NISZ

Nemzeti Infokommunikációs Szolgáltató Zrt.

Hitelesítési Rend
titkosító és autentikációs tanúsítványokhoz
(HR-TET)

Verziószám	1.4
OID	0.2.216.1.200.1100.100.42.3.5.22.1.4
Hatályba lépés dátuma	2022.09.23.
Dokumentum besorolása	nyilvános
Jóváhagyó	Adorján István

Adorján István

Digitálisan aláírta: Adorján István
Dátum: 2022.09.22 17:39:03 +02'00'

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
1.0	2013.08.01.	Első változat	Kővári Ferenc Jolláthy Dániel	Kővári Ferenc	Ferencz Attila
1.1	2014.03.17.	CAB BR követelmények szerint módosított változat	Kővári Ferenc Jolláthy Dániel	Kővári Ferenc	Ferencz Attila
1.2	2014.05.14.	Jogi hivatkozásokkal és pontosításokkal módosított változat	Kővári Ferenc	dr. Sandl Judit	Ferencz Attila
1.3	2016.08.01	• RFC 3647 szerint átdolgozás • SSL szerver tanúsítványok kivezetése • OID változás: 0.2.216.1.200.1100.100.42.3.5.9 → 0.2.216.1.200.1100.100.42.3.5.22	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.4	2022.09.23.	• új algoritmuskészletek bevezetésével kapcsolatos módosítások • egyéb pontosítások	Kővári-Szabó Zoltán	Nagy Benjámin Melo Sándor	Adorján István

Tartalomjegyzék

1 BEVEZETÉS

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban: Szolgáltató) Hitelesítési Rendje, mely a titkosító, autentikációs és egyéb speciális célú tanúsítványokkal kapcsolatos szolgáltatásaira vonatkozik (továbbiakban: HR-TET).

Jelen hitelesítési rend a kibocsátott tanúsítványok kezelésére (előállítás, kibocsátás, közzététel, kulcsletét, megújítás, felfüggesztés, újraérvényesítés, visszavonás, továbbiakban együttesen: Szolgáltatások) vonatkozó követelményeket, a tanúsítványok tartalmának és érvényességének ellenőrzési eljárásait és a Szolgáltatások működtetésének követelményeit tartalmazza.

A Szolgáltató a Szolgáltatásokat a vele szerződéses viszonyban álló ügyfelek részére nyújtja, és egyes szolgáltatási elemeket hozzáférhetővé tesz a tanúsítványok hitelességét ellenőrző Érintett Felek részére is.

1.1 Áttekintés

A HR-TET egy olyan szabálygyűjtemény, amely a Szolgáltatások használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára, valamint meghatározza a tanúsítványok felhasználhatóságát.

Jelen hitelesítési rend az {Sz1} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában szigorúan követi annak előírásait.

Jelen hitelesítési rend előírja a tanúsítványokkal kapcsolatos, a Szolgáltatások nyújtása során teljesíteni szükséges összes követelményt, melyeket az alábbi nemzetközi szabványok határoznak meg:

- EN 319 401: General policy requirements for Trust Service Providers {Sz2}
- EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates {Sz3}
- EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures {Sz4}
- EN 319 412-2: Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons {Sz5}
- EN 319 412-3: Certificate Profiles; Part 3: Certificate profiles for certificates issued to legal persons {Sz6}

Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a „Szolgáltatási Szabályzat titkosító és autentikációs tanúsítványokhoz” (HSZSZ-T) dokumentum tartalmazza.

A jelen hitelesítési rendnek megfelelően kibocsátott tanúsítványok tartalmazzák jelen dokumentum objektum azonosítóját, mely alapján az érintett felek képesek meghatározni az adott tanúsítvány alkalmazhatóságát és megbízhatóságát.

1.2 Dokumentum neve és azonosítása

Jelen hitelesítési rend teljes neve NISZ Zrt. „Hitelesítési Rend titkosító és autentikációs tanúsítványokhoz”.

A hitelesítési rend rövid neve: HR-TET.

A hitelesítési rend objektum azonosítója és verziószáma a címlapon található.
A jelen HR-TET hatálya alatt kiadott tanúsítványok kibocsátására és felhasználására vonatkozó részletes szabályokat a HSZSZ-T szolgáltatási szabályzat tartalmazza. Jelen BR-TET-nek csak a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával ellátott változata tekinthető hitelesnek.

1.2.1 Hitelesítési rendek

A HR-TET hitelesítési rend megfelel az {Sz3} EN 319 411-1 szabvány 5.3 fejezet c) pontjában meghatározott LCP hitelesítési rendnek:

```
LCP: Lightweight Certificate Policy
itu-t(0) identified-organization(4) etsi(0) other-certificate- policies(2042)
policy-identifiers(1) lcp (3)
```

1.3 PKI közösség

1.3.1 Hitelesítő szervezet

A hitelesítő szervezet a Szolgáltató központi szervezete, amely a hitelesítő központokból (CA), a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, az ezt körülvevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll.

A Szolgáltató saját szervezetén kívül más szervezetek is közreműködhetnek a Szolgáltatások nyújtásában, azonban a Szolgáltató teljes körű felelősséggel tartozik azért, hogy a jelen szabályzatban foglalt követelmények teljesülnek.

1.3.2 Regisztrációs szervezet

A Szolgáltató – saját szervezetén belül – ügyfélkapcsolati irodát és regisztrációs irodát működtet.

Az Ügyfélkapcsolati Iroda végzi az ügyfelekkel való kapcsolattartást, az előfizetők és tanúsítvány alanyok adatainak felvételét, az előfizetők és tanúsítvány alanyok azonosítását, a tanúsítvány

kérelmek összeállítását, az elkészült tanúsítványok szétosztását, valamint gondoskodik a szolgáltatási szerződésben foglaltak teljesítéséről.

A Regisztrációs Iroda végzi az előfizetők és tanúsítvány alanyok technikai regisztrációját, a tanúsítványok előállításának, felfüggesztésének és visszavonásának jóváhagyását és kezelését, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat lát el.

A Szolgáltató saját szervezetén kívüli regisztrációs szervezetet (ügyfélkapcsolati irodát) is működtethet, a vele szerződéses alapon együttműködő társaságokkal (mint szerződött közreműködők) együtt. Ezen regisztrációs szervezetek elvégzik a saját igénylőik adatainak rögzítését, ellenőrzését, az igénylők személyazonosságának megállapítását, a tanúsítvány kérelmek összeállítását és Szolgáltatóhoz történő továbbítását. Biztosítják a tanúsítványok és a kulcstároló eszközök (chipkártya, USB token) szétosztását, a tanúsítvány kibocsátását és visszavonását, és egyéb azonosítási, tanúsítványmenedzsment és adminisztrációs feladatokat látnak el. Azon tevékenységek vonatkozásában, melyeket a Szolgáltató nem maga lát el, teljes körű felelősséget vállal azért, hogy a jelen szabályzatban foglalt követelmények teljesülnek.

1.3.3 Előfizetők és Alanyok

Előfizető az {D1} ÁSZF-GOVCA szerinti feltételeknek megfelelő, Szolgáltatóval szerződéses viszonyban álló jogi személy vagy közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet, amely megrendeli a Szolgáltatótól a Szolgáltatásokat, jellemzően tanúsítvány kibocsátását az általa megnevezett tanúsítvány alanyok számára.

A tanúsítvány alanya (továbbiakban: Alany)

a) természetes személy: az Előfizetővel kapcsolatban álló személy;

b) jogi személy: az Előfizető szervezete, vagy annak valamely szervezeti egysége;

c) eszköz: az Előfizető által vagy nevében működtetetett informatikai eszköz vagy rendszer.

1.3.3.1 Előfizető Kapcsolattartója

A Szolgáltatási Szerződés megkötése során az Előfizető kapcsolattartó személyt jelölhet meg, akit a képviseleti joggal rendelkező személy (pl. cégjegyzésre jogosult) felhatalmaz, illetve feljogosít a tanúsítványokkal kapcsolatos ügyekben Előfizető szervezete nevében eljárni, akár meghatározott esetekre kiterjedő aláírási joggal is. Szolgáltató a későbbiekben – a képvisletre jogosult személy(ek)en felül – ezen személy aláírását fogadja el a tanúsítványokkal kapcsolatos ügyekben, különösen a tanúsítvány igénylési folyamatban, vagy a tanúsítvány visszavonási folyamatban, az

ezekhez kapcsolódó kérelmeken. Kapcsolattartó kijelölésének hiányában Szolgáltató csak a képviseleti joggal rendelkező személy (pl. cégjegyzésre jogosult) aláírását fogadja eltanúsítványokkal kapcsolatos ügyekben.

Jelen dokumentumban a továbbiakban az Előfizető Kapcsolattartója kifejezés a fentiek szerint kijelölt személyt, illetve kijelölés hiányában a képviseleti joggal rendelkező (pl. cégjegyzésre jogosult) személyt jelenti.

1.3.4 Érintett felek

Érintett Fél: olyan természetes vagy jogi személy, aki/amely a HR-TET hitelesítési rend hatálya alatt kiadott tanúsítvány érvényességét ellenőrzi, és erre hagyatkozva jár el.

1.3.5 Egyéb felek

Nincs kikötés.

1.4 A tanúsítvány alkalmazhatósága

A HR-TET hatálya alatt kiadott titkosító és autentikációs tanúsítványok típusai az {Sz3} EN 319 411-1 szerint az alábbiak lehetnek:

a) üzleti tanúsítvány: a tanúsítvány Alanya az Előfizetővel kapcsolatban álló természetes személy (képviseleti joggal rendelkező vagy cégjegyzésre jogosult személy, vagy Előfizető szervezete által foglalkoztatott személy, akinek Előfizetővel való kapcsolata a tanúsítványban megjelölésre került;

b) személyes tanúsítvány: a tanúsítvány Alanya az Előfizetővel kapcsolatban álló természetes személy (akinek Előfizetővel való kapcsolata a tanúsítványban megjelölésre nem került;

c) szervezeti tanúsítvány: a tanúsítvány Alanya az Előfizető szervezet, vagy annak valamely szervezeti egysége;

d) eszköz tanúsítvány: a tanúsítvány Alanya az Előfizető által vagy nevében működtetett informatikai eszköz vagy rendszer.

A titkosító tanúsítvány, illetve a hozzá kapcsolódó kulcspár adatok vagy üzenetek titkosításához és visszafejtéséhez alkalmazható.
Az autentikációs tanúsítvány, illetve a hozzá kapcsolódó kulcspár személy, eszköz vagy szervezet PKI alapú azonosítására alkalmazható.

Teszt tanúsítványok

A Szolgáltató - egyrészt saját rendszerének tesztelése céljából, másrészt azért, hogy harmadik felek a Szolgáltatásokat kipróbálhassák - teszt tanúsítványokat is kibocsát. A Szolgáltató semmilyen felelősséget nem vállal a teszt tanúsítványok kibocsátásáért, felhasználásukért, a hozzájuk kapcsolódó szolgáltatások rendelkezésre állásáért.

Szolgáltató az éles szolgáltatást nyújtó gyökér hitelesítő központ hierarchiájában nem bocsát ki teszt tanúsítványt. A teszt tanúsítványok a külön az erre a célra létesített teszt gyökér hitelesítő központ hierarchiájában kerülnek kiadásra.

A teszt tanúsítványok megjelölése olyan módon történik, hogy a tanúsítványban feltüntetett hitelesítési rend objektumazonosító: 0.2.216.1.200.1100.100.42.3.999.

A teszt tanúsítványokhoz semmilyen joghatás nem kapcsolódik.

1.4.1 Engedélyezett tanúsítvány használat

A titkosító tanúsítványhoz kapcsolódó nyilvános kulcs kizárólag adatok vagy üzenetek titkosítására (kódolására), a kapcsolódó magánkulcs kizárólag a titkosított adatok vagy üzenetek visszafejtésére (dekódolására) használható fel.

Az autentikációs tanúsítványok, illetve a kapcsolódó magánkulcs személyek, eszközök vagy szervezetek hiteles azonosítására használható fel, a vonatkozó műszaki szabványok és protokollok szerint (pl. {Sz7} RFC 5246}).

A személyes tanúsítványokat az Alanyok csak és kizárólag az Előfizetőhöz kapcsolódó tevékenységükhöz (munkaviszonyukból fakadó feladataik elvégzéséhez) használhatják fel. A fentieken túl, a Szolgáltató a kibocsátott tanúsítványok és kapcsolódó kulcspárok használatára további korlátozásokat szabhat, melyeket a szolgáltatási szabályzatban kell megadnia.

1.4.2 Tiltott tanúsítvány használat

Tilos a tanúsítványt, illetve a hozzá kapcsolódó kulcspárt felhasználni az 1.4.1 fejezetben leírt célokon kívüli bármilyen más célra, vagy bármilyen – Szolgáltatóval nem egyeztetett - hitelesítés szolgáltatás nyújtásához.

A fentieken túl, tilos felhasználni a titkosító tanúsítványt és a kapcsolódó kulcspárt titkosításra vagy visszafejtésre minden olyan esetben, amelyben valamilyen jogszabály korlátozásokat vagy tiltásokat ír elő (pl. államellenes tevékenységek). Tilos felhasználni az autentikációs tanúsítvány és a kapcsolódó kulcspárt bármilyen csalárd indíttatású azonosítási, illetve félrevezetési céllal, vagy szándékos megtévesztés céljából.

Mind a személyes, mind pedig az üzleti, szervezeti és eszköz tanúsítványokat az Alanyok csak az Előfizetőhöz kapcsolódó tevékenységükhöz használhatják fel; a tanúsítványok bármilyen személyes célra történő felhasználása tilos.

1.5 Szabályzat adminisztráció

1.5.1 Szabályzatot karbantartó szervezet

A Szolgáltatónak szervezetén belül Hitelesítési Rend és Szabályozási Csoportot kell működtetnie, amely többek között jelen hitelesítési rend karbantartásáért is felelős.

1.5.2 Kapcsolat

Az Ügyfélkapcsolati Iroda elérhetőségét, nyitva tartását, a Szolgáltatóval való kapcsolattartás módját és az illetékes fogyasztóvédelmi szerv elérhetőségét a szolgáltatási szabályzat tartalmazza.

1.5.3 Szabályzat alkalmasságának meghatározása

A Szolgáltató legalább évente egyszer meg kell vizsgálja a hitelesítési rend, illetve a szolgáltatási szabályzat tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek eredményeit változtatási igényként figyelembe kell vegye.

1.5.4 Szabályzat jóváhagyásának eljárása

Szolgáltatónak rendelkeznie kell a szabályzatainak jóváhagyására és kiadására vonatkozó eljárásrenddel, melyet a szolgáltatási szabályzatában ismertetnie kell. Az eljárásrendben meg kell jelölni az eljárásért felelős személyt, valamint az egyéb fontos részleteket (pl. hatályba lépés napja).

1.6 Fogalmak, rövidítések és hivatkozások

1.6.1 Fogalmak

Jelen szabályzatban használt fogalmak értelmezése megegyezik a Szolgáltatásokra vonatkozó jogszabályokban (1.6.3.1 fejezet) és szabványokban szereplő (1.6.3.2 fejezet) meghatározásokkal.

Az ezen felül alkalmazott fogalmak meghatározása az alábbiakban olvasható.

Alany: a tanúsítványban a Szolgáltató által igazolt azonosságú vagy tulajdonságú természetes személy vagy jogi személy, illetve közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet.

Előfizető: a Szolgáltatóval kapcsolatban álló jogi személy, illetve közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet, amely megrendeli a Szolgáltatótól a Szolgáltatásokat, jellemzően tanúsítvány kibocsátását az általa megnevezett tanúsítvány alanyok számára.

Előfizető Kapcsolattartója: az Előfizető kapcsolattartó személyt jelölhet meg, akit a képviseleti joggal rendelkező személy (pl. cégjegyzésre jogosult) felhatalmaz, illetve feljogosít a tanúsítványokkal kapcsolatos ügyekben Előfizető szervezete nevében eljárni. Alap (nem emelt szintű) regisztráció (3.2.3.2 fejezet) esetén Kapcsolattartó kijelölése kötelező. Jelen dokumentumban az Előfizető Kapcsolattartója kifejezés a fentiek szerint kijelölt személyt, illetve kijelölés hiányában a képviseleti joggal rendelkező (pl. cégjegyzésre jogosult) személyt jelenti.

1.6.2 Rövidítések

CA	Certification Authority	hitelesítő központ
CRL	Certificate Revocation List	tanúsítvány visszavonási lista
CP	Certificate Policy	Hitelesítési Rend
CPS	Certification Practice Statement	Hitelesítési Szolgáltatás Szabályzat
LCP	Lightweight Certificate Policy	könnyűsúlyú hitelesítési rend
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
RA	Registration Authority	regisztrációs szervezet
SSL	Secure Socket Layer	a TLS protokoll elődje
TSL	Transport Layer Security	Interneten keresztüli kommunikációhoz védelmet biztosító titkosítási protokoll

1.6.3 Hivatkozások

1.6.3.1 Jogszabályi hivatkozások

{J1} 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
(továbbiakban: E-ügyintézési tv.)

{J2} 2013. évi V. törvény a Polgári Törvénykönyvről
(továbbiakban: Ptk.)

{J3} 451/2016. (XII. 19.) Korm. rendelet
az elektronikus ügyintézés részletszabályairól

{J4} 84/2012. (IV. 21.) Korm. rendelet
egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről

1.6.3.2 Szabványok és műszaki-technikai specifikációk

{Sz1}	RFC 3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework	
{Sz2}	EN 319 401	General policy requirements for Trust Service Providers
{Sz3}	EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements	
{Sz4}	EN 319 412-1	Certificate Profiles; Part 1: Overview and common data structures
{Sz5}	EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons	
{Sz6}	EN 319 412-3	Certificate Profiles; Part 3: Certificate profile for certificates issues to legal persons
{Sz7}	RFC 5246	The Transport Layer Security (TSL) Protocol, Version 1.2
{Sz8}	RFC 5280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz9}	ITU-T X.520	Information technology - Open Systems Interconnection - The Directory: Selected attribute types
{Sz10}	RFC 4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz11}	ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework
{Sz12}	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
{Sz13}	MSZ/ISO/IEC 15408	ISO/IEC 15408 (parts 1 to 3): Information technology – Security techniques – Evaluation criteria for IT security
{Sz14}	ISO/IEC 19790	ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz15}	FIPS 140-2	FIPS PUB 140-2 (2001): Security Requirements for Cryptographic Modules
{Sz16}	ETSI TS 119 312	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

1.6.3.3 Hivatkozott dokumentumok

{D1}	ÁSZF-GOVCA Általános Szerződési Feltételek a NISZ Zrt. kormányzati hitelesítés szolgáltatásaihoz	
{D2}	SZSZ	Szolgáltatási Szerződés

{D3}	NISZ Zrt. Szervezeti és Működési Szabályzata
{D4}	NISZ Zrt. Adatvédelmi és adatbiztonsági előírásai
{D5}	NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}	NISZ Zrt. PKI szolgáltatások biztonsági szabályzata
{D7}	NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}	Tanúsítvány profilok a NISZ eIDAS Rendelet szerinti bizalmi szolgáltatásaihoz

2 KÖZZÉTÉTEL ÉS TANÚSÍTVÁNYTÁR

2.1 Tanúsítványtár

A Szolgáltatónak gondoskodnia kell arról, hogy az általa kibocsátott végfelhasználói és szolgáltatói tanúsítványok, a tanúsítványokkal kapcsolatos szabályzatok, a tanúsítványok visszavonási állapotára vonatkozó információk, valamint az egyéb közérdekű szolgáltatói információk az Előfizetők és Érintett Felek részére folyamatosan, napi 24 órában, heti hét napban rendelkezésre álljanak. A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy az információk elérhetetlensége ne haladhassa meg a szolgáltatási szabályzatban meghatározott időtartamot.

2.2 A szolgáltatói információ közzététele

A Szolgáltató a szolgáltatói tanúsítványokat, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokat internetes honlapján közzé kell tegye.

A Szolgáltató a végfelhasználói tanúsítványt internetes honlapján nyilvánosan elérhető, kereshető tanúsítványtárában csak akkor teheti közzé, ha a tanúsítvány alanya a tanúsítvány közzétételéhez hozzájárult.

Szolgáltatónak a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos visszavonási állapot információkat CRL és OCSP formájában is biztosítania kell. A visszavonási állapot információk közzétételével kapcsolatos követelményeket a 4.10 fejezet tartalmazza.

2.3 A közzététel gyakorisága

Szolgáltató a szolgáltatói tanúsítványokat legkésőbb azok éles üzembe helyezését megelőző 24 órán belül teszi közzé.

Szolgáltató a végfelhasználói tanúsítványokat a nyilvánosan kereshető tanúsítványtárban Előfizető hozzájárulása esetén a kibocsátást követő 24 órán belül teszi közzé.

Szolgáltató a tanúsítványokkal kapcsolatos szabályzatokat azok változása esetén közzé teszi legalább 30 nappal a változás hatályba lépését megelőzően.

Szolgáltató a CRL-t legalább 24 óránként frissíti, azaz két egymást követő CRL kibocsátási között idő nem haladja meg a 24 órát. Amennyiben egy tanúsítvány állapota megváltozik, a Szolgáltató a változást követően haladéktalanul, de legfeljebb a szolgáltatási szabályzatban meghatározott időtartamon belül új CRL-t állít elő és tesz közzé.

Szolgáltató az OCSP szolgáltatása keretében minden OCSP kérésre friss választ állít elő és ad vissza.

2.4 Hozzáférés-ellenőrzések

Szolgáltató olvasás céljára korlátozás nélküli hozzáférést biztosít a szolgáltatói tanúsítványokhoz, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokhoz, a tanúsítványokkal kapcsolatos visszavonási információkhoz.

A végfelhasználói tanúsítványokkal kapcsolatban biztosítja a nyilvános tanúsítványtár kereshetőségét a tanúsítványban tárolt adatok alapján.

Szolgáltató biztonsági intézkedésekkel és eljárási szabályokkal gondoskodik az információk jogosulatlan megváltoztatása, törlése, sérülése és megsemmisülése elleni védelemről.
A kibocsátott tanúsítványokkal kapcsolatos szabályzatoknak csak az elektronikus, aláírással vagy bélyegzővel ellátott formája tekinthető hitelesnek, a dokumentumok nyomtatott változatai semmilyen formában nem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

3 AZONOSÍTÁS ÉS HITELESÍTÉS

3.1 Elnevezések

3.1.1 Név típusok

A tanúsítványban szereplő nevek megadása meg kell, hogy feleljen az {Sz9} ITU-T X.520 szabványnak. Ezen túl:

A tanúsítvány alanya (`Subject`) mező tartalma meg kell, hogy feleljen:

- üzleti vagy személyes tanúsítvány esetén: az {Sz5} EN 319 412-2 szabvány 4.2.4 fejezetében foglalt előírásoknak;
- szervezeti vagy eszköz tanúsítvány esetén: az {Sz6} EN 319 412-3 szabvány 4.2.1 fejezetében foglalt előírásoknak.

A tanúsítvány kibocsátója (`Issuer`) mező tartalma meg kell, hogy feleljen:

- az {Sz5} EN 319 412-2 szabvány 4.2.3.1 fejezetében foglalt előírásoknak.

3.1.2 Nevek jelentése

A tanúsítványban szereplő név-attribútumok jelentése megegyezik az {Sz9} ITU-T X.520 szerintivel.

Ezen felül, a szolgáltatási szabályzatban ismertetni kell az 1.4 fejezet szerinti tanúsítványtípusokra vonatkozóan a tanúsítvány `Subject` mezőjében szereplő név-attribútumok képzési és igazolási szabályait.

3.1.3 Előfizetők névtelensége és álnév használata

Az Előfizetők névtelensége nem megengedett.

A természetes személy Alanyok számára kiadott tanúsítványokban Előfizető ezirányú rendelkezése esetén az álnév használata megengedett.

Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell az álneves tanúsítvány felismerhetőségére vonatkozó szabályokat.

3.1.4 Különféle név formák megjelenítési szabályai

A tanúsítványba foglalt megkülönböztető nevek (`Distinguished Name`) ASN.1 szintaxisa az [Sz8} RFC 5280 szerinti, megjelenítési szabályait az {Sz10} RFC 4514 adja meg.

3.1.5 A nevek egyedisége

A Szolgáltatónak biztosítania kell a tanúsítvány `Subject` mezőjébe foglalt megkülönböztető név (`Distinguished Name`) egyediségét, azaz gondoskodnia kell arról, hogy egy adott megkülönböztető nevet soha nem fog egy másik Alanyhoz rendelni.

3.1.6 Márkanevek elismerése, hitelesítése és szerepe

A szolgáltatási szabályzatban ismertetni kell a márkanevek, védjegyek stb. elismerésével, hitelesítésével kapcsolatos információkat.

3.2 Kezdeti azonosítás

Szolgáltatónak a vonatkozó szabványoknak megfelelően kell elvégeznie Előfizető szervezeti azonosságának, a képviseleti joggal rendelkező (pl. cégjegyzésre jogosult) személy képviseleti jogának, valamint Előfizető Kapcsolattartója és a természetes személy alanyok személyazonosságának ellenőrzését és igazolását.

3.2.1 A magánkulcs birtoklása

Szolgáltatónak meg kell győződnie arról, hogy az Alany a tanúsítványhoz kapcsolódó magánkulcsot birtokolja. A szolgáltatási szabályzatban ismertetni kell a magánkulcs birtoklás ellenőrzésének módszerét és eljárását.

3.2.2 A szervezeti azonosság hitelesítése

Ha a tanúsítvány alanya nem természetes személy, akkor Szolgáltatónak ellenőriznie kell Előfizető szervezetének hivatalos nevét és egyedi azonosító adatát (adószámát vagy cégjegyzékszámát). Az adatok valódiságát és hatályosságát közhiteles nyilvántartás alapján, vagy ha ilyen közhiteles nyilvántartás nincsen, az igényléshez csatolt hivatalos dokumentum alapján kell ellenőrizni. Szolgáltató köteles a tanúsítvány kibocsátása előtt, a képviseleti joggal rendelkező (pl. cégjegyzésre jogosult) személy képviseleti jogának fennállásáról jogszabály, közhiteles nyilvántartás, létesítő okirat, vagy ezek hiányában meghatalmazás alapján meggyőződni.

3.2.3 A személyazonosság hitelesítése

A természetes személy alany személyazonosságát az alany vagy nem természetes személy alany esetén alany kapcsolattartója személyes megjelenését igénylő emelt regisztrációval kell Szolgáltatónak ellenőriznie.

A tanúsítvány alany személyesen megjelenik Szolgáltató előtt, melynek során a tanúsítvány megrendelő és regisztrációs űrlapon megadott, a regisztráció és a személyazonosság ellenőrzése alapjául szolgáló, rögzítendő adatok helyességét az adott személy az űrlapon saját kezű aláírásával igazolja.

Szolgáltató köteles a tanúsítvány kibocsátása előtt az alany személyazonosságát, a személyazonosság megállapításához használt adatok valódiságát és – ha van ilyen – közhiteles vagy más központi nyilvántartásban foglalt adatokkal való megegyezőségét ellenőrizni.

3.2.4 Előfizető nem ellenőrzött adatai

Szolgáltatónak ellenőriznie kell minden, a tanúsítvány alany mezőjébe (`Subject`) kerülő adatot.

A tanúsítvány egyéb mezőibe és kiterjesztéseibe kerülő adatok tekintetében Szolgáltatónak a szolgáltatási szabályzatában meg kell jelölnie azokat, melyek nem kerülnek ellenőrzésre.

3.2.5 Jogosultság ellenőrzése

Szolgáltatónak ellenőriznie kell, hogy a tanúsítvány megrendelő és regisztrációs űrlapot az arra jogosult személy – Előfizető Kapcsolattartója – írta alá.

Az egyes tanúsítvány alanyok tanúsítványra való jogosultságának elbírálása és ellenőrzése Előfizető döntésköre és felelőssége.

3.2.6 Együttműködési kritériumok

Nincs kikötés.

3.3 Azonosítás és hitelesítés kulcscsere esetén

A kulcscsere az a folyamat, melynek során az eredeti tanúsítványba foglalt változatlan adatokhoz, megegyező érvényességi időtartammal új nyilvános kulcs kerül hitelesítésre.

A Szolgáltató nem nyújt kulcscsere szolgáltatást.

A tanúsítvány kulcsának cseréjéhez Előfizető új tanúsítványt kell igényeljen.

3.3.1 Azonosítás és hitelesítés érvényes tanúsítvány esetén

Nincs kikötés.

3.3.2 Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Nincs kikötés.

3.4 Azonosítás és hitelesítés visszavonási vagy felfüggesztési kérelem esetén

Szolgáltatónak azonosítania és hitelesítenie kell a visszavonási és felfüggesztési kérelmeket azok feldolgozása előtt. Ennek eljárását a szolgáltatási szabályzatban kell ismertetni.

4 A TANÚSÍTVÁNYOK ÉLETCIKLUSA

4.1 Tanúsítványigénylés

4.1.1 Ki nyújthat be tanúsítványigénylést

Tanúsítvány igénylést Előfizető Kapcsolattartója nyújthat be Szolgáltató részére.

4.1.2 Igénylési folyamat és felelősségek

A tanúsítványigénylés folyamata röviden a következő:

- tanúsítványigénylést, szerződéskötést megelőző tájékoztatás,
- szerződéskötés előkészítése, adatok előzetes megküldése
- Szolgáltatási Szerződés megkötése
- tanúsítvány alanyok regisztrációja és a tanúsítványba kerülő adatok ellenőrzése és igazolása
- tanúsítványkérelmek összeállítása.

Szolgáltatónak a szolgáltatási szabályzatban részletesen ismertetnie kell a fenti folyamat eljárását és az egyes lépéseket.

Az igénylési folyamattal kapcsolatos felelősségeket a 9.6 fejezet és annak alfejezetei tartalmazzák.

4.2 Tanúsítványigénylés feldolgozása

4.2.1 Azonosítási és hitelesítési műveletek

A tanúsítványigénylés elfogadása előtt Szolgáltatónak el kell végeznie Előfizető Kapcsolattartójának, valamint a tanúsítvány alanyának azonosítását és adatainak ellenőrzését.

4.2.2 Tanúsítványigénylés elfogadása vagy visszautasítása

Szolgáltatónak el kell fogadnia a tanúsítványigénylést, ha:

- Előfizető szervezeti azonosságát sikeresen igazolta; és
- Előfizető Kapcsolattartóját, valamint üzleti- és személyes tanúsítvány esetén a természetes személy alanyt is sikeresen azonosította; és
- a regisztrációs és a tanúsítványba kerülő adatokat sikeresen ellenőrizte és igazolta. Szolgáltatónak vissza kell utasítania a tanúsítványigénylés elfogadását, ha valamely adat, bemutatott okmány vagy dokumentum eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel vagy az igényelt tanúsítvány valamely jogszabály (különösen a {J3} 451/2016 és {J4} 84/2012) vonatkozó rendelkezése miatt nem adható ki.

4.2.3 Tanúsítványigénylés feldolgozás időtartama

Szolgáltatónak a tanúsítványigényléseket azok benyújtását követően a Szolgáltatási Szerződésben rögzített időtartamon belül, ennek hiányában a {D1} Általános Szerződési Feltételekben jelzett 15 naptári napon belül fel kell dolgoznia.

4.3 Tanúsítvány kibocsátás

4.3.1 Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek

Az Ügyfélkapcsolati Iroda továbbítja az elfogadott tanúsítványigénylést a Regisztrációs Irodának.

A Regisztrációs Iroda elindítja a Szolgáltatásokat támogató informatikai rendszerben a tanúsítvány létrehozását, majd értesíti az Ügyfélkapcsolati Irodát a tanúsítvány elkészültéről.

4.3.2 Előfizető értesítése a tanúsítvány kibocsátásról

Az Ügyfélkapcsolati Iroda emailben vagy telefonon értesíti Előfizető Kapcsolattartóját – és üzleti- és személyes tanúsítvány esetén az Alanyt - a tanúsítvány elkészültéről és átvételének módjáról.

A tanúsítvány átadása csak az arra jogosult személy részére történhet.

4.4 Tanúsítvány-elfogadás

4.4.1 Tanúsítvány Előfizető általi elfogadása

Az üzleti- és személyes tanúsítványok esetén az Alany, a szervezeti- és eszköz tanúsítványok esetén az Előfizető Kapcsolattartójának kötelezettsége, hogy az átvett tanúsítványban feltüntetett adatok helyességét mihamarabb ellenőrizze. Amennyiben bármilyen eltérést talált, haladéktalanul intézkednie kell a tanúsítvány visszavonásáról.

4.4.2 Tanúsítvány közzététele

Az Előfizető - valamint az üzleti- és személyes tanúsítványok esetén az Alany – írásos hozzájárulása esetén Szolgáltatónak a kibocsátott tanúsítványt közzé kell tennie a Szolgáltatások internetes honlapján elérhető nyilvános tanúsítványtárban.

4.4.3 További felek értesítése a tanúsítvány kibocsátásáról

Nincs kikötés.

4.5 A kulcspár és a tanúsítvány használata

4.5.1 Az Előfizető magánkulcs- és tanúsítvány használata

Az Alany csak azt követően használhatja a tanúsítványt és a kapcsolódó magánkulcsot, hogy a tanúsítványban foglalt adatok helyességéről meggyőződött.

Az Alany csak az 1.4.1 fejezetben ismertetett célokra és módon használhatja a magánkulcsot és a tanúsítványt.

Az Alanynak a magánkulcs és tanúsítvány használata során be kell tartania a 9.6.3 fejezetben ismertetett kötelezettségeit, különösen gondoskodnia kell a kulcstároló eszköz (chipkártya, USB token vagy a PKCS#12 formátumnak megfelelő szoftveres kulcstároló) és aktivizáló adat (PIN kód) illetéktelen hozzáférés elleni védelméről.

4.5.2 Az Érintett felek nyilvános kulcs- és tanúsítvány használata

A jelen hitelesítési rend hatálya alatt kibocsátott tanúsítvány elfogadása során szükséges, hogy az Érintett Fél megfelelő körültekintéssel járjon el, melyhez javasolt betartania a szolgáltatási szabályzatban leírt követelményeket, különös tekintettel az alábbiakra:

- a tanúsítványokat csak olyan alkalmazásokban fogadja el, melyek összhangban vannak a tanúsítvány „kulcshasználat” (`KeyUsage`) és „kiterjesztett kulcshasználat” (`ExtendedKeyUsage`) kiterjesztésének tartalmával;
- ellenőrizze a tanúsítvány érvényességét és visszavonási állapotát;
- vegyen figyelembe minden korlátozást, amely a tanúsítványban vagy a tanúsítvány által hivatkozott szabályzatokban szerepel.

4.6 Tanúsítványok megújítása

Az irányadó szabvány ({Sz1} RFC 3647) szerint a tanúsítványmegújítás az a folyamat, amikor az eredeti tanúsítványba foglalt változatlan adatokhoz az Alany változatlan nyilvános kulcsa új érvényességi időtartamra kerül hitelesítésre.

A Szolgáltató nem nyújt tanúsítványmegújítás szolgáltatást.

Ha a tanúsítvány lejár, de a szolgáltatásra továbbiakban is szükség van, Előfizető új tanúsítványt kell igényeljen, az erre vonatkozó folyamatok szerint. Szolgáltató a lejárat előtt 30 nappal értesítést küld Előfizetőnek.

4.6.1 Tanúsítvány megújítás körülményei

Nincs kikötés.

4.6.2 Ki kérelmezhet tanúsítvány megújítást

Nincs kikötés.

4.6.3 Tanúsítvány megújítási kérelmek feldolgozása

Nincs kikötés.

4.6.4 Az Előfizető értesítése a megújított tanúsítvány kibocsátásáról

Nincs kikötés.

4.6.5 Tanúsítvány Előfizető általi elfogadása

Nincs kikötés.

4.6.6 Megújított tanúsítvány közzététele

Nincs kikötés.

4.6.7 További felek értesítése tanúsítvány megújításról

Nincs kikötés.

4.7 Kulcscsere

A kulcscsere az a folyamat, melynek során az eredeti tanúsítványba foglalt változatlan adatokhoz, megegyező érvényességi időtartammal új nyilvános kulcs kerül hitelesítésre.

A Szolgáltató nem nyújt kulcscsere szolgáltatást.

A tanúsítvány kulcsának cseréjéhez Előfizető új tanúsítványt kell igényeljen.

4.7.1 Kulcscsere körülményei

Nincs kikötés.

4.7.2 Ki kérelmezhet kulcscserét

Nincs kikötés.

4.7.3 Kulcscsere kérelmek feldolgozása

Nincs kikötés.

4.7.4 Előfizető értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.7.5 Új tanúsítvány Előfizető általi elfogadása

Nincs kikötés.

4.7.6 Új tanúsítvány közzététele

Nincs kikötés.

4.7.7 További felek értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.8 Tanúsítvány-módosítás

A tanúsítvány módosítása az a folyamat, melynek során az eredeti tanúsítvánnyal hitelesített nyilvános kulcshoz, de megváltozott (pl. név, szervezeti egység) adatokkal új tanúsítvány kerül kiadásra.

A Szolgáltató nem nyújt tanúsítvány-módosítás szolgáltatást.

A tanúsítványba foglalt adatok változása esetén új tanúsítvány kell igényelnie és intézkednie kell a meglevő tanúsítvány visszavonásáról.

4.8.1 Tanúsítvány-módosítás körülményei

Nincs kikötés.

4.8.2 Ki kérelmezhet tanúsítvány-módosítást

Nincs kikötés.

4.8.3 Tanúsítvány-módosítási kérelmek feldolgozása

Nincs kikötés.

4.8.4 Előfizető értesítése az új tanúsítvány kibocsátásáról

Nincs kikötés.

4.8.5 Módosított tanúsítvány Előfizető általi elfogadása

Nincs kikötés.

4.8.6 Módosított tanúsítvány közzététele

Nincs kikötés.

4.8.7 További felek értesítése a módosított tanúsítvány kibocsátásáról

Nincs kikötés.

4.9 Tanúsítvány visszavonás és felfüggesztése

A tanúsítvány visszavonása a tanúsítvány érvényességének a tervezett érvényességi idő lejárat előtti megszüntetését jelenti. A visszavonás végleges és visszafordíthatatlan állapot.

Felfüggesztés esetén a tanúsítvány csak rövid, átmeneti időszakra lesz érvénytelen. A tanúsítvány felfüggesztett állapotban csak ideiglenesen lehet, az engedélyezett időtartam után állapotát újra érvényesre kell állítani, vagy a tanúsítványt vissza kell vonni. A visszavont / felfüggesztett tanúsítványt nem lehet felhasználni.

Az Érintett Feleknek javasolt ellenőrizniük a tanúsítvány visszavonási állapotát a tanúsítvány elfogadása előtt.

4.9.1 Visszavonás körülményei

Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell a visszavonáshoz vezető körülményeket.

4.9.2 Ki kezdeményezheti a visszavonást Visszavonást

kezdeményezhet:

- Előfizető, illetve Előfizető Kapcsolattartója, továbbá üzleti- és személyes tanúsítvány esetén az Alany;
- Szolgáltató.

4.9.3 Visszavonási kérelemre vonatkozó eljárás

Szolgáltatónak ellenőriznie kell a visszavonást kérelmező azonosságát és jogosultságát, valamint ellenőriznie kell a visszavonási kérelemben foglalt adatokat. Ha az ellenőrzések sikeresek, Szolgáltató el kell végezze a tanúsítvány visszavonását és a megváltozott visszavonási állapot információt közzé kell tennie, valamint értesítenie kell az Alanyt a tanúsítvány visszavonásáról.

A tanúsítvány visszamenőleges visszavonása nem megengedett.

Szolgáltató az egyszer már visszavont tanúsítvány érvényességét nem állíthatja vissza érvényesre.

4.9.4 Kivárási idő visszavonási kérelem esetén

Szolgáltató nem alkalmaz kivárási időt a visszavonási kérelmek teljesítése során.

4.9.5 Visszavonási kérelem feldolgozásának időbelisége

Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia azt a maximális időtartamot, melyen belül a visszavonási kérelmet feldolgozza.

4.9.6 Visszavonás ellenőrzésének ajánlása az Érintett felek számára

Az Érintett Feleknek a tanúsítvány és az ahhoz felépített tanúsítványlánc minden elemének visszavonási állapotát javasolt ellenőriznie a tanúsítványból megállapított vagy a 4.10.1 fejezetben megadott elérhetőségekről letöltött CRL vagy megkért OCSP válasz alapján.

4.9.7 CRL kibocsátási gyakoriság

Az előfizetői tanúsítványokra vonatkozó CRL kibocsátásának gyakorisága: 24 óránként legalább egy CRL.

A Szolgáltató egy-egy tanúsítvány felfüggesztését, visszavonását, illetve újra-érvényesítését követően egy órán belül új CRL-t tesz közzé.

Szolgáltató minden kibocsátáskor törli a CRL-ről azokat a tanúsítványokat, melyek érvényessége a CRL kibocsátásnak időpontjában már lejárt.

A szolgáltatói tanúsítványokhoz kapcsolódó CRL kibocsátásának gyakorisága: 30 naponként legalább egy CRL.

A CRL-nek tartalmaznia kell a következő kibocsátás időpontját (a `nextUpdate` mezőben).

4.9.8 CRL előállítása és közzététele között leghosszabb idő

Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia azt a maximális időtartamot, melyen belül a CRL-t az előállítását követően közzéteszi.

4.9.9 OCSP szolgáltatás biztosítása

Szolgáltatónak az előfizetői és szolgáltatói tanúsítványok visszavonási állapotának megállapításához OCSP szolgáltatást is kell nyújtania.

4.9.10 OCSP alapú visszavonás ellenőrzés követelményei

Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia az OCSP alapú visszavonás ellenőrzésével kapcsolatban az Érintett Felek számára fontos figyelmeztetéseket.

4.9.11 Visszavonási állapot közlés más formái

Szolgáltató a honlapján elérhető nyilvános tanúsítványtárban is közzé teszi a visszavonási állapot információt, tájékoztatási jelleggel.

4.9.12 Különleges követelmények a kulcs kompromittálódása esetére

Szolgáltatónak mindent meg kell tennie annak érdekében, hogy a szolgáltatói magánkulcsának kompromittálódása esetén az eseményről az Érintett Feleket értesítse.

A produktív hitelesítő központ magánkulcsának kompromittálódása esetén a Szolgáltatónak képesnek kell lennie az összes érintett végfelhasználói tanúsítvány visszavonására, valamint az adott szolgáltatói tanúsítvány visszavonására. Ebben az esetben a CRL-ben és OCSP válaszokban a tanúsítványok visszavonási ok információt "kulcs kompromittálódás" (`keyCompromise`) értékre kell állítani.

4.9.13 Felfüggesztés körülményei

Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell a felfüggesztéshez vezető körülményeket.

4.9.14 Ki kérelmezhet felfüggesztést Felfüggesztést

kezdeményezhet:

- Előfizető, illetve Előfizető Kapcsolattartója, továbbá üzleti- és személyes tanúsítvány esetén az Alany;
- Szolgáltató.

4.9.15 Felfüggesztésre vonatkozó eljárás

Szolgáltatónak ellenőriznie kell a felfüggesztést kérelmező azonosságát és jogosultságát, valamint ellenőriznie kell a felfüggesztési kérelemben foglalt adatokat. Ha az ellenőrzések sikeresek, Szolgáltató el kell végezze a tanúsítvány felfüggesztését és a megváltozott visszavonási állapot információt közzé kell tennie.

4.9.16 A felfüggesztés megengedett időtartama

Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a felfüggesztés megengedett időtartamát. Ha a tanúsítvány újra-érvényesítése a felfüggesztésre megengedett időtartamon belül nem történik meg, Szolgáltatónak vissza kell vonnia a tanúsítványt.

4.10 Visszavonási állapot szolgáltatások

4.10.1 Működési jellemzők

Szolgáltató a végfelhasználói és szolgáltatói tanúsítványokhoz kapcsolódó visszavonási információkat mind CRL, mind OCSP formájában biztosítja.

Szolgáltatónak biztosítania kell, hogy a visszavonási állapot információ változása mind a CRL, mind az OCSP szolgáltatásban azonosan, konzisztens módon megjelenjen, figyelembe véve az egyes szolgáltatásokban eltérő frissítési időket is.

CRL

A Szolgáltató által kibocsátott CRL meg kell feleljen az {Sz8} RFC 5280 szabványnak.

Szolgáltató a CRL aláírásához ugyanazt a szolgáltatói magánkulcsot használja, melyet a kérdéses tanúsítvány aláírására használt.

A CRL-nek tartalmaznia kell minden olyan visszavont tanúsítványt, amelynek érvényessége a CRL kibocsátásának időpontjában nem járt még le.

OCSP

A Szolgáltató által biztosított OCSP szolgáltatás meg kell feleljen az {Sz12} RFC 6960 szabványnak.

Az OCSP szolgáltatást Szolgáltató az {Sz12} RFC 6960 2.2 fejezetében meghatározott "Authorized Responder" elvnek megfelelően működteti.

Az OCSP válaszadó számára minimum 7 és maximum 21 óránként új, 24 órás érvényességű tanúsítvány kerül kiadásra, annak érdekében, hogy az OCSP választ aláíró tanúsítvány érvényességét ne kelljen ellenőrizni.

Az OCSP szolgáltatás keretében a Szolgáltató biztosítja a visszavonási információt a tanúsítvány lejárját követően is, 10 évig.

4.10.2 Szolgáltatás rendelkezésre állása

A CRL, illetve az OCSP szolgáltatás az év minden napján, napi 24 órában elérhető kell legyen, 99%-os rendelkezésre állással, úgy, hogy a kiesés nem lépheti túl esetenként a 24 órás időtartamot.

4.10.3 Opcionális funkciók

Nincs kikötés.

4.11 Az előfizetés vége

Előfizető szerződéses viszonya megszűnik a tanúsítvány érvényességének lejáratával vagy ha a tanúsítvány az érvényességének lejárata előtt Előfizető kérésére vagy bármely más okból kifolyólag visszavonásra kerül.

4.12 Kulcsletét és visszaállítás

A Szolgáltató nem nyújt kulcsletét szolgáltatást.

4.12.1 Kulcsletét és visszaállítás szabályai

Nem értelmezett.

4.12.2 Rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Nem értelmezett.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

Szolgáltatónak gondoskodnia kell arról, hogy kellő, az irányadó szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, illetve az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra.

5.1 Fizikai óvintézkedések

5.1.1 Telephely elhelyezése és szerkezeti felépítése

A Szolgáltató a Szolgáltatások nyújtásában közreműködő informatikai rendszereit fizikai és logikai védelemmel ellátott, legmagasabb védelmi szintet képező objektumában kell elhelyezni és üzemeltetni. A telephely elhelyezése és kialakítása során olyan egymásra épülő és egymást támogató védelmi megoldásokat kell alkalmazni, melyek képesek megakadályozni az illetéktelen hozzáférést és alkalmasak az informatikai rendszerek és Szolgáltató által tárolt bizalmas adatok megóvására.

5.1.2 Fizikai hozzáférés

Szolgáltatónak védenie kell a Szolgáltatások nyújtásában közreműködő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében.

Ehhez biztosítania kell az alábbiakat:

- a gépterembe történő minden belépés naplózásra kerül;
- a gépterembe csak a bizalmi szerepkört betöltő, erre feljogosított munkatárs léphet be, azonosítást követően;
- önálló jogosultsággal nem rendelkező személy csak indokolt és engedélyezett esetben, a szükséges időtartamig tartózkodhat a gépteremben megfelelő jogosultságú kísérő személy állandó felügyelete mellett;
- az eszközök aktivizáló adatai (jelszavak, PIN kódok, stb.) a géptermen belül sem tárolhatók nyílt formában;
- jogosulatlan személy jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják; ○ a bejelentkezett terminálok nem maradnak felügyelet nélkül;
- nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet; □ a gépterem elhagyásakor ellenőrzésre kerül:
- minden eszköz és berendezés megfelelően biztonságos üzemállapotban van; ○ minden terminálon megtörtént a kijelentkezés; ○ a fizikai tároló eszközök megfelelően elzárásra kerültek; ○ a fizikai védelmet biztosító rendszerek és berendezések megfelelően működnek.

5.1.3 Áramellátás és légkondicionálás

Szolgáltató a gépteremben olyan szünetmentes áramellátó rendszert kell biztosítson, amely:

- megfelelő teljesítménnyel rendelkezik a gépterem informatikai és kisegítő létesítményi berendezései áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózat feszültség ingadozásai, feszültség kimaradásai és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramellátó berendezés biztosítja - üzemanyag utántöltéssel - tetszőlegesen hosszú időtartamig az áramellátást.

Szolgáltatónak a gépteremben olyan légkondicionáló berendezést kell alkalmazni, mely biztosítja az alábbiakat:

- az operátorok biztonságos munkavégzéséhez szükséges mennyiségű oxigén biztosított; □ a levegő nedvességtartalma nem haladja meg az informatikai rendszerek által megkívánt szintet;
- hűtés történik a szükséges üzemi hőmérséklet biztosítására, az eszközök és berendezések túlhevülésének megakadályozására.

5.1.4 Beázás és elárasztás veszélyeztetettség

Szolgáltatónak a géptermet meg kell védenie a beázástól, víz betöréstől és elárasztástól.

5.1.5 Tűzmegelőzés és tűzvédelem

Szolgáltatónak a géptermet füst- és tűzérzékelőkkel kell felszerelni, melyek automatikusan riasztják az illetékes személyzetet. Minden helyiségben jól látható helyen kell elhelyezni a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készüléket. A gépteremben automatikus tűzoltó rendszert kell kialakítani, amely emberi egészségre nem veszélyes és nem károsítja az informatikai eszközöket.

5.1.6 Adathordozók tárolása

Szolgáltatónak meg kell védenie valamennyi adathordozóját a jogosulatlan hozzáféréstől, a megsemmisüléstől vagy véletlen rongálódástól.

5.1.7 Selejt kezelése és megsemmisítése

Szolgáltatónak a környezetvédelmi előírások betartásával kell gondoskodnia feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről. A felesleges eszközöket és adathordozókat az erre kijelölt munkatárs személyes felügyelete mellett, széleskörűen elfogadott módszerekkel használhatatlanná kell tenni vagy visszaállíthatatlan módon törölni kell.

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

Szolgáltatónak azt az adatmentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható, olyan – az üzemeltetés helyétől eltérő - helyszínen kell tárolnia, mely megfelelő fizikai és működési védelemmel rendelkezik. Biztosítani kell a helyszínek között a mentett adatok biztonságos továbbítását.

Szolgáltatónak biztosítania kell, hogy az adatmentést vagy abból a helyreállítást csak rendszerüzemeltető bizalmi munkakört betöltő személy végezze el.

5.2 Eljárásbeli előírások

Szolgáltatónak gondoskodnia kell arról, hogy informatikai rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék. Szolgáltató személyzete a feladatokat olyan eljárásbeli előírások alapján kell végezze, melyek szinkronban vannak a jogszabályi, szabványi és belső biztonsági előírásokkal.

5.2.1 Bizalmi munkakörök

Szolgáltatónak egyértelműen azonosítania kell azokat a munkaköröket, amelyektől a Szolgáltatások biztonsága függ. Ezeket a bizalmi munkaköröket és felelősségeket dokumentálni kell. A jogosultságokat és funkciókat olyan módon kell megosztani az egyes bizalmi munkakörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére. Szolgáltatónak biztosítania kell, hogy minden bizalmi munkakör betöltésre kerüljön.

A bizalmi munkakört betöltő személynek munkaviszonyban kell állnia Szolgáltatóval. Bizalmi munkakörbe a Szolgáltató felső vezetősége kell kinevezze a munkatársakat.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Szolgáltató biztonsági szabályzataiban elő kell írni, hogy csak védett környezetben, legalább kettő, bizalmi munkakört betöltő munkatárs egyidejű fizikai jelenlétében végezhetők el az alábbi műveletek:

- szolgáltatói kulcspár létrehozása;
- szolgáltatói magánkulcs mentése és visszaállítása; szolgáltató magánkulcs aktiválása;
- szolgáltatói magánkulcs megsemmisítése.

5.2.3 Bizalmi munkakörökben elvárt azonosítás és hitelesítés

A bizalmi munkaköröket betöltő személyeket azonosítani és hitelesíteni kell, mielőtt a Szolgáltatások nyújtásában érintett, kritikus informatikai rendszerekhez hozzáférnének.

5.2.4 Egymást kizáró munkakörök

A Szolgáltatónak biztosítania kell, hogy a bizalmi munkakörök vonatkozásában:

a) biztonsági tisztviselő nem láthatja el a független rendszervizsgáló, a rendszeradminisztrátor, és az informatikai rendszerért általánosan felelős vezető feladatait;
b) a független rendszervizsgáló nem láthatja el az informatikai rendszerért általánosan felelős vezető, a regisztrációs felelős, és a rendszeradminisztrátor feladatait; c) törekedni kell a bizalmi munkakörök teljes személyi szétválasztására.

5.3 Személyzetre vonatkozó előírások

Szolgáltatónak gondoskodnia kell arról, hogy személyzeti előírásai, a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák a Szolgáltató működésének megbízhatóságát.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

Biztosítani kell, hogy bizalmi munkakört csak olyan személyek tölthetnek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét a Szolgáltató erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

5.3.2 Biztonsági háttér ellenőrzés eljárásai

A Szolgáltató vezetői munkakörben, illetve bizalmi munkakörben csak olyan alkalmazottakat foglalkoztathat, akik:

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, ami a büntetlenséget befolyásolhatja (a büntetlen előéletet három hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni);
- nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkoztatástól eltiltás hatálya alatt.

5.3.3 Képzési követelmények

A bizalmi munkakörökben Szolgáltató olyan személyeket foglalkoztathat, akik az adott munkakör ellátásához szükséges mértékben elsajátították:

- a PKI elméletet;
- Szolgáltató informatikai rendszerének sajátosságait és kezelésének módját;
- a szerepkör ellátáshoz szükséges speciális ismereteket;
- Szolgáltató nyilvános és belső szabályzataiban meghatározott folyamatokat és eljárásokat; az egyes tevékenységek jogi következményeit; az alkalmazandó biztonsági szabályokat.

A Szolgáltató éles informatikai rendszereihez csak a képzést sikeresen záró alkalmazottak kaphatnak hozzáférési jogosultságot.

5.3.4 Továbbképzési gyakoriságok és követelmények

Szolgáltatónak gondoskodnia kell arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést kell tartania.

Legalább évente egyszer továbbképzést kell biztosítani az újonnan ismertté vált jogszabályokról, sebezhetőségekről, az IT biztonság aktuális gyakorlatáról, a munkatársak saját szakterületét érintően.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Nincs kikötés.

5.3.6 Felhatalmazás nélküli tevékenységek büntető következményei

Szolgáltatónak a dolgozókkal kötendő munkaszerződésben szabályoznia kell a dolgozó felelősségre vonásának lehetőségét a dolgozó által elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

5.3.7 Szerződéses munkavállalókra vonatkozó követelmények

Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztathat.

Az egyéb feladatok ellátására, vállalkozási vagy megbízási szerződésben foglalkoztatott személyeket Szolgáltató csak előzetes biztonsági ellenőrzést követően foglalkoztathatja. Az ellenőrzött személyekkel írásos megállapodást kell kötni, melyben rögzíteni kell az esetleges biztonsági szabályokat és a titoktartásra vonatkozó kikötéseket.

5.3.8 A személyzet számára biztosított dokumentációk

Szolgáltatónak folyamatosan biztosítania kell a személyzet részére a munkakörük ellátásához szükséges dokumentációk és szabályzatok rendelkezésre állását.

5.4 A biztonsági naplózás folyamatai

5.4.1 Naplózott esemény típusok

Szolgáltatónak minden, az informatikai rendszerével és a Szolgáltatások nyújtásával kapcsolatos eseményt naplóznia kell. A naplózott adatállománynak a szolgáltatás nyújtásának teljes folyamatát át kell fognia, és lehetővé tennie, hogy a valós helyzetek megítéléséhez a szükséges mértékben minden, a Szolgáltatásokkal kapcsolatos eseményt rekonstruálni lehessen.

5.4.2 Naplóállomány feldolgozásának gyakorisága

Szolgáltatónak biztosítania kell a naplóállományok rendszeres ellenőrzését és kiértékelését.

5.4.3 Naplóállomány megőrzési időtartama

A naplóállományokat archiválni kell és gondoskodni azok biztonságos megőrzéséről az 5.5.2 fejezetben előírt időtartamig.

5.4.4 Naplóállomány védelme

A naplóállomány minden bejegyzését védeni kell a módosítástól, illetve biztosítani kell, hogy a napló tartalmához csak arra feljogosított személyek férhessenek hozzá.

A naplóállományok kezelését olyan módon kell megoldani, hogy kizárható legyen a napló megsemmisülése, a napló bejegyzések törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása.

5.4.5 Naplóállomány mentési folyamatai

A naplóállományokról rendszeres mentést kell készíteni.

5.4.6 Naplózás gyűjtési rendszere

A naplóbejegyzések gyűjtését belső komponenssel kell megoldani. A naplóbejegyzések gyűjtésének meg kell kezdődnie rendszer indításkor és rendszer leállításig folyamatosan működnie kell, és

közben biztosítania kell a gyűjtött bejegyzések integritását és rendelkezésre állását, szükség esetén a bizalmasságát is.

A naplóbejegyzések gyűjtési rendszerének működési rendellenessége esetén Szolgáltatónak fel kell függesztenie az érintett területek működését az üzemzavar elhárításáig.

5.4.7 Rendellenes eseményeket kiváltó alanyok értesítése

Nincs kikötés.

5.4.8 Sebezhetőség értékelések

Szolgáltatónak rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot és behatolás tesztet kell végeznie, mely segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek jogosulatlan hozzáférést eredményezhetnek vagy hatással lehetnek a tanúsítvány kibocsátási folyamatra, a tanúsítványban tárolandó adatok megmásítását, módosítását, sérülését vagy megsemmisülését eredményezhetik.

Szolgáltatónak folyamatosan figyelemmel kell kísérnie az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül meg kell tennie, illetve – ha az ellenintézkedés költsége nem áll arányban a sebezhetőség lehetséges kihatásaival – cselekvési tervet kell készítenie és végrehajtania annak érdekében, hogy a sebezhetőség ne legyen kihasználható vagy annak hatása elhanyagolható legyen.

5.5 Adatok archiválása

5.5.1 A tárolt adatok típusai

Szolgáltatónak gondoskodnia kell arról, hogy megőrzésre kerüljön minden olyan információ, amely szükséges ahhoz, hogy egy tanúsítvány bizonyítható legyen, továbbá amely a Szolgáltató és a rendszereinek megfelelő működését alátámasztja. Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:

- tanúsítványok igénylésével, regisztrációval kapcsolatos minden adat vagy irat, különösen a Szolgáltatási Szerződés, Előfizető által aláírt nyilatkozatok és átvételi elismervények;
- tanúsítványokkal kapcsolatos valamennyi információ a teljes életciklusra vonatkozóan;
- a hitelesítési rend és szolgáltatási szabályzat valamennyi kibocsátott verziója;

- az Általános Szerződési Feltételek valamennyi kibocsátott verziója; a Szolgáltató működésével kapcsolatos szerződések valamennyi naplóállomány.

5.5.2 Archívum megőrzési időtartama

Szolgáltató az 5.5.1 fejezetben meghatározott archivált adatokat köteles megőrizni, a tanúsítványokkal kapcsolatos adatok esetében a tanúsítvány érvényességnek lejáratáról számított 10 évig, illetve a tanúsítvánnyal kapcsolatos jogvita jogerős lezárásáig, szabályzatok, szerződések esetében a hatályon kívül helyezés vagy megszűnés utáni 10 évig.

5.5.3 Archívum védelme

Szolgáltatónak biztosítania kell valamennyi archivált adatra azok sértetlenségét és hitelességét, a rendelkezésre állását és a bizalmasságát.

5.5.4 Archívum mentési eljárásai

Szolgáltatónak biztosítania kell az iratok, dokumentumok, elektronikus állományok biztonságos, hosszú távú megőrzését, illetve tárolását, továbbá az elektronikus formában archivált állományok adathordozóinak elavulás elleni védelmét a megőrzési időn belül.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi naplóbejegyzést el kell látni olyan időjellel, melyben legalább egy másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

Az elektronikus formában archivált adatokon legalább fokozott biztonságú elektronikus aláírást vagy bélyegzőt, valamint minősített időbélyeget kell elhelyezni.

Az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodni kell az elektronikus aláírások, bélyegzők és időbélyegzők hitelességének fenntartásáról.

5.5.6 Archívum gyűjtési rendszere

A naplóállományokat és az egyéb elektronikusan keletkezett adatokat a Szolgáltatónak védett informatikai rendszerén belül kell gyűjteni. A védett informatikai rendszerből történő kimozgatás során az adatokat minősített időbélyeget tartalmazó elektronikus aláírással vagy bélyegzővel kell ellátni.

A papíralapú iratokat Szolgáltató dokumentumtárában kell tárolni.

5.5.7 Archívum hozzáférés és ellenőrzés eljárásai

Szolgáltatónak az archivált adatokat meg kell védenie a jogosulatlan hozzáféréstől. A jogosult hozzáféréseket naplózni kell.

5.6 Kulcs átállás

Szolgáltatónak biztosítania kell, hogy a hitelesítő központok folyamatosan rendelkezzenek a működésükhöz szükséges érvényes kulccsal és tanúsítvánnyal.

Amennyiben új szolgáltatói kulcspár és tanúsítvány előállítása szükséges, Szolgáltatónak ezt olyan módon kell kiviteleznie, hogy az átállás az Előfizetők és Érintett Felek számára a lehető legkisebb kényelmetlenséget jelentse és megfeleljen a vonatkozó jogszabályi és szabványi követelményeknek.

5.7 Helyreállítás rendkívüli üzemi helyzetek esetén

Szolgáltató köteles meghozni minden szükséges intézkedést annak érdekében, hogy rendkívüli üzemeltetési helyzet, katasztrófa esetén a szolgáltatás kiesésből származó károkat minimalizálja és a Szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa. A rendkívüli üzemeltetési helyzet bekövetkezése esetén a visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását meg kell, hogy előzze.

Egyéb incidens esetén - amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra – az esetről való értesüléstől számított 24 órán belül értesíteni kell az Érintett Feleket.

A bekövetkezett incidens kiértékelése alapján Szolgáltatónak meg kell hoznia a szükséges módosító, javító intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

Szolgáltatónak rendelkeznie kell üzletmenet folytonossági tervvel.
Rendkívüli üzemeltetési helyzetben Szolgáltatónak dokumentálnia kell az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.

Szolgáltatónak ki kell alakítani és fenntartani egy tartalék CA rendszert, mely a rendkívüli üzemeltetési helyzetben képes a tanúsítványtár és a nyilvános szabályzatok elérhetőségét, a visszavonás kezelési szolgáltatások teljes értékű működését, a CRL-ek közzétételét biztosítani. A rendkívüli üzemeltetési helyzetben Szolgáltatónak a lehető legrövidebb időn belül tájékoztatást kell közzé tennie internetes honlapján, valamint - lehetőség szerint - elektronikus levélben kell értesítenie azokat a személyeket, akiket az esemény érint.

5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

Szolgáltatónak olyan megbízható rendszert kell működtetni, mely a rendszerben bekövetkezett hiba esetén is biztosítja a Szolgáltatások működtetését és elérhetőségét.

5.7.3 Szolgáltató magánkulcsának kompromittálódása esetén követendő eljárás

A Szolgáltató magánkulcsának kompromittálódása esetén haladéktalanul meg kell tenni a szükséges lépéseket:

- visszavonni az összes érintett tanúsítványt;
- megszüntetni az érintett magánkulcs használatát; új szolgáltatói kulcspárokat és tanúsítványokat hozni létre; intézkedni valamennyi érintett fél értesítéséről.

5.7.4 Üzletmenet folytonosság helyreállás katasztrófát követően

Szolgáltatónak rendelkeznie kell tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.

5.8 A szolgáltatási tevékenység megszüntetése

Szolgáltatónak rendelkeznie kell a szolgáltatási tevékenység megszüntetésére vonatkozó, aktualizált tervvel.

A szolgáltatási tevékenység megszüntetésére vonatkozó tervnek tartalmaznia kell legalább az alábbiakat:

- Előfizetők és Érintett Felek értesítésének módja;
- a Szolgáltatásokkal kapcsolatos azon kötelezettségeknek átadása egy másik szolgáltatónak, melyek arra vonatkoznak, hogy bizonyítékot szolgáltassanak a Szolgáltató működésével kapcsolatban - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig;
- szolgáltatói magánkulcsok és azok mentései megsemmisítésének módja; Szolgáltató informatikai rendszerében foglalt adatokról teljes körű mentés készítése.

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK / TECHNICAL SECURITY CONTROLS

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

6.1.1.1 Szolgáltatói kulcspárok előállítása

Szolgáltató maga kell előállítsa a tanúsítványok és visszavonási listák aláírására használandó kulcspárokat fizikailag védett környezetben, kriptográfiai modulban (HSM), legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétének kizárásával. A kriptográfiai modulnak meg kell felelnie a 6.2.1 fejezet szerinti követelményeknek. A kulcspárok előállítását Szolgáltató dokumentált „kulcs-ceremónia" eljárás szerint kell végezze, melyről a vonatkozó szabvány követelményeinek megfelelő tartalmú jegyzőkönyvet kell felvennie. A szolgáltató magánkulcsai teljes életciklusuk alatt a kriptográfiai modulban kell maradjanak.

Szolgáltató maga kell előállítsa az OCSP válaszokat aláíró kulcspárokat, fizikailag védett környezetben, HSM modul használata nem követelmény. Az OCSP választ aláíró magánkulcs teljes életciklusa alatt ezen fizikailag védett környezetben kell maradjon.

6.1.1.2 Előfizetői kulcspárok előállítása □ Szolgáltatónak a 6.1.5 és 6.1.6 fejezetek szerinti algoritmusú és kulcshosszú kulcspárt szigorúan védett környezetben, a hitelesítő-központi rendszerében, kizárólag bizalmi munkakört betöltő személyek jelenlétében kell előállítania;

- a magánkulcsot annak átadásáig Szolgáltató megfelelően biztonságos környezetben kell tárolnia a felfedés megakadályozása érdekében;
- a magánkulcs dokumentált átadását követően Szolgáltatónak haladéktalanul meg kell semmisíteni a magánkulcs minden tárolt példányát olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

Szolgáltatónak biztosítania kell, hogy a magánkulcsot és az ahhoz tartozó aktivizáló adatokat csak a jogosult Alany vehesse át.

6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A titkosító és autentikációs tanúsítványokhoz kapcsolódó kulcspárt Szolgáltatónak kell előállítania, így annak eljuttatása nem szükséges.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

Szolgáltatónak biztosítania kell, hogy a szolgáltató nyilvános kulcsa a kicserélésen alapuló támadás (substitution attack) ellen védett módon legyen eljuttatva az Érintett Felekhez.

6.1.5 Kulcs méretek

A Szolgáltatónak a Szolgáltatások nyújtása során - mind a szolgáltatói, mind a végfelhasználói kulcsok tekintetében – a vonatkozó nemzetközi szabványoknak és ajánlásoknak megfelelő szabványos algoritmusokat, paramétereket és kulcshosszakat kell használnia.

6.1.6 A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

A Szolgáltatói kulcspárok előállítása a 6.1.1.1 fejezet szerint védett környezetben és tanúsított HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétét kizárva kell történjen. A szolgáltatói kulcspárok generálása során Szolgáltatónak be kell tartania a HSM modul tanúsítási jelentésében foglalt előírásokat is.

Az előfizetői kulcspárok tekintetében Szolgáltató a kulcspárt védett környezetben, a hitelesítőközponti rendszerében vagy – Előfizető kérelmére – a kulcstároló eszközön (chipkártya, USB token), kizárólag bizalmi munkakört betöltő személyek jelenlétében kell előállítania. Az előfizetői kulcspárok generálása során Szolgáltatónak be kell tartania a vonatkozó nemzetközi szabványokban és szakmai ajánlásokban foglalt előírásokat is.

6.1.7 A kulcs használat célja (X.509 v3 kulcs használati mezőnek megfelelően)

Szolgáltatónak a tanúsítványokban a `KeyUsage` és `ExtendedKeyUsage` kiterjesztésekben az {Sz11} ITU-T X.509 v3 szabványnak megfelelően kell jeleznie a kulcs használat célját.

6.2 Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1 Kriptográfiai modul szabványok és műszaki szabályozások

Szolgáltató a szolgáltatói magánkulcsok előállítására, tárolására és használatára csak olyan kriptográfiai modult alkalmazhat, amely:

- olyan megbízható rendszer, amelynek értékelése az MSZ/ISO/IEC 15408 {Sz13} szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten történt meg; vagy

- megfelel az ISO/IEC 19790 {Sz14} követelményeinek; vagy
- megfelel a FIPS 140-2 {Sz15} 3-as, illetve annál magasabb szintű követelményeknek.

6.2.2 Több szereplős ("n-ből m") ellenőrzés

Szolgáltató a hitelesítő központokban alkalmazza a több szereplős "n-ből m" ellenőrzést a gyökér hitelesítő központ kulcsgondozási funkcióinak aktivizálásánál.

6.2.3 Magánkulcs letét

Szolgáltató a hitelesítő központok magánkulcsait nem teszi letétbe.

Szolgáltató az Előfizetők számára kizárólag csak a titkosító tanúsítványokhoz kapcsolódóan nyújt magánkulcs letét szolgáltatást a 4.12 fejezetben leírtak szerint.

6.2.4 Magánkulcs visszaállítása

A hitelesítő központok szolgáltatói magánkulcsai biztonsági okokból mentésre kell kerüljenek. A mentést titkosított formában, speciális eszközök alkalmazásával kell megvalósítani. Szolgáltató a hitelesítő központok magánkulcsait rendkívüli üzemi helyzetek esetén a titkosított mentésből visszaállíthatja, hasonlóan szigorú fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a magánkulcs előállítása eredetileg történt.

Szolgáltató az Előfizetők számára kizárólag csak a titkosító tanúsítványokhoz kapcsolódóan nyújt magánkulcs letét szolgáltatást a 4.12 fejezetben leírtak szerint.

6.2.5 Magánkulcs mentése

Szolgáltatói hitelesítő központok magánkulcsai biztonsági okokból mentésre kell kerüljenek. A mentést titkosított formában, speciális eszközök alkalmazásával kell megvalósítani, megfelelő biztonsági óvintézkedések és eljárási szabályok betartásával. Szolgáltató az Előfizetők számára kizárólag csak a titkosító tanúsítványokhoz kapcsolódóan nyújt magánkulcs letét szolgáltatást a 4.12 fejezetben leírtak szerint.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

A hitelesítő központok magánkulcsai teljes életciklusuk alatt a 6.2.1 fejezetben leírt HSM modulban kerülnek tárolásra.

Amennyiben az Előfizető a tanúsítvánnyal együtt kulcstároló eszköz (chipkártya, USB token) szolgáltatását is kérte, akkor a kulcspár ezen az eszközön (kriptográfiai modulban) került létrehozásra, így a bejuttatására nincs szükség.

Előfizető nem kért kulcstároló eszköz (chipkártya, USB token) szolgáltatást, Szolgáltató a magánkulcsot szabványos, titkosított kulcstároló formátumban (PKCS#12) készíti elő az átadásra, és ha ezt Előfizető kriptográfiai modulban kívánja tárolni, akkor a kulcstárolót az Előfizető Kapcsolattartója veszi át, és gondoskodik annak bejuttatásáról a kriptográfiai modulba. Előfizető feladata a kriptográfiai modulba bejuttatást követően a magánkulcs minden példányának haladéktalan és visszaállíthatatlan módon történő megsemmisítése.

6.2.7 Magánkulcs kriptográfiai modulban történő tárolásának módja

A hitelesítő központok magánkulcsainak a tárolása a kulcsok teljes életciklusa alatt tanúsítással rendelkező HSM modulban kell történjen.

6.2.8 Magánkulcs aktiválásának módja

A hitelesítő központok magánkulcsainak aktiválását Szolgáltató a HSM modul gyártói dokumentációjában előírtak szerint kell végezze.

Az előfizetői tanúsítványok esetében az Alany a magánkulcs aktiválását a lezárt borítékban átadott PIN kód megadásával végzi.

6.2.9 Magánkulcs aktív állapotának megszüntetési módja

Szolgáltatónak biztosítani kell, hogy az aktivált HSM modul jogosulatlan hozzáférés ellen védett legyen. A HSM modul működése során csak a kiadott tanúsítványok, visszavonási listák és opcionálisan OCSP válaszok hitelesítésére használható. A magánkulcs eltávolításra kerül a HSM modulból, amikor a hitelesítő központ működése megszűnik.

6.2.10 Magánkulcs megsemmisítésének módja

A hitelesítő központok magánkulcsát visszaállíthatatlan módon meg kell semmisíteni, amikor használatuk már nem szükséges vagy a kapcsolódó tanúsítvány lejárt vagy visszavonásra került. A magánkulcsot és az aktiválásához szükséges minden adatot olyan módon kell megsemmisíteni, hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkezhető vagy levezethető.

6.2.11 Kriptográfiai modul értékelése

A 6.2.1 fejezet tartalmazza.

6.3 Kulcspár gondozás egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

Szolgáltató köteles minden általa kibocsátott tanúsítvánnyal hitelesített nyilvános kulcsot a tanúsítványba foglalva archiválni és az érvényesség lejártától számított tíz évig megőrizni.

6.3.2 Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

A kulcspár felhasználás időtartama azonos a nyilvános kulcs hitelességét igazoló tanúsítvány érvényességi idejével:

Gyökértanúsítvány	legfeljebb 25 év
Produktív (köztes) kiadói tanúsítvány	legfeljebb 20 év
OCSP válaszadó	legfeljebb 30 nap
Előfizetői tanúsítvány	legfeljebb 2 év

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

A magánkulcs aktiválásához aktivizáló adatokat megfelelő minőségű véletlenszám-generátor segítségével, fizikailag védett környezetben és biztonságos körülmények között kell Szolgáltatónak előállítania, és hozzárendelnie a szolgáltatott kulcstároló eszközhöz (chipkártya, USB token), illetve a PKCS#12 formátumnak megfelelő kulcstárolóhoz.

6.4.2 Aktivizáló adatok védelme

Az aktivizáló adatokat azok átadásáig biztonságosan, az eszköztől, illetve kulcstárolótól elkülönítve kell tárolni. Az aktivizáló adatokat Szolgáltató csak az arra jogosult személynek adhatja át.
Az átvételt követően az Alanynak kell biztosítania az aktivizáló adatok kizárólagos birtoklását és védelmét.

6.4.3 Aktivizáló adatok egyéb szempontjai

Nincs kikötés.

6.5 Informatikai biztonsági óvintézkedések

6.5.1 Informatikai biztonsági műszaki követelmények meghatározása

Az informatikai biztonság műszaki követelményeit a Szolgáltató az {Sz1} EN 319 401és {Sz2} EN 319 411-1 szabványoknak a nyilvános kulcsú tanúsítványokat kibocsátó bizalmi szolgáltatás nyújtására vonatkozó, informatikai biztonsági műszaki követelményeiben határozza meg.

Ennek alapján Szolgáltatónak olyan megbízható informatikai rendszert (beleértve a redundáns kiépítést) és technikákat kell kialakítania és üzemeltetnie, melyek biztosítják a Szolgáltató megbízható működését a Szolgáltatások nyújtásához. Ennek ismertetését Szolgáltató részben a szolgáltatási szabályzatában (HSZSZ-T), részben a belső biztonsági szabályzataiban írja le.

6.5.2 Informatikai biztonsági értékelés

Szolgáltatónak az informatikai rendszerek biztonsági értékelését az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezései szerint kell elvégeznie.

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

Szolgáltatónak gondoskodnia kell arról, hogy az általa vagy a nevében végzett valamennyi rendszerfejlesztési projektjében a biztonság követelményeit már a tervezési és követelmény meghatározási fázisban figyelembe vegyék annak érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.

6.6.2 Biztonságkezelési óvintézkedések

Szolgáltató olyan eszközöket és eljárásokat kell alkalmazzon, melyek garantálják a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

A biztonságkezelési szabályokat a Szolgáltató belső társasági szintű és rendszer szintű információbiztonsági szabályzata tartalmazza.

6.6.3 Életciklus biztonsági óvintézkedések

Szolgáltatónak rendszeres időközönként el kell végeznie a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

6.7 Hálózatbiztonsági óvintézkedések

A hálózati védelmi intézkedéseket a Szolgáltató belső biztonsági szabályzatában meghatározott követelményeknek megfelelően kell megvalósítani, figyelembe véve az {Sz2} EN 319 411-1 szabvány 6.5.7 fejezetében leírt követelményeket is.

6.8 Időforrások

A Szolgáltatások nyújtásához használt megbízható rendszereket 24 óránként legalább egyszer, megbízható időforrásokkal (NTP) szinkronizálni kell.

7 TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

7.1 Tanúsítvány profil

Szolgáltató által kiadott tanúsítványok profilja megfelel az {Sz8} RFC 5280, {Sz4} EN 319 412-1, {Sz5} EN 319-412-2, {Sz6} EN 319 412-3 szabványoknak.

7.1.1 Verziószám

A tanúsítványok verziószáma: V3.

7.1.2 Tanúsítvány kiterjesztések

A tanúsítványokban alkalmazott kiterjesztések mindenben követik az {Sz8} RFC 5280, {Sz4} EN 319 412-1, {Sz5} EN 319-412-2, {Sz6} EN 319 412-3 szabványok előírásait.

7.1.3 Algoritmus azonosítók

Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a tanúsítvány aláírásához használt algoritmusok azonosítóit.

7.1.4 Név formák

A név formák leírását és azok értelmezési szabályait a 3.1 fejezet tartalmazza.

7.1.5 Név megszorítások

Szolgáltató a tanúsítványokban név megszorításokat (`NameConstraints`) nem tüntet fel.

7.1.6 Hitelesítési end objektumazonosító

Szolgáltató a tanúsítványokban feltünteti a hitelesítési rend objektumazonosítóját.

7.1.7 Szabályzati megszorítások kiterjesztés használata

Szolgáltató a tanúsítványokban szabályzati megszorításokat (`PolicyConstraints`) nem tüntet fel.

7.1.8 Szabályzat minősítők szintaktikája és szemantikája

A tanúsítványban feltüntetett szabályzat minősítők (`PolicyQualifiers`) és megfelelő szöveg (`UserNotice`) jelzi a tanúsítvány alkalmazhatóságát.

7.1.9 A kritikus hitelesítési rendek (Certificate Policies) kiterjesztés feldolgozása

A tanúsítvány hitelesítési rendek (`CertificatePolicies`) kiterjesztése nincs kritikusként megjelölve.

7.2 CRL profil

Szolgáltató által kiadott visszavonási listák megfelelnek az {Sz8} RFC 5280 műszaki szabványnak.

7.2.1 Verziószám

A visszavonási listák verziószáma: V2.

7.2.2 CRL és CRL bejegyzés kiterjesztések

A visszavonási lista az alábbi kiterjesztéseket tartalmazza „nem kritikus” megjelöléssel:

`CRLNumber`	a visszavonási lista szigorúan növekvő sorszáma
`AuthorityKeyIdentifier`	a kibocsátó CA kulcs azonosítója

A visszavonási lista a fentieken túl más szabványos kiterjesztést is tartalmazhat, azonban ezek a kiterjesztések nem lehetnek „kritikus” jelzésűek.

7.3 OCSP profil

Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz12} RFC 6960 műszaki szabványnak.

7.3.1 Verziószám

Az OCSP válaszok verziószáma: V1.

7.3.2 OCSP kiterjesztések

Az OCSP válasz az alábbi kiterjesztéseket kell tartalmazza „nem kritikus” megjelöléssel:

`Nonce`	az OCSP kérésben megadott, visszajátszásos támadások

	megelőzésére szolgáló véletlenszám (csak akkor, ha a kérés tartalmazta azt)
`AuthorityKeyIdentifier`	az időpont, ameddig a Szolgáltató a tanúsítvány lejárata után is biztosítja a visszavonási státuszt

Az OCSP válasz fentieken túl más szabványos kiterjesztést is tartalmazhat, azonban ezek a kiterjesztések nem lehetnek „kritikus” jelzésűek.

8 MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

Jelen hitelesítési rend előírja az összes, a nyilvános körben kibocsátott, autentikációs és titkosító tanúsítványokkal kapcsolatos szolgáltatás nyújtása során teljesíteni szükséges követelményt, melyet különösen az alábbi szabványok határoznak meg:

- EN 319 401: General policy requirements for Trust Service Providers {Sz2}
- EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates {Sz3}

8.1 Vizsgálatok gyakorisága és körülményei

Szolgáltatónak megfelelőségi vizsgálatokat és értékeléseket kell elvégeznie, illetve elvégeztetnie annak érdekében, hogy a Szolgáltatásaival kapcsolatos folyamatai, személyzete, eszközei és környezete mindenkor megfeleljen a vonatkozó jogszabályi és szakmai követelményeknek.

8.2 Auditor azonosítása és képesítése

A külső rendszervizsgálói auditokra Szolgáltató olyan szakértőt vagy szakértői szolgáltatásokat nyújtó szervezetet kell megbízzon, aki független Szolgáltatótól, illetve az ellenőrzött rendszertől, területtől, és szakértelmét biztosítani tudja a PKI és az informatikai biztonság, valamint az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában.

A Szolgáltató tevékenységére és az informatikai biztonságra vonatkozó belső ellenőrzéseket a Szolgáltató belső szervezete végzi, az ott dolgozó biztonsági tisztviselők bevonásával.

8.3 Auditor függetlensége

A külső vizsgálatokat végző szervezet, illetve annak munkatársai teljes mértékben függetlenek Szolgáltatótól.

8.4 Audit során vizsgált területek

Az audit az alábbi területeket kell lefedje:

- szabályzatok és dokumentációk;
- irányítási és ellenőrzési követelmények;
- személyzeti biztonsági követelmények;
- a szolgáltatói kulcspár kezeléséhez kapcsolódó követelmények;
- üzemeltetési és hozzáférési biztonság;
- fizikai és környezeti biztonság; folyamatos szolgáltatás biztosítása; adatbiztonság és archiválás.

Az audit során megvizsgálásra kerül, hogy Szolgáltató és az általa nyújtott Szolgáltatások megfelelnek-e:

- a hatályos jogszabályoknak és szabványoknak;
- a szolgáltatási szabályzatnak, illetve a hitelesítési rendnek.

8.5 Hiányosságok esetén végrehajtandó tevékenységek

Az üzemszerű ellenőrzések, belső és külső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére Szolgáltató intézkedési tervet kell készítsen. A hiányosságokat köteles késlekedés nélkül orvosolni, az intézkedéseket dokumentálni és ellenőrizni.

8.6 Eredmény kommunikációja

A belső és külső auditot, szakértői elemzést végző személyek csak a megbízójuknak adhatnak információt a Szolgáltató tevékenységével kapcsolatban. Az audit és az ellenőrzés eredményei a Szolgáltató bizalmas üzleti információi, ezért azokat a társaság titokvédelmi előírásai szerint kell kezelni. Szolgáltató nem köteles a konkrét hiányosságot nyilvánosságra hozni.

9 EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1 Díjak

A Szolgáltatások díjaival kapcsolatos információkat a szolgáltatási szabályzat kell tartalmazza.

Szolgáltató nem számíthat fel díjat a tanúsítványok visszavonási állapotára vonatkozó státusz információk szolgáltatásáért, valamint a szolgáltatói és a nyilvános tanúsítványtárban közzétett előfizetői tanúsítványoknak az eléréséért.

9.2 Anyagi felelősség

Szolgáltatónak az anyagi felelősség mértékéről, illetve annak korlátairól a szolgáltatási szabályzatban rendelkeznie kell.

9.2.1 Biztosítási fedezet

Szolgáltatónak felelősségbiztosítással kell rendelkeznie, mely egyaránt kiterjed a tanúsítványokkal kapcsolatos, szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, és amely fedezetet biztosít az összes károsultnak okozott kárra, a tanúsítványban jelzett, vagy a {D1} Általános Szerződési Feltételekben rögzített tranzakciós limit értékének legalább háromszorosáig.

9.2.2 További követelmények

Nincs kikötés.

9.2.3 Felelősségbiztosítás vagy garancia végfelhasználók számára

Nincs kikötés.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a bizalmasan kezelendő információk körét.

9.3.2 Nem bizalmasnak tekintett információk köre

Nincs kikötés.

9.3.3 Bizalmas információk védelmének felelőssége

Szolgáltatónak meg kell védenie a bizalmas információkat. A bizalmas információk védelmét a személyzet megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel kell érvényre juttatni.

9.4 Személyes adatok védelme

9.4.1 Adatvédelmi terv

Szolgáltató rendelkezik mind társasági szintű adatvédelmi tervvel ({D4}), mind pedig a Szolgáltatásokra vonatkozó adatvédelmi tájékoztatóval, melyek nyilvános dokumentumok, és elérhetők Szolgáltató internetes honlapján. Ezen dokumentumok összhangban vannak a nemzetközi és hazai vonatkozó jogszabályokkal.

Szolgáltató, mint adatkezelő, szerepel a Nemzeti Adatvédelmi és Információszabadság Hivatal Adatvédelmi Nyilvántartásában.

9.4.2 Bizalmasként kezelendő személyes adatok

Szolgáltató csak Előfizetőtől és az Alanytól közvetlenül, azok kifejezett írásos hozzájárulásával gyűjt személyes adatot és csak olyan mértékben, ami a tanúsítvány kiállításához, valamint az Alany tájékoztatásához, személyazonosságának megállapításához szükséges. Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

- Előfizető részéről a Szolgáltatási Szerződésben érintett személyek (pl. cégjegyzésre jogosult vezető, vagy Előfizető Kapcsolattartója) minden adatát;
- az Alany azon adatait, melyek a tanúsítványba nem kerülnek befoglalásra.

9.4.3 Bizalmasként nem kezelendő személyes adatok

Szolgáltató nem bizalmasként kezelendő személyes adatnak tekinti az Alanynak a tanúsítványba foglalt adatait, amennyiben az Alany tanúsítványa közzétételéhez írásban hozzájárult.

Továbbá, nem bizalmas adat a tanúsítványhoz kapcsolódó státusz információ, minden tanúsítvány vonatkozásában. A státusz információba beleértendő a tanúsítvány - esetleges - visszavonásának oka és időpontja.

9.4.4 Személyes adatok védelmének felelőssége

Szolgáltató felelős a személyes adatok védelméért.

9.4.5 Hozzájárulás a személyes adatok felhasználásához

Előfizetőnek – és üzleti- és személyes tanúsítvány esetén az Alanynak is - a regisztrációs űrlap kitöltésével és aláírásával hozzá kell járulnia a tanúsítvány kiállításához szükséges adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához, valamint a kibocsátott tanúsítvány nyilvános közzétételéhez.

Előfizetőnek a Szolgáltatási Szerződés aláírásával hozzá kell járulnia a tanúsítvány kiállításához és a szerződés megkötéséhez szükséges adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához.

9.4.6 Felfedés bírósági vagy polgári peres eljárás keretében

A Szolgáltató bűncselekmények felderítése vagy megelőzése céljából, illetve nemzetbiztonsági érdekből - az adatigénylésre meghatározott jogszabályi feltételek teljesülése esetén - a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak haladéktalanul és egyéb feltételek nélkül feltárja a jogszabályban meghatározott bizalmas információkat. Szolgáltató rögzíti az adatátadás tényét, de arról nem tájékoztatja érintett Előfizetőt és/vagy az Alanyt.

Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az ellenérdekű peres félnek vagy képviselőjének, valamint a megkereső bíróságnak feltárhatja a jogszabályban meghatározott bizalmas információkat. Szolgáltató rögzíti az adatátadás tényét, és arról tájékoztatja érintett Előfizetőt és/vagy az Alanyt.

Álneves tanúsítvány esetén Szolgáltató a tanúsítvány alany valódi személyazonosságára vonatkozó adatot is – mint jogszabályban meghatározott bizalmas információt – feltárja a fentiek szerint. Álneves tanúsítvány esetén Szolgáltató a tanúsítvány alany valódi személyazonosságára vonatkozó adatot harmadik félnek – ide nem értve az első két bekezdésben leírt esetet – csak az Előfizető és az Alany beleegyezésével adhatja át.

9.4.7 Egyéb, felfedést eredményező körülmények

Szolgáltató a szolgáltatási tevékenység, illetve a Szolgáltatások nyújtásának megszüntetése esetén Előfizetők és az Alanyok adatait átadja harmadik félnek.

9.5 Szellemi tulajdonjogok

A Szolgáltató által ügyfelei részére kibocsátott tanúsítványok és az ahhoz tartozó kulcspár tulajdonosa az Előfizető, teljes jogú használója pedig az Alany, aki/amely számára a tanúsítvány kibocsátásra került, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat. Szolgáltató a szabályzataiban és feltételeiben ismertetett esetekben és módon a tanúsítványt közzé teheti, sokszorosíthatja, felfüggesztheti, visszavonhatja és egyéb módon is kezelheti. A végfelhasználói tanúsítványokban szereplő megkülönböztető név és egyéb azonosítók használatára Előfizető és/vagy az Alany jogosult.

A Szolgáltató tulajdonát képezik a szolgáltatói tanúsítványok, visszavonási információk, a végfelhasználói tanúsítványokban szereplő, Szolgáltató által létrehozott azonosítók.

Szolgáltató kizárólagos tulajdonát képezik a szabályzatai, szerződéses feltételei és egyéb, a Szolgáltatások internetes honlapján közzétett dokumentumai. Ezen dokumentumok felhasználása csak és kizárólag a Szolgáltatások használatával összefüggésben engedélyezett, minden egyéb kereskedelmi vagy egyéb célú felhasználása szigorúan tilos.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 Szolgáltató felelőssége és helytállása

Szolgáltató felel a jelen hitelesítési rendben és a vonatkozó szolgáltatási szabályzatban, valamint az Előfizetővel megkötött Szolgáltatási Szerződésben megfogalmazott valamennyi kötelezettsége maradéktalan betartásáért, még akkor is, ha a Szolgáltatások nyújtásához kapcsolódó egyes feladatokat egyéb alvállalkozók végzik.

9.6.2 A regisztrációs szervezet felelőssége és helytállása

A regisztrációs tevékenységeket Szolgáltató saját szervezetén belül üzemeltetett Ügyfélkapcsolati Irodája és Regisztrációs Irodája kell végezze. Az Ügyfélkapcsolati Iroda és a Regisztrációs Iroda betartja a rá vonatkozó, jogszabályokban, illetve a Szolgáltató szabályzataiban foglalt előírásokat.
Szolgáltató felelőssége a tanúsítvány kiadása során:

- szerződéskötést megelőző tájékoztatás;
- a tanúsítvány alanyának azonosítása (a természetes személy alany személyazonosságának és/vagy a szervezeti azonosságának ellenőrzése);
- Előfizető Kapcsolattartója személyének azonosítása és eljárási jogosultságának megállapítása;
- emelt szintű regisztráció (3.2.3.1 fejezet) esetén: - a tanúsítvány alanyának megkülönböztető nevébe kerülő minden adat ellenőrzése közhiteles nyilvántartások alapján, ahol ez lehetséges;
- a tanúsítvány egyéb mezőibe és kiterjesztéseibe kerülő adatok ellenőrzése;
- a regisztrációhoz és a tanúsítvány kiállításához szükséges adatok rögzítése az erre szolgáló informatikai rendszerben;
- a rögzített kérelemben foglalt adatokkal a megfelelő tanúsítvány előállítása;

- az opcionálisan megrendelt kulcstároló eszköz (chipkártya, USB token) megfelelő megszemélyesítése;
- a titkosító tanúsítványhoz kapcsolódó, opcionálisan megrendelt kulcsletét szolgáltatás esetén a megőrzött magánkulcsok biztonságos tárolásáért, továbbá azért, hogy a tárolt magánkulcs csak az arra jogosult, megfelelő személynek kerüljön kiadásra;
- a magánkulcshoz tartozó aktivizáló adatok biztonságos előállítása, tárolása, és átadása az arra jogosult személynek.

9.6.3 Előfizető felelőssége és helytállása

Előfizető jogai

Előfizető jogosult:

- a Szolgáltatásokat igénybe venni a szolgáltatási szabályzatban, a Szolgáltatási Szerződésben és a {D1} Általános Szerződési Feltételekben leírtak szerint; kapcsolattartó személyt kijelölni;
- az általa meghatározott Alanyok számára tanúsítványt igényelni;
- a tanúsítványok felfüggesztését és visszavonását kérni;
- a felfüggesztett tanúsítvány újra-érvényesítését kérni.

Előfizető felelőssége

Az Előfizető felelősségét a Szolgáltatási Szerződés és a {D1} Általános Szerződési Feltételek határozzák meg.

Előfizető kötelezettségei

Előfizető kötelessége a Szolgáltató szabályzatainak és szerződéses feltételeinek megfelelően eljárni a Szolgáltatások használata során, beleértve a tanúsítványok igénylését és felhasználását. Az Előfizető kötelezettségeit a szolgáltatási szabályzat, a Szolgáltatási Szerződés és a {D1} Általános Szerződési Feltételek tartalmazzák.

Az Alany jogai Az

Alany jogosult:

- a számára kiadott tanúsítványt és a kapcsolódó magánkulcsot az 1.4.1 fejezetben leírt célokra és jelen szabályzatban leírt módon használni;
- a tanúsítvány felfüggesztését vagy visszavonását kérni;
- a felfüggesztett tanúsítvány újra-érvényesítését kérni;
- a tanúsítványhoz kapcsolódó egyéb szolgáltatásokat használni a szolgáltatási szabályzatban leírt módon.

Az Alany felelőssége Az

Alany felelős:

- a regisztráció során megadott adatainak valódiságáért, pontosságáért és érvényességéért;
- a tanúsítványba foglalt adatok ellenőrzéséért;
- az adataiban bekövetkezett változás haladéktalan bejelentéséért;

- a kulcstároló eszköze (chipkártya, USB token) biztonságos kezeléséért;
- a magánkulcs és az aktivizáló adat biztonságos kezeléséért;
- a tanúsítvány és a magánkulcs szabályzatoknak megfelelő felhasználásáért;
- a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyek esetén; általában, a jelen szabályzatban előírt kötelezettségei betartásáért.

Az Alany kötelezettségei:

Az Alany köteles:

- a Szolgáltatások használata előtt megismerni a szolgáltatási szabályzatot;
- a Szolgáltató által kért, a Szolgáltatások igénybe vételéhez szükséges adatokat hiánytalanul és a valóságnak megfelelően megadni;
- a Szolgáltatásokat kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a jelen szabályzatban és a hivatkozott dokumentumokban foglaltaknak megfelelően használni;
- adat változás (különösen a tanúsítványba foglalt valamely adat) esetén haladéktalanul írásban értesíteni erről Szolgáltatót, a tanúsítvány felfüggesztését vagy visszavonását kezdeményezni és beszüntetni a tanúsítvány használatát;
- biztosítani, hogy a Szolgáltatás igénybe vételéhez szükséges adatokhoz és eszközökhöz (különösen a kulcstároló eszközhöz (chipkártya, USB token) és az aktivizáló adatokhoz) illetéktelen személy ne férhessen hozzá;
- haladéktalanul kezdeményezni a tanúsítvány felfüggesztését vagy visszavonását, amennyiben a tanúsítványhoz kapcsolódó magánkulcs, a kulcstároló eszköz vagy az aktivizáló adat illetéktelen kezekbe került vagy megsemmisült, megrongálódott, elveszett, valamint haladéktalanul megszüntetni a tanúsítvány és magánkulcs használatát;
- kulcs kompromittálódás vagy jogellenes használat gyanúja esetén a Szolgáltató megkereséseire a Szolgáltató által megadott időtartamon belül reagálni;
- tudomásul venni, hogy Előfizető jogosult a tanúsítvány visszavonását vagy felfüggesztését kérni;
- tudomásul venni, hogy Szolgáltató a tanúsítványt a jelen szabályzatban leírt módon és ellenőrzési lépések elvégzése után bocsátja ki;
- tudomásul venni, hogy Szolgáltató a 4.9.1 fejezetben ismertetett körülmények esetén jogosult a tanúsítványt visszavonni;
- a magánkulcs és a kapcsolódó tanúsítvány használatát haladéktalanul és végérvényesen beszüntetni, amennyiben tudomására jut, hogy a Szolgáltató valamely, a tanúsítvány kibocsátásában érintett hitelesítő központja kompromittálódott;

- haladéktalanul, írásban értesíteni Szolgáltatót, ha a tanúsítvánnyal kapcsolatban jogvita indul.

9.6.4 Érintett felek felelőssége és helytállása

Az Érintett Felek a saját belátásuk és/vagy szabályzataik szerint dönthetnek az egyes tanúsítványok elfogadásáról és a felhasználás módjáról. A tanúsítvány érvényességének elbírálása során az Érintett Félnek megfelelő körültekintéssel kell eljárnia, ezért különös tekintettel javasolt:

- a szolgáltatási szabályzatban foglalt követelmények és előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- a tanúsítvány felhasználására vonatkozó valamennyi korlátozás figyelembe vétele, amely a tanúsítványban vagy a szolgáltatási szabályzatban szerepel;
- a tőle elvárható magatartás tanúsítása a tanúsítvány ellenőrzésekor.

9.6.5 Egyéb felek felelőssége és helytállása

Nincs kikötés.

9.7 Helytállás érvénytelenségi köre

A helytállás érvénytelenségi körét a szolgáltatási szabályzatban meg kell határozni.

9.8 Felelősség korlátozása

Szolgáltató korlátozhatja a kártérítési felelősségét:

- a tanúsítvánnyal egy alkalommal vállalható kötelezettség mértékében (tranzakciós limit);
- összességében az összes tanúsítvánnyal és káreseménnyel kapcsolatban fizetendő kártérítési összeg tekintetében.

9.9 Kártérítések

A kártérítésekről a szolgáltatási szabályzatban kell rendelkezni.

9.10 Hatályosság és megszűnés

9.10.1 Hatályosság

Időbeli hatály

A hitelesítési rend egy adott verziójának időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik és határozatlan időre szól. Az időbeli hatály megszűnik a hitelesítési rend újabb verziójának hatályba lépésével vagy a Szolgáltatások befejezésekor.

Tárgyi hatály

A hitelesítési rend tárgyi hatálya kiterjed a Szolgáltatások nyújtására és igénybe vételére.

Személyi hatály

A hitelesítési rend személyi hatálya kiterjed Szolgáltatónak a Szolgáltatások nyújtásában közreműködő munkatársaira, továbbá az Előfizető kapcsolattartójaként kijelölt személyekre, az Alanyokra, és Előfizető szervezetén belül az tanúsítványok felhasználásáért felelős személyekre.

9.10.2 Megszűnés

A hitelesítési rend a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

9.10.3 Megszűnés után is hatályban maradó rendelkezések

A megszűnés után is hatályban maradó rendelkezéseket a szolgáltatási szabályzatban meg kell határozni.

9.11 Egyéni hirdetmények és kommunikáció a részvevőkkel

A szolgáltatási szabályzatban rendelkezni kell a felek és részvevők közötti kommunikáció joghatást kiváltó módjairól.

9.12 Módosítások

9.12.1 Módosítás eljárása

A hitelesítési rend módosítása az 1.5.3 és 1.5.4 fejezetekben leírt szabályok szerint történik. A hitelesítési rend módosulását a verziószám megfelelő változása jelzi.

9.12.2 Értesítés módszere és időtartama

A Szolgáltatások jelentős vagy lényeges változása esetén Szolgáltatónak internetes honlapján közleményt kell közzé tennie, a hatályba lépést megelőzően kellő időben ahhoz, hogy az érintett felek a változásokra felkészülhessenek.

9.12.3 OID megváltozását előidéző körülmények

A hitelesítési rend új verziójával az OID verziószámot jelentő része megfelelően változik.

9.13 Vitás kérdések rendezése

A vitás kérdések rendezéséről a szolgáltatási szabályzatban kell rendelkezni.

9.14 Irányadó jog

Szolgáltató szerződéseire, szabályzataira és azok teljesítésére a magyar jog az irányadó és azokat a magyar jog szerint kell értelmezni.

9.15 Hatályos jognak megfelelés

Szolgáltató tevékenységét a mindenkor hatályos Európai Uniós, illetve magyar jogszabályoknak megfelelően köteles végezni.

9.16 Vegyes rendelkezések

Nincs kikötés.

9.16.1 Teljességi záradék

Nincs kikötés.

9.16.2 Átruházás

Nincs kikötés.

9.16.3 Részleges érvénytelenség

A jelen hitelesítési rend egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4 Igényérvényesítés

Szolgáltató kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben Szolgáltató egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben a hitelesítési rend más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5 Force Majeure (Vis maior)

A szolgáltatási szabályzat tartalmazza.

9.17 Egyéb rendelkezések

A Szolgáltatásokat és a Szolgáltatások során alkalmazott végfelhasználói termékeket hozzáférhetővé kell tenni a fogyatékossággal élő személyek számára, amennyiben az lehetséges.