1.4.1.1 Fokozott biztonságú tanúsítványok

A fokozott biztonságú tanúsítvány olyan személyeknek, szervezeteknek vagy eszközöknek kiadott tanúsítvány, amely alanyát szigorú ellenőrzési lépések során azonosította a szolgáltató. Használata pénzügyi tranzakcióknál, utasításoknál és információk eredetiségének és sértetlenségének ellenőrzésénél ajánlott.

A fokozott szintű tanúsítvány további biztosítékokkal szolgál az előfizető személyazonosságát illetően azáltal, hogy megköveteli a személyes (fizikai) megjelenést a Regisztrációs Szervezetnél. Regisztrációs Szervezet a hitelesítési kérelemben feltüntetett adatokat és tényeket a bemutatott okmányok alapján ellenőrzi

1.4.1.2 Szolgáltatói osztályú tanúsítványok

A szolgáltatói tanúsítványokat Szolgáltató saját célra bocsátja ki, a Szolgáltatás biztosítására.
Előfizető nem igényelheti.

1.4.1.3 Teszt osztályú tanúsítványok

Teszttanúsítványokat Szolgáltató kizárólag tesztelési célokból ad ki. A Szolgáltató ilyen tanúsítványok esetében nem végez entitás-azonosítást. A teszt tanúsítványban található információ nem ellenőrzött információnak tekintendő.

A teszt tanúsítványokat Szolgáltató saját célra bocsátja ki, Előfizető nem igényelheti.

1.4.2 Tanúsítványtípusok

A Szolgáltató a következő alfejezetekben ismertetett típusú tanúsítványok kiadását végzi. Az egyes típusokra vonatkozó egyedi szabályzások a Hitelesítési Szabályzatokban találhatóak.
A tanúsítványok felhasználásának joghatásairól az Általános Szerződési feltételek rendelkeznek.

1.4.2.1 Személyes aláíró és titkosító tanúsítványok

Személyes tanúsítványokat természetes személy igényelhet a saját nevében. Előfizetőnek az igénylő személy számít, s ő az Aláíró is.

1.4.2.2 Szervezet típusú tanúsítványok

Szervezet típusú tanúsítványokat a szervezet képviselője igényelhet saját, vagy munkatársa, tagja, megbízottja számára. A szervezet - többek között - lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület, alapítvány. Ebben az esetben Előfizetőnek az igénylő szervezet számít. Előfizető

kötelezettségei egyetemlegesen érvényesek arra a személyre (Aláíró), aki számára a szervezet a tanúsítványt igényelte.

1.4.2.3 Eszköz tanúsítvány

Eszköz tanúsítványt természetes személy vagy szervezet igényelhet az általa működtetett IP címmel rendelkező eszköz részére. Ebben az esetben Előfizetőnek az igénylő szervezet számít.

1.5 Szolgáltató adatai

1.5.1 Cím, cégjegyzékszám, kontakt információk

A Szolgáltató teljes neve:	GIRO Elszámolásforgalmi Rt., röviden: GIRO Rt.
Cégjegyzékszám:	01-10-041159
Székhelye:	Budapest 1054 Vadász utca 31.
Telephelye:	Budapest 1205 Mártonffy u. 25-27.
Postacím:	Budapest 1054 Vadász u. 31.
Telefonszám:	428-5600
Fax:	269-5458
Honlap:	www.giro.hu/hiteles
Email cím:	hiteles@hiteles.giro.hu

Illetékes fogyasztóvédelmi felügyelőség:

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

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/hiteles/partner címen.

Az Igénylők bármely Regisztrációs Szervezet ügyfélszolgálatát felkereshetik, Érintett fél a tanúsítványban szereplő Regisztrációs Szervezet ügyfélszolgálatához fordulhat.

A Hitelesítő Központ az előfizetők részére ügyfélszolgálatot nem működtet.

A Szolgáltatással kapcsolatos kérdésekkel, amennyiben a Regisztrációs szervezet ügyfélszolgálati irodájában nem tudta megoldani, vagy annak működésére van panasza, a Hitelesítő Központ a következő címen kereshető meg: kerdes@hiteles.giro.hu.

1.5.3 Szabályzat kibocsátó adatok

A Szabályzatot kibocsátó és karbantartó szervezet a Szolgáltató Szabályozó Szervezete. Bármilyen e szabályzatot érintő kérdéssel és észrevétellel e szervezet kereshető fel.

Postacím:	Budapest 1051 Vadász utca 31.
Telefonszám:	428-5600
Fax:	269-5458
Email cím:	szabalyzat@hiteles.giro.hu

2 Általános rendelkezések

Jelen fejezet a Közösség tagjaira, így a Szolgáltatóra- az Előfizetőre és Igénylőre, valamint az Érintett Félre tartalmaz kötelezettségeket és jogosítványokat. Az itt meghatározott kötelezettségeken kívül további kötelezettségeket határozhatnak meg a Szabályzat egyéb fejezetei, a Szolgáltató Általános Szerződési Feltételei, és egyéb nyilvános szabályzatai, szerződései.

A GIRO Rt. és az Intézmények együtt – jelen Szabályzatban meghatározott feladat, – és felelősség megosztás alapján – végzik a szolgáltatást a Közösség részére.

Jelen Hitelesítési Szolgáltatási Szabályzat a szolgáltatási folyamatból az Intézmény feladat- és hatáskörébe telepíti a Regisztrációs tevékenységet, így az Intézmény egyúttal Regisztrációs Szervezet, melyre a Regisztrációs Szervezet – jelen Szabályzatban részletesen meghatározott - kötelezettségei és felelőssége vonatkozik.

2.1 Kötelezettségek

A Közösség mindegyik tagjának kötelessége a hatályos jogi szabályozásnak, a Hitelesítési Szolgáltatási Szabályzatnak, és a Szolgáltató egyéb nyilvánosságra hozott szabályzatainak való megfelelés és megfeleltetés.

2.1.1 GIRO Rt. kötelezettségei

A GIRO Rt.-nek kötelessége a szolgáltatás nyújtásában közreműködő belső szervezetek létrehozása és működtetése, illetve külső (Intézmény által működtetett) szervezetek tekintetében annak elbírálása és ellenőrzése.

1. Szabályozó Szervezet működtetése
2. Elsődleges Hitelesítő Központ működtetése
3. Szolgáltatói Hitelesítő Központ működtetése
4. Tanúsítványtár működtetése
5. Regisztrációs Szervezetek elbírálása és folyamatos ellenőrzése

2.1.1.1 Szabályozó Szervezet kötelezettségei

A Szabályozó Szervezetnek kötelessége a Közösség igényeinek felmérése és folyamatos követése, ezek alapján a közösség működésére vonatkozó alapelvek lefektetése, s ebből levezetve a tagok tevékenységét részletesen tárgyaló szabályzatok – különösen az Általános Szerződési Feltételek és a Hitelesítési Szolgáltatási Szabályzat - készítése és rendszeres felülvizsgálata.

1. Közösség igényeinek felmérése
2. Szolgáltatók közös szabályzatainak elkészítése
3. Szolgáltatók közös szabályzatainak karbantartása és változáskezelése
4. Közös szabályzatok verzióinak nyilvántartása és megőrzése
5. A közösség tájékoztatása
6. Nyilvános szabályzatok publikálása
7. A regisztrációs folyamat szabályozása, ellenőrzése, felülvizsgálata

2.1.1.2 Elsődleges Hitelesítő Központ kötelezettségei

Az Elsődleges Hitelesítő Központ kötelessége a Szolgáltatói Hitelesítő Központ, és a Szolgáltató döntése alapján további hitelesítő szervezetek hitelesítése.

1. Saját kulcs-pár generálása
2. Magánkulcsának teljes körű védelme
3. Saját tanúsítvány előállítása önhitelesítéssel
4. Saját tanúsítvány nyilvánosságra hozatala
5. Hitelesítő Szervezetek hitelesítési kérelmeinek fogadása és ellenőrzése
6. Kulcs-pár generálás és tanúsítvány előállítás a Hitelesítő Szervezet részére
7. Hitelesítő Szervezetek tanúsítvány visszavonási kérelmeinek feldolgozása
8. Hitelesítő Szervezetek tanúsítvány megújítási kérelmeinek feldolgozása
9. Magánkulcs és tanúsítvány Hitelesítő Szervezethez való eljuttatása
10. Tanúsítványok és Hitelesítő Szervezet visszavonási listák publikálása a tanúsítványkönyvtárban
11. Tanúsítványának visszavonása, illetve felfüggesztése, amennyiben magánkulcsa kompromittálódik, vagy ennek gyanúja áll fenn
12. Az általa tanúsított Hitelesítő Szervezetek elbírálása és ellenőrzése

2.1.1.3 Szolgáltatói Hitelesítő Központ kötelezettségei

A Szolgáltatói Hitelesítő Központ kötelessége a Regisztrációs Szervezetek és a Regisztrációs Szervezetek által ellenőrzött és regisztrált Előfizetők hitelesítése.

1. Magánkulcsának teljes körű védelme
2. Regisztrációs Szervezetek hitelesítési kérelmeinek fogadása és ellenőrzése
3. Kulcs-pár generálás és tanúsítvány előállítás a Regisztrációs Szervezet részére
4. Kulcs-pár és tanúsítvány eljuttatása a Regisztrációs Szervezethez
5. Regisztrációs Szervezetektől előfizetői hitelesítési kérelmek fogadása és ellenőrzése
6. Tanúsítvány előállítás az Előfizetők részére
7. Regisztrációs Szervezetektől érkező tanúsítvány visszavonási, felfüggesztési és újraérvényesítési kérelmek feldolgozása
8. Regisztrációs Szervezetektől érkező tanúsítvány megújítási kérelmek feldolgozása
9. Tanúsítványok és tanúsítvány visszavonási listák publikálása a tanúsítványkönyvtárban
10. Intézkedni tanúsítványának visszavonása, illetve felfüggesztése végett, amennyiben magánkulcsa kompromittálódik, vagy ennek gyanúja áll fenn
11. Folyamatos rendelkezésre állás a tanúsítvány felfüggesztési és visszavonási kérelmek végrehajtása érdekében
12. A Regisztrációs Szervezetek elbírálása és ellenőrzése

2.1.1.4 Tanúsítványtár kötelezettségei

A tanúsítványtárnak kötelessége a tanúsítványok, tanúsítvány visszavonási listák közzététele minden Érintett fél által folyamatosan elérhető módon.

1. Tanúsítványok, tanúsítvány visszavonási listák publikálására vonatkozó kérelmek azonnali végrehajtása
2. Megfelelő teljesítménnyel történő folyamatos rendelkezésre állás
3. Lekérdezési és keresési kérelmek kiszolgálása

2.1.2 Regisztrációs szervezet kötelezettségei

A Regisztrációs Szervezetek kötelessége az Előfizetők kiszolgálása, valamint az aláíró eszközök biztosítása és megszemélyesítése.

1. Magánkulcsának teljes körű védelme
2. Előfizető személyes identitásának ellenőrzése
3. Előfizető szervezeti identitásának ellenőrzése
4. Előfizetők tájékoztatása, technikai támogatása
5. Regisztrációs adatok felvétele, ellenőrzése és tanúsítványkérelem összeállítása
6. Hiányos, hibás, valótlan vagy nem igazolt adatokat tartalmazó tanúsítványkérelmek visszautasítása
7. Kulcs-pár generálás az előfizetők részére
8. Előfizetői tanúsítványkérelem Hitelesítő Szervezethez való eljuttatása és hitelesíttetése
9. Előfizetők tanúsítvány megújítási kérelmeinek fogadása és Hitelesítő Szervezethez való továbbítása

10. Előfizetők tanúsítvány visszavonási, felfüggesztési és újraérvényesítési kérelmeinek fogadása és Hitelesítő Szervezethez való továbbítása
11. Előfizető tanúsítványának átvétele a Hitelesítő Szervezettől és a magánkulccsal való összepárosítása
12. Előfizető tanúsítványának és magánkulcsának kulcshordozó eszközre írása és átadása Előfizetőnek
13. Intézkedni saját tanúsítványának visszavonása, illetve felfüggesztése végett, amennyiben magánkulcsa kompromittálódott, vagy ennek gyanúja áll fenn
14. Papíralapú, illetve elektronikus adatok archiválása, megőrzése
15. Ügyfélszolgálat biztosítása az Igénylők, Előfizetők, Érintett felek részére

2.1.3 Igénylő és Előfizető kötelezettségei

Az Előfizető kötelessége a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a tanúsítvány és magánkulcs igénylése és felhasználása során.

1. Tanúsítvány igénylése előtt megismerni és elfogadni Szolgáltató szerződéses feltételeit és szabályzatait
2. Teljes, pontos és valós adatokkal szolgálni Szolgáltató részére személyazonosságát, szervezeti identitását és egyéb adatait illetően
3. Magánkulcsának átvétele és felhasználása előtt megismerni a magánkulcs tárolásával, s az elektronikus aláírás megtételével kapcsolatos technikai, jogi, biztonsági feltételeket
4. Magánkulcsának, kulcshordozójának, és az aktiválási adatának védelme
5. Magánkulcsát csak (a tanúsítványban is feltűntetett) saját, illetve szervezete nevében használhatja, kizárólag arra a célra, amelyre kibocsátásra került
6. Aláíró magánkulcsát csak annak érvényességi ideje alatt használhatja fel
7. Tanúsítvány igénylését és a kulcs-pár felhasználását úgy végezheti, hogy az harmadik fél jogait ne sértse
8. Azonnal intézkedni tanúsítványának visszavonása, illetve felfüggesztése végett, amennyiben magánkulcsa kompromittálódik, vagy ennek gyanúja áll fenn
9. 5 munkanapon belül jelezni Szolgáltatnál a regisztráció során felvett adataiban történő változásokat, különös tekintettel a tanúsítványba foglalt adatokra

2.1.4 Érintett fél kötelezettségei

Érintett félnek kötelessége Szolgáltató szabályzatainak megfelelően a legnagyobb gondossággal eljárni az elektronikus aláírás és a tanúsítvány elbírálásakor.

1. Elektronikus aláírás elfogadása előtt megérteni az elektronikus aláírással kapcsolatos technikai, jogi, biztonsági és egyéb vonatkozásokat
2. Megismerni Szolgáltató szabályzatait és az elektronikus aláírással ellátott dokumentum alapján végzett bármilyen tevékenység Szolgáltató szabályzatának elfogadását jelenti.

3. Elektronikus aláírás ellenőrzést végezni az aláíró tanúsítványának segítségével, meggyőződve az üzenet eredetiségéről és az aláírás valódiságáról
4. A tanúsítványban feltűntetett azonosító alapján, és egyéb adatok, rendelkezésre álló módszerek segítségével az aláíró személyéről egyértelműen meggyőződni
5. A tanúsítvány érvényességének és hatályosságának ellenőrzése
6. Szükség esetén az aláíró személyének más forrásból való ellenőrzése
7. A teljes tanúsítási lánc vizsgálatát elvégezni az alábbiak szerint:
   - A tanúsítvány kibocsátójának azonosítója alapján a kibocsátó kilétéről meggyőződni
   - A kibocsátó tanúsítványának segítségével az aláíró tanúsítványának integritásáról meggyőződni
   - A tanúsítvány állapotának ellenőrzése a tanúsítvány visszavonási listák (CRL) áttanulmányozásával
   - Áttanulmányozni a tanúsítvány összes attribútumát, és az adott tranzakcióra vonatkozó előírásoknak, valamint józan megfontolásoknak megfelelően döntést hozni az aláírás elfogadásáról
8. Az elektronikus aláírás elfogadásának visszautasítása, ha az elektronikus aláírás, az aláíró tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata, annak érvénytelenségére utal, illetve ha az az adott kontextusban nem elfogadható

Az aláírás elfogadása nem jelenti az aláírt üzenet tartalmának tudomásul vételét vagy elfogadását.

2.2 A közösség tagjainak felelőssége

2.2.1 Giro Rt. felelőssége

Giro Rt. teljes mértékben felelős a Szolgáltató tevékenységéért.

- Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel – Érintett fél – szemben a Polgári Törvénykönyv szerződésen kívüli károkozásról szóló szabályai (Ptk. 339. §) szerint felelős, azzal, hogy a vonatkozó Hitelesítési Szabályzatban meghatározott kártérítés mértéke tanúsítvány típusonként és egyedi tanúsítványonként is maximált összegű. A kártérítési kötelezettség korlátozására tekintettel történt a Szolgáltatás díjainak meghatározása.
- Szolgáltató a vele szerződéses jogviszonyban álló személlyel – Előfizető – szemben a Polgári Törvénykönyv szerződésszegésért való felelősség szabályai szerint felelős.
- A Szolgáltató nem vagyoni felelőssége az Előfizető és Érintett fél felé a Polgári Törvénykönyv nem vagyon felelősségről szóló szabályai szerint alakul.
- A tanúsítvány lejárat előtti megszüntetése esetén, a kártérítési felelősség korlátozásáról a 4.4.4. pont rendelkezik.

2.2.1.1 Szabályozó Szervezet felelőssége

A Szabályozó Szervezet felelős a Szolgáltató által kibocsátott közös szabályzatokért, azok törvényi megfelelőségéért és betartatásáért.

- A Szabályozó Szervezet nem felelős az Előfizetők, az Érintett felek, és mások által kibocsátott szabályzatokért.

2.2.1.2 Elsődleges Hitelesítő Központ felelőssége

Elsődleges Hitelesítő Központ felelős a közvetlenül alá rendelt hitelesítő szervezetek hitelesítésért.

- Elsődleges Hitelesítő Központ nem felelős az alá rendelt hitelesítő szervezetek működéséért.

2.2.1.3 Szolgáltatói Hitelesítő Központ felelőssége

Szolgáltatói Hitelesítő Központ felelős az általa kibocsátott tanúsítványok hitelességéért.

- Szolgáltatói Hitelesítő Központ felelős a regisztrációs szervezetek működéséért.
- Szolgáltatói Hitelesítő Központ nem felelős az Előfizetők aláírási és egyéb magánkulcs felhasználási tevékenységért.
- Szolgáltatói Hitelesítő Központ nem felelős az Érintett felek aláírás ellenőrzési és tanúsítvány elbírálási tevékenységért.

2.2.2 Regisztrációs Szervezet felelőssége

Regisztrációs Szervezet felelőssége az Előfizetők személyazonosságának és szervezeti identitásának megállapítása, valamint a regisztrációs adatok egyezőségének ellenőrzése a bemutatott dokumentumokkal. Regisztrációs Szervezet felelőssége ezen túl az előfizetői kulcs-pár generálása, és tanúsítvánnyal együtt történő kulcshordozóra írása, s a kulcshordozó megszemélyesítése.

2.2.3 Előfizető felelőssége

Előfizetőnek büntetőjogi felelőssége áll fenn Szolgáltatóval szemben a regisztráció során megadott adatai valódisága tekintetében. Előfizetőnek kártérítési felelőssége áll fenn Szolgáltatóval szemben azokért a veszteségekért és károkért, melyeket a regisztráció során megadott helytelen adataival, vagy az azokban bekövetkezett változások be nem jelentésével, illetve magánkulcsának neki felróható biztonsági sérülésével, vagy egyéb kötelezettségeinek be nem tartásával számára okoz. Az Előfizető felelős azért, ha magánkulcsát nem a Hitelesítési Szolgáltatási Szabályzatban, az ÁSzF-ben és a jogszabályokban meghatározott célra használta.

2.2.4 Érintett fél felelőssége

Az érintett fél felelős az elektronikus aláírás és a Szolgáltató által kibocsátott tanúsítványok elfogadása során tanúsított körültekintő eljárásért, valamint kötelezettségeinek betartásáért. Érintett fél felelőssége fennáll, ha a tanúsítvány érvényességének és hatályosságának ellenőrzése során nem a Hitelesítési Szolgáltatási Szabályzat, illetve a hatályos jogszabályok szerint jár el.

2.3 Pénzügyi felelősség korlátai

2.3.1 Kártérítés

Szolgáltató nem felelős az olyan kárért, mely abból adódott, hogy az Érintett fél a tanúsítványok, illetve az elektronikus aláírások hitelességének ellenőrzésénél nem a hatályos jogszabályok, szerződéses feltételek, és szolgáltatói szabályzatai szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

Szolgáltató felelősségének korlátait – kártérítés felső határa - az általa kibocsátott tanúsítványok tartalma szerint kell értelmezni. Szolgáltató – helytállási kötelezettsége esetén – csak a tanúsítványban megjelölt összeghatárig köteles kártérítésre.

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

2.3.2 Megbízotti kapcsolatok

Szolgáltató semmilyen körülmények között nem tekinthető Előfizetők és Érintett felek megbízottjának, képviselőjének, vagy bármilyen partnerének, hitelesítési tevékenységével összefüggésben.

2.3.3 Adminisztratív eljárások

Szolgáltató a Szolgáltatás végzését 30 nappal a megkezdést megelőzően bejelenti a Hírközlési Főfelügyeletnek. A bejelentéshez csatolja Hitelesítési Szolgáltatási Szabályzatát és Általános Szerződési Feltételeit.

2.4 Értelmezés és alkalmazás

2.4.1 Alkalmazott jogszabályok

Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. Szolgáltató szerződéseire és szabályzataira, és azok teljesítésére, a magyar jog az irányadó, és azok a magyar jog szerint értelmezendőek.

Szolgáltató tevékenységét elsősorban az elektronikus aláírásról rendelkező 2001. évi XXXV. törvény (Törvény) és az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről rendelkező 16/2001. MeHVM rendelet (Miniszteri rendelet) szabályozza.

Szolgáltató ezen túl az Európai Parlament és Európa Tanács az elektronikus aláírások közösségi programjáról szóló 1999/93/EK irányelvére tekintettel végzi tevékenységét.

2.4.2 Érvénytelenség, hatályosság, megszűnés, értesítések

2.4.2.1 Érvénytelenség

Amennyiben a Szolgáltató szerződéseinek vagy szabályzatainak valamely pontja érvénytelen lenne, az az egész szabályzat vagy szerződés egyéb pontjainak érvényességét nem érinti.

2.4.2.2 Hatályosság

Jelen Hitelesítési Szolgáltatási Szabályzat időbeli hatálya az 1.3.5.1 pontnak megfelelően a Főfelügyelet engedélyének keltétől a – módosításokkal egységes szerkezetbe foglaltan – a Szolgáltatási tevékenység megszüntéig tart. Személyi hatályát az 1.3.5.1 pont meghatározza.

2.4.2.3 Megszűnés

A Hitelesítési Szolgáltatási Szabályzat a Szolgáltatás befejezésével veszti hatályát.

2.4.2.4 Értesítések

Előfizetők, Érintett felek és bármely harmadik fél Szolgáltatót elektronikus üzenetben, levélben, vagy faxon értesítheti, aláírt módon. Szolgáltató értesítési címei az 1.5 „Szolgáltató adatai” fejezetben találhatóak. A Szolgáltató az Előfizetőket és Érintett feleket web oldalain, illetve ügyfélszolgálaton történő közzététellel tájékoztatja. Az Előfizetőket esetenként emailen is értesítheti.

2.4.3 Vitás kérdések kezelése

Bármely vitás kérdés felmerülése esetén Előfizetőnek, Érintett félnek, vagy bármely harmadik félnek kötelessége Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása a kérdés minden vonatkozását érintően, a vita jogi útra terelése előtt. A felek a Hitelesítés Szolgáltatással kapcsolatos jogvitáikat mindenkor megkísérlik békés tárgyalásos úton rendezni.

A panaszt az Előfizetőt nyilvántartó Regisztrációs Szervezet ügyfélszolgálatán lehet írásban vagy szóban előterjeszteni. A panasz előterjesztésétől számított 8 munkanapon belül a Szolgáltató kivizsgálja azt és írásban válaszol.

Amennyiben a Felek közötti egyeztetés annak megkezdésétől számított harminc napon belül nem vezetne eredményre, arra az esetre a Felek kölcsönösen alávetik magukat a Kereskedelmi és Iparkamara mellett szervezett Állandó Választottbíróság kizárólagos illetékességének.

2.5 Díjak

Az Előfizetők által fizetendő díjakat az Általános Szerződési Feltételeknek megfelelően a Regisztrációs szervezet által közzétett díjszabás tartalmazza.

2.6 Nyilvánosságra hozatal és tárolás

A Szolgáltató a nyomtatott médiában, saját web oldalain, az általa üzemeltetett tanúsítványtáron keresztül, valamint emailben hoz nyilvánosságra információkat.

2.6.1 Szolgáltatói információk publikálása

Szolgáltató információ közzétételi kötelezettségét az alábbiak szerint teljesíti:

- Legalább két országos napilapban hirdetést jelentet meg a szolgáltatás beindításáról az Elsődleges Hitelesítő Központ tanúsítványának aláírásával, a szolgáltatás beszüntetéséről, új tanúsítvány osztály bevezetéséről, valamint magánkulcsának kompromittálódásáról amennyiben ilyen esemény bekövetkezik.
- A tanúsítványtárban tárolja és teszi elérhetővé a kibocsátott tanúsítványokat, köztük az Elsődleges Hitelesítő Központ és a Szolgáltatói Hitelesítő Központ tanúsítványát, a tanúsítvány visszavonási listákat.

- Szolgáltató saját web oldalain keresztül elérhetővé teszi a Szabályzatot, az Általános Szerződési Feltételeket, az egyéb nyilvános szabályzatokat, valamint a Regisztrációs szervezetek listáját, elérhetőségét

2.6.2 Publikálás gyakorisága

Szolgáltató a kibocsátott tanúsítványokat publikálja a tanúsítványtárban, tanúsítvány visszavonási listát a 4.4.9 pontnak megfelelő gyakorisággal tesz közzé.

Szolgáltató a Hitelesítési Szolgáltatási Szabályzatban és Általános Szerződési Feltételekben tervezett változásokról a hatályba lépést megelőzően 30 nappal tájékoztatja a Főfelügyeletet, s a változásokkal egységes szerkezetbe foglalva közzéteszi egyéb nyilvános szabályzatait pedig a hatályba lépést megelőző 30 nappal hozza nyilvánosságra.

2.6.3 Elérési szabályok

Szolgáltató minden Előfizető és Érintett fél számára elérhetővé teszi web oldalait és tanúsítványtárát olvasás céljából. A tanúsítványtárban alapszintű keresési lehetőséget biztosít a tanúsítvány sorszáma és az azonosítója alapján.

A tanúsítványtár és a web oldalak tartalmát csak és kizárólag a Szolgáltató módosítja.

2.6.4 Tanúsítványtár

Szolgáltató a tanúsítványokat tanúsítványtárban tárolja és LDAP protokollokon keresztül teszi lekérdezhetővé.
Tanúsítványtár címe:
LDAP:// tar.giro.hu

A tanúsítványtár elérhetőségét Szolgáltató a hét első munkanapján reggel 6.00-tól a hét utolsó munkanapját követő nap reggel 6.00-ig biztosítja. Munkanapnak az a nap számít, amely egyúttal banki munkanap is.

2.7 Tanúsítás

Szolgáltató független auditor céggel tanúsíttatja tevékenységét .

2.7.1 Vizsgálatok gyakorisága

A vizsgálatokat Szolgáltató rendszeres időszakonként megismételteti, azt a törvényi feltételek vagy szabályzataiban bekövetkezett jelentősebb változások esetén, döntése alapján, soron kívül elvégezteti.

2.7.2 Vizsgálatot végző adatai

A vizsgálatot Szolgáltató olyan, széles körben ismert auditor céggel végezteti el, amely szakértelmét bizonyítani tudja általános és informatikai biztonsági; a publikus kulcsú infrastruktúra technikai, technológiai, jogi, szabályzati, és egyéb területein, és auditálási módszertanok vonatkozásában.

2.7.3 Vizsgálatot végző kapcsolata a céggel

A vizsgálatot végző cég független Szolgáltatótól. A vizsgálatot végző cég nem rendelkezik tulajdonrésszel, vagy érdekeltséggel a Szolgáltatóban, és a Szolgáltató úgyszintén nem tulajdonosa se közvetlenül, se közvetve a vizsgálatot végző cégnek.

2.7.4 A vizsgálatok kiterjedése

A független auditor cég abból a szempontból, vizsgálja a Szolgáltató tevékenységét, hogy az megfelel-e a törvényi előírásoknak, Szolgáltató saját szabályzatainak, egyéb ajánlásoknak, szabványoknak, minősítési rendszereknek.

2.7.5 Hiányosságok kezelése

Amennyiben a vizsgálat a jogszabályoknak való megfelelőség vonatkozásában, vagy Szolgáltató szabályzatai és tevékenysége között nem megfelelőségeket tár fel, Szolgáltató és intézkedik a tprobléma felszámolásáról.

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

2.7.6 Eredmény kommunikációja

Szolgáltató a vizsgálatok eredményét web oldalain nyilvánosságra hozza.

2.8 Bizalmasság – Adatkezelési szabályzat

Szolgáltató az Előfizető által a regisztrációs űrlapon megadott adatait a vonatkozó törvényeknek és jogszabályoknak megfelelően tárolja. A regisztráció során felhasznált dokumentumok egy példányát a regisztrációs szervezetek nyilvántartják és tárolják.

Előfizető az Előfizetői szerződés aláírásával hozzájárul ahhoz, hogy a Szolgáltató a személyes adatait tárolja és kezelje, továbbá hozzájárul ahhoz, hogy a személyes adatait tartalmazó tanúsítványt Szolgáltató a tanúsítványtárban tárolja, és publikálja.

A szolgáltató által kért és kezelt adatok egy része a tanúsítványban nyilvánosságra kerül a nyilvános kulcs tulajdonosának alapszintű azonosítása céljából, másik részét Szolgáltató védett módon tárolja Előfizető személyazonosságának igazolása és egyéb adatszolgáltatási kötelezettsége végett, azokra az esetekre, melyeket a „Feltárás tulajdonos kérésére” és a „Feltárás más esetekben” fejezetek tárgyalnak.

A nyilvánosságra hozandó és bizalmasan kezelt adatok a regisztrációs űrlapon egyértelműen megkülönböztetésre kerülnek.

Szolgáltató az aláíró személyazonosságának ellenőrzése céljából a személyi adat- és lakcímnyilvántartással, az aláírási jogosultság ellenőrzése céljából a cégnyilvántartással, a jogszabályoknak megfelelően adategyeztetést végezhet.

Szolgáltató a tudomására jutott adatokat a tanúsítvány érvényességének lejártától számított minimum öt évig, de legkésőbb az elektronikus aláírással, illetve az elektronikusan aláírt dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrzi. Szolgáltató a megőrzési idő lejáratát követő 3 hónapon belül az információkat törli rendszeréből.

2.8.1 Bizalmas információk

Szolgáltató bizalmas információként kezel minden tudomására jutott adatot, kivéve azokat, amelyeket a „Nem bizalmas információk” fejezetben részletez. Szolgáltató a birtokába jutott bizalmas információkat a személyes adatok védelméről szóló 1992 évi LXIII. törvénynek megfelelően kezeli.

2.8.2 Nem bizalmas információk

Szolgáltató nem bizalmas információként kezeli azokat az adatokat, melyeket a tanúsítványban fel kíván tüntetni. Ezeket az adatokat a regisztrációs űrlapon külön jelöli.

2.8.3 Tanúsítvány visszavonási és felfüggesztési információk felfedése

Szolgáltató az általa kibocsátott tanúsítványok visszavonását és felfüggesztését tanúsítvány-visszavonási listában teszi közzé a 7.2. pont szerint.

2.8.4 Feltárás törvényi meghatalmazással rendelkezők részére

Szolgáltató az elektronikus aláírás felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak, a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során az ellenérdekű peres félnek vagy képviselőjének, illetőleg a megkereső bíróságnak tár fel információkat a 2001. évi XXXV. Törvény 11.§ paragrafusa szerint.

2.8.5 Feltárás tulajdonos kérésére

Szolgáltató a törvényi meghatalmazással rendelkezők részére történő adatszolgáltatáson túl csak Előfizető írásos (hagyományos vagy elektronikus aláírással ellátott) meghatalmazása alapján tár fel információt harmadik fél részére.

2.8.6 Feltárás más esetekben

Szolgáltatónak tevékenysége befejezésekor nyilvántartásait, a bizalmas adatokkal együtt, át kell adnia más - vele azonos besorolású – szolgáltató részére a 2001. évi XXXV. törvény 16. § 7. pontja szerint.

2.9 Szellemi tulajdonhoz fűződő jogok

A megkülönböztetett nevek a név használatára jogosult személy (vagy szervezet) tulajdonát képezik.

A kulcs-pár és a tanúsítvány tulajdonosa az Előfizető, annak teljes jogú használója az Aláíró, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

3 Azonosítás és hitelesítés

3.1 Kezdeti regisztráció

3.1.1 Nevek típusa

Az Előfizető tanúsítványba foglalt azonosítója (Subject) az International Telecommunication Union által kiadott ITU-T X.500 „Information Technology - Open Systems Interconnection - The directory: Overview of concepts, models and services" ajánlása (továbbiakban X.500) egyedi név formátum előírásainak felel meg.

3.1.2 Név szemantika

A tulajdonos azonosító kitöltésekor a következő szabályok szerint kell eljárni:

- Álnevek használata nem megengedett.
- Az azonosító nem tartalmazhat olyan speciális karaktereket, amelyek megjelenítése az általánosan használt ügyfél alkalmazásokban nem lehetséges helyesen.
- Az azonosító mezői esetében a magyar ABC ékezetes karakterei helyett azok ékezet nélküli megfelelőit kell használni.
- Csak olyan szervezet tüntethető fel a természetes személlyel összefüggésben, amely írásos formában hozzájárult a tanúsítvány kiadásához az Előfizető számára.
- Amennyiben a szervezet gazdasági társaság, akkor annak a cégbejegyzésben szereplő rövid nevét, és a szervezet típusát kell felvenni a Szervezet mezőben.

3.1.3 Különböző név formátumok értelmezése

Az előfizető azonosítójának értelmezése érdekében Érintett félnek a Szolgáltató nyilvános szabályzatai alapján kell eljárnia. Szolgáltató által kibocsátott tanúsítványoknak nem célja, hogy a tulajdonosként megjelölt entitásokat a tanúsítványban feltüntetett adatok alapján egyértelműen azonosítani lehessen. Érintett fél szükség esetén felveheti a kapcsolatot a Szolgáltatóval a tanúsítványban foglalt adatok értelmezése céljából, de Szolgáltató az Előfizető adatairól többlettájékoztatást annak írásbeli hozzájárulása nélkül nem adhat.

3.1.4 Nevek egyedisége

Előfizető azonosítójának egyedinek és egyértelműen megkülönböztethetőnek kell lennie a Szolgáltató tanúsítványtárában.

3.1.5 Név igénylési viták feloldása

Az előfizető azonosítók kiosztása a regisztráció elbírálásának sorrendje alapján történik.

Szolgáltató fenntartja magának a jogot a név kiosztással kapcsolatos mindennemű döntés tekintetében.

Szolgáltatónak joga van visszavonni egy tanúsítványt, amennyiben jogszerűtlen név vagy adathasználat miatt erre bíróság kötelezi, vagy saját maga ilyen döntést hoz.

3.1.6 Védjegyek elismerésének és hitelesítésének módszere

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

3.1.7 Privát kulcs birtoklás ellenőrzésének módszere

A Szolgáltató maga generálja a felhasználói kulcspárt, s nem fogad el az Előfizető által generált magánkulcsot, ezért minden esetben biztosított a tanúsítványkérelemben szerepelő nyilvános kulcs és a magánkulcs összetartozása.

3.1.8 Szervezeti identitás hitelesítése

Amennyiben a Szervezet neve a tanúsítványban feltüntetésre kerül a Szolgáltatónak kötelessége az Igénylő adott szervezetthez való tartozásáról meggyőződni. A szervezethez tartozás céljából köteles olyan azonosító kártyát, iratot, vagy dokumentumokat elkérni, mely alapján egyértelműen megállapítható a személy szervezethez tartozása, a szervezet felhatalmazása a tanúsítvány kiadására, s meghatározhatók a szervezet hivatalos adatai, vezető tisztségviselői, és értesítési címe.

A Szolgáltató a tanúsítvány kibocsátásáról, a tanúsítvány kibocsátásának megtagadásáról és ennek okáról értesíti a tanúsítványban feltüntetett Szervezetet.

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

Az adatok felvétele folyamán a Szolgáltató minden tőle telhetőt megtesz annak érdekében, hogy meggyőződjön a bemutatott okmányok érvényességéről és hitelességéről. Szolgáltató az aláírási jogosultság ellenőrzése céljából adategyeztetést végezhet a cégnyilvántartással.

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

3.1.9 Személyes identitás hitelesítése

A Szolgáltatónak kötelessége a tanúsítványigénylő személyazonosságáról meggyőződni, s ebből a célból legalább a személyi igazolványát vagy útlevélét, illetve szükség esetén további iratokat, mint gépjárművezetői engedélyét, adókártyáját vagy TB kártyáját elkérni és arról fénymásolatot készíteni. A személyazonosságról való meggyőződés az okmányokban szereplő fénykép és egyéb adatok alapján történik.

Az adatok felvétele során Szolgáltató minden tőle telhetőt megtesz annak érdekében, hogy meggyőződjön a bemutatott okmányok eredetiségéről, érvényességéről és hitelességéről. A szolgáltató ebből a célból adategyeztetést végezhet a személyi adat- és lakcímnyilvántartással, az úti-okmány nyilvántartással, és a gépjárművezetői nyilvántartással.

A Szolgáltató köteles a tanúsítvány kibocsátás megtagadni, amennyiben az okmányok személyhez tartozásával, hitelességével vagy érvényességével kapcsolatban kétsége merül fel.

3.2 Tanúsítvány megújítás

Szolgáltató által kibocsátott előfizetői tanúsítványok érvényességi ideje 1 év. Előfizetői tanúsítvány megújítása akkor lehetséges, ha:

- a tanúsítvány érvényes,
- a tanúsítvány nem szerepel a tanúsítvány visszavonási listán,
- a kezdeti regisztráció alkalmával rögzített összes (nem csak a tanúsítványba foglalt) adat még érvényes,
- a tanúsítványhoz tartozó privát kulcs nem kompromittálódott.

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

3.3 Tanúsítvány megújítása visszavonás után

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

3.4 Visszavonási kérés

A tanúsítvány visszavonási kérés azonosítási és hitelesítési vonatkozásai megtalálhatóak a "Tanúsítvány felfüggesztés és visszavonás" fejezetben.

4 Üzemeltetési követelmények

4.1 Tanúsítványigénylés

Tanúsítvány kibocsátása Szolgáltatótól a Regisztrációs Szervezetek valamelyikénél igényelhető, az adott tanúsítvány típusnak és osztálynak megfelelő regisztrációs eljárás lefolytatásával Tanúsítvány igénylésekor a Regisztrációs Szervezet egy tájékoztató füzetet ad át, és amennyiben az Előfizető igényeli az egyéb nyilvános dokumentumok tanulmányozásának lehetőségét is biztosítja, valamint szóban tájékoztatja az ügyfelet a szolgáltatás feltételeiről és a lehetőségekről. A tájékoztató füzet tartalma:

- A Szolgáltató Általános Szerződési Feltételei
- A Hitelesítési Szolgáltatási Szabályzat, valamint a Hitelesítési Szabályzatok szerepe, elérhetősége
- A Szolgáltató további nyilvános dokumentumainak szerepe és elérhetősége
- Az Előfizető jogai és kötelezettségei
- Tájékoztató az elektronikus aláírás jogi hátteréről
- Összefoglaló a Szolgáltatás tartalmáról
- A kibocsátott tanúsítványok és magánkulcsok felhasználási módjának rövid leírása
- A magánkulcs biztonsági tényezői, a kompromittálódás veszélyei
- Egyéb technikai eligazítás

A regisztrációs űrlap aláírásával az Előfizető nyilatkozik arról, hogy a fent felsorolt pontokban tájékoztatást kapott, a Szolgáltató szerződéses feltételeit, valamint szabályzatait megértette és elfogadta, hozzájárul tanúsítványa publikálásához.

A regisztrációs interjú során a személyazonosság és a szervezethez tartozás a "Személyes identitás hitelesítése" és "Szervezeti identitás hitelesítése" fejezetben leírtak szerint történik. Az identitások hitelesítése után a regisztrációt végző személy ellenőrzi a regisztrációs űrlapon szereplő adatok egyezőségét az Előfizető hivatalos iratai alapján. Ha az adatok helyesek, az űrlap tartalmát rögzíti a Szolgáltató informatikai rendszerében, ellenkező esetben az űrlapot visszaadja.

4.2 Tanúsítvány kibocsátás

Tanúsítvány kibocsátására az Előfizető igénylése alapján történik. Az Intézmény lehetővé teheti 1 évnél régebben aktív ügyfelei részére, hogy az igénylést ne személyesen tegyék meg. Ebben az esetben a

rendelkezésére álló adatok alapján történik meg a tanúsítvány kibocsátás. A 4.1 pontban leírt lépéseknek ekkor is meg kell történnie a tanúsítvány átadása előtt.
A tanúsítvány elkészítését és kibocsátását a regisztráció során felvett űrlap, illetve az Intézménytől kapott adatok alapján végzi a Szolgáltató.
Ezen adatokat valamint a kulcspár nyilvános tagját a Regisztrációs Szervezet elküldi a Hitelesítő Szervezetnek, ahol megtörténik a tanúsítvány összeállítása, aláírása és publikálása. A Hitelesítő Szervezet az előállított tanúsítványt visszaküldi a Regisztrációs Szervezethez. Amennyiben a tanúsítványkérelem visszautasításra kerül ennek tényéről és okáról a Regisztrációs Szervezet értesítést kap.

4.3 Tanúsítvány elfogadás

A Regisztrációs Szervezet, a Szolgáltató felelősségi körében eljárva az elkészült tanúsítványt ellenőrzi, kulcshordozó eszközre írja a magánkulccsal együtt, majd a kulcshordozót átadja az Előfizető részére.

Amennyiben a regisztrációs eljárás és a magánkulcs átadása között az Előfizetővel való személyes kapcsolat megszakadt, az Előfizető személyazonosságát újra ellenőrizni kell a kulcshordozó átadása előtt. A kulcshordozót kizárólag személyesen veheti át a regisztrációs űrlapon megjelölt Aláíró, illetve eszköztanúsítvány esetén az Előfizető meghatalmazottja.

A magánkulcs és a tanúsítvány elfogadása a kulcs első felhasználásával történik meg. A felhasználás előtt az előfizetőnek kötelessége ellenőrizni a tanúsítványban feltűntetett adatainak helyességét. Amennyiben bármilyen rendellenességet talál a magánkulcsot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonása érdekében.

Az átadás során átadásra kerül:

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

A kulcshordozó eszköz átvételének megtagadása visszavonási kérelemnek számít.

4.4 Tanúsítvány visszavonás és felfüggesztés

4.4.1 Visszavonáshoz vezető körülmények

Tanúsítvány visszavonásához az alábbiakban felsorolt körülmények vezethetnek.

Előfizető kezdeményezése alapján:

- Magánkulcs kompromittálódása, vagy annak gyanúja
- Magánkulcsot védő jelszó kompromittálódása, vagy annak gyanúja
- Kulcshordozó eszköz elvesztése, eltulajdonítása, megrongálódása
- Magánkulcs átvételének visszautasítása
- Tanúsítványban feltűntetett hibás adatok
- Tanúsítványban feltűntetett előfizetői adatok megváltozása
- Tanúsítványban feltűntetett szervezet adatainak megváltozása
- Tanúsítványban feltűntetett Előfizető és szervezet kapcsolatnak megszűnése
- Előfizető visszavonási kérelme (indoklás nélkül is)

Szolgáltató kezdeményezése alapján:

- Tanúsítvány felfüggesztési idejének lejárata
- Amennyiben a törvény erre kötelezi
- Általános Szerződési Feltételek, Előfizetői Szerződés megszegése Előfizető által
- Előfizető kötelezettségeinek be nem tartása
- Szolgáltató tudomására jutott tény, vagy alapos gyanú, a regisztrációs adatok valótlanságáról
- Tanúsítványban feltűntetett kibocsátó adatok megváltozása
- Hitelesítési Szolgáltatás megszűnése
- Regisztrációs Szervezet megszűnése
- Szolgáltató valamely magánkulcsának kompromittálódása

Harmadik fél kezdeményezése alapján:

- Tanúsítványban feltűntetett szervezet kérelme

4.4.2 Visszavonás kérelmezése

Tanúsítvány visszavonását az előző pontban feltűntetett körülmények alapján az előfizető, a Szolgáltató, vagy más harmadik fél kezdeményezheti. Előfizetőnek és Szolgáltatónak kötelessége, harmadik félnek

joga, a feltűntetett esetekben a visszavonás azonnali kezdeményezése. A visszavonási kérelem személyesen nyújtható be Szolgáltató azon Regisztrációs Szervezeténél, ahol a tanúsítvány készült.

A visszavonási kérelemnek a következő adatokat kell tartalmazni:

- Tanúsítvány sorszáma
- Visszavonást kérő megnevezése
- Visszavonást kérő email címe
- Visszavonási jelszó
- Visszavonás oka

Visszavonási kérelmet a tanúsítványban megjelölt szervezeten kívül harmadik fél nem adhat be.

4.4.3 Visszavonási eljárás

A visszavonási eljárás első lépéseként Szolgáltató ellenőrzi a kérelemben szereplő adatokat. Ha z adatok helytelenek, vagy a kérelmező személye nem állapítható meg, akkor Szolgáltató a visszavonást visszautasítja. Az előfizető által beterjesztett, helyes és hiteles kérelem esetén a szolgáltatónak nincs mérlegelési joga a végrehajtás tekintetében, egyéb esetekben választhatja a tanúsítvány ideiglenes felfüggesztését. Regisztrációs Szervezetnél bejelentett visszavonási kérelmeket a Regisztrációs Szervezet a Hitelesítő Szervezetnek haladéktalanul továbbítja.

Amennyiben a visszavonási kérelem megfelelő, Szolgáltató haladéktalanul intézkedik a tanúsítvány visszavonásáról. A visszavont tanúsítvány bekerül a következő alkalommal kibocsátott Tanúsítvány Visszavonási Listába.

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

4.4.4 Visszavonás időbelisége

A visszavonási kérelem esetén a bejelentési kötelezettség azonnali, a Szolgáltató ennek végrehajtását soron kívül végrehajtja.

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

Felelősségi szabályok:

- A visszavonási kérelem bejelentésének a Szolgáltatóhoz történő megérkezéséig az Általános Szerződési Feltételeknek megfelelően az előfizető felelős a felmerülő károkért.
- A visszavonási kérelem megérkezésétől a visszavonás tényének tanúsítványtárban való megjelenésig a Szolgáltató felelős a felmerülő károkért.
- A visszavonás tanúsítványtárban való megjelenése után az Érintett fél felelős a felmerülő károkért.

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

4.4.5 Felfüggesztéshez vezető körülmények

A tanúsítvány felfüggesztése az előfizető, vagy a tanúsítványban megjelölt szervezet erre vonatkozó kérelme alapján történhet. A Szolgáltató a felfüggesztéshez vezető körülmények fennállása, illetve ezek alapos gyanúja esetén, dönthet a tanúsítvány felfüggesztéséről. Ilyen esetekben a Szolgáltatónak a felfüggesztett állapot időtartama alatt intézkednie kell a körülmények tisztázása, s szükséges esetén annak visszavonás érdekében. Tanúsítvány felfüggesztését harmadik fél is kérheti, amennyiben bizonyítani tud olyan körülményt, mely alapján Előfizetőnek vagy Szolgáltatónak kezdeményeznie kellene a visszavonást.

Amennyiben Előfizetőnek kötelessége a tanúsítvány visszavonásának kérelmezése, de személyes megjelenése akadályoztatva van, vagy nem lehetséges, akkor haladéktalanul intézkednie kell tanúsítványának felfüggesztése érdekében.

4.4.6 Felfüggesztés kérelmezése

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

- E-mail írásával, a megfelelő adatok megadásával
- Szolgáltató azon Regisztrációs Szervezeténél személyesen, ahol a tanúsítvány készült
- Szolgáltató ügyfélszolgálati telefonszámán

A felfüggesztési kérelemnek a következő adatokat kell tartalmazni:

- Tanúsítvány sorszáma
- Felfüggesztést kérő megnevezése
- Felfüggesztést kérő email címe
- Felfüggesztés oka

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

4.4.7 Felfüggesztési eljárás

A felfüggesztési eljárás első lépéseként Szolgáltató ellenőrzi a kérelemben szereplő adatokat. Amennyiben azok helytelenek, a kérelem nem megalapozott, vagy a kérelmező személye nem megállapítható, akkor Szolgáltató a felfüggesztési kérelmet visszautasítja. Amennyiben a kérelmet az előfizető terjesztette be, a szolgáltatónak nincs mérlegelési joga a végrehajtás tekintetében. A bejelentett felfüggesztési kérelmeket a Regisztrációs Szervezet a Hitelesítő Szervezetnek továbbítja.

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

A felfüggesztési kérelem bejelentésének és végrehajtásának magánkulcs kompromittálódás esetén késlekedés nélkül, minden más műveletet megelőzve meg kell történnie az észlelést követően.

4.4.8 Felfüggesztett állapotra vonatkozó korlátozások

Felfüggesztett állapotban legfeljebb 30 naptári napig lehet a tanúsítvány.

Ha a felfüggesztésről a Szolgáltató határozott, akkor ezen időszakon belül dönt a tanúsítvány állapotáról. Amennyiben Szolgáltató ezen időszak alatt nem képes a körülmények kivizsgálására, akkor a tanúsítványt visszavonja. Előfizető igénye estén térítésmentesen részére új tanúsítványt bocsát ki.

Ha a felfüggesztést az előfizető, vagy a tanúsítványban feltűntetett szervezet kérte, akkor a kérelmezőnek ezen időszak alatt értesítenie kell a Szolgáltatót a tanúsítvány érvényesítése vagy visszavonása felől. Ha ilyen értesítés nem történik Szolgáltató a tanúsítványt visszavonja.

A felfüggesztés megszüntetése az időszak vége előtt is kérvényezhető. A felfüggesztés megszűntetése csak a Regisztrációs Szervezetnél történő személyes megjelenés, és Előfizető hitelt érdemlő azonosítása után történik meg.

4.4.9 CRL kibocsátás gyakorisága

Szolgáltató a 2.6.4 pontban meghatározott időszakban rendszeresen, 4 óránként bocsát ki Tanúsítvány Visszavonási Listát. Ezen időközönként Tanúsítvány Visszavonási Lista akkor is kibocsátásra kerül, ha a legutóbbi kibocsátás óta nem történt tanúsítvány visszavonás. A Hitelesítő Szervezet a Tanúsítvány Visszavonási Listában jelöli a következő CRL kibocsátásának tervezett idejét. Tanúsítvány Visszavonási Lista a megjelölt tervezett idő előtt is kibocsátható.

4.4.10 CRL ellenőrzési követelmények

Tanúsítvány Visszavonási Lista ellenőrzése ajánlott az Érintett fél részére az elektronikus aláírás ellenőrzési eljárás során. A Szolgáltató által Tanúsítvány Visszavonási Listában közzétett érvénytelen, vagy felfüggesztett tanúsítvány elfogadásából keletkező bárminemű kár Érintett felet terheli. Lásd még a 2.2.4. pontot.

4.4.11 On-line visszavonási státusz-szolgáltatás

Szolgáltató nem üzemeltet On-line visszavonási állapot-szolgáltatást.

4.4.12 On-line visszavonás ellenőrzési követelmények

Szolgáltató nem üzemeltet On-line visszavonási állapot-szolgáltatást.

4.4.13 Visszavonási állapot közlés más formái

Szolgáltató nem alkalmaz a Tanúsítvány Visszavonási Listától különböző visszavonási állapot közlő eljárást.

A tanúsítványt igénybe vevő Érintett feleknek ugyanakkor, minden hagyományosan alkalmazott, és ésszerűen elvárható módszert igénybe kell venniük az általuk tanúsítvány segítségével ellenőrzött műveletek biztonsága érdekében. Amennyiben módjuk van az aláírás és tanúsítvány érvényességének más forrásból való ellenőrzésére, akkor azt a tanúsítvány állapotától függetlenül is meg kell tenniük. Amennyiben Érintett fél más forrásból tudomást szerezhet, vagy ésszerű és elvárható gondossággal más forrásból megbizonyosodhat a tanúsítvánnyal igazolt művelet érvényességéről, akkor ezeket a lépéseket a tanúsítvány állapotától függetlenül is meg kell tennie. Szolgáltató ilyen esetekben nem felelős a bekövetkező károkért.

4.4.14 Visszavonási állapot közlés más formáinak ellenőrzési követelményei

Szolgáltató nem alkalmaz a Tanúsítvány Visszavonási Listától különböző visszavonási állapot közlő eljárást.

4.4.15 Magánkulcs kompromittálódás speciális követelményei

Magánkulcs kompromittálódása, vagy vélelmezett kompromittálódása esetén a tanúsítvány visszavonásáról azonnal intézkedni kell. Alapos gyanú esetén a magánkulcs használatát azonnal fel kell függeszteni. Kompromittálódott magánkulcs tovább nem használható. A kompromittálódott magánkulcs a megsemmisítéséig ugyanolyan felügyeletben részesítendő, mint egy érvényes magánkulcs. Előfizetőnek kötelessége a kompromittálódott magánkulcs által esetlegesen érintett felek értesítése, és minden intézkedés megtétele az esetleges károk megelőzése és enyhítése érdekében.

4.4.16 Tanúsítvány megújítás

A tanúsítvány megújítása a tanúsítványban feltűntetett érvényességi idő meghosszabbítását jelenti.

Előfizetői tanúsítvány csak az eredeti érvényességi időtartammal megegyező időtartamra újítható meg. A tanúsítvány megújítása előtt az előfizetőnek nyilatkozni kell arról, hogy a tanúsítványba foglalt adatai továbbra is érvényesek.

4.5 Biztonsági audit eljárások

4.5.1 Naplózott esemény típusok

A Szolgáltató rendszere széleskörű naplózási lehetőségeket biztosít.

A hitelesítő és a regisztrációs rendszerhez történő valamennyi hozzáférés, tevékenységek naplózásra kerülnek oly módon, hogy azokból a tevékenység és annak időpontja és végrehajtója egyértelműen megállapítható legyen. A naplózás elemei elkülönülten keletkeznek a különböző modulokban.

Naplózásra kerülnek kiemelten a következő események:

- a tanúsítványok generálására, felfüggesztésére illetve visszavonására vonatkozó események,
- a tanúsítványokkal kapcsolatos egyéb változások adatai,
- az adatbázis kezelő rendszer műveletei,
- az operációs rendszer műveletei,
- az esetleges hibaesemények,

4.5.2 Napló adatok feldolgozásának gyakorisága

A kritikus bejegyzések feldolgozása a rendellenesség észleléskor, az egyéb napló adatok feldolgozása az üzemeltetési rendnek megfelelően, rendszeresen megtörténik.

4.5.3 Napló adatok tárolási ideje

A napló adatokat Szolgáltató a Törvényben meghatározott ideig tárolja. A papír alapú adathordozóra kinyomtatott napló adatok közül Szolgáltató azokat, amelyek más adathordozón archiválásra kerülnek, a feldolgozás után papírhulladéknak tekinti és az 5.1. pontban leírtaknak megfelelően megsemmisíti. A csak papír alapú hordozón létező eseménynaplókat a Szolgáltató a Törvényben meghatározott ideig tárolja.

4.5.4 Napló adatok védelme

A naplózás zárt rendszerben, automatikusan történik. Minden egyes naplóbejegyzés egyedi sorszámot kap, és az információ minden esetben elektronikusan aláírásra kerül a későbbi módosítások megakadályozása céljából.

4.5.5 Napló adatok mentési eljárásai

A Hitelesítő központ napló adatai összegyűjtésre kerülnek a központi mentő szerverre. A mentő szerver és az egyedi eszközök tartalmának mentése tervszerűen és rendszeresen történik. A mentést tartalmazó adathordozók tárolása az 5.1. pontban leírtaknak megfelelően történik. A mentésekről biztonsági másolat

készül, mely földrajzilag elkülönülten, megfelelő biztonsági körülmények között kerül tárolásra. Szolgáltató biztosítja a mentésekből történő visszaállíthatóságot.

4.5.6 Rendkívüli eseményekről történő értesítés

A működési zavarokat, a leállást nem okozó hibabejegyzéseket, valamint az informatikai védelmi rendszer megkerülésének, megzavarásának kísérleteit a rendszer naplózza. A rendkívüli események kivizsgálását a Szolgáltató azonnal megkezdi. A vizsgálatba szükség esetén bevonja az Előfizetőt is.

4.5.7 Sebezhetőség kiértékelése

Szolgáltató folyamatosan ellenőrzi, és rendszeresen ellenőrizteti a tanúsítvány kibocsátó rendszerének sebezhetőségét.

4.6 Adatarchiválás

A Szolgáltató hitelesítési szolgáltatást nyújtó rendszerének adat állományai és a napló adatai a rendszeresen archiválásra kerülnek. Az archivált adathordozók kezelése a 4.5.5 és az 5.1 pontokban leírtaknak megfelelően történik. Az archivált adatok a Törvényben előírt ideig kerülnek megőrzésre és abból információ kiadását a Szolgáltató a Törvénynek megfelelően biztosítja.

4.7 Szolgáltatói kulcs csere

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

4.8 Katasztrófa elhárítás

4.8.1 Hardver, szoftver, vagy adatsérülés esete

Szolgáltató megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik, a hardver-, szoftver-meghibásodások, vagy adatsérülés kivédésére, továbbá rendszeres mentésekkel és tranzakció naplózással biztosítja szolgáltatások visszaállíthatóságát a rendszer kiesésének esetére.

4.8.2 Szolgáltatói nyilvános kulcs visszavonás esete

Szolgáltató katasztrófa elhárítási terve kitér a szolgáltatói nyilvános kulcs visszavonás esetére.

4.8.3 Szolgáltatói magánkulcs kompromittálódás esete

A Szolgáltató magánkulcsának kompromittálódása valószerűtlen, a védelmére foganatosított szabályoknak, eljárásoknak, berendezéseknek és mechanizmusoknak köszönhetően.
Szolgáltató katasztrófa elhárítási terve kitér a szolgáltatói magán kulcs kompromittálódásának esetére.

4.8.4 Természeti katasztrófa esete

A Szolgáltató a mentések másolati példányainak más helyszínen történő tárolásával, és azok rendszeres frissítésével biztosítja az archivált adatok és a szolgáltatások visszaállíthatóságát, melynek ideje a katasztrófa természetéből és mértékéből adódóan változó lehet..

4.8.5 Üzletfolytonossági és katasztrófa elhárítási terv

A Szolgáltató rendelkezik katasztrófa elhárítási tervvel, mely dokumentum biztonsági okokból nem nyilvános.

4.9 Hitelesítés szolgáltató tevékenység megszüntetése

Szolgáltató a Szolgáltatás megszűnése esetén késlekedés nélkül értesíti a Közösség tagjait és a Hírközlési Főfelügyeletet. Amennyiben a megszűnés tervezett, az értesítés legkevesebb 60 nappal megelőzi a szolgáltatás leállítását. Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezd más szolgáltatókkal a szolgáltatás átvételéről. A tárgyalások végeredményéről tájékoztatja a közösséget. Az értesítést a Szolgáltatás nyújtásában részt vevő szervezeteknek és az előfizetőknek elektronikus aláírásával ellátott e-mailben küldi el, s az Érintett felek tájékoztatása végett a web oldalain és két országos napilapban is közzé teszi. A bejelentéssel egyidejűleg leállítja az új tanúsítványok kibocsátását és a tanúsítványok megújítását. Szolgáltató a tervezett megszűnés előtt 20 nappal intézkedik az előfizetői tanúsítványok és saját felhasználású tanúsítványok visszavonásáról.

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

Eljárás Regisztrációs szervezet megszűnése esetén:

A Regisztrációs szervezet megszűnése előtt 60 nappal értesíti azon Előfizetőket, akik a megszűnő regisztrációs szervezettől kapott, a Szolgáltató által kibocsátott érvényes tanúsítvánnyal rendelkeznek. Az értesítésben jelzi, hogy a tanúsítványt milyen határidővel vonja vissza, és tájékoztatja az Előfizetőt arról, hogy mely Regisztrációs Szervezeteknél igényelhet díjmentesen új tanúsítványt.

A Regisztrációs Szervezet megszűnéséről a Közösség tagjait Szolgáltató a web oldalain történő közzététel útján tájékoztatja.

5 Fizikai, eljárásrendi, és humán biztonsági szabályozások

5.1 Fizikai biztonsági szabályozások

A Szolgáltatói környezet kialakítása a vonatkozó magyar szabványok figyelembe vételével történt. Az épületnek a szolgáltatás céljára használt helyiségei közvetlenül nem érintkeznek közterülettel és elektromágneses ki- és besugárzás elleni védelemmel ellátottak. A fizikai behatolás elleni védelemre a megfelelően szilárd falak, ajtók, zárak, élőerős védelem, beléptető rendszer naplózással, videofigyelő és vagyonvédelmi rendszer szolgálnak. A Hitelesítési szolgáltatás céljára használt helyiségekbe a bejutás csak korlátozott kör számára engedélyezett

A GIRO Rt. szolgáltatást nyújtó telephelyének villamos energia ellátása több irányból történik. Az informatikai rendszer folyamatos működését szünetmentes tápegység és saját aggregátor biztosítja. A szolgáltatást nyújtó berendezések elhelyezésére szolgáló központi helyiségek klimatizáltak.

A központi gépterem építészeti és villamossági kialakítása a tűzvédelmi előírásoknak megfelelő, valamint rendelkezik beépített automata oltórendszerrel. A személyzet rendszeres képzése kiterjed a tűz elleni védelmi feladatokra.

Az adathordozók tárolása külön, speciális védelmi előírásoknak megfelelő helyiségben történik, amelybe a bejutás csak korlátozott kör számára engedélyezett. A mozgások naplózását külön nyilvántartási rendszer végzi. Mentések másolatának tárolása másik helyszínen, napi frissítéssel történik.

A keletkezett papírhulladékok zúzása géppel történik a Szolgáltató munkatársának jelenlétében. A selejtezett mágneses adathordozók megsemmisítése a felülíráson túl, fizikai roncsolással, az egyszer írható adathordozók megsemmisítése fizikai roncsolással történik. A hulladékkezeléssel kapcsolatos tevékenységeket jegyzőkönyv rögzíti.

5.2 Eljárásrendi szabályozások

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.

5.3 Humán szabályozások

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

6 Technikai szabályozások

6.1 Kulcs-pár generálás és installáció

6.1.1 Kulcs-pár generálás

Előfizetői aláíró kulcs-pár a Regisztrációs Hatóságnál, a Hatóság által alkalmazott szoftvermodulban vagy az általa biztosított aláíró eszközön generálódik.

Szolgáltató saját felhasználású kulcsai a kulcs tárolását végző hardver modulban generálódnak.

6.1.2 Magánkulcs felhasználóhoz történő eljuttatása

Az előfizetői magánkulcsot az előfizető a Regisztrációs Szervezettől személyesen veszi át személyazonosságának igazolása után a kulcshordozó eszközön.

6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

Az előfizető tanúsítványba foglalandó nyilvános kulcsa a Regisztrációs Szervezettől PKCS#10 tanúsítványigénylés formában, a Regisztrációs Szervezet magánkulcsával digitálisan aláírt elektronikus üzenetben kerül a Hitelesítő Szervezethez.

6.1.4 Hitelesítő Szervezet nyilvános kulcsának eljuttatása a felhasználókhoz

Az Elsődleges Hitelesítő Központ és a Szolgáltatói Hitelesítő Központ nyilvános kulcsa azok tanúsítványába foglalva a tanúsítványtárba íródik. A tanúsítványok felkerülnek a Szolgáltató nyilvános web oldalaira is a https://www.giro.hu/tanusitvany címen. A tanúsítványok mindkét helyről letölthetőek és a felhasználó kliensalkalmazásába installálhatóak. Szolgáltató az Elsődleges Hitelesítő Központ nyilvános kulcsának digitális lenyomatát hexadecimális formában közzéteszi két országos napilapban. A Regisztráció Szervezetek ügyfélszolgálatai, kérés esetén, telefonon is rendelkezésre állnak a digitális lenyomat egyeztetése végett.

6.1.5 Kulcs méretek

Előfizetők részére Szolgáltató legalább 1024 bites RSA kulcsokat generál. A Szolgáltató Hitelesítő központjának rendszerében alkalmazott kulcsok mérete 2048 bit.

6.1.6 Előfizetői nyilvános kulcs előállításához használt paraméterek előállítása

Az előfizetői nyilvános kulcs előállításához használt paraméterek előállítását a Regisztrációs Szervezet szoftvere, vagy az aláíró eszköz automatikusan elvégzi.

6.1.7 Előfizetői nyilvános kulcs előállításához használt paraméterek minőségellenőrzése

Az előfizetői nyilvános kulcs előállításához használt paraméterek minőségellenőrzését a Regisztrációs Szervezet szoftvere, vagy az aláíró eszköz automatikusan elvégzi.

6.1.8 Szoftveres / hardveres kulcsgenerálás

A végfelhasználói kulcs-pár előállításakor Szolgáltató, mind a szoftveres, mind a hardveres kulcsgenerálás módszerét alkalmazza a kulcshordozó eszköztől függően.

6.1.9 Kulcs felhasználási célok

Szolgáltató Előfizető részére a kulcs-párt aláírási vagy rejtjelezési céllal bocsátja ki. Ennek érdekében a tanúsítványban található KeyUsage mezőt *Digital Signature* vagy *Key Encipherment* értékkel tölti ki. A kulcspár kizárólag arra a célra használható, amelyre Szolgáltató kibocsátotta, Szolgáltató szabályzatainak és szerződéses feltételeinek megfelelően.

6.2 Magán kulcs védelme

6.2.1 Kriptográfiai modulra vonatkozó szabványok

Előfizetők magánkulcsának tárolására Szolgáltató olyan hardveres modult bocsát ki, mely teljesíti legalább a FIPS 140-1 szabvány első fokozatának (FIPS 140-1 Level 1) követelményeit. A magánkulcsot Szolgáltató mindig jelszóval vagy PIN kóddal védve bocsátja ki. A magánkulcs átvétele után Előfizető felelős a kulcshordozó, a magánkulcs, és a jelszó védelméért.

Szolgáltató saját kulcsainak tárolására hardveres modult alkalmaz, amely teljesíti legalább a FIPS 140-1 szabvány első fokozatát (FIPS 140-1 Level 1). A hitelesítő központok aláíró kulcsainak tekintetében a tároló eszköz teljesíti a FIPS 140-1 szabvány harmadik fokozatát (FIPS 140-1 Level 3).

6.2.2 Magánkulcs több-személyes kontrollja

Szolgáltató nem alkalmaz több-személyes kontrollt az Előfizetők magánkulcsának védelméül. Szolgáltató a hitelesítő központok kulcsainak biztonsági mentésének biztonsága érdekében alkalmaz többszemélyes kontrollt.

6.2.3 Magánkulcs letét

Szolgáltató nem nyújt magánkulcs letét szolgáltatást. Előfizetői magánkulcsot, vagy annak előállítására, visszafejtésére alkalmas adatot nem tárol.

6.2.4 Magánkulcs mentése

Szolgáltató az Előfizető aláírói magánkulcsát semmilyen formában sem menti, vagy tárolja.

6.2.5 Magánkulcs archiválása

Szolgáltató az Előfizetői magánkulcsot nem archiválja.

6.2.6 Magánkulcs kriptográfiai modulba helyezése

A szoftveres úton generált előfizetői magánkulcsot Szolgáltató intelligens kártyára írja. Az intelligens kártyán generált kulcs az eszközt nem hagyja el.

6.2.7 Magánkulcs aktiválása

Az előfizetői magánkulcsok aktiválása a felhasználó által történik a jelszó vagy PIN kód megadásával, azokban az esetekben, amikor a magánkulcs használatára szükség van.

6.2.8 Magánkulcs deaktiválása

Az előfizetői magánkulcsok deaktiválását a felhasználó alkalmazása végzi, vagy a felhasználó a kulcshordozó eszköz eltávolításával az aláíró környezetből.

6.2.9 Magánkulcs megsemmisítése

Az előfizetői aláíró magánkulcs lejárat utáni megsemmisítésről Előfizetőnek kötelessége gondoskodni. A szolgáltatói kulcsok megsemmisítése a Szolgáltató kötelessége.

6.3 Kulcs-pár kezelés egyéb aspektusai

6.3.1 Nyilvános kulcs archiválása

Az előfizetői tanúsítványokat Szolgáltató az érvényesség lejáratától számított 5 évig archív formában megőrzi. Az archív adatállományt Szolgáltató az erre a célra létrehozott magánkulcsával aláírja, s legalább két példányban menti. Az adathordozók Szolgáltató központjában és telephelyén tárolódnak, biztonságos környezetben, a megőrzési idő végéig.

6.3.2 Nyilvános és magánkulcs felhasználási ideje

Az előfizetői nyilvános és magánkulcs érvényességi ideje megegyezik a tanúsítvány érvényességi idejével.

6.4 Aktiválási adatok

6.4.1 Aktiválási adatok generálása és installációja

Az előfizetői magánkulcs aktiválási adatát (jelszavát vagy PIN kódját) Előfizető adhatja meg a Regisztráció alkalmával. A jelszó vagy PIN kód rendszerbe táplálását a regisztráló munkatárs végzi. Az előfizető köteles az első használat előtt megváltoztatni jelszavát vagy PIN kódját.

6.4.2 Aktiválási adatok védelme

Előfizetői magánkulcs aktiválási adatát a Szolgáltató nem hozza harmadik fél tudomására, s a kulcs előállítása után megsemmisíti. Az aktiválási adat védelme Előfizető kötelessége. Az előfizető bármikor megváltoztathatja a jelszavát vagy PIN kódját.

6.4.3 Aktiválási adatok egyéb aspektusai

Az előfizetői magánkulcs aktiválási adatát Szolgáltató nem tárolja, s semmilyen körülmények között nem képes annak ismételt előállítására, visszatöltésére, az Előfizető, harmadik fél, vagy hatóság kifejezett kérése esetén sem.

6.5 Számítógép biztonsági szabályok

6.5.1 Számítógép biztonság technikai követelményei

Szolgáltató hitelesítési szolgáltatást nyújtó központi eszközei védett, az 5.1. pontban leírt, biztonságos környezetben működnek. A számítógépes rendszer emelt szintű felhasználó azonosítást, jogosultság kezelést alkalmaz és naplózza a rendszerben történt eseményeket.

6.5.2 Számítógép biztonsági értékelések

Az eszközök biztonsági paraméterei teljesítik az alábbi követelményeket:

Üzembiztonság: UL 1950, UL Canada C22.2 No. 950, TUV EN 60950, UL CB Scheme to IEC 950 with full deviations,RFI/EMI FCC Class A, DOC Class B, VCCI Class A, EN 55022 Class B

Védettség EN 50082-1

Elektromágneses sugárzás DHHS 21 Subchapter J; PTB German X-ray Decree

Szolgáltató független szakértővel rendszeresen ellenőrizteti a tanúsítvány kibocsátó rendszerének biztonságát.

6.6 Életciklus technikai szabályok

6.6.1 Rendszerfejlesztési szabályok

A Szolgáltató tanúsítvány kibocsátó rendszere nemzetközi minősítéssel ellátott alkalmazási elemekből áll. A rendszer bővítése, továbbfejlesztése csak olyan elemekkel történhet, amely a rendszer egyenszilárdságát nem rontja.

6.6.2 Biztonságkezelési szabályok

Szolgáltató tesztkörnyezettel rendelkezik és a továbbfejlesztett rendszereket csak a megbízható működés, és a belső előírásoknak történő megfelelés, és tesztelés után vezeti be az éles üzembe.

6.6.3 Életciklus biztonsági értékelések

Szolgáltató a bővített, továbbfejlesztett rendszert a 2.7 pontnak megfelelően független szakértővel ellenőrizteti.

6.7 Hálózati biztonsági szabályok

A Szolgáltató központi hitelesítés szolgáltató rendszere és a regisztrációs pontok közötti kommunikáció VPN illetve SSL biztonsági megoldással valósul meg, A belső és a külső hálózatok biztonságos elválasztására tűzfal szolgál. A hálózati csatlakozási pontok biztonságát behatolás figyelő rendszer (IDS) növeli.

6.8 Kriptográfiai modul műszaki szabályok

A Szolgáltató tanúsítvány kibocsátó rendszerének kriptográfiai modulja FIPS 140-1 Level 3/ ITSEC E3 nemzetközi minősítéssel rendelkezik.

7 Tanúsítvány és kulcs-visszavonási profil

Jelen fejezetben bemutatott általános tanúsítvány profilt Szolgáltató Hitelesítési Szabályzatai még bővíthetik és részletezhetik.

7.1 Tanúsítvány profil

7.1.1 Verziószám

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 3. verziójának megfelelő tanúsítványokat bocsát ki. Előfizető és Érintett fél által alkalmazott eljárásoknak és alkalmazásoknak támogatnia kell az ilyen típusú tanúsítványok helyes kezelését. Szolgáltató a kibocsátott tanúsítványok Version mezőjébe V3 értéket ír.

7.1.2 Alap mezők

7.1.2.1 Sorozatszám

Szolgáltató a kibocsátott tanúsítványok Serial Number mezőjébe 10 karakter hosszúságú sorozatszám értéket ír, amely egyedi a Szolgáltató által kiadott tanúsítványoknál.

7.1.2.2 Algoritmus azonosító

Szolgáltató a kibocsátott tanúsítványok Signature Algorithm Identifier mezőjébe a tanúsítványt hitelesítő elektronikus aláírásának algoritmus azonosítóját helyezi el.

7.1.2.3 Aláírás

Szolgáltató a kibocsátott tanúsítványok Signature mezőjébe a tanúsítványt hitelesítő elektronikus aláírását helyezi el.

7.1.2.4 Kibocsátó

Szolgáltató a kibocsátott tanúsítványok Issuer mezőjébe a tanúsítványt kibocsátó Hitelesítő Szervezet egyedi azonosítóját írja. Ez előfizetői tanúsítványok esetében a következő: `c=hu/cn=Giro Hitelesítő Központ/o=giro/ou=giro`

7.1.2.5 Érvényesség

Szolgáltató a kibocsátott tanúsítványok Validity Period mezőjébe a tanúsítvány érvényességének kezdetét és végét írja.

7.1.2.6 Előfizető

Szolgáltató a kibocsátott tanúsítványok Subject mezőjébe az előfizető (Aláíró) egyedi azonosítóját írja.

7.1.2.7 Előfizető nyilvános kulcsának algoritmus azonosítója

Szolgáltatón a kibocsátott tanúsítványok Subject Public Key Algorithm Identifier mezőjébe Előfizető nyilvános kulcs algoritmusának azonosítóját helyezi el.

7.1.2.8 Előfizető nyilvános kulcsa

Szolgáltató a kibocsátott tanúsítványok Subject Public Key Value mezőjébe Előfizetőnek nyilvános kulcsát írja.

7.1.3 Opcionális mezők

7.1.3.1 Kibocsátó egyedi azonosító

Szolgáltató a kibocsátott tanúsítványok Issuer Unique Identifier mezőjét nem tölti ki.

7.1.3.2 Előfizető egyedi azonosító

Szolgáltató a kibocsátott tanúsítványok Subject Unique Identifier mezőjét nem tölti ki.

7.1.4 Tanúsítvány kiterjesztések

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 3. verziójának megfelelő tanúsítvány kiterjesztéseket támogatja.

7.1.5 Algoritmus azonosító

Szolgáltató az RSA kriptográfiai algoritmust támogatja, a NIST FIPS PUB 186-1 szabványával konform módon. Szolgáltató opcionális módon a DSA és ECDSA kriptográfiai algoritmusokat támogatja, a NIST FIPS PUB 186-1, illetve az ANSI X9.62 szabványával konform módon.

Szolgáltató az SHA1 és MD5 digitális lenyomat előállító algoritmusokat támogatja. Az SHA-1 támogatása a FIPS Pub 180-1 szabvány szerint (OID=1.3.14.3.2.26), az MD5 támogatása pedig az IETF RFC 1321 szabványnak megfelelően (OID=1.2.840. 113549.2) történik.

7.1.6 Név-formák

A Szolgáltató által kibocsátott tanúsítványok, mind a kibocsátó, mind az előfizető azonosítója esetében az egyedi X.500 név formátumot alkalmazza, X.501 printable string formátumban. (Az X.501 az International Telecommunication Union által kiadott ITU-T X.501 “Information Technology - Open systems interconnection - The directory: Models” ajánlás)

7.1.7 Név megkötések

Szolgáltató által kibocsátott tanúsítványok nem tartalmazhatnak álnevet, vagy fantázianevet.

7.1.8 Tanúsítási szabályzat objektum azonosító

Szolgáltató által kibocsátott tanúsítványok a Certificate Policy mezőben a Szolgáltatói Hitelesítési Szabályzat egyedi objektum azonosítóját tartalmazzák.

7.1.9 Szabályzat megkötési mezők használata

Nincs megkötés.

7.1.10 Szabályzat minősítő szintaxis és szemantika

Szolgáltató által kibocsátott tanúsítványok a PolicyQualifier kiterjesztésben a Szolgáltatói Hitelesítési Szabályzatának web címét tartalmazzák, a UserNotice kiterjesztésben pedig a következő szöveget: ”A tanúsítvány értelmezéséhez és elfogadásához a Szolgáltató Hitelesítési Szabályzatában és Hitelesítési Szolgáltatási Szabályzatában foglaltak szerint kell eljárni, melyek megtalálhatók a következő címen: https://www.giro.hu/hiteles/szabalyzat”.

7.1.11 Kritikus szabályzat kiterjesztés feldolgozása

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

7.2 Kulcs-visszavonási profil

7.2.1 Verziószám

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.

7.2.2 Visszavonási lista és visszavonás bejegyzési kiterjesztések

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 specifikáció adminisztrációját a Szolgáltató Szabályozó Szervezete végzi. Elérhetősége a Szabályzat 1.5.4. pontjában található.

8.1 Specifikáció változáskezelési eljárásai

A Szolgáltató saját döntése alapján, a 2001. évi XXXV. Eat.), 7. § a 151/2001 Kormány rendelet 2. §é s a 16/2001. (IX. 1.) MeHVM rendelet 5. § figyelembe vételével jogosult a Hitelesítési Szolgáltatási Szabályzat és az Általános szerződési feltételek módosítására.

A módosított Hitelesítési Szolgáltatási Szabályzatot és az Általános szerződési feltételeket új verziószámmal hozza létre.

A tervezett módosítást 30 nappal az életbe lépés előtt a felügyeleti szerv részére bejelenti.

8.2 Publikációs és értesítési szabályok

A változások bejelentéséről az értesítést a GIRO Rt. az Interneten a következő címen: https://www.giro.hu/hiteles/szabalyzat közzéteszi.

8.3 Hitelesítési Szolgáltatási Szabályzat elfogadási eljárások

A Hitelesítési Szolgáltatási Szabályzat és az Általános szerződési feltételek bármely módosítását a Szolgáltató Szabályozó Szervezete hagyja jóvá.

9 Hivatkozások és Meghatározások

9.1 Hivatkozások

- Jogszabályi hivatkozások

  A jelen szabályzat vonatkozásában

  - a Törvény a „2001. évi XXXV. törvény az elektronikus aláírásról” szóló jogszabály,
  - a Kormányrendelet a „151/2001 (IX.1.) Korm, rendelet a Hírközlési Főfelügyeletnek az elektronikus aláírással kapcsolatos feladat- és határköréről, valamint eljárásának részletes szabályairól” szóló jogszabály,
  - a Miniszteri rendelet vagy MeHVM rendelet a „16/2001 (IX.1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről” szóló jogszabály.

- Szerződés hivatkozások

  A jelen szabályzat vonatkozásában

  - Az Általános Szerződési Feltételek a Szolgáltató és az Előfizető közötti jogviszonyt meghatározó nyilvános dokumentum, melyet Előfizető az Előfizetői Szerződés aláírásával elfogad. Tartalmazza a Szolgáltató szolgáltatásainak, tanúsítványainak igénybevételéhez szükséges, illetve egyéb szerződési feltételeket.
  - Előfizetői Szerződés az Intézmény és az Előfizető közötti jogviszonyt meghatározó, kitöltés és aláírás előtt nyilvános dokumentum, melyet Előfizető aláírásával elfogad
  - Együttműködési Szerződés a GIRO Rt. és az Intézmény közötti jogviszonyt meghatározó, nem nyilvános dokumentum, melynek nyilvános vonatkozásait a jelen Szabályzat tartalmazza.
  - Üzletszabályzat nem önálló dokumentum, hanem azon szabályzatok együttesét jelenti, amely alapján Szolgáltató a Közösség tagjai részére a Szolgáltatást biztosítja. Az üzletszabályzat elemei a GIRO Rt. Hitelesítési Szolgáltatási Szabályzata, az Általános Szerződési Feltételek, az Előfizetői Szerződés és az Együttműködési Szerződés.

9.2 Meghatározások

A meghatározások fejezet nem ismétli a Törvényben, a Kormányrendeletben és a Miniszteri rendeletben leírt fogalmakat, mert a Szabályzat azokat ugyanolyan értelemben használja.

- **Aláírás-ellenőrző adat:** Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.
- **Aláírás-létrehozó adat:** Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az aláíró az elektronikus aláírás létrehozásához használ.
- **Aláírás-létrehozó eszköz:** Szoftver vagy hardver, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.
- **Aláírás-létrehozó rendszer:** Az a rendszer, illetve alkalmazás az aláírás-létrehozási környezeten belül, amelyik egy aláírás-létrehozó eszközt használ fel elektronikus aláírás létrehozásához.
- **Aláíró:** Az a természetes személy, akihez a hitelesítés szolgáltató által közzétett aláírás-ellenőrző adatok jegyzéke szerint az aláírás-ellenőrző adat kapcsolódik.
- **Aláíró környezet**: Az a fizikai és logikai környezet, melyben az aláírási folyamat lezajlik, és amely egy aláírás-létrehozó rendszert tartalmaz egy aláírás-létrehozó eszközzel, az aláíróval és az aláíró által kezelt rendszerelemekkel.
- **Aláíró eszköz**: Megegyezik az aláírás-létrehozó eszközzel.
- **Biztonságos aláírás-létrehozó eszköz:** Az elektronikus aláírás törvény 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz.
- **Biztonságos környezet:** Olyan fizikai környezet, mely védett illetéktelen hozzáféréstõl, és bizonyos mértékig tûz, víz és egyéb katasztrófaeseményektõl, egyéb erõszakos behatásoktól.
- **Elektronikus aláírás:** elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum.
- **Ellenőrzési lépések:** Az elektronikus aláírás ellenőrzésekor kötelezően elvégzendő műveletsor.
- **Előfizető:** Az a személy vagy szervezet, amely Szolgáltatóval érvényes előfizetői szerződéssel rendelkezik hitelesítés-szolgáltatás igénybe vételére, és így a Szolgáltató által kiadott tanúsítvány tulajdonosának tekinthető.
- **Érintett fél:** Az elektronikus dokumentum fogadója, aki egy adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el.
- **Fokozott biztonságú elektronikus aláírás:** Elektronikus aláírás, amely megfelel a következő követelményeknek:

  alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető,

  olyan eszközzel hozták létre, amely kizárólag az aláíró befolyása alatt áll,

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

- **Hitelesítés szolgáltató:** Személy (szervezet), amely a hitelesítés szolgáltatás keretében azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványokhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat és a tanúsítvány visszavonási listát.
- **Igénylő:** Az a személy vagy szervezet, amely Szolgáltatóhoz fordul a hitelesítés-szolgáltatás igénybe vétele céljából.
- **Kompromittálódás:** Az az eset, amikor az aláírást létrehozó eszköz használatára, illetve az aláírás elhelyezésére arra nem jogosított személy képessé válik.
- **Központ:** Szolgáltató azon egysége, mely a hitelesítés-szolgáltatás hitelesítő kulccsal folytatott tevékenységét végzi. A központ fizikailag egy telephelyre koncentráltan, védett, biztonságos körülmények között működik.
- **(Kriptográfiai) Kulcs:** Kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.
- **Kriptográfiai modul:** Hardver alapú biztonsági megoldás, amely alkalmas beépített eljárások segítségével biztonságos kulcsgenerálásra és tárolásra.
- **Kulcshordozó eszköz:** Aláírás-létrehozó adat tárolására szolgáló eszköz.
- **Magánkulcs aktiválása:** A magánkulcs aktiválása az a folyamat, melynek során a jogosult – különböző azonosító elemek pl. jelszó, PIN kód megadásával – engedélyezi, hogy a leolvasóba helyezett magánkulcs megkezdje üzemszerű működését. Az aktiválás általában a magánkulcsot igénylő aláíró környezetben (dokumentum aláíró-, levelező rendszer) történik, és érvényes lehet a visszavonásig (deaktiválásig) illetve egyszeri használatra.
- **Magánkulcs deaktiválása:** A magánkulcs deaktiválása az a folyamat, melynek során a magánkulcs üzemszerű működése megszüntetésre kerül. Ez olyan kulcshordozó esetén, amikor a kulcs üzemszerű működés során nem hagyja el a kulcshordozó eszközt, történhet a kulcshordozó olvasóból történő eltávolításával, más esetekben a kulcshordozó eszköz aláíró környezetből való eltávolításával, vagy az alkalmazásból való kilépéssel.
- **Nyilvános (publikus) kulcsú infrastruktúra:** Az elektronikus aláírás létrehozására, ellenőrzésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.
- **Regisztrációs szervezet:** Pénzügyi Intézmények, a Magyar Nemzeti Bank, a Magyar Államkincstár, a KELER Rt. amennyiben a Hitelesítés szolgáltatásra a GIRO Rt-vel külön szerződést kötöttek. Az aktuális listát lásd a www.giro.hu/hiteles/partner weboldalon.

- **Regisztrációs egység**: a Regisztrációs szervezet azon szervezeti egysége(i), amely(ek) az Előfizetővel közvetlen kapcsolattartás útján együttműködve teljesíti, illetőleg gyakorolja a HSzSz-ben, illetőleg az ÁSzF-ben meghatározott jogait és kötelezettségeit.
- **Regisztrációs adatok:** Azon információk összessége, amelyeket a Szolgáltató a tanúsítványkiadás érdekében Előfizetőről begyűjt.
- **Szolgáltatás:** Elektronikus aláírás hitelesítés-szolgáltatás (röviden: hitelesítés-szolgáltatás) és aláírás-létrehozó adat előállítása és elhelyezése az aláírás-létrehozó adatot tároló eszközön.
- **Szolgáltatási szabályzat:** A hitelesítés szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó nyilvános dokumentum.
- **Szolgáltató:** A Giro Rt. és hitelesítési szolgáltatásban tevékenyen részt vevő, vele kapcsolatban álló partnerek és alvállalkozók.
- **Tanúsítvány:** A hitelesítés szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot az elektronikus aláírásról szóló törvény szerint egy meghatározott személyéhez kapcsolja és igazolja e személy személyazonosságát.
- **Tanúsítványok osztályai:** A tanúsítványok megbízhatósága szerinti megkülönböztetés. A kibocsátást megelőző ellenőrző lépések biztonságosságának jelzésére is szolgál (a jelenleg létező osztályok: Szolgáltatói, fokozott biztonságú, teszt).
- **Tanúsítvány típus:** A tanúsítványok megkülönböztetése az alkalmazó közösség és/vagy az alkalmazás módja alapján.
- **Tanúsítvány visszavonási lista:** Valamely okból visszavont, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, amelyet a hitelesítés szolgáltató bocsát ki.