

SZOLGÁLTATÁSI REND

NEM eIDAS TANÚSÍTVÁNYSZOLGÁLTATÁSOKRA

A NETLOCK Kft. titkosító, autentikációs és DV SSL tanúsítványkibocsátásának és a kapcsolódó állapotszolgáltatások nyújtásának és igénybevételének előírásait tartalmazó követelménygyűjteménye



NETLOCK Informatikai és Hálózatzbiztonsági Szolgáltató Korlátolt Felelősségű Társaság

A dokumentum magyar neve: Szolgáltatási Rend
Nem eIDAS Tanúsítványszolgáltatásokra

A dokumentum angol neve Service Policy
for Non-eIDAS Certification Service

Dokumentum rövid neve: SP-C-HU

Verzió: 240901

Azonosító szám (OID): 1.3.6.1.4.1.3555.1.1.16.0.240901

Jóváhagyás időpontja: 2024.08.29.

Közzététel időpontja: 2024.08.29.

Hatály kezdőnapja: 2024.09.01.

Oldalak száma: fedlappal együtt 104 oldal

Jóváhagyó: **Nyíri Balázs,**
CEO, NETLOCK Kft.

© COPYRIGHT, NETLOCK KFT. 2021. – MINDEN JOG FENNTARTVA

Tartalom

1 BEVEZETÉS	8
1.1 ÁTTEKINTÉS	8
1.1.1. Szabványok és előírások	8
1.1.2 A Szolgáltató adatai	9
1.2 A DOKUMENTUM NEVE ÉS AZONOSÍTÁS	9
1.2.1 Hitelesítési Rendek	10
1.2.2 Dokumentum revíziók	11
1.3 A PKI SZEREPLŐK	12
1.3.1 A Hitelesítő egység és a Kiadó	12
1.3.2 Regisztrációs Egység	13
1.3.3 Előfizető, Végfelhasználó és Igénylő	13
1.3.4 Érintett felek	13
1.3.5 Egyéb szereplők	13
1.4 TANÚSÍTVÁNYOK ALKALMAZHATÓSÁGA	14
1.4.1. A megfelelő tanúsítvány használat	14
1.4.2. Tiltott tanúsítvány használat	15
1.5 A SZOLGÁLTATÁSI REND ADMINISZTRÁCIÓJA.....	15
1.5.1 A dokumentum adminisztrációját végző szervezet	15
1.5.2 A dokumentum kapcsolattartó személye	15
1.5.3 A szolgáltatási szabályzat szolgáltatási rendnek megfelelésért felelős szervezet	16
1.5.4 A Szolgáltatási szabályzat elfogadása	16
1.6 FOGALMAK ÉS RÖVIDÍTÉSEK.....	16
1.6.1 Fogalmak	16
1.6.2 Rövidítések	27
2. KÖZZÉTÉTELRE ÉS TANÚSÍTVÁNYTÁRRÁ VONATKOZÓ FELELŐSSÉGEK	30
2.1 ADATTÁRAK	30
2.1.1. A tanúsítványokra vonatkozó információk közzététele.....	30
2.1.2 Kikötések és feltételek közzététele	31
2.2 KÖZZÉTÉTEL IDŐPONTJA ÉS GYAKORISÁGA.....	31
2.3 TANÚSÍTVÁNYTÁR ELÉRÉSÉNEK SZABÁLYAI	31
3 AZONOSÍTÁS ÉS HITELESÍTÉS	32
3.1 ELNEVEZÉSEK	32
3.1.1. Névtípusok	32
3.1.2. A nevek értelmezhetősége.....	32
3.1.3. Álnevek	34
3.1.4. A különböző elnevezési formák értelmezési szabályai	34
3.1.5. A nevek egyedisége.....	34
3.1.6. Védjegyek elismerése, azonosítása, szerepük	35
3.2. KEZDETI AZONOSÍTÁS	35
3.2.1. A magánkulcs birtoklásának igazolása	36
3.2.2. Szervezet azonosságának hitelesítése.....	37
3.2.3. Természetes személy azonosságának hitelesítése	37
3.2.4. Nem ellenőrzött alany információk	39
3.2.5. Jogok, felhatalmazások ellenőrzése	39
3.2.6. Együttműködési képességre vonatkozó követelmények.....	41
3.3 AZONOSÍTÁS ÉS HITELESÍTÉS TANÚSÍTVÁNYKEZELÉSI ELJÁRÁS ESETÉN	41
3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén	41

3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén	41
3.4. AZONOSÍTÁS ÉS HITELESÍTÉS TANÚSÍTVÁNYÁLLAPOT-VÁLTOZTATÁS ESETÉN	42
4 ÉLETCIKLUS KÖVETELMÉNYEK.....	43
4.1 TANÚSÍTVÁNYIGÉNYLÉS	43
4.1.1 Ki nyújthat be tanúsítványigénylést?	43
4.1.2 Az igénylés folyamata és a résztvevők felelőssége	43
4.2 TANÚSÍTVÁNYIGÉNYLÉSEK FELDOLGOZÁSA.....	44
4.2.1. Azonosítás és hitelesítés	44
4.2.2. Tanúsítványigénylések elfogadása vagy visszautasítása	44
4.2.3. A tanúsítványigénylés feldolgozásának időtartama	45
4.3 TANÚSÍTVÁNY KIBOCSÁTÁSA	45
4.3.1. A Szolgáltató tevékenysége a tanúsítvány kibocsátás során	45
4.3.2. Értesítés a tanúsítvány kibocsátásáról	46
4.4 TANÚSÍTVÁNY ELFOGADÁSA	46
4.4.1. A tanúsítványelfogadás módja	46
4.4.3. További szereplők értesítése a tanúsítvány kibocsátásáról	46
4.5 KULCSPÁR ÉS TANÚSÍTVÁNY ALKALMAZHATÓSÁGA	46
4.5.1. A magánkulcs és a tanúsítvány használata	46
4.5.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata	47
4.6 TANÚSÍTVÁNYMEGÚJÍTÁS	47
4.6.1. A tanúsítványmegújítás körülményei	47
4.6.2. Ki igényelheti a tanúsítványmegújítást?	48
4.6.3. A tanúsítványmegújítási igénylések feldolgozása	48
4.6.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról	48
4.6.5. A megújított tanúsítvány elfogadása	49
4.6.6. A megújított tanúsítvány közzététele	49
4.6.7. További szereplők értesítése a tanúsítvány kibocsátásáról	49
4.7 KULCSCSERE.....	49
4.7.1. A kulcscsere körülményei	49
4.7.2. Ki igényelheti a kulcscserét	49
4.7.3. A kulcscsere igénylések feldolgozása	49
4.7.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról	50
4.7.5. A kulcscserével megújított tanúsítvány elfogadása	50
4.7.6. A kulcscserével megújított tanúsítvány közzététele	50
4.7.7. További szereplők értesítése a tanúsítvány kibocsátásáról	50
4.8 TANÚSÍTVÁNYMÓDOSÍTÁS.....	50
4.8.1. A tanúsítványmódosítás körülményei	50
4.8.2. Ki igényelheti a tanúsítványmódosítást	50
4.8.3. A tanúsítványmódosítási igénylések feldolgozása	51
4.8.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról	51
4.8.5. A módosított tanúsítvány elfogadása	51
4.8.6. A módosított tanúsítvány közzététele	51
4.8.7. További szereplők értesítése a tanúsítvány kibocsátásáról	51
4.9 VISSZAVONÁS ÉS FELFÜGGESZTÉS	51
4.9.1 A visszavonást és a felfüggesztést indukáló körülmények	51
4.9.2 Állapotváltoztatási ügyféligényre jogosultak	53
4.9.3 A visszavonási, felfüggesztési és aktiválási eljárás	53
4.9.4 Az igénylések feldolgozása	54
4.9.5 Állapotváltoztatási igények feldolgozásának maximális ideje	54
4.9.6 Javasolt eljárás az tanúsítványállapot ellenőrzésére	55
4.9.7 A visszavonási lista kibocsátás gyakorisága	55
4.9.8 A visszavonási lista előállítás és közzététele közötti idő maximális hossza	55
4.9.9 Tanúsítványállapot szolgáltatás rendelkezésre állása	55

4.9.10 Tanúsítványállapot szolgáltatásra vonatkozó követelmények.....	56
4.9.11 A visszavonási hirdetmények egyéb formái	56
4.9.12 A kulcs kompromittálódásra vonatkozó speciális követelmények	56
4.9.13 A felfüggesztés maximális ideje	57
4.10 VISSZAVONÁSI NYILVÁNTARTÁSOK	57
4.10.1 Működési jellemzők.....	57
4.10.2 Szolgáltatások elérhetősége és rendelkezésre állása	58
4.10.3 További lehetőségek.....	58
4.11 A SZOLGÁLTATÁSI SZERZŐDÉS MEGSZŰNÉSE.....	58
4.12 KULCSLETÉT ÉS KULCSHELYREÁLLÍTÁS	58
4.12.1 A kulcsletét és -helyreállítás rendje és szabályai	58
4.12.2 Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai	58
5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK.....	59
5.1 FIZIKAI ÓVINTÉZKEDÉSEK	59
5.1.1 Telephely felépítése	59
5.1.2 Fizikai hozzáférés	60
5.1.3 Áramellátás, légkondicionálás.....	60
5.1.4 Beázás és elárasztódás veszélyeztetettsége.....	61
5.1.5 Tűzmelegelőzés és tűzvédelem.....	61
5.1.6 Adathordozók kezelése	61
5.1.7 Hulladékelhelyezés	61
5.1.8 Mentés külső helyszínen.....	61
5.2 ELJÁRÁSRENDI BIZTONSÁGI INTÉZKEDÉSEK	62
5.2.1 Bizalmi munkakörök	62
5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám	63
5.2.3 Az egyes szerepkörökhöz tartozó azonosítás és hitelesítés	63
5.2.4 Egyes szerepkörök összeférhetetlensége	63
5.3 SZEMÉLYZETI BIZTONSÁGI INTÉZKEDÉSEK.....	64
5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények.....	64
5.3.2 Ellenőrzési eljárások	65
5.3.3 Képzési követelmények	65
5.3.4 Továbbképzési gyakoriságok és követelmények	66
5.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága	66
5.3.6 Jogosulatlan tevékenységek büntető következményei	66
5.3.7 Szerződéses közreműködőkre vonatkozó követelmények.....	66
5.3.8 A személyzet számára biztosított dokumentációk.....	67
5.4 NAPLÓZÁSI ELJÁRÁSOK	67
5.4.1 A tárolt események típusai.....	68
5.4.2 A naplófájl feldolgozásának gyakorisága	69
5.4.3 A naplófájl megőrzési időtartama	69
5.4.4 A naplófájl védelme.....	70
5.4.5 A naplófájl mentési eljárásai	70
5.4.6 A naplózás adatgyűjtési rendszere	70
5.4.7 Az eseményeket kiváltó Ügyfelek értesítése.....	70
5.4.8 Sebezhetőség felmérése	70
5.5 ADATOK ARCHIVÁLÁSA	70
5.5.1 Az archiválendő adatok típusa	71
5.5.2 Archiválási időtartam.....	71
5.5.3 Az archívum védelme	71
5.5.4 Az archívum mentési folyamatai	71
5.5.5 Az adatok időbélyegzésére vonatkozó követelmények	71
5.5.6 Az archívum gyűjtési rendszere.....	71
5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások	72
5.6 KULCSCSERE.....	72
5.7 KATASZTRÓFAELHÁRÍTÁS ÉS HELYREÁLLÍTÁS	72

5.7.1 Incidens- és kompromittálódáskezelési eljárások	72
5.7.2 IT erőforrások, szoftverek és/vagy adatok meghibásodása	74
5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás	74
5.7.4 A működés folytonosságának fenntartása katasztrófaesemény után	75
5.8 A HITELESÍTŐ VAGY REGISZTRÁCIÓS EGYSÉG VAGY A SZOLGÁLTATÁS MEGSZŰNÉSE.....	75
6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK.....	77
6.1 KULCSPÁR GENERÁLÁS ÉS TELEPÍTÉS	77
6.1.1. Kulcspár előállítása	77
6.1.2. Magánkulcs eljuttatása Végfelhasználóhoz	79
6.1.3. A nyilvános kulcs eljuttatása a tanúsítványkibocsátóhoz	79
6.1.4. A szolgáltatói nyilvános kulcs közzététele.....	79
6.1.5. Kulcsméretetek	79
6.1.6. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése.....	79
6.1.7. A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)	79
6.2 MAGÁNKULCS VÉDELEM ÉS KRIPTOGRÁFIAI MODUL ELŐÍRÁSOK	80
6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások	81
6.2.2. Magánkulcs többszereplős (n-ből m) használata	81
6.2.3. Magánkulcs letétbe helyezése	81
6.2.4. Magánkulcs mentése	81
6.2.5. Magánkulcs archiválása	82
6.2.6. Magánkulcs bejuttatása kriptográfiai modulba, vagy onnan történő exportja	82
6.2.7. Magánkulcs tárolása kriptográfiai modulban	82
6.2.8. A magánkulcs aktiválásának módja	82
6.2.9. A magánkulcs deaktiválásának módja	82
6.2.10. A magánkulcs megsemmisítésének módja	82
6.2.11. A kriptográfiai modulok értékelése	83
6.3 A KULCSPÁRKEZELÉS TOVÁBBI SZEMPONTJAI	83
6.3.1 Nyilvános kulcs archiválása	83
6.3.2 Tanúsítvány és kulcspár használati idő	83
6.4 AKTIVÁLÓ ADAT	84
6.4.1 Aktiváló adat generálás és telepítés	84
6.4.2 Aktiváló adat védelme	84
6.4.3 Egyéb aktiváló adattal kapcsolatos előírások.....	84
6.5 INFORMATIKAI BIZTONSÁGI ELŐÍRÁSOK	84
6.5.1. Speciális informatikai biztonsági műszaki követelmények	85
6.5.2. Az informatikai biztonság értékelése.....	85
6.6 ÉLETCIKLUSRA VONATKOZÓ BIZTONSÁGI ELŐÍRÁSOK	85
6.6.1 Rendszerfejlesztési előírások	85
6.6.2 Biztonságkezelési előírások.....	85
6.6.3 Életciklusra vonatkozó biztonsági előírások.....	86
6.7 HÁLÓZATI BIZTONSÁG	86
6.8 IDŐBÉLYEGZÉS	87
7 TANÚSÍTVÁNY-, CRL- ÉS OCSP- ÉS PROFILOK	88
7.1. TANÚSÍTVÁNYPROFIL	88
7.1.1. Verzió szám(ok)	88
7.1.2. Tanúsítvány kiterjesztések.....	88
7.1.3. Az algoritmus objektum azonosítója	88
7.1.4. Névformák.....	88
7.1.5. Névhasználati megkötések	88
7.1.6. A Hitelesítési rendek azonosítói.....	88
7.1.7. A szabályzati korlátozás kiterjesztés használata	88
7.1.8. Szabályzatminősítő szintaxis és szemantika	89
7.1.9. A kritikus Hitelesítési rend kiterjesztés feldolgozása	89

7.2. TANÚSÍTVÁNYVISSZAVONÁSI PROFIL	89
7.2.1. Verziószám(ok)	89
7.2.2. Tanúsítványvisszavonási lista kiterjesztések	89
7.3. TANÚSÍTVÁNYÁLLAPOT-SZOLGÁLTATÁS PROFILOK.....	89
7.3.1. Verziószám(ok)	89
7.3.2. OCSP kiterjesztések	89
8 A MEGFELELŐSÉG VIZSGÁLATA	90
8.1. AZ ELLENŐRZÉSEK KÖRÜLMÉNYEI ÉS GYAKORISÁGA	90
8.2 AZ ÉRTÉKELŐ ÉS SZÜKSÉGES KÉPESÍTÉSE	90
8.3 AZ AUDITOR ÉS AZ AUDITÁLT ENTITÁS KAPCSOLATA	91
8.4. AZ ÉRTÉKELÉS ÁLTAL LEFEDETT TERÜLETEK	91
8.5. A HIÁNYOSSÁGOK KEZELÉSE.....	91
8.6. AZ EREDMÉNYEK KÖZZÉTÉTELE.....	92
9. EGYÉB ÜZLETI ÉS JOGI TUDNIVALÓK	93
9.1. DÍJAK.....	93
9.1.1 Tanúsítványszolgáltatás díjai	93
9.1.2 Tanúsítvány-hozzáférési díjak	93
9.1.3 Tanúsítványállapot változtatás és a tanúsítványállapot-információk díjai	93
9.1.4 Egyéb szolgáltatások díjai.....	93
9.1.5 Visszatérítési politika	93
9.2. PÉNZÜGYI FELELŐSSÉG.....	94
9.2.1 Biztosítási fedezet.....	94
9.2.2 Egyéb eszközök.....	94
9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák	94
9.3. BIZALMAS ÜZLETI INFORMÁCIÓK KEZELÉSE	95
9.3.1 A bizalmas információk köre	95
9.3.2 A bizalmas információk körén kívül eső adatok	95
9.3.3 A bizalmas információk védelme.....	95
9.4. SZEMÉLYES ADATOK KEZELÉSE.....	95
9.4.1 Adatkezelési szabályok.....	96
9.4.2. Személyes adatok.....	96
9.4.3. Személyes adatnak nem minősülő információk	96
9.4.4. Személyes adatok védelme	97
9.4.5. Személyes adatok felhasználása	97
9.4.6. Adatkezelés	97
9.4.7. Egyéb adatvédelmi követelmények.....	97
9.5 SZELLEMI TULAJDONHOZ FÜZŐDŐ JOGOK	97
9.6 FELELŐSSÉG ÉS GARANCIÁK	98
9.6.1 A Hitelesítő Egység felelőssége.....	98
9.6.2 A Regisztrációs Egység felelőssége	98
9.6.3 Ügyfelek felelőssége és kötelezettségei	99
9.6.4 Érintett felek felelőssége	99
9.6.5 Egyéb résztvevők felelőssége.....	100
9.7 SZAVATOSSÁG KIZÁRÁSA	100
9.8 FELELŐSSÉG KORLÁTOZÁSA	100
9.9 KÁRTÉRÍTÉS, KÁRTALANÍTÁS.....	100
9.10 A SZOLGÁLTATÁSI REND HATÁLYA	101
9.10.1 Érvényesség	101
9.10.2 Megszűnés.....	101
9.10.3 A megszűnés következményei.....	101
9.11 EGYEDI ÉRTESÍTÉSEK ÉS A RÉSZTVEVŐK KÖZTI KOMMUNIKÁCIÓ	101
9.12 MÓDOSÍTÁSOK.....	101

9.12.1 A módosítási eljárás.....	102
9.12.2 Az értesítések módja és határideje	102
9.12.3 A dokumentumazonosító változása	102
9.13 VITÁS KÉRDÉSEK RENDEZÉSE.....	103
9.14 IRÁNYADÓ JOG.....	103
9.15 A HATÁLYOS JOGSZABÁLYOKNAK VALÓ MEGFELELÉS	103
9.16 VEGYES RENDELKEZÉSEK	104
9.16.1 Teljességi záradék	104
9.16.2 Átruházás.....	104
9.16.3 Részleges érvénytelenség	104
9.16.4 Igényérvényesítés.....	104
9.16.5 Vis maior	104
9.17 EGYÉB RENDELKEZÉSEK	104

1 BEVEZETÉS

Jelen dokumentum a NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság (továbbiakban: Szolgáltató) szabálygyűjteménye, melynek célja, hogy összefoglalja és rendszerezze azokat a minimum követelményeket és feltételeket, amelyek a Szolgáltató nem eIDAS tanúsítványszolgáltatásainak nyújtására és igénybevételére vonatkoznak (a továbbiakban: Szolgáltatási Rend).

Jelen Szolgáltatási Rend kizárólag az LCP, NCP, NCP+ és DVCP hitelesítési rendek szerinti (lásd 1.2.1. Hitelesítési rendek) végfelhasználói tanúsítványok kibocsátásának és kezelésének és a hozzájuk kapcsolódó állapotszolgáltatások nyújtásával kapcsolatos követelményeket és elvárásokat fogalmaz meg. Szolgáltató a jelen Szolgáltatási Rend alapján készült Szolgáltatási Szabályzat alapján csak a fent sorolt hitelesítési rendekbe tartozó tanúsítványokat bocsáthat ki az 1.1. fejezetben leírt nem- eIDAS szolgáltatások keretében.

A hitelesítési rendek leírását lásd az 1.2.1 pontban.

A dokumentumban alkalmazott fogalmakat és rövidítéseket illetően lásd az 1.6 fejezetet.

1.1 Áttekintés

Jelen dokumentum Szolgáltató alábbi nem eIDAS szolgáltatásaira vonatkozó elvárásokat tartalmazza:

- LCP, NCP, NCP+ hitelesítési rendek szerint:
 - Személyes autentikáció
 - Üzleti autentikáció
 - Kamarai jogosult autentikáció
 - Ügyvédi autentikáció
 - Ügyvédi irodai autentikáció
 - Szervezeti autentikáció
 - Álneves autentikáció
 - OCCSZ autentikáció
 - Személyes titkosító
 - Üzleti titkosító
 - Kamarai jogosult titkosító
 - Ügyvédi titkosító
 - Szervezeti titkosító
 - Ügyvédi irodai titkosító
 - Álneves titkosító
- DVCP hitelesítési rend szerint:
 - DV SSL tanúsítvány kiadás
- nem eIDAS tanúsítványszolgáltatásokhoz kapcsolódó tanúsítványállapot-szolgáltatások.

1.1.1. Szabványok és előírások

A dokumentum az RFC 3647 szabvány szerinti szerkezetet követve készült. A dokumentum

az eIDAS, a DÁP (lásd [1.6.2 Rövidítések](#)) és egyéb releváns hazai jogszabályok, valamint az ETSI EN 319401, ETSI EN 319411-1, ETSI EN 319412, szabványok elvárásait foglalja össze (az alkalmazott jogszabályok, szabványok és ajánlások teljes listáját és pontos megnevezésüket lásd a 9.15 A hatályos jogszabályoknak való megfelelés).

Az egyes fejezetek és pontjaik csak a tartalom adott logikai rend szerinti rendezésére szolgálnak, a rendelkezések értelmezése tekintetében nem irányadók.

A szabályoknak való megfelelést a *Szolgáltatási Szabályzat Nem eIDAS Tanúsítványszolgáltatásokra* dokumentum (a továbbiakban szabályzat) ismerteti. A szabályzatnak illetve az abban hivatkozott egyéb Kikötéseknek egyértelműen meg kell határozniuk a nyújtandó szolgáltatás részleteit, az igénybevételhez szükséges eszközöket.

1.1.2 A Szolgáltató adatai

NÉV:	NETLOCK Informatikai és Hálózatzbiztonsági Szolgáltató Korlátolt Felelősségű Társaság
RÖVIDÍTETT NÉV:	NETLOCK Kft.
SZÉKHELY:	1101 Budapest, Expo tér 5-7.
TELEPHELY (ÜGYFÉLSZOLGÁLAT):	1143 Budapest, Hungária körút 17.
POSTÁZÁSI CÍM:	1439 Budapest, Pf. 663
CÉGJEGYZÉKSZÁM:	01-09-563961
ADÓSZÁM:	12201521-2-42
TELEFONSZÁM:	(1) 437-6655 (Tanúsítvány állapotváltozás igénylése: 3. menüpont)
WEBOLDAL:	netlock.hu
KIKÖTÉSEK ÉS FELTÉTELEK KÖZZÉTÉTELE:	netlock.hu/aktualis-szabalyzatok
ÜGYFÉLKAPCSOLATI E-MAIL:	info@netlock.hu
MEGRENDELÉSEK, DOKUMENTUMMÁSOLATOK, SZERZŐDÉSEK KÜLDÉSE:	igenylesek@netlock.hu vagy kerelmek@netlock.hu
NETLOCK SZABÁLYZATELFOGADÓ EGYSÉG EMAIL CÍME:	szee@netlock.hu
COMPLIANCE EGYSÉG EMAIL CÍME:	compliance@netlock.hu
ÜGYFÉLFOGADÁS / NYITVA TARTÁS	A Szolgáltató weboldalán feltüntetett helyen és időintervallumban.

Jelen Szolgáltatási Rend az eIDAS rendelkezésein kívül eső nem eIDAS tanúsítványszolgáltatás nyújtásával kapcsolatos követelményeket tartalmaz.

1.2 A dokumentum neve és azonosítás

A dokumentum nevét és OID azonosítóját lásd a fedlapon (első számozás nélküli oldal a Szolgáltató logójával) - "A dokumentum magyar neve" és "A dokumentum angol neve" valamint az "Azonosító szám (OID)" sorokban.

A dokumentum többi oldalain a dokumentum magyar neve a láblécben, OID azonosítója pedig a fejlécben kerül feltüntetésre.

A dokumentum jóváhagyásának, közzétételének és hatálybalépésének idejét valamint

verziószámát szintén lásd a fedlapon.

Jelen dokumentum egyike a Szolgáltató által kiadott azon dokumentumoknak, amelyek az általa nyújtott szolgáltatások feltételeit együttesen szabályozzák. Ilyen dokumentumok továbbá például az Általános szerződési feltételek, a Szolgáltatási szerződés, a szolgáltatási szabályzatok, az Ügyfelekkel és a Partnerekkel kötött egyéb szerződések.

A jelen dokumentumban Szolgáltatónak nevezett entitás a NETLOCK Kft. - adatait lásd az 1.1.2 pontban.

1.2.1 Hitelesítési Rendek

A Szolgáltatónak a végfelhasználói tanúsítványokban hivatkozást kell elhelyeznie az alkalmazott hitelesítési rendre (lásd 1.6.1 Fogalmak), hogy azonosítsa az adott tanúsítványra vonatkozó szabványos hitelesítési szabályokat és kinyilvánítsa az azoknak való megfelelést. A hivatkozás lehet a hitelesítési rend szabványban megadott jelölése és/vagy az ahhoz tartozó szabványos OID azonosító (lásd az alábbi táblázatot). A szabványos hitelesítési rendek mellett Szolgáltató a legalapvetőbb információkról szöveges tájékoztatást is megjeleníthet.

Az azonosítókat, hivatkozásokat és a szöveges tájékoztatást a Szolgáltató a tanúsítvány hitelesítési rendek jelzésére szolgáló mezőiben tünteti fel (lásd 7.1.6. A Hitelesítési rendek azonosítói). Az RFC 5280 ajánlásai szerint ilyen azonosítóból egy javasolt, ezért Szolgáltatónak törekednie kell rá, hogy ahol lehetséges, szabványos azonosító egyedül kerüljön feltüntetésre.

A Szolgáltatónak valamennyi jelen szolgáltatási rend alapján kibocsátott tanúsítványban el kell helyeznie egy hivatkozást az alkalmazott hitelesítési rendre vonatkozóan. Jelen dokumentum az alábbi Hitelesítési Rendeknek megfelelő tanúsítványokra és szolgáltatásokra vonatkozó rendelkezéseket tartalmazza. Amennyiben jelen dokumentum egyes rendelkezései csak egyes Hitelesítési Rendek alapján kibocsátott tanúsítványok esetén érvényesek, az adott rendelkezéseknél a szöveg ezt egyértelműen jelzi zárójelben feltüntetve az adott hitelesítési rend azonosítót is.

Az ETSI 319 411-2 szabványban meghatározott hitelesítési rendek		
<i>Hitelesítési rend jelölése a szabványban</i>	<i>A hitelesítési rend jelentése</i>	<i>A hitelesítési rendet jelölő OID</i>
LCP	Lightweight Certificate Policy Könnyített hitelesítési Hitelesítési Rend E hitelesítési rendnek megfelelően kibocsátott nem eIDAS tanúsítványok bármilyen felhasználási célra igénybe vehetők, kiadásuk során nincs személyes megjelenési kötelezettség.	0.4.0.2042.1.3
NCP	Normalized Certificate Policy Normalizált Hitelesítési Rend E hitelesítési rendnek megfelelően kibocsátott nem eIDAS tanúsítványok bármilyen felhasználási célra igénybe vehetők.	0.4.0.2042.1.1

NCP+	Extended Normalized Certificate Policy Kiterjesztett (Kriptográfiai eszköz használatát megkövetelő) normalizált Hitelesítési Rend Az NCP-nek megfelelő nem eIDAS tanúsítványokat hoz létre a magánkulcs Kriptográfiai eszközön való kezelésével.	0.4.0.2042.1.2
-------------	--	----------------

Az CAB Forum meghatározott hitelesítési rendek		
<i>Hitelesítési rend jelölése a szabványban</i>	<i>A hitelesítési rend jelentése</i>	<i>A hitelesítési rendet jelölő OID</i>
DVCP	Domain Validation Certificate Policy Technikai ellenőrzés alapján csak az ellenőrzött domain nevet tartalmazó tanúsítványra vonatkozó Hitelesítési Rend	2.23.140.1.2.2

1.2.2 Dokumentum revíziók

OID	Hatálya	Változás leírása	Készítő
1.3.6.1.4.1.3555.1.65.20170721	2017.07.21- 2018.09.17.	A nem eIDAS tanúsítványszolgáltatásokra vonatkozó szolgáltatási rend első verziója.	Varga Viktor Szabó Zoltán
1.3.6.1.4.1.3555.1.65.20180913	2018.09.18- 2019.10.16.	- Dokumentum címének rövidítése. - Fedlap módosítása, kiegészítése. - Egyes értelmezési nehézséget okozó megfogalmazások javítása (pl. 1.2.1). - A másodlagos hitelesítési rend azonosítókba a teszttanúsítványt jelölő azonosító tag megszüntetése (1.2.1). - Weboldal-hitelesítő tanúsítványokhoz kapcsolódó ellenőrzések kiegészítése egyéb, a Szolgáltató által előírható ellenőrzési eljárásokra való lehetőséggel (3.2.5). - Felfüggesztett tanúsítvány aktiválására vonatkozó szabályok pontosítása (4.9.2). - Adatkezeléssel kapcsolatos előírások pontosítása (9.4) - Módosításra vonatkozó előírások pontosítása (9.12) - Egyes – a közelmúltban változott – jogszabályok hivatkozásának frissítése.	Szabó Zoltán

1.3.6.1.4.1.3555.1.65.20191015	2019.10.17- 2020.08.30.	- Alkalmazott hitelesítési rendek módosítása (1.2.1) - A <i>Regisztrációs ügyintéző</i> és az <i>Ügyféleszköz</i> fogalmának pontosítása (1.6.1)	Szabó Zoltán Varga Viktor
1.3.6.1.4.1.3555.1.65.20200731	2020.08.31- 2021.04.29.	A Mozilla Root Store Policy weboldal-hitelesítő tanúsítványok érvényességi idejére vonatkozó, legkésőbb 2020. szeptember 1-jétől alkalmazandó korlátozásának implementálása (6.3.2).	Kövári-Szabó Zoltán
1.3.6.1.4.1.3555.1.65.20210429	2021.04.30- 2024.08.31.	A dokumentum 1.1.2 A Szolgáltató adatai pont kiegészítése a Szolgáltató telephelyével	Varga-Szabó Éva
1.3.6.1.4.1.3555.1.1.16.0.240901	2024.09.01-től visszavonásig vagy új verzió hatálybalépéséig	- Jogszabályváltozás miatti frissítések: 1.1.1; 1.6.1; 1.6.2; 5.8 - Kódaláíró tanúsítvány kivezetése a rendből: 1; 1.1; 1.2.1; 1.4; 1.4.1; 1.4.2 - Szolgáltatói elérhetőségek frissítése: 1.1.1; 1.5.2	NETLOCK Compliance

1.3 A PKI szereplők

Jelen Szolgáltatási Rend keretében a PKI szereplők alatt a nem eIDAS tanúsítványszolgáltatás Ügyfeleit - a tanúsítványok Igénylőit és szolgáltatás Előfizetőit, a tanúsítványok Végfelhasználóit, a Szolgáltatót és szervezeti egységeit, valamint az Érintett feleket kell érteni.

Lásd még az 1.6.1 Fogalmak fejezet releváns fogalom meghatározásait.

1.3.1 A Hitelesítő egység és a Kiadó

A Szolgáltatónak általános felelőssége van az általa nyújtott szolgáltatások tekintetében. Ezek nyújtásához igénybe vehet külső feleket, de szerződésében biztosítania kell a kikötéseinek és feltételeinek való megfelelést az általuk nyújtott szolgáltatások tekintetében, s tevékenységükért felelősséggel tartozik az Ügyfelek felé.

A Hitelesítő Egység működésének meg kell felelnie a vonatkozó Szolgáltatási rend(ek)ben, Szolgáltatási szabályzat(ok)ban és egyéb Kikötésekben megfogalmazott, a Hitelesítő Egységre vonatkozó követelményeknek. A Hitelesítő Egység munkatársainak be kell tartaniuk a belső működési szabályzatukban foglalt előírásokat is, tevékenységüket aszerint kell végezniük.

A Szolgáltató minden esetben teljes felelősséggel tartozik a Hitelesítő Egységre vonatkozó előírások betartásáért.

A Szolgáltató és a Kiadója az általa kibocsátott tanúsítványokban (mint kibocsátó)

megnevezésre kell, hogy kerüljön, s a tanúsítványt az ő magánkulcsával kell hitelesíteni.

1.3.2 Regisztrációs Egység

Regisztrációs Egység működhet a Szolgáltató részeként, de lehet önálló, független szervezet is (Kihelyezett Regisztrációs Egység).

A Regisztrációs Egység működésének meg kell felelnie a vonatkozó Szolgáltatási rend(ek)ben, Szolgáltatási szabályzat(ok)ban és egyéb Kikötésekben megfogalmazott Regisztrációs egységre vonatkozó követelményeknek. A Regisztráció Egység munkatársainak be kell tartaniuk a belső működési szabályzatukban foglalt előírásokat is, tevékenységüket aszerint kell végezniük.

A Szolgáltató minden esetben teljes felelősséggel tartozik a Regisztrációs Egységre vonatkozó előírások betartatásáért.

Kihelyezett Regisztrációs Egység működése esetén a Szolgáltatónak szerződésben köteleznie kell azt a vonatkozó követelmények betartására.

1.3.3 Előfizető, Végfelhasználó és Igénylő

Előfizető és Igénylő a Szolgáltató Ügyfelei, akikkel Szolgáltató szerződéses kapcsolatba kerül. Végfelhasználó személyét az Előfizető határozza meg.

Lásd még a 1.6 Fogalmak és rövidítések fejezet vonatkozó fogalommagyarázatait.

A Szolgáltató, annak munkatársa, szervezeti egysége vagy Szolgáltatói partnere csak abban az esetben lehet a szolgáltatás Ügyfele, ha Szolgáltató a szabályzatában ezt kifejezetten lehetővé teszi.

1.3.4 Érintett felek

Az Érintett felek jellemzően nem állnak szerződéses kapcsolatban a Szolgáltatóval, de részükre a jelen Szolgáltatási Rend alapján készült szolgáltatási szabályzat ajánlásokat fogalmazhat meg az általuk igénybevett - jellemzően - nem díjköteles szolgáltatások - jellemzően tanúsítvány-állapotszolgáltatások - kapcsán. A Szolgáltató az Érintett Felekkel elsősorban a tanúsítványtáron keresztül tart kapcsolatot.

Lásd még az 1.6.1 fejezet Érintett Fél fogalmát.

1.3.5 Egyéb szereplők

Titkosító partnerek

A titkosító tanúsítvány nyilvános kulcsával elkódolás bárki számára lehetővé teszi titkosított üzenetek küldését. A titkosító tanúsítványra kódolás előtt a titkosítást végző partnernek meg kell győződnie a tanúsítvány visszavonási állapotáról az érintett felekre vonatkozó eljárások alapján.

1.4 Tanúsítványok alkalmazhatósága

Az LCP, NCP és NCP+ hitelesítési rendek szerint kibocsátott tanúsítványok használata, tanúsítvány kiterjesztések alapján lehet:

- titkosító tanúsítványok, melyek magánkulcsa a nyilvános kulcsra elkódolt adatok dekódolására alkalmas
- autentikációs tanúsítványok, melyek azonosítási műveletben részvétel célját szolgálják, PKI aláírás művelet végzésével, de nem alkalmasak jogi szempontból elfogadott elektronikus aláírás létrehozására.
- A DVCP hitelesítési rendek szerint kibocsátott tanúsítványok weboldal-hitelesítő tanúsítványok, melyek SSL és TLS protokollon keresztül elért webszerverek, levelező és egyéb szerverek azonosítására használhatók.

A tanúsítványok alkalmazhatósága tekintetében lásd a másodlagos hitelesítési rend Kulcsfelhasználás mezőjét, valamint a Key Usage mező tartalmát, s a tanúsítványba foglalt egyéb (akár szöveges) korlátozásokat.

1.4.1. A megfelelő tanúsítvány használat

a. Végfelhasználói tanúsítványok

Jelen Szolgáltatási Rend alapján kibocsátott végfelhasználói tanúsítványokhoz tartozó magánkulcsok kizárólag a bennük foglalt céloknak megfelelően titkosításra, autentikációra vagy weboldal hitelesítésre használhatóak fel.

Az NCP+ hitelesítési rend szerint kibocsátott tanúsítványokhoz tartozó magánkulcsot elektronikus aláírás-létrehozó eszköz védi.

Az NCP hitelesítési rend szerint kibocsátott tanúsítványokhoz tartozó magánkulcs tárolása szoftveres kulcstárolással történik.

Az LCP hitelesítési rend szerint kibocsátott tanúsítványok esetében esetében a fentiekhez hasonló előírás a kulcstárolással kapcsolatban nincs, ezen hitelesítési rend esetében nincs személyes találkozás előírva.

Az DVCP hitelesítési rendek szerint kibocsátott weboldal-hitelesítő tanúsítványok esetében a fentiekhez hasonló előírás a kulcstárolással kapcsolatban nincs. Az ilyen weboldal-hitelesítő tanúsítványok szerverek, weboldalak hitelesítésére alkalmazhatók.

b. Szolgáltatói tanúsítványok

A szolgáltatói gyökér és a végfelhasználói tanúsítványokat hitelesítő köztes tanúsítványok és kulcsaik nem használhatók tanúsítványok hitelesítésére a szolgáltatói tanúsítvány és nyilvános kulcsának közzétételét megelőzően.

1.4.2. Tiltott tanúsítvány használat

a. Végfelhasználói tanúsítványok

A jelen Szolgáltatási Rend szerint kibocsátott titkosító és autentikációs tanúsítványokat (LCP, NCP és NCP+) és a hozzájuk tartozó kulcsokat tilos a titkosítás dekódolásán és autentikáción kívül másra használni.

A jelen Szolgáltatási Rend szerint kibocsátott weboldal-hitelesítő tanúsítványokat (DVCP,) és a hozzájuk tartozó kulcsokat tilos weboldalak, szerverek hitelesítésétől eltérő célra használni.

b. Szolgáltatói tanúsítványok

A szolgáltatói gyökér és a végfelhasználói tanúsítványokat hitelesítő köztes tanúsítványok és kulcsaik nem használhatók tanúsítványok hitelesítésére a szolgáltatói tanúsítvány és nyilvános kulcsának közzétételét megelőzően.

1.5 A Szolgáltatási Rend adminisztrációja

Jelen Szolgáltatási Rend kibocsátását és karbantartását a Szolgáltató szabályzatért felelős egysége végzi. A Szolgáltató a szabályzatért felelős egységet saját egységén belül működteti s ennek pontos felépítését, feladatát, hatáskörét és felelősségét külön szabályzat tartalmazza.

1.5.1 A dokumentum adminisztrációját végző szervezet

A Szolgáltató szabályzatokért (kikötésekért) felelős egységének neve NETLOCK Szabályzatelfogadó Egység. A Szabályzatelfogadó Egység állandó tagjai a Szolgáltató munkatársai, akiket a Szolgáltató Ügyvezetése írásban jelöl ki. Az Egység működését a Szabályzatelfogadó Egység belső, nem nyilvános működési szabályzata írja le.

A Szolgáltató szabályzatainak módosításával kapcsolatban lásd a 9.12 fejezetet.

1.5.2 A dokumentum kapcsolattartó személye

Jelen dokumentummal kapcsolatban a Szabályzatelfogadó Egység kapcsolattartásért felelős személye a jelen dokumentum jóváhagyója (lásd a dokumentum fedlapját).

Jelen dokumentummal kapcsolatos kérdésekkel és észrevételekkel az Ügyfelek, a Végfelhasználók és az Érintett felek elektronikus levélben a compliance@netlock.hu címen kereshetik meg a NETLOCK Compliance Egységét.

Szolgáltató munkatársai észrevételeiket egyéb csatornán keresztül is, de szintén csak írásban juttathatják el a Szabályzatelfogadó Egységhez.

A Szabályzatelfogadó Egységnek elektronikus levélben küldött megkeresések megválaszolásáért, illetve - amennyiben szükséges az észrevétel nyomán megtenni szükséges egyéb intézkedések megtételéért a kapcsolattartó személy felelős.

A Szabályzatelfogadó Egység részére jelen dokumentummal kapcsolatban eljuttatott kérdés vagy észrevétel esetén a kapcsolattartónak kell kijelölnie az Egység azon munkatársát, aki a megkeresést feldolgozza. Összetettebb tárgyú megkeresés esetén összehívja a

Szabályzatelfogadó Egység ülését - az Egység szabályzatában foglaltaknak megfelelően.

A megkeresés feldolgozása során, az Egység vagy munkatársa azonosítja a dokumentum észrevétellel, kérdéssel érintett pontját/pontjait, majd az Egység többi munkatársával egyeztetve - és szükség esetén más munkatársak véleményét is kikérve - küld választ elektronikus levélben az megkeresést küldőnek.

Amennyiben a megkeresés nyomán jelen Szolgáltatási Rend vagy más dokumentum módosítása szükségessé válik, a módosítással kapcsolatban a 9.12 fejezet szerint kell Szolgáltatónak eljárnia.

Magánkulcs kompromittálódásának gyanúja esetén, tanúsítványvisszaélés, vagy más típusú csalás, kompromittálás, visszaélés, nem megfelelő magatartás, vagy bármely más, a Tanúsítványokkal kapcsolatos ügyben a compliance.info@netlock.hu címen kereshetik a Szolgáltatót.

1.5.3 A szolgáltatási szabályzat szolgáltatási rendnek megfelelésért felelős szervezet

A jelen Szolgáltatási Rend alapján nyújtott nem eIDAS tanúsítványszolgáltatás nyújtásának és igénybevételének részletes gyakorlati előírásait tartalmazó Szolgáltatási Szabályzat jelen Szolgáltatási Rendnek való megfelelését a NETLOCK Szabályzatelfogadó Egység ellenőrzi. A jelen Szolgáltatási Rend alapján készült szolgáltatási szabályzatot a Szabályzatelfogadó Egység a jelen Szolgáltatási Rendnek való maradéktalan megfelelés esetén hagyhatja jóvá.

A Szolgáltatási rend vagy nyilvános tervezete közzétételének feltétele, annak jóváhagyása.

1.5.4 A Szolgáltatási szabályzat elfogadása

A jelen Szolgáltatási Szabályzat elfogadási eljárását a Szolgáltatónak ismertetnie kell a szolgáltatási szabályzatban.

A Szolgáltatási Rend módosításával kapcsolatban lásd a 9.12 fejezetet.

1.6 Fogalmak és rövidítések

1.6.1 Fogalmak

AIA	CAI (Authority Information Access:Certificate Authority Issuers): Az adott tanúsítvány kiadói tanúsítványára vonatkozó elérhetőséget (URL) tartalmazó tanúsítványmező.
Alárendelt szolgáltatás	Szolgáltató szabályzatai alapján működő nem-minősített bizalmi szolgáltatás, mely számára Szolgáltató biztosít tanúsítványt.
Aktíváló adat	Olyan a szolgáltató által előállított vagy végfelhasználó által megadott, kizárólag a végfelhasználó által ismert kódsorozat (jelszó, PIN kód), ami a magánkulcsot alkalmazásra képes állapotba helyezi. Tanúsítványaktiváláshoz nincs köze.
Aláírás	Lásd elektronikus aláírás

Aláírás / Bélyegző Létrehozó eszköz	Olyan kriptográfiai eszköz, amely minősített aláírás / bélyegző létrehozására nem alkalmas (lásd még 1.6.2. Rövidítések, SCD).
Aláírói partner	Szolgáltatói partner, aki az aláírási szolgáltatást saját ügyfelei számára biztosítja, amelynek részeként részt vehet a Végfelhasználók azonosításában (akik tekintetében korlátozott információs és adminisztrációs jogokkal bír), s aki az aláírási szolgáltatást saját szolgáltatásával integráltan szolgáltatás nyújtására használja, s aki Előfizetőként vállalja a díjfizetést a végfelhasználók után.
Alany	Lásd a DÁP vonatkozó rendelkezései szerinti meghatározását. Jelen szabályzat keretében a tanúsítvány Subject és SAN mezőit, illetve az ezekben feltüntetésre kerülő adatokat értjük alatta, amelyek utalhatnak egy természetes személyre és/vagy egy szervezetre és/vagy egy védjegyre/terméknévre vagy egy eszköz/rendszer azonosítójára/más elnevezésére vagy egy álnévre. Lásd az Igénylő, Előfizető, Ügyfél és Végfelhasználó entitásokat.
Állapotváltoztatás	Az az eljárás, aminek eredményeként a tanúsítvány állapota (érvényes, felfüggesztett) megváltozik és új értéket vesz fel (érvényes, felfüggesztett, visszavont).
Archiválási szolgáltatás	Az elektronikus dokumentumok hosszú távú megőrzésére vonatkozó szolgáltatás. Olyan elektronikus archiválási szolgáltatás, amelyet valamely minősített bizalmi szolgáltató nyújt, és amely megfelel a 45j. cikkben meghatározott követelményeknek. Jelen szabályzat keretén belül olyan minősített bizalmi szolgáltatás, mely során a Bizalmi Szolgáltató a hozzá archiválás céljából eljuttatott elektronikusan hitelesített (aláírt vagy bélyegzett) dokumentumok aláírása vagy bélyegzője teljes érvényességi láncát létrehozza vagy kiegészíti, az érvényességi láncot archív időbélyeggel ellátja, majd az így kiegészített dokumentumot vagy fájlt biztonságosan eltárolja. Ha az elektronikus aláírással vagy bélyegzővel ellátott elektronikus dokumentum archiválását minősített bizalmi szolgáltató végzi, az ellenkező bizonyításáig vélelmezni kell, hogy az elektronikus dokumentumon elhelyezett elektronikus aláírás, bélyegző vagy időbélyegző és az azokhoz kapcsolódó tanúsítvány az aláírás, bélyegző vagy időbélyegző elhelyezésének időpontjában érvényes volt.
Átvevő	A végfelhasználó valamely kulcsát vagy eszközét (pl. Ügyféleszköz) és aktiváló adatát Szolgáltatótól (személyesen, hagyományos vagy elektronikus kézbesítés útján) átvevő személy, aki az lehet, aki az adott tanúsítvány esetében Igénylő lehet.
Bélyegző	Lásd elektronikus bélyegző
Bizalmi lista	Hatóság vagy szoftvergyártó által kezelt lista, amely a megbízhatónak tartott bizalmi szolgáltatások azonosítóit (jellemzően tanúsítványait) tartalmazza. Egy adott bizalmi listát kezelő szoftver a benne lévő szolgáltatásokra

	visszavezethető aláírásokat, bélyegzőket és időbélyegzőket elfogadja. Jellemzően az EU bizalmi listát értjük alatta, ahol az eIDAS szerinti nem minősített és minősített szolgáltatások kerülnek feltüntetésre az egyes tagországok felügyeleti szervei által. Lásd: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-certification-service-providers
Szolgáltatási Rend	Szolgáltatási Rend Nem eIDAS Tanúsítványszolgáltatásra
Bizalmi Felügyelet	A DÁP által a bizalmi szolgáltatások felügyeletére kijelölt szerv. Konkrétan a Nemzeti Média- és Hírközlési Hatóság.
Bizalmi munkakör	A szolgáltató informatikai rendszeréért általánosan felelős vezetői munkakör. Lásd az 5.2.1 Bizalmi munkakörök fejezetet.
Bizalmi munkatárs	A Szolgáltatónál vagy Szolgáltatói partnerénél bizalmi munkakört betöltő személy.
Bizalmi szolgáltatás	Az eIDAS 3. cikk 16. Pontja szerint: "Rendszerint díjazás ellenében nyújtott, jelen Szabályzat keretében az alábbiakból álló elektronikus szolgáltatások: - elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy - weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése." Jelen szabályzat keretén belül a Szolgáltató elektronikus aláírásokhoz, elektronikus bélyegzőkhöz és weboldal hitelesítéshez kapcsolódó, a tanúsítványok kibocsátását és életciklusmenedzsmentjét biztosító, valamint az időbélyegző szolgáltatását értjük alatta.
Biztonságos zóna:	Olyan (logikailag vagy fizikailag) védett terület, amely védi a titkosságát, integritását és elérhetőségét a Szolgáltató által használt rendszereknek.
CAA ellenőrzés	Olyan ellenőrzés, amikor a DNS bejegyzésben RFC 6844 szerinti CAA rekordokat keres a Szolgáltató. Ha itt arra utaló bejegyzés van, hogy más Szolgáltatóval tart kapcsolatot a domain tulajdonos, akkor nem adható ki tanúsítvány.
Eakta (formátum)	Elektronikus aláírás konténerformátum, amely dokumentumokat, illetve hozzájuk kapcsolódó profilokat (metaadatokat), aláírásokat, ellenjegyzéseket és időbélyegzőket tartalmazhat, szabványos, az ETSI TS 101 903 (XAdES) specifikációnak megfelelően. Lásd bővebben: https://e-szigno.hu/tudasbazis/e-akta-formatum-specifikacioja.html
EV tanúsítvány Extended Validation Certificate (EVC)	Olyan weboldal-hitelesítő tanúsítvány ami megfelel az EVCG követelményeinek.

Elektronikus aláírás	Olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ (eIDAS 3 cikk 10. pont). Jelen szabályzat keretén belül: A Szolgáltató által kibocsátott aláíró tanúsítvány magánkulcs párjával természetes személy által létrehozott elektronikus adat, amelyet az aláírandó elektronikus dokumentumhoz (vagy más elektronikus adatokhoz) csatolnak, s ami a tanúsítvánnyal és a benne foglalt nyilvános kulccsal ellenőrizhető.
Elektronikus bélyegző	Olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét. (eIDAS 3 cikk 25. pont) Jelen szabályzat keretén belül: A Szolgáltató által kibocsátott bélyegző tanúsítvány magánkulcs párjával jogi személy által létrehozott elektronikus adat, amelyet az bélyegzendő elektronikus dokumentumhoz (vagy más elektronikus adatokhoz) csatolnak, s ami a tanúsítvánnyal és a benne foglalt nyilvános kulccsal ellenőrizhető. Az elektronikus aláírás jogi személy által létrehozott megfelelője.
Előfizető	Szolgáltató azon szerződéses partnere, aki a szolgáltatási díjak fizetését vállalja. Jogai és kötelezettségei az ÁSZF-ben és a Szolgáltatási szerződésben különösen megjelennek. Tanúsítványszolgáltatás esetén amennyiben a tanúsítvány Alanyként szervezet is megnevezésre került vagy csak egy természetes személy van benne megnevezve, akkor jellemzően azzal megegyezik. NL Sign szolgáltatás esetén megegyezik az Aláírói Partnerrel vagy a Végfelhasználóval. Lásd még az Ügyfél, Igénylő és Végfelhasználó entitásokat, valamint az 1.3.3 Előfizető, Végfelhasználó és Igénylő fejezetet.
Érintett fél	Természetes vagy jogi személy, aki Szolgáltatóval nem kerül szerződéses kapcsolatba, de annak valamely - jellemzően ingyenes - tanúsítvány állapot szolgáltatását igénybe veszi (pl. elektronikus aláírást, bélyegzőt vagy időbélyegzőt ellenőriz és ennek kapcsán az egyes tanúsítványok érvényességi információit vagy szolgáltató szabályzatait ellenőrzi). Lásd az 1.3.4 Érintett felek fejezetet.
Érvényes tanúsítvány	Olyan tanúsítvány, amelynek az érvényességi idejébe esik a mindenkor jelen időpont, és amelynek állapota nem felfüggesztett vagy visszavont (lásd Tanúsítványállapot).
Érvényességi idő(tartam)	Egy kezdeti és végső időpont közötti időtartam, amelyre a tanúsítvány kiadásra került.
Eszközös tanúsítvány	Olyan tanúsítvány, aminek magánkulcsa Kriptográfiai eszközre kerül kiadásra.
Érvényességi lánc	Az elektronikus dokumentum vagy annak lenyomata és azon egymáshoz rendelhető információk (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás vagy bélyegző létrehozásához használt adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató érvényességi

	adatára és annak visszavonására vonatkozó információk) sorozata, amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, bélyegző vagy időbélyegző, az aláírás, bélyegző vagy időbélyegző elhelyezésének időpontjában érvényes volt. Általánosabb értelemben egymást hitelesítő tanúsítványok hierarchiája, egészen a gyökér tanúsítványig.
Fokozott biztonságú elektronikus aláírás	Olyan elektronikus aláírás, amely megfelel az eIDAS 26. cikkben meghatározott követelményeknek.
Fokozott biztonságú elektronikus bélyegző	Olyan elektronikus bélyegző, amely megfelel az eIDAS 36. cikkben meghatározott követelményeknek.
Hitelesítési rend	A DÁP vonatkozó rendelkezései szerint: olyan bizalmi szolgáltatási rend, amely bizalmi szolgáltatás keretében kibocsátott tanúsítványra vonatkozik. Szolgáltató szabályzati keretében egy szabványos eljárásrend, ami alapján Szolgáltató tanúsítványt bocsát ki és kezel. Szolgáltató szabályzatai több hitelesítési rendet is magukban foglalnak, megkülönböztetve a nekik megfelelő követelményeket és eljárásokat.
Hitelesítő egység	Szolgáltató szervezeti egysége, amely a Regisztrációs egység kérelme alapján a tanúsítványok kiadását, publikálását, visszavonását, felfüggesztését, valamint a Tanúsítványvisszavonási lista publikálását végzi. Lásd az 1.3.1 fejezetet.
Hitelesítési Ügyintéző	A Hitelesítő Egységen belül e munkakörben dolgozó munkatársak a tanúsítványok kibocsátásának jóváhagyását végzik.
Hozzáférfő	Az archiválássléolgáltatás Előfizetőjének kezdeményezésére a szolgáltatás bizonyos funkcióit a kezdeményező Előfizető által meghatározott dokumentumok tekintetében díjmentesen elérő Érintett fél. Lásd az 1.3.5 Érintett felek fejezetet.
Igénylő	Tanúsítványszolgáltatás esetén a tanúsítványkibocsátási tanúsítványkezelési és állapotváltoztatási eljárásban eljáró, a szolgáltatói szerződést Ügyfél részéről elfogadó természetes személy, aki lehet: • a tanúsítvány Alanyaként megjelölt természetes személy (Álnév esetén az álnév kérelmezője); • ennek hiányában a tanúsítvány Alanyaként megjelölt szervezet képviselője vagy meghatalmazottja; • ezek hiányában a tanúsítvány Alanyaként megjelölt domain név, trademark vagy terméknév tulajdonosa, ill. szervezet tulajdonos esetén annak képviselője vagy meghatalmazottja, illetve a domain név fölött kontrollal rendelkező személy. Előfizetővel megegyezik, amennyiben a tanúsítvány Alanyaként egy természetes személy kerül feltüntetésre (és szervezetnem). NL Sign szolgáltatás esetén megegyezik Végfelhasználóval. Archiválás- és Időbélyegszolgáltatás esetén megegyezik Előfizetővel.
Időbélyegző	Olyan elektronikus adat, amely más elektronikus adatokat egy adott

	időponthoz köt, amivel igazolja, hogy utóbbi adatok léteztek az adott időpontban.
Időbélyegző Kiszolgáltató	A Szolgáltató időbélyegzőket kibocsátó műszaki rendszere.
Időbélyegző szolgáltatás	Szolgáltató azon szolgáltatása, amely a számára küldött elektronikus adatok lenyomata alapján egy időbélyegzőt állít elő, az adott adatokhoz.
Időbélyeg-URL	Az időbélyeg-szolgáltatás elérését biztosító, az Előfizető egyedi azonosítóját tartalmazó virtuális token, melyen keresztül Végfelhasználó időbélyeg kéréseket továbbíthat Szolgáltató felé, Szolgáltató pedig a kérés alapján időbélyeg választ továbbít Végfelhasználó felé.
Kézbiztosítási Megbízott	Olyan Szolgáltatói partner, aki Szolgáltató megbízásából - Igénylő ilyen irányú igénye esetén - az Igénylővel egyeztetett helyen és időben végzi el a Tanúsítványkibocsátáshoz kapcsolódóan az ügyfélszervező átadását. Adott esetben megegyezhet a Regisztrációs Megbízottal.
KGyHSz	Közigazgatási Gyökér Hitelesítés-Szolgáltató Lásd 1.3.5 és http://www.kgyhsz.gov.hu/
Központi Regisztrációs Egység	A Szolgáltató azon saját szervezetén belül működtetett szervezeti egysége, mely feldolgozza a szolgáltatások igényléseit, azonosítja azok Igénylőjét és Előfizetőjét, ellenőrzi az eljárási jogukat és adataikat.
Kezdeti felfüggesztés	A Tanúsítványfelfüggesztés egy speciális esete, amikor a Szolgáltató a tanúsítványt kibocsátása után azonnal felfüggeszti, így megóvva azt a visszaélésektől arra az időszakra, míg a Tanúsítvány és a magánkulcs biztonságosan eljut az Ügyfélhez.
Képviselési jog	Teljes vagy részleges képviselési jog vagy ekként is értelmezhető jogviszony (lásd DÁP).
Kiadó	Szolgáltató tanúsítványokat kibocsátó műszaki rendszere. Szolgáltatónál létezik végfelhasználói és egyes szolgáltatói tanúsítványokat kibocsátó Köztes Kiadó, valamint az ezen egységeket hitelesítő legfelső szintű Gyökér Kiadó, amelyek hierarchiába szervezetten működnek.
Kihelyezett Hitelesítő Egység	A Szolgáltatótól független, önálló szervezet vagy személy (mint Szolgáltatói partner) által, a Szolgáltató előírásai alapján működtetett Hitelesítő Egység.
Kihelyezett Regisztrációs Egység	A Szolgáltatótól független, önálló szervezet vagy személy (mint Szolgáltatói partner) által, a Szolgáltató előírásai alapján működtetett Regisztrációs Egység.
Kikötések (és feltételek)	Szolgáltató azon dokumentumai, amelyek ismertetik, hogy a szolgáltatások nyújtásával kapcsolatosan, milyen elvárásoknak, milyen módon felel meg, s ismertetik a többi szereplő kötelezettségeit és jogait. Ide tartozik a Szolgáltató Szolgáltatási kivonata, Hitelesítési rendje, Szolgáltatási szabályzata, ÁSZF-e,

	szolgáltatási szerződése, valamint a közöttük létrejött egyéb megállapodások együttesen.
Kriptográfiai eszköz	Olyan biztonságos hardver eszköz, amely a Végfelhasználó magánkulcsát tartalmazza, azt védi a kompromittálódás ellen, s a kulccsal kriptográfiai műveleteket (pl. aláírás, titkosítás) végez a Végfelhasználó számára. Lehet SCD és QSCD, HSM vagy más nem aláírás célú eszköz is. Lehet a Szolgáltató vagy az Ügyfél kezelésében. Utóbbi esetben "Ügyféleszközként" hivatkozunk rá.
Kritikus szolgáltatások	A Szolgáltató tanúsítvány- és kulcselőállítás, az Ügyfelek eszközzel való ellátásával és az állapotváltoztatással kapcsolatos szolgáltatásai.
Kulcscsere	Az a folyamat, amikor a Szolgáltató egy már regisztrált Ügyfél (vagy saját maga) részére bocsát ki új Tanúsítványt és magánkulcsot, annak egy már létező tanúsítványát alapul véve. Az új tanúsítványban a végfelhasználó nyilvános kulcsa megváltozik. Lásd a 4.7 fejezet.
Kulcsletét szolgáltatás	Olyan szolgáltatás, amely a végfelhasználó magánkulcsának megőrzését és annak végfelhasználó számára történő átadását biztosítja (arra az esetre, ha a végfelhasználó kulcs elveszne, megsemmisülne vagy más okból használhatatlanná válna).
Magánkulcs	A szolgáltató vagy ügyfél által generált kulcspár egyik kulcsa, amit végfelhasználó kezel. Lásd nyilvános kulcs. Amennyiben a nyilvános kulcs aláíró vagy bélyegző tanúsítványba kerül, akkor megfelel az eIDAS elektronikus aláírás létrehozásához használt adat és elektronikus bélyegző létrehozásához használt adatok definíciójának.
Minősített Aláírás / Bélyegző Létrehozó eszköz	Olyan kriptográfiai eszköz, amely minősített aláírás / bélyegző létrehozására alkalmas (lásd még 1.6.2. Rövidítések, QSCD).
Minősített tanúsítvány	Olyan tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel az eIDAS Annex I, III vagy IV részének vagy a 1999/93/EC direktívának, attól függően, hogy a tanúsítvány kiadásakor melyik volt hatályban.
Minősített weboldal hitelesítő tanúsítvány	Az eIDAS 3. cikk 39. Pontja szerint: "Olyan weboldal-hitelesítő tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel az eIDAS IV. mellékletben megállapított követelményeknek." Olyan minősített tanúsítvány, amely a benne megjelölt weboldalak hitelesítésével biztosítja az oldal látogatóit, hogy a mögött egy valódi és legitim szervezet áll.
Mobil Regisztrációs Munkatárs	Olyan regisztrációs ügyintéző, aki - amennyiben személyes találkozó szükséges - az Igénylő azonosítását - ilyen irányú igénye esetén - az Igénylővel egyeztetett helyen és időben végzi el.
NL Sign szolgáltatás	Biztonságos központi kulcstárolási (menedzselt SCD) és kulcsmenedzsment-szolgáltatás, mely webes felületen keresztül feltöltött dokumentumok

	elektronikus aláírását/bélyegzését (és időbélyegzését) valamint az ily' módon hitelesített dokumentumok aláírásának/bélyegzőjének ellenőrzését teszi lehetővé. Az NL Sign szolgáltatás keretében használható tanúsítványok igénylése és az ehhez szükséges regisztrációs adatok bekérése valamint a tanúsítvány kibocsátását követően annak használatba vétele az NL Sign szolgáltatás webes felületein történik.
Nyilvános kulcs	A szolgáltató vagy ügyfél által generált kulcspár egyik kulcsa, amit szolgáltató az általa létrehozott tanúsítványban helyez el. Lásd magánkulcs.
Permanens azonosító	Olyan azonosító, mely a tanúsítvány birtokosát egyedileg azonosítja. A tanúsítványban történő megvalósítása az RFC 4043 alapján történik. Lehet szolgáltató által képzett, vagy hivatalos nyilvántartásban szereplő egyedi azonosító adat. A szolgáltató által képzett azonosító egy OID, ami két részből áll: a Szolgáltató (1.3.6.1.4.1.3555) és az Ügyfél egyedi azonosítójából, ami ezt követi. Az Ügyfél egyedi azonosítója 5-tel kezdődik, amelyet egy szám követ, ami a következő értékeket veheti fel: • 1,6,8,10: személyes vagy üzleti tanúsítványok esetén, amikor az azonosító a természetes személy adataiból képzett. • 2,7,9,11: szervezeti tanúsítványok esetén, amikor az azonosító a szervezet adataiból képzett. Alkalmazása esetén a tanúsítvány Subject/SerialNumber mezőjébe kerül.
Regisztráció	Kezdeti azonosítási eljárás, amelyet Szolgáltató Igénylő és Előfizető személyazonosságának megállapítására, eljárási joguk ellenőrzésére, valamint adatainak felvételére végez.
Regisztrációs egység	A Szolgáltató azon egysége, amely a szolgáltatások igénylésének feldolgozását, az Igénylő és Előfizető regisztrációját, valamint tanúsítványszolgáltatás esetén a tanúsítványba kerülő adatok ellenőrzését végzi. Létezhet a Szolgáltatón belül (mint belső szervezeti egység) vagy kívül (Kihelyezett Regisztrációs Egység) egyaránt.
Regisztrációs felelős	Bizalmi munkakör. Lásd az 5.2.1 Bizalmi munkakörök fejezetet.
Regisztrációs megbízott	Olyan Szolgáltatói partner (illetve annak munkatársa), aki Szolgáltató megbízásából Igénylő helyszínén végzi el a tanúsítványkibocsátáshoz kapcsolódó személyazonosítási feladatokat.
Regisztrációs (validációs és visszavonási) ügyintéző	Szolgáltató Regisztrációs egységén belül e munkakörben dolgozó munkatársak feladata a tanúsítványigénylések kezelése és a tanúsítványigénylésben megadott adatok valóságának ellenőrzése (lásd 4.2.1 fejezet) valamint a visszavonási igények feldolgozása és végrehajtása (4.9). Jelen szolgáltatói szerepkör megegyezik a BRG 1.6.1-ben meghatározott „Validation Specialists” fogalmával: az a személy, aki az adatellenőrzési eljárásokat végzi.
SSL tanúsítvány	Weboldal-hitelesítő tanúsítvány

Szabályzatok	Jelen Szolgáltatási Rend és a Szolgáltatási Szabályzat együttes említése.
Szervezet	Tanúsítvány alanya vagy előfizetője tekintetében: jogi személy vagy egyéni vállalkozó vagy egyéni ügyvéd.
Szoftveres tanúsítvány	Olyan tanúsítvány, aminek magánkulcsa nem Kriptográfiai eszközre kerül kiadásra.
Szolgáltatás	Jelen szabályzat keretén belül Szolgáltató szolgáltatásai (lásd 1.1 fejezet).
Szolgáltatási Szabályzat, Szabályzat	Szolgáltatási Szabályzat Nem eIDAS Tanúsítványszolgáltatásokra c. dokumentum. A szolgáltató nyilatkozata az egyes tanúsítványszolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről, mely Szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmaz, a jelen Szolgáltatási Rend alapján.
Szolgáltatási szerződés	Szolgáltató és Ügyfél között létrejött szerződés, amely a szolgáltatás nyújtására és igénybevételére vonatkozó feltételeket tartalmazza. Megkötése a szolgáltatás igénybevételének előfeltétele.
Szolgáltató	Jelen Szolgáltatási Rend szerinti szolgáltatásokat nyújtó NETLOCK.
Szolgáltató szabályzatai	Jelen Szolgáltatási Rend, a Szolgáltatási Szabályzat, az ÁSZF, a szolgáltatási szerződés, a Szolgáltatási kivonat. Valamint egyéb nem nyilvános szabályzatok.
Szolgáltatói partner	Olyan a szolgáltatótól független, önálló természetes vagy jogi személyek, amelyek a Szolgáltatóval való megállapodás alapján a Szolgáltatás nyújtásában részt vesznek.
Szolgáltatói rendszer	Szolgáltató szolgáltatásnyújtást végző rendszereinek együttese.
Szolgáltatói tanúsítvány	Szolgáltató azon tanúsítványai, amelyeket a szolgáltatásnyújtás érdekében használ (pl. Kiadók és Időbélyegző Kiszolgálók tanúsítványai).
Tanúsítvány	Szolgáltató által kibocsátott hiteles igazolás, amely a nyilvános kulcsot az Alanyhoz kapcsolja, és igazolja e Tanúsítványban közzétett adatok valóságát.
Tanúsítványaktiválás	Az az állapotváltoztatási eljárás, amely felfüggesztett tanúsítvány érvényességét visszaállítja. Aktiválása után a tanúsítvány visszamenőlegesen, azaz a felfüggesztés időtartamára is újra érvényessé válik, mintha a felfüggesztés meg sem történt volna..
Tanúsítványállapot	A szolgáltató által a tanúsítványok érvényességi ideje alatt nyilvántartott érvényes / visszavont / felfüggesztett státusza, amelyről a tanúsítványvisszavonási listán és a Tanúsítványállapot szolgáltatáson keresztül ad tájékoztatást Ügyfelei és az Érintett felek részére.

Tanúsítványállapot-szolgáltatás (OCSP)	Olyan szolgáltatás, ami egy adott tanúsítvány állapotáról ad valós idejű információt az érintett felek számára. Lásd még: tanúsítványvisszavonási lista.
Tanúsítványfelfüggesztés	Az az állapotváltoztatási eljárás, amelyben a Szolgáltató egy még érvényes Tanúsítvány érvényességét átmenetileg megszünteti az eredetileg tervezett érvényességi idő vége előtt. A tanúsítványfelfüggesztés egy átmeneti állapot, a felfüggesztett Tanúsítvány visszavonható, vagy a Tanúsítvány eredeti érvényességi idejében újra érvényessé tehető. A felfüggesztés visszavonása esetén a Tanúsítvány visszamenőleges hatállyal érvényessé válik, mintha a felfüggesztés meg sem történt volna.
Tanúsítványigénylés	Az a folyamat, amikor Igénylő tanúsítványt igényel, azaz a tanúsítvány elkészítéséhez szükséges adatokat megadja és igazolja a Szolgáltatónak, végül pedig Szolgáltatási szerződés Igénylő és - amennyiben nem egyezik Igénylővel - Előfizető általi aláírásával hitelesíti kérelmét az igényelt tanúsítványra vonatkozóan és ezzel felhatalmazza Szolgáltatót az igényelt tanúsítvány kibocsátására.
Tanúsítványkezelési eljárás	Olyan eljárás, ami új tanúsítvány kibocsátását eredményezi egy meglévő tanúsítvány illetve korábbi ügyfél-regisztráció adatai alapján (lásd 3.3 Azonosítás és hitelesítés tanúsítványkezelési eljárás során és 4. Életciklus követelmények fejezeteket).
Tanúsítványszolgáltatás	Szolgáltató azon szolgáltatása, amelynek keretén belül új tanúsítványt állít elő. Ez történhet egy már létező tanúsítvány alapján (követő kibocsátás tanúsítványkezelési eljárással) vagy ilyen előzmények nélkül (eredeti kibocsátás).
Tanúsítványmegújítás	Az a folyamat, amikor a Szolgáltató ugyanarra a nyilvános kulcsra, változatlan Alannyal egy új Tanúsítványt állít ki, új érvényességi időszakra. Lásd a 4.6 fejezet.
Tanúsítványmódosítás	Az a folyamat, amikor a Szolgáltató egy már regisztrált Igénylő részére bocsát ki új Tanúsítványt egy korábban kibocsátott Tanúsítványa alapján, az abban szereplő nyilvános kulccsal, de megváltozott Alany vagy Szolgáltató adatokkal. Lásd a 4.8 fejezet.
Tanúsítványtár	Szolgáltató kibocsátott tanúsítványokat tartalmazó nyilvántartása, amelyen keresztül lekérdezhetők a szolgáltató által kiadott nyilvános tanúsítványok és a Tanúsítványvisszavonási lista.
Tanúsítványtípus	Szolgáltató által kibocsátott különböző tanúsítványok megkülönböztetése valamilyen jellemző szerint, legfőképpen a felhasználási cél alapján. Lásd a Szolgáltatási szabályzat 1.2.1 pontját.
Tanúsítvány-visszavonás	Az az állapotváltoztatási eljárás, amelyben a Szolgáltató a tanúsítvány érvényességét megszünteti az eredetileg tervezett érvényességi idő lejártá előtt. A tanúsítvány-visszavonás visszafordíthatatlan és végleges állapotváltozást jelent, a visszavont tanúsítvány a visszavonás időpontjában érvényességét veszti, s már soha többé nem lehet újra érvényes.
Tanúsítványvisszavonási lista	Szolgáltató által rendszeres időközönként, valamint állapotváltozások

(CRL)	hatására a Tanúsítványtárban közzétett hiteles lista azon tanúsítványokról, amelyek ideiglenesen vagy véglegesen nem érvényesek. A listán szereplő tanúsítványok elfogadása, illetve alkalmazása nem ajánlott. A 24/2016. BM rendelet 17. szerinti visszavonási nyilvántartás egy fajtája.
Teszttanúsítvány	A Szolgáltató által tesztelési célra kibocsátott tanúsítvány, ami tartalmában valamely valódi tanúsítvánnyal egyezik meg, de hitelesítési rend mezője és az Alany elnevezése jelzi a felhasználás teszt voltát. Az ilyen tanúsítványok köztelezésékvállalásra nem használhatók, joghatás nem kapcsolódik hozzájuk, elfogadásuk csak tesztelési céllal lehetséges. Szolgáltató nem vállal felelősséget az ilyen tanúsítványok adattartalma, felhasználása, és a hozzájuk kapcsolódó szolgáltatások rendelkezésre állása tekintetében.
UCC weboldal-hitelesítő tanúsítvány	Olyan weboldal-hitelesítő tanúsítvány, melyben több különböző domain név kerül feltüntetésre (a SubjectAltName/DNSname mezőben).
Ügyfélmenü	A Szolgáltató ügyfelei számára a tanúsítványokkal és hozzájuk kapcsolódó szolgáltatásokkal kapcsolatos különböző igénylések elvégzésére illetve a folyamatban lévő igénylések állapotának megtekintésére biztosított, a Szolgáltató weboldalán keresztül elérhető felület, melybe egyedi felhasználónév és jelszó megadásával lehet belépni (ügyfélmenü regisztrációt követően). A minősített tanúsítványok kezeléséhez a minősített ügyfélmenübe, a nem-minősített tanúsítványok kezeléséhez a fokozott biztonságú ügyfélmenübe kell regisztrálni és bejelentkezni.
Ügyfélmenü regisztráció	Az a folyamat, amikor egy természetes vagy jogi személy adatai megadásával létrehozza saját Ügyfélmenüjét, illetve az Ügyfélmenübe való bejelentkezéshez szükséges bejelentkező nevét és jelszavát.
Ügyfél	A Szolgáltatóval szerződést kötő fél. Tanúsítványszolgáltatás esetén a tanúsítvány Igénylője és Előfizetője (adott esetben ezek a szereplők meg is egyeznek). NL Sign szolgáltatás esetén az Aláírói Partner és a Végfelhasználó. Lásd még az 1.3.3 Előfizető, Végfelhasználó és Igénylő fejezetet
Ügyféleszköz	Az Ügyfél kezelésében lévő Kriptográfiai eszköz. Ügyféleszköz kizárólag a Szolgáltató által beszerzett, ellenőrzött és az Ügyfél rendelkezésére bocsátott, a Szabályzat 6.2.1 pontjában meghatározott Kriptográfiai eszköz lehet.
Ügyfél-regisztráció	Természetes és nem természetes személyek azonosítása, adataik ellenőrzése és rögzítése az első szolgáltatási szerződés és az első tanúsítványkibocsátás megelőzően. Lásd a 3.2 Kezdeti azonosítás fejezetet.
Végfelhasználó	Az a természetes személy, aki a tanúsítványban szereplő nyilvános kulcs magánkulcs párja felett rendelkezik (kizárólagosan használja vagy a használatáért felelős). NL Sign szolgáltatás esetén az a személy, aki az aláírási szolgáltatás keretén belül a magánkulcsa aktiválásával elektronikus aláírási/bélyegző műveletet hajt végre vagy aki elektronikus aláírás/bélyegző ellenőrzést végez, illetve aki

	e műveletekért felelős. Lásd még az Ügyfél és Előfizető entitásokat, valamint az 1.3.3 Előfizető, Végfelhasználó és Igénylő fejezetet
Végfelhasználói tanúsítvány, Végfelhasználói kulcs	Az Előfizetők tanúsítványát és kulcsát jelöli, megkülönböztetve a Szolgáltató saját tanúsítványaitól és kulcsaitól.
Weboldal-hitelesítő tanúsítvány	Az eIDAS 3. cikk 38. pontja szerinti tanúsítvány.
Wildcard weboldal-hitelesítő tanúsítvány	Olyan weboldal-hitelesítő tanúsítvány, melyet több aldomain hitelesítésére bocsátott ki szolgáltató (a domain név *.domain.hu formában kerül feltüntetésre, így magában foglalja a domain.hu cím alá tartozó valamennyi aldomaint).

1.6.2 Rövidítések

Hivatkozott jogszabályok rövidítései

eIDAS	Az Európai Parlament és Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről.
DÁP	A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény.
Nyvtv.	A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény.
Szmtv.	2007. évi I. törvény a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról.
Harmtv.	2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló törvény
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
24/2016 BM rendelet	A bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI. 30.) BM rendelet.

Műszaki szakkifejezések rövidítései

ASN.1	Abstract Syntax Notation 1
CA	Certification Authority Kiadó
CAA	Certification Authority Authorization Bizalmi szolgáltató Felhatalmazás
IP	Internet Protocol
IT	Information Technology
BRG	Baseline Requirements Guidelines
CAB Forum	CA/Browser Forum
CP	Certificate Policy Hitelesítési Rend
CPS	Certification Practice Statement
CRL	Certificate Revocation List Tanúsítványvisszavonási lista
CSP	Certification Service Provider
EAL	Evaluation Assurance Level
EV	Extended Validation
EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
FQDN	Fully qualified domain name
gTLD	Generic top-level domain
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
OCSP	Online Certificate Status Protocol Tanúsítványállapot-szolgáltatás
OID	Object Identifier Azonosító

OVC	Organizational Validation Certificate
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SAN SubjectAltName	Subject Alternative Name
SCD	Signature / Seal Creation Device Aláírás / Bélyegző Létrehozó eszköz (Nem-minősített)
SSL	Secure Socket Layer
TLS	Transport Layer Security
TSP	Trust Service Provider Bizalmi Szolgáltató
QSCD (korábbi nevén SSCD)	Qualified Signature / Seal Creation Device Minősített Aláírás / Bélyegző Létrehozó eszköz
UN	United Nations
IETF	Internet Engineering Task Force
QC	Qualified Certificate
URL	Uniform Resource Locator

Lásd még a dokumentum 9.15 pontjában foglaltakat.

2. KÖZZÉTÉTELRE ÉS TANÚSÍTVÁNYTÁRRÁ VONATKOZÓ FELELŐSSÉGEK

Szolgáltató köteles a tanúsítványokra vonatkozó különböző információk (szabályzatok, tanúsítványok, érvényességi információk, s az ezeket nyilvánosságra hozó szervezetek - ha eltér a szolgáltatótól) nyilvánosságra hozatalára vonatkozó adatokat a szabályzatában ismertetni, és ezt a szabályzatot közzé tenni.

2.1 Adattárak

Szolgáltatónak nyilvános tanúsítványtárat és tanúsítvány visszavonási információkat (CRL, OCSP) közlő rendszereket kell fenntartania, valamint biztosítania kell, hogy a weboldalon folyamatosan elérhetők és olvashatók legyenek a jelen Szolgáltatási Rend szerint kibocsátható tanúsítványokhoz kapcsolódó Kikötések és feltételek.

Szolgáltatónak garantálnia kell, hogy szolgáltatói tanúsítványait, a nyilvános tanúsítványtárat és a visszavonási információkat közzétevő rendszerek rendelkezésre állása éves szinten legalább 99% -os legyen, az eseti szolgáltatás kiesés hossza pedig egyszer legfeljebb 3 óra legyen.

2.1.1. A tanúsítványokra vonatkozó információk közzététele

Amennyiben az Előfizető hozzájárult, Szolgáltató köteles a végfelhasználói tanúsítvány alany adatait nyilvános tanúsítványtárában közzétenni.

Szolgáltató köteles a tanúsítványtárat folyamatosan naprakészen tartani.

A Szolgáltató köteles az általa kibocsátott tanúsítványokról, különösen azok állapotáról szóló információkat közzétenni az Ügyfelek és Érintett felek számára - így különösen:

- Szolgáltatónak a Végfelhasználó rendelkezésre kell bocsátania az igényelt teljes végfelhasználói tanúsítványt, annak előállítását követően.
- A végfelhasználói tanúsítványok csak akkor publikálhatók, amennyiben a végfelhasználó ehhez hozzájárul.
- Szolgáltatónak a tanúsítvány használatával kapcsolatos kikötéseket és feltételeket az érintett felek számára elérhetővé kell tennie nyilvánosan és nemzetközi szinten;
- Az egyes tanúsítványtípusok kapcsán alkalmazandó eltérő kikötéseknek és feltételeknek jól azonosíthatónak kell lenniük;
- A publikált tanúsítványokat és a kikötéseket Szolgáltatónak folyamatosan elérhetővé kell tennie. Szolgáltatónak mindent meg kell tennie annak érdekében, hogy ezek az információk ne legyenek hosszabb ideig elérhetetlenek, mint ahogy azt a szolgáltatási szabályzatában jelezte.
- A tesztelési célokra Szolgáltató biztosít visszavont, lejárt és érvényes weboldal-hitelesítő tanúsítványokat.

Szolgáltatónak a tanúsítványállapot-információk közlésére jelen szolgáltatási rend előírásainak megfelelő Visszavonáslista-szolgáltatást (CRL) és Online Tanúsítványállapot-

szolgáltatást (OCSP) kell fenntartania.

2.1.2 Kikötések és feltételek közzététele

A jelen Szolgáltatási rendet és az ez alapján készült szolgáltatási szabályzatot – a szükséges Szolgáltatóra specifikus eltérésektől eltekintve – az RFC 3647 szerinti tartalommal és struktúrában kell közzétenni. A szolgáltatási szabályzat 4.2. fejezetének tartalmaznia kell, hogy a Szolgáltató a CAA Rekordokat felülvizsgálja-e, és ha igen, akkor milyen eljárással dolgozza fel a domain neveket. Szolgáltatónak e tevékenységét - ha végez ilyet - naplózni kell. A szolgáltatási szabályzatnak tartalmaznia kell a BRG¹ és EV nyilatkozatokat² amennyiben értelmezettek.

Szolgáltatónak weboldalán (lásd 1.1.2) legalább a hatálybalépése előtt publikálnia kell a Szolgáltatási Rend és a Szolgáltatási Szabályzat valamint jelen Szolgáltatási rend szerinti szolgáltatásokra vonatkozó más nyilvános dokumentumok bevezetésre váró új verzióit. Szolgáltatónak gondoskodnia kell róla, hogy a hatályos kikötéseken és feltételeken túl a dokumentumok azon korábbi verziói is elérhetők legyenek, melyek alapján kibocsátott tanúsítvány még érvényben van.

Szolgáltatónak a szolgáltatási szerződés megkötését követően tartós adathordozón Ügyfél rendelkezésére kell bocsátania vonatkozó szolgáltatási szabályzatot és a Szolgáltatási szerződést.

2.2 Közzététel időpontja és gyakorisága

Szolgáltatónak a Kikötéseket és feltételeket, illetve azok újabb verzióit weboldalán (lásd 1.1.2) a hatálybalépés előtt publikálnia kell. Szolgáltatónak gondoskodnia kell róla, hogy a hatályos kikötéseken és feltételeken túl a dokumentumok azon korábbi verziói is folyamatosan elérhetők legyenek, melyek alapján kibocsátott tanúsítvány még érvényben van.

A szolgáltatónak legalább évente felül kell vizsgálnia a Szolgáltatási Rendjét és szabályzatait, szükség esetén módosítva azokat (lásd 9.12).

2.3 Tanúsítványtár elérésének szabályai

Szolgáltatónak biztosítania kell a nyilvános tanúsítványtár, a tanúsítványállapot-szolgáltatás valamint Kikötések és feltételek nyilvános elérhetőségét - olvasási jogosultsággal.

E szolgáltatásokat, adattárakat és információkat Szolgáltatónak korlátozás nélkül kell hozzáférhetővé tennie az Ügyfelek és Érintett felek számára. Túlzott használat esetén azonban szolgáltatásvédelmi okokból Szolgáltató átmenetileg korlátozhatja a hozzáféréseket. A korlátozások feltételei közzétételre kerülnek a Szolgáltató weboldalán.

¹ <https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.4.4.pdf> (2.2 fejezet)

² https://cabforum.org/wp-content/uploads/EV-V1_6_2.pdf (8.3 fejezet)

3 AZONOSÍTÁS ÉS HITELESÍTÉS

Szolgáltatónak a tanúsítványszolgáltatások igénybevételével kapcsolatos azonosítási és hitelesítési eljárásokat az alábbi fejezetekben foglalt előírásoknak megfelelően kell elvégeznie, az eljárásokat pedig ismertetnie kell a Szolgáltatási Szabályzat 3. pontjában.

3.1 Elnevezések

A tanúsítvány Kibocsátó azonosító (Issuer) és Alany azonosító (Subject) mezői feleljenek meg az ITU-T X.509, RFC 5280 és az ETSI EN 319 412 ajánlások név formátum előírásainak. A kibocsátó és Alany azonosító mezők értelmezését Szolgáltató a Szolgáltatási Szabályzatban közli.

3.1.1. Névtípusok

Szolgáltatónak a tanúsítványok Subject mezőjének képzése esetében az RFC 5280 szabványnak megfelelően az X.500 distinguished name előírásait kell követni (email címek esetén az RFC-822 előírásait). Ezen belül többfajta névtípust különböztethet meg a végfelhasználói tanúsítványok esetén.

Szolgáltatónak a szolgáltatási szabályzat 3.1. pontjában kell részletesen közzétennie a jelen Szolgáltatási Rend szerint kibocsátott tanúsítványok esetében alkalmazott konkrét névtípusokat, azok értelmezhetőségét és az értelmezhetőségi szabályokat illetve egyéb vonatkozó információkat pl. a tanúsítvány alany- és kibocsátó azonosítójáról.

3.1.2. A nevek értelmezhetősége

Természetes személyek számára kibocsátott tanúsítvány Subject mezőjének a következő adatokat kell tartalmaznia:

- countryName (Országkód);
- givenName+surname vagy pseudonym (Vezeték és Családnév vagy Álnév)
- commonName (Név)
- serialNumber (Alany egyedi azonosítója)

Jogi személyek számára kibocsátott tanúsítvány Subject mezőjének a következő adatokat tartalmaznia kell:

- countryName (Országkód);
- commonName (Név)
- organizationIdentifier (szervezetazonosító)

Amennyiben a tanúsítvány Alanyaként kizárólag jogi személy kerül feltüntetésre, Szolgáltatónak fel kell tüntetnie a szervezet egyedi azonosítóját a tanúsítvány Subject/organizationIdentifier mezőjében.

Amennyiben a tanúsítvány Alanyaként természetes személy és szervezet egyaránt feltüntetésre kerül, a Szolgáltató a szolgáltatási szabályzatban határozza meg, hogy mely esetekben tünteti fel ezt kötelező jelleggel.

A weboldal-hitelesítő (DVCP) tanúsítványok SAN mezőjének tartalmaznia kell a commonName mezőben feltüntetett domain nevet.

A fenti kötelező mezőkből csak egyet szabad feltüntetni.

A tanúsítványban szereplő természetes személy és szervezet nevét közhiteles nyilvántartásban, annak hiányában más megbízható adatforrásban, hivatalos azonosító dokumentumban, vagy az alapító okiratban szereplő írásmóddal kell feltüntetni.

A teszttanúsítványok Subject mezője felveheti bármely a Szolgáltató által kibocsátott tanúsítvány formáját, de a commonName mezőben minden esetben jól látható, egyértelmű módon jelölni kell a teszt jelleget, ügyelve arra, hogy az tartalmában ne lehessen megtévesztő, s valódi személlyel összekeverhető.

A Subject/organizationIdentifier mezőben egy hivatalos nemzeti vagy más azonosító rendszerben kapott egyedi azonosító szerepelhet kötött formátumban, amelyet az ETSI EN 319 412-1 5.1.4 definiál (*REFCO-szervezetazonosító* formában szerepel, ahol a REF és CO helyére három és két karakter kerül az alábbiak szerint).

Kitöltése:

1. Ha a szervezet rendelkezik adószámmal, az alapján kell kitölteni a mezőt: magyar adószám esetén "VATHU", EU-s adószám esetében "VATEU" értékkel.
2. Ha előző pont nem alkalmazható, akkor Cégjegyzékszám "NTRHU" értékkel.
3. Ha előző pontok nem alkalmazhatók, akkor nemzeti bejegyzett séma alapján "XX:HU" értékkel, amelyben az „XX” a nemzeti vagy EU-s azonosítási séma két karakteres jelölése.
4. Ha előző pontok nem alkalmazhatók, akkor más egyedi hivatalos azonosító is alkalmazható.
5. Ha egyik említett azonosító sem áll rendelkezésre, az alapító okirat azonosítója és az alapító jogszabály megnevezése is kerülhet ide.

Más országok azonosító rendszerei esetében az ISO 3166 szerinti országkód alkalmazandó a HU országkód helyett.

Amennyiben Subject/Serialnumber mező tartalma egy hivatalos (okmány alapján ellenőrzött) nemzeti azonosító, Szolgáltató azt is a fenti szabványos formátumban tölti ki. A mező az útleveél, személyi igazolvány, jogosítvány, adószám és más, egyedi azonosítórendszerek alapján kerülhet kitöltésre, az ETSI EN 319 412-1 5.1.3-nak megfelelően.

Ezek szerint, amennyiben nemzeti azonosító kerül feltüntetésre, annak kötelező formátuma: <REF>HU-<igazolványszám>, ahol a <REF> helyére három karakter kerül a következők szerint:

- "PAS" útleveél szám esetében
- "IDC" személyi igazolvány vagy jogosítvány számának esetén
- "TIN" adóazonosító jel esetében

Egyedi azonosítórendszerek esetén Szolgáltató szintén a szabvány szerinti formát használja, ahol a <REF> helyére „XX:” formátumú karaktersorozat kerül, amelyben az „XX” a nemzeti vagy EU-s azonosítási séma két karakteres jelölése.

Amennyiben a további serialnumber mező nem a fenti igazolványok alapján kerül kitöltésre,

formai előírás nincs, kivéve a külön tárgyalt eseteket.

3.1.3. Álnevek

A szolgáltató természetes személyek részére kiadhat álneves tanúsítványt is. Igénylőnek rendelkeznie kell az Előfizető hozzájárulásával az alkalmazott Álnévhez. Álneves Tanúsítvány esetén a "Common Name" és "Pseudonym" mezők megegyező módon tartalmazzák az álnevet. A Szolgáltató az egyes személyeket vagy csoportokat esetlegesen sértő (pl. jóízlést, szemérmét, etnikai hovatartozást sértő) vagy megtévesztő álnevek és egyéb adatok alkalmazását elutasíthatja.

3.1.4. A különböző elnevezési formák értelmezési szabályai

Az azonosítók értelmezése tekintetében a jelen dokumentumban leírtak alapján kell eljárni. A Kibocsátó és Alany megkülönböztető név mezőket (Distinguished Name) az X.500 szabvány és az ASN.1 szintaxis szerint kell értelmezni (lásd RFC 2253 and RFC 2616).

A Szolgáltató által természetes személyek számára kibocsátott tanúsítványoknak nem célja, hogy az Alanyaként megjelölt személyt a tanúsítványban feltüntetett adatok alapján azonosítani lehessen. Természetes személyeknek kiadott olyan tanúsítványok esetén, amelyben szervezet is megjelenítésre került, nem cél, hogy a természetes személy szervezettel való viszonyát vagy képviseleti jogosultságát a tanúsítvány igazolja – kivéve, ha a tanúsítvány egy kifejezetten erre vonatkozó – a szolgáltatási szabályzatban részletezett jelölést tartalmaz.

Amennyiben a tanúsítványban foglalt bármely adat értelmezésével kapcsolatban az Érintett félnek segítségre lenne szüksége, akkor a Szolgáltatóval közvetlenül is felveheti a kapcsolatot. A Szolgáltató ilyen esetben az Ügyfél egyéb adatairól többlet tájékoztatást – feltéve, hogy jogszabály ezt nem írja elő – nem adhat, csak a Tanúsítványban feltüntetett adatok értelmezését segítő információkat szolgáltatathat.

3.1.5. A nevek egyedisége

A Szolgáltató tanúsítványtárában minden Alanynak egyedi névvel (Subject mező) kell rendelkeznie, hogy egyértelműen azonosítható legyen. Ennek érdekében a Szolgáltató minden személynek egy, a Szolgáltató nyilvántartásában egyedi alanyazonosítót (OID alapú permanentID) kell adjon, melyet köteles szerepeltetni a tanúsítvány Subject/Serialnumber mezőjében (ha az Alany egy személy). Ez az azonosító egyedien azonosítsa a tanúsítványban szereplő természetes személyt vagy annak hiányában a benne szereplő jogi személyt, azonban egy ügyfélnek lehessen több azonosítója is. Ezt az azonosítót soha nem kaphatja meg egy másik természetes vagy jogi személy.

Az egyediség az álneves tanúsítványok esetében is biztosított, bár a permanens azonosító el fog térni az ügydél által használt hasonló nem álneves tanúsítványokétól.

A Szolgáltató e mellett egy további Subject/Serialnumber mezőben más egyedi azonosítót (pl. személyi igazolvány szám, adószám, szervezeten belüli azonosító) is feltüntethet.

Lásd még 3.1.2.

3.1.6. Védjegyek elismerése, azonosítása, szerepük

Szervezetek részére kiállított tanúsítványokban feltüntethető az Ügyfél birtokában lévő DBA vagy Trademark vagy terméknév és termékazonosító is. Ez szerepelhet a Subject/CN mezőben vagy a subjectAltName/dirname mezőben.

Az adatok ellenőrzésére vonatkozó előírásokat lásd a 3.2.2 fejezetben.

3.2. Kezdeti azonosítás

A végfelhasználói nem eIDAS tanúsítványok kibocsátásához kapcsolódó, Szolgáltatási Szabályzatban részletezett ügyfél-regisztrációs (azonosítási és hitelesítési) eljárásoknak meg kell felelniük az ETSI 319411-1 szabványban foglaltaknak.

Amennyiben a Szolgáltató még nem ellenőrizte - a 3.3 fejezetben megadott esetektől eltekintve - jelen kezdeti azonosítási eljárással ellenőriznie kell

1. az Igénylő és - amennyiben eltér - Előfizető képviselőjének, meghatalmazójának személyazonosságát (lásd 3.2.3);
2. Igénylő és Előfizető képviselőjének, jogosultságát a képviseletre (lásd 3.2.5);
3. azon adatok valóságát, érvényességét és jogos használatát, amiket Igénylő a tanúsítvány Alanyaként fel kíván tüntetni, illetve
4. amelyeket Igénylőről (mint Végfelhasználóról) és Előfizetőről el kíván tárolni (lásd 3.2.2, 3.2.3 és 3.2.5);
5. és a tanúsítványba foglalandó nyilvános kulcs magánkulcs párjának birtoklását (lásd 3.2.1).

Az 1.-5. pontokhoz: Szolgáltatónak az ellenőrzéshez olyan érvényes hivatalos okmányokat, dokumentumokat és/vagy megbízható adatforrásokat kell felhasználnia, amelyek kellő biztonsággal igazolják az adatok valóságát és érvényességét.

A 3. ponthoz: Ha a tanúsítvány Alanya nem természetes személy, a Szolgáltatónak legalább az Alany tanúsítványba foglalt teljes nevét és egyedi azonosító adatát kell ellenőrizni. Ha a tanúsítvány Alanya Magyarországon bejegyzett személy, Szolgáltatónak ezen adatok valóságát és hatályosságát megbízható nyilvántartás tartalma alapján, vagy ha ilyen megbízható nyilvántartás nincsen, a bejegyzést igazoló közokirat alapján kell ellenőrizni.

Amennyiben az azonosítás technikai (domain kontroll ellenőrzése), a tanúsítványba foglalt hitelesítés rend ez esetben felveheti a DVCP értéket (ekkor sem személyes, sem szervezeti adatot nem tartalmaz a tanúsítvány).

Amennyiben az azonosítás személyes találkozás útján történik, a tanúsítványba foglalt hitelesítés rend ez esetben felveheti az NCP, NCP+, kódalírás értékeket.

Amennyiben az azonosítás NEM személyes találkozás útján történik, a tanúsítványba foglalt hitelesítés rend ez esetben felveheti az LCP, kódalírás értékeket.

Az ellenőrzés során alapelv:

- a tanúsítványban feltüntetett tények ellenőrzése megbízható adatforrás alapján szükséges;
- az ellenőrzésnek nem kell közhiteles adatbázison alapulnia;

- a szolgáltató dönthet úgy, hogy a fentiek ellenére egyes adatokat közhiteles adatbázisban ellenőriz.

A Szolgáltató az NCP, NCP+ és LCP tanúsítványba foglalandó adatokat köteles ellenőrizni, így különösen:

- az Alanyként feltüntetésre kerülő (természetes és/vagy jogi) személy azonosságát,
- a személyazonosság megállapításához használt azonosító adatok valódiságát és - ha elérhető - közhiteles vagy más megbízható központi nyilvántartásban foglalt adatokkal való megegyezőségét,
- az Igénylő eljárási jogosultságát,
- a tanúsítványba foglalandó képviseleti jog meglétét (jogszabály, közhiteles nyilvántartás, létesítő okirat vagy ezek hiányában meghatalmazás alapján),
- a tanúsítványba foglalandó szervezeti egység létezését,
- a tanúsítványba foglalandó szabályozott szakma megnevezése esetén az annak gyakorlására való jogosultságot.

A Szolgáltató a DVCP tanúsítványba foglalandó adatokat köteles ellenőrizni, így különösen:

- a tanúsítvány által igazolt címtartomány (domain) fölötti rendelkezési jogot, képességet
- a tanúsítványban feltüntetendő IP-cím fölötti rendelkezési jogot, képességet

Mielőtt Szolgáltató bármilyen adatforrást megbízható adatforrásként kezd el alkalmazni, értékelnie kell annak megbízhatóságát, pontosságát, és a módosításnak vagy hamisításnak való ellenállását. Szolgáltatónak figyelembe kell venni a következőket az értékelése során:

1. A biztosított információk származási ideje,
2. Az információforrás frissítési gyakorisága,
3. Az adatszolgáltató és az adatgyűjtés célja,
4. Az adatok nyilvános elérhetősége,
5. Az adatok meghamisításának vagy megváltoztatásának relatív nehézsége.

Szolgáltató (vagy tulajdonosa, leányvállalata) által fenntartott adatbázis nem minősül megbízható adatforrásnak, ha az elsődleges célja jelen hitelesítési követelmények teljesítése céljából való információgyűjtés.

A jelen Szolgáltatási Rend alapján készülő szolgáltatási szabályzatnak minden gyakorlati szabályt tartalmaznia kell, melyek a jelen (3.2) fejezetben részletezett elvárásoknak való megfelelést garantálják, s melyek alapján a Szolgáltató szervezeti Egységei saját belső működési szabályzataikat kialakíthatják.

3.2.1. A magánkulcs birtoklásának igazolása

A végfelhasználói tanúsítvány kibocsátása előtt Szolgáltatónak biztosítania kell illetve meg kell győződnie arról, hogy az Igénylő (Végfelhasználó) valóban birtokolja és ellenőrzése alatt tartja az igénylés során a tanúsítványhoz generált kulcspár magánkulcsát. Ennek módját a Szolgáltatónak szolgáltatási szabályzatban kell rögzítenie.

Amennyiben a végfelhasználói magánkulcsot egy harmadik fél generálja és kezeli, Szolgáltatónak kötelessége meggyőződnie arról, hogy a magánkulcs, melynek nyilvános kulcsával tanúsítványt készül kibocsátani valóban az Igénylő által jelzett harmadik fél

kezelésében van, és Előfizető kizárólagos befolyása alatt áll, a kulcskezelési eljárás pedig megfelel a jelen Szolgáltatási Rend követelményeinek és az ezen alapuló szolgáltatási szabályzatban megfogalmazott egyéb szabálynak.

Amennyiben nem a Szolgáltató generálja a végfelhasználói kulcspárt, akkor Szolgáltatónak egyértelmű bizonyíték útján meg kell győződnie arról, hogy a számára átadott nyilvános kulcshoz tartozó magánkulcsot az Ügyfél birtokolja.

Amennyiben a végfelhasználói kulcspárt Szolgáltató generálta, a magánkulcs Átvevőjét Szolgáltatónak azonosítani kell és átvételi jogosultságát meg kell állapítania (lásd 3.2.3), majd az átadást dokumentálnia kell.

3.2.2. Szervezet azonosságának hitelesítése

Amennyiben a tanúsítvány Alanyaként (a Subject vagy SubjectAltname mezőkben) nem természetes személy adatai feltüntetésre kerülnek, akkor a tanúsítvány kibocsátása előtt Szolgáltatónak azonosítania és ellenőriznie kell az adatait, különös tekintettel a tanúsítványban feltüntetendő teljes nevére és egyedi azonosítójára. Igénylőnek rendelkeznie kell a szervezet nevében való eljárási jogosultsággal (lásd 3.2.5 fejezet).

A nem természetes személyek tanúsítványban feltüntetendő teljes nevének és egyedi azonosítójának ellenőrzésére Szolgáltatónak megbízható nyilvántartást vagy ennek hiányában a bejegyzést és a fenti adatait igazoló közokiratot kell felhasználnia. Amennyiben ezek közül egyik sem elérhető, akkor felhasználható más megbízható adatforrás vagy jogszabály.

Amennyiben a tanúsítvány Alanyaként egy eszköz, rendszer vagy termék neve, illetve azonosítója vagy DBA / Védjegy esetleg más egyedi elnevezés kerül feltüntetésre (önállóan vagy egy természetes vagy jogi személy mellett), akkor a 3.2-ben írtakon túl meg kell győződni arról, hogy az Ügyfél jogosan birtokolja a terméknevet, azonosítót vagy egyedi nevet, és az nem megtévesztő (amennyiben ezek értelmezhetők). Az ellenőrzésnek hivatalos dokumentumon, megbízható adatforráson, vagy a nevet/azonosítót kezelő hivatalos szervvel való egyeztetésen kell alapulni.

3.2.3. Természetes személy azonosságának hitelesítése

Szolgáltatónak az alábbi követelményeknek megfelelően kell a természetes személyek személyazonosságát ellenőriznie.

a. Igénylő személyazonosságának ellenőrzése

Amennyiben az igényelt tanúsítványban egy természetes személy adatai kerülnek feltüntetésre, vagy természetes személy jár el szervezet számára kibocsátandó tanúsítvány igénylésében, a természetes személy, mint Igénylő személyazonosságát Szolgáltatónak ellenőriznie kell.

b. Előfizető képviselője, meghatalmazottja személyazonosságának ellenőrzése

Szolgáltatónak ellenőrizni kell az Előfizető képviselőjének/képviselőinek vagy a képviselő/képviselők meghatalmazottjának személyazonosságát is. Ebben az esetben a személyazonosításhoz nem szükséges személyes találkozás. Szolgáltatónak megbízható adatforrások alapján kell megbizonyosodnia a képviselő vagy meghatalmazott személyazonosságáról.

Amennyiben Igénylő és Előfizető ugyanaz a személy, külön az Előfizetőre vonatkozó személyazonosítást Szolgáltató nem folytat le.

a. Átvevő személyazonosítása

Amennyiben Átvevő és Igénylő eltérő személyek, illetve ha az Igénylés és az Átvétel időben elválik, akkor Átvevőt is azonosítani kell Szolgáltatónak, s meg kell győződnie az átvételi jogosultságáról. Ha az átvétel személyesen, illetve hagyományos kézbesítés útján történik, akkor az azonosításhoz személyazonosság igazolására alkalmas hatósági igazolványt kell igénybe venni, a jogosultságot pedig Igénylő/Előfizető hiteles rendelkezése alapján kell megállapítani. Elektronikus kézbesítés esetén a tanúsítványosztálynak megfelelő szintű, az Igénylőre előírt azonosítási szintnek megfelelő, ill. arra visszavezethető módszert kell alkalmazni.

b. További előírások természetes személyek személyazonosításával kapcsolatban

Amennyiben a tanúsítványban egy természetes személy kerül feltüntetésre, akkor a személyazonosításra felhasznált hiteles okmányok és nyilvántartások adatai alapján meg kell állapítani azon adatait, amelyek a tanúsítványba feltüntetésre kerülnek. Szolgáltatónak továbbá hasonló módon kell megállapítani Igénylő és Előfizető saját nyilvántartásában eltárolt adatait, különös tekintettel az egyértelmű személyazonosító adatokra (pl. név, születési adatok, anyja neve).

Amennyiben a természetes személy egy szervezettel együtt kerül a tanúsítványban feltüntetésre, akkor a szervezet képviselőjének/meghatalmazottjának hiteles igazolása szükséges a szervezet szerepeltetéséhez.

Az Előfizetőnek és Igénylőnek az általuk biztosított adatok valódiságát (kézi vagy elektronikus) aláírásukkal el kell ismerniük. Az elfogadott elektronikus aláírások és bélyegzők körét Szolgáltató korlátozhatja.

A teszttanúsítványok Alanyként (ha a tanúsítvány tartalma alapján egyértelműen jelzésre kerül annak teszt jellege) Szolgáltatónak nem kell valódi természetes vagy jogi személyt feltüntetni, ezért az ilyen (nem létező) Alanyok ellenőrzése értelemszerűen nem elvár.

Igénylő, Átvevő és Előfizető képviselőjének, meghatalmazójának azonosítását, valamint az adatok ellenőrzésére használt információkat (mint pl. dokumentumok típusa, azonosítószáma, érvényességi ideje), valamint az Előfizető eléréséhez szükséges adatokat (pl. postacím, telefonszám) Szolgáltatónak dokumentálnia kell (papír alapú vagy elektronikus evidenciák

rögzítésével). Egyéb, az Előfizető és Igénylő azonosításához és a kapcsolattartáshoz nem szükséges információkat nem tárolhat (az adatkezeléssel kapcsolatosan lásd 9.3 és 9.4 fejezeteket).

A Szolgáltatási szerződés érvényességének időtartama alatt Szolgáltató nem köteles Igénylő és Előfizető képviselőjének/meghatalmazottjának személyes azonosítását újból elvégezni. Amennyiben ezen időintervallumban Igénylő újabb tanúsítványigénylést kezdeményez, Szolgáltató a korábban elvégzett személyazonosítások eredményét az új igényléshez is elfogadja. A tanúsítványba kerülő valamint Igénylő és Előfizető igénylésben résztvevő adatainak pontosságát és valóságát Szolgáltatónak ebben az esetben is ellenőriznie kell.

A szolgáltatási szerződés érvényességének időtartama alatt kezdeményezett tanúsítványigénylés esetén a tanúsítványba kerülő valamint Igénylő és Előfizető igénylésben résztvevő adatainak pontosságát és valóságát Szolgáltató a saját adatbázisában eltárolt adatok alapján is ellenőrizheti, melyek hitelességét az érvényben levő szolgáltatási szerződés megkötését megelőző közhiteles és/vagy (köz)okiratokon alapuló adatellenőrzés adja.

Szolgáltatónak a szolgáltatási szabályzatban részletesen meg kell határozni az egyes általa alkalmazott személyazonosítási és adatellenőrzési módszereket és az ellenőrzési eljárások folyamatát.

Szolgáltatónak a szolgáltatási szabályzatban részletesen meg kell határozni az ellenőrzés folyamatát és biztosítani kell, hogy a regisztráció során az adatok valóságának és pontosságának jelen fejezet szerinti ellenőrzését és annak eredményét a tanúsítvány kibocsátást jóváhagyó munkatárs a jóváhagyás előtt még felülvizsgálhassa. A tanúsítványkiadás jóváhagyását csak olyan személy végezheti, aki a regisztrációs folyamat során az adatok valóságának és pontosságának ellenőrzésében és Igénylő személyazonosításában nem vett részt (lásd 5.2.4).

3.2.4. Nem ellenőrzött alany információk

A Szolgáltató által kibocsátott Tanúsítvány Alanyaként csak olyan adatok kerülhetnek feltüntetésre, amelyeket a Szolgáltató ellenőrzött, vagy amelyek valóságáról az Igénylő, illetve Előfizető írásban, büntetőjogi felelősségének tudatában nyilatkozott.

3.2.5. Jogok, felhatalmazások ellenőrzése

Amennyiben Előfizető nem a saját nevében jár el Szolgáltató előtt (pl. Igénylőként vagy Átvevőként), hanem képviselőn vagy annak meghatalmazottján keresztül, akkor Szolgáltatónak minden esetben egyértelműen azonosítani kell a képviselő/meghatalmazott személyét (lásd 3.2.3) és ellenőriznie kell az Előfizető nevében történő eljárási jogosultságát a Szolgáltató előtt, az adott tanúsítványigénylési, állapotváltoztatási eljárás kapcsán.

A képviseleti jogot hiteles okmánnal vagy megbízható adatbázisban ellenőrizni szükséges.

A meghatalmazó azonosságát és a meghatalmazás hitelességét és érvényességét ellenőrizni szükséges (lásd a 3.2.2 és 3.2.3 pontot is).

Szolgáltatónak a szolgáltatási szabályzatában részletesen meg kell határozni az ellenőrzés folyamatát.

Szolgáltatónak a szolgáltatási szabályzatában lehetőséget kell biztosítania arra, hogy a jogi személy Előfizető saját szervezetén belül kijelölhessen egy vagy több ügyintézőt, aki(k) jogosult(ak) az Előfizető szervezeteéhez köthető tanúsítványigénylést kezdeményezni és az ilyen tanúsítványigénylések kapcsán Előfizető nevében eljárni a szolgáltatási szerződés aláírása, a kiadott tanúsítvány elfogadása, jóváhagyása és kezelése (állapotváltoztatása, megújítása, módosítása stb.) kapcsán. Az ügyintézőt Előfizető képviselőjére jogosult személy nevezhet ki.

Jogok, felhatalmazások ellenőrzése weboldal-hitelesítő tanúsítványok esetén (DVCP)

Amennyiben a tanúsítvány Alanyaként (Subject vagy SAN mezők) domain név, ill. IP cím kerül feltüntetésre, a Szolgáltatónak a fentiekben túl ellenőriznie kell, hogy Előfizető a domain név / IP cím felett kontrollal bír.

Ezt DVCP esetében a Szolgáltató technikai ellenőrzéssel valósítja meg.

A domain ellenőrzésre felhasználható metódusok:

1. Egyeztetett weboldal módosítással

Ahol az igényelt domainről a szolgáltatónak egy random értéket tartalmazó fájlt kell leolvasnia, http vagy https protokollon az FQDN `"/.well-known/pki-validation"` könyvtárból, és a válasz eseménynek tartalmaznia kell a véletlent.

Az érték 30 napig használható fel, a kérésre egyedinek kell lennie.

Több FQDN is validálható egyszerre, a fődomain validálása az aldomainek validálását is lehetővé teszi, az aldomain validálása azonban fődomainre nem eredményezhet kibocsátást.

A szolgáltató a kérésben nem adhatja meg a véletlen általa várt értékét.

Az igénylés megvalósítható ACME protokollon keresztül is, teljesen automatikusan.

2. DNS bejegyzés módosítással

Ahol az igényelt domainhez DNS TXT bejegyzést olvas a szolgáltató amely „_netlock=” bevezető taggal tartalmazza a random értéket, és az olvasott értéknek tartalmaznia kell a véletlent.

Az érték 30 napig használható fel, a kérésre egyedinek kell lennie.

Több FQDN is validálható egyszerre, a fődomain validálása az aldomainek validálását is lehetővé teszi, az aldomain validálása azonban fődomainre nem eredményezhet kibocsátást.

A szolgáltató a kérésben nem adhatja meg a véletlen általa várt értékét.

Szolgáltató jelen Szolgáltatási Rend alapján DVCP rend esetén nem bocsáthat ki wildcard karaktert tartalmazó domainre tanúsítványt.

Amennyiben Előfizető nem egyedül kontrollálja a domain nevet, akkor - az összes tulajdonos hozzájárulásának hiányában - a tanúsítvány kibocsátását vissza kell utasítani.

Szolgáltató a weboldal-hitelesítő tanúsítványok kibocsátásához Szabályzatában a fentiekben kívül más ellenőrzéseket is előírhat.

3.2.6. Együttműködési képességre vonatkozó követelmények

A Szolgáltató a szolgáltatásnyújtása során együttműködhet más Szolgáltatókkal, akik magukra kötelező érvényűnek ismerik el jelen Szolgáltatási rend követelményeinek betartását.

A Szolgáltatónak közzé kell tennie minden kereszthitelesített tanúsítványt, amely Alanyaként vagy kibocsátójaként szerepel.

3.3 Azonosítás és hitelesítés tanúsítványkezelési eljárás esetén

Olyan eljárás esetén, ami új tanúsítvány kibocsátását eredményezi (lásd a 4. Életciklus követelmények fejezetet, különösen a 4.6 Tanúsítványmegújítás, 4.7. Kulcscsere, 4.8 Tanúsítványmódosítás alfejezeteket), Szolgáltatónak a 3.2 fejezetben ismertetett Kezdeti azonosítási eljárás szerint kell azonosítania és ellenőriznie az Ügyfelet vagy ügyfeleket és az igénylésben szereplő adatokat.

Abban az esetben, amennyiben

- Igénylő eljárási jogosultságának ellenőrzését;
- Előfizető képviselőjére jogosult vagy jogosultak személyének azonosítását;
- Előfizető képviselője vagy képviselői meghatalmazottjának azonosítását és a meghatalmazás ellenőrzését;
- a tanúsítvány Alanyaként feltüntetésre kerülő és Szolgáltató nyilvántartásában eltárolt adatok ellenőrzését; valamint
- a magánkulcs birtoklásának ellenőrzését

Szolgáltató korábban már elvégezte, akkor ezen eljárásokat Szolgáltató csak akkor köteles megismételni a 3.2 fejezetben ismertetett kezdeti azonosítási eljárásrend szerint, amennyiben a korábbi ellenőrzése már elavult vagy nem megbízható, illetve ha a korábban felvett Igénylői, Előfizetői, vagy Alany adatok megváltoztak, illetőleg az új tanúsítványhoz új kulcspár készül.

A megismételt ellenőrzés történhet részlegesen is (amennyiben az érintettnek csak egyes adatai szorulnak újbóli megerősítésre, pl. egyes dokumentumok érvényességének lejáratára miatt).

Amennyiben az igénylés új nyilvános kulcsot tartalmaz és/vagy új Ügyféleszköz igénylésére is kiejtőd, akkor a 3.2.1 fejezet szerinti rendelkezéseket minden esetben be kell tartani.

Weboldal-hitelesítő tanúsítványok (DVCP) kezeléséhez az adatok ellenőrzését és az azonosítást meg kell ismételni

3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén

Nincs megkötés.

3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén

Érvénytelen tanúsítvánnyal hitelesítendő igényléseket szolgáltató nem fogadhat el.

3.4. Azonosítás és hitelesítés tanúsítványállapot-változtatás esetén

Szolgáltatónak fogadnia kell és fel kell dolgoznia az általa kibocsátott tanúsítványok állapotváltoztatására irányuló igényeket, valamint kezelnie kell a tanúsítványok visszavonásával járó események (pl. a magánkulcs kompromittálódása, sérülése; a tanúsítvány nem megfelelő használata vagy a tanúsítvánnyal vagy kulcsaival való más visszaélés) bejelentését.

Szolgáltatónak biztosítania kell, hogy az állapotváltozási igényeket csak az arra jogosultaktól fogad el. Ennek érdekében az állapotváltoztatás igénylőjét Szolgáltatónak azonosítania kell és meg kell állapítania, hogy jogosult-e az adott tanúsítvány állapotának megváltoztatását igényelni. Szolgáltatónak az Igénylőt legalább egy kódszóval vagy a Szolgáltató informatikai rendszerében automata azonosítás útján felhasználóneve és jelszava megadásával kell azonosítani.

Szolgáltatónak továbbá biztosítania kell, hogy az igényeket a lehető leggyorsabb (lehetőleg más szolgáltatás-igénylések feldolgozása elé sorolva) feldolgozza és teljesíti.

Elektronikusan hitelesített elektronikus visszavonási vagy felfüggesztési igény esetén Szolgáltató nem fogadhatja el a visszavonással vagy felfüggesztéssel érintett tanúsítvány magánkulcsával hitelesített igénylést.

Olyan eljárás esetén, ami a tanúsítvány állapotát megváltoztatja, de új tanúsítvány kibocsátását nem eredményezi Szolgáltatónak azonosítania kell az Igénylőt és meg kell győződnie az adott művelethez való jogosultságáról. Az Igénylőt legalább egy kódszóval vagy a Szolgáltató informatikai rendszerében automata azonosítás útján felhasználóneve és jelszava megadásával kell azonosítani.

Az állapotváltozási igények benyújtásának és feldolgozásának körülményeit és feltételeit a szolgáltatási szabályzatban kell rögzíteni.

4 ÉLETCIKLUS KÖVETELMÉNYEK

A Szolgáltatási Rend jelen (4.) fejezete ismerteti a tanúsítvány igényléséhez és kiadásához valamint a tanúsítvánnyal az életciklusán belül végezhető egyéb műveletekhez kapcsolódó elvárásokat. Szolgáltatónak a szolgáltatási szabályzatában részletesen ismertetnie kell azokat az eljárásokat, melyek garantálják, hogy a tanúsítványok kezelését lehetővé tevő szolgáltatások ezen elvárásoknak megfelelőek.

4.1 Tanúsítványigénylés

Új tanúsítvány kiadásához Igénylőnek Tanúsítványigénylést kell benyújtani Szolgáltató felé. A Tanúsítványigénylés alapján a Szolgáltatónak el kell készíteni az Igénylővel és Előfizetővel kötendő szolgáltatási szerződést, amit saját vagy képviselője aláírásával hitelesítve el kell juttatni a Szolgáltató számára. A szerződésnek tartalmaznia kell az Igénylő és Előfizető nyilatkozatát arra vonatkozóan, hogy kötelezettségeiket megismerték és azok betartását vállalják.

A Szolgáltató köteles a szerződést a tanúsítvánnyal kapcsolatos adatokkal együtt megőrizni.

Amennyiben a szolgáltatási szerződés elektronikusan készül el, akkor azt legalább fokozott biztonságú elektronikus aláírással / bélyegzővel kell ellátnia az Ügyfélnek.

A Szolgáltatónak a szolgáltatási szerződés megkötését megelőzően teljes körűen tájékoztatnia kell Igénylőt a szolgáltatás nem eIDAS voltáról, a szolgáltatás igénybevételeire vonatkozó pontos szerződési feltételekről, beleértve az igénybevételekre vonatkozó bármely korlátozást is, a tanúsítvány használatával kapcsolatos kikötésekről és feltételekről, valamint a kapcsolódó jogszabályokról. A tájékoztatást és a hozzá tartozó dokumentumokat honlapján meg kell, hogy jelenítse elektronikusan, változtatásoktól védett formában (melynek módját a Szabályzatban határozza meg), valamint a legkésőbb a szerződéskötést követően tartós adathordozón vagy elektronikus levélbe illesztett link(ek)en keresztül elérhetővé kell tennie a szolgáltatási szerződést, a szolgáltatási rendet és a szolgáltatási szabályzatot.

4.1.1 Ki nyújthat be tanúsítványigénylést?

Tanúsítványigénylést természetes személy Igénylők nyújthatnak be a saját maguk vagy egy szervezet, mint Előfizető nevében, annak felhatalmazásával.

Szolgáltató kockázatlistát kezelhet azon személyekről, akik esetében a tanúsítványigényléssel kapcsolatos kockázatokat tart nyilván, valamint külső adatforrásokat is felhasználhat kockázatértékeléshez. Szolgáltató a kockázatértékelés alapján visszautasíthatja a tanúsítványigényléseket.

4.1.2 Az igénylés folyamata és a résztvevők felelőssége

Szolgáltatónak a 3. fejezetben írtak szerint meg kell győződnie Igénylő személyazonosságáról, eljárási jogáról, valamint az Igénylésben szereplő adatok megfelelőségéről.

Igénylő és Előfizető adjon meg minden szükséges információt az azonosítási és ellenőrzési

eljárások lefolytatásához. A Szolgáltatónak nyilvántartásba kell vennie az Igénylő és Előfizető azonosságára vonatkozó, a szolgáltatás nyújtásához és a kapcsolattartáshoz szükséges minden információt, valamint az Igénylő által aláírt szolgáltatási szerződést.

A tanúsítványigényléshez nyilvántartásba vett adatokat meg kell őrizni legalább a hatályos jogszabályokban előírt időtartamig.

A szolgáltatási szerződésnek tartalmaznia kell a következőket:

- Igénylő nyilatkozatát arról, hogy a tanúsítványigénylésben megadott adatok teljesek és pontosak;
- azt, hogy hozzájárul-e a Tanúsítvány közzétételéhez;
- nyilatkozatát arról, hogy a Tanúsítványban feltüntetett adatok jogos felhasználója, s azok más érdekeit nem sértik.

Weboldal-hitelesítő tanúsítványok igénylése (DVCP)

A fentiek betartása mellett tanúsítványigénylésnek tartalmaznia kell legalább egy FQDN-t vagy IP-cím-et is, ami a tanúsítvány Subject/CommonName mezőjébe és a subjectAltName kiterjesztésébe foglalandó.

4.2 Tanúsítványigénylések feldolgozása

4.2.1. Azonosítás és hitelesítés

Lásd a 3.2 fejezetet, az alábbi kiegészítéssel.

Az azonosítási és hitelesítési feladatokat a Szolgáltató - vagy a Szolgáltató megbízásából eljáró, a Szolgáltató szabályzata szerint működő - Regisztrációs Egysége hajthatja végre.

Szolgáltatónak a Regisztrációs Ügyintézőket megbízható módon azonosítania kell.

A tanúsítványigénylésnek tartalmaznia kell az összes tanúsítványban megjelenő Alany információt, valamint az összes további információt, amire Szolgáltatónak szükséges van annak érdekében, hogy szabályzatainak megfelelően tudja kiadni a tanúsítványt. Abban az esetben, ha a tanúsítványigénylés nem tartalmazza az összes szükséges információt Szolgáltatónak be kell szerezni a hiányzó adatokat az Igénylőtől vagy megbízható, független forrásból, amelyeket Igénylőnek meg kell erősíteni.

Szolgáltatónak dokumentált folyamatban kell szabályozni a tanúsítványba foglalandó adat ellenőrzésére, továbbá a kiemelt kockázatú tanúsítványkérelmek azonosítására és kiegészítő ellenőrzési eljárására vonatkozó szabályokat.

4.2.2. Tanúsítványigénylések elfogadása vagy visszautasítása

Szolgáltatónak vissza kell utasítani azon Tanúsítványigényléseket, amelyek megfelelőségét nem tudja teljes körűen ellenőrizni.

A Szolgáltató saját hatáskörében, külön indoklás nélkül dönthet az igényelt tanúsítvány kiadásának megtagadásáról, melyről tájékoztatja Igénylőt.

Az összeférhetetlenség elkerülése érdekében Szolgáltatónak kötelessége biztosítani a személyi és szervezeti függetlenségét az Előfizetőkkel szemben. Nem minősül az összeférhetetlenség megsértésének, amikor Szolgáltató saját munkatársai, megbízottai vagy partnerei számára bocsát ki tanúsítványt.

A nyilvános kulcsot a Regisztrációs Egységnek úgy kell továbbítani a Hitelesítő Egység felé, hogy a megfelelő regisztrációs adatokhoz való kapcsolat biztosított legyen és a kulcs ne változhasson meg.

Weboldal-hitelesítő tanúsítványigénylések elfogadása vagy visszautasítása (DVCP)

A fenti eseteken túl Szolgáltatónak vissza kell utasítani azon Tanúsítványigényléseket is, amelyek olyan gTLD-khez tartoznak, amelyeket az ICANN megfontolás alatti fázisban tart, és amelyek belső IP címekhez tartoznak.

4.2.3. A tanúsítványigénylés feldolgozásának időtartama

A Szolgáltatónak a Szolgáltatási szabályzatban meg kell határoznia, hogy milyen határidőn belül vállalja az elfogadott Tanúsítványigénylések feldolgozását.

4.3 Tanúsítvány kibocsátása

A Szolgáltató csak a Tanúsítványigénylés elfogadása után állíthatja ki a Tanúsítványt. A tanúsítványkibocsátási eljárásnak biztonságosan kell kötődnie a regisztrációs, igénylési és életciklus menedzsment eljárásokhoz, beleértve az Ügyfél vagy a Szolgáltató által generált nyilvános kulcs alkalmazását. A kiállított Tanúsítvány csak az Tanúsítványigénylésben megadott (hibás adat esetén a javított) és az eljárás során a Szolgáltató által ellenőrzött adatokat tartalmazhat. Képviselési jogosultságot igazoló tanúsítvány esetén a képviselőt elektronikus úton értesíti.

A Gyökér Kiadó általi tanúsítványkibocsátás

A Gyökér Kiadó által történő tanúsítványkibocsátás csak a szolgáltatási szabályzat által felhatalmazott szolgáltatói munkatársak kontrolljával valósulhat meg.

4.3.1. A Szolgáltató tevékenysége a tanúsítvány kibocsátás során

A Szolgáltatónak biztosítani kell a tanúsítványok kibocsátásának biztonságát, megakadályozva a tanúsítványok hamisíthatóságát.

Szolgáltatónak biztosítania kell, hogy a tanúsítványigénylés feldolgozását és a tanúsítvány kibocsátását különböző személyek végezzék.

A gyökér Kiadó által történő tanúsítványok kibocsátását egy, a Szolgáltató által felhatalmazott természetes személynek kell kezdeményezni.

4.3.2. Értesítés a tanúsítvány kibocsátásáról

A Szolgáltató a Tanúsítvány kibocsátásáról értesítse a Végfelhasználót a tanúsítványban megjelölt vagy külön felvett email címen, és tegye lehetővé számára a Tanúsítvány átvételét.

4.4 Tanúsítvány elfogadása

4.4.1. A tanúsítványelfogadás módja

A Szolgáltató által kiállított tanúsítványok tartalmát az Ügyfélnek ellenőrizni kell és el kell azokat fogadnia az első használatot megelőzően. Hibás tanúsítványt az Ügyfélnek - megfelelő indoklással - vissza kell utasítania és annak (illetve a hozzá tartozó magánkulcsnak) a használatát nem szabad megkezdenie. Az elfogadás megvalósulhat direkt és indirekt módon egyaránt.

4.4.2. A tanúsítvány közzététele

Előfizető vagy Igénylő hozzájárulása esetén a kiállított tanúsítványt a szolgáltató köteles nyilvánosságra hozni a nyilvános tanúsítványtárán keresztül.

4.4.3. További szereplők értesítése a tanúsítvány kibocsátásról

Amennyiben a kibocsátott tanúsítvány képviseleti jogot is igazol, a kibocsátás tényéről haladéktalanul értesíteni kell az Előfizető kapcsolattartóját is.

4.5 Kulcspár és tanúsítvány alkalmazhatósága

4.5.1. A magánkulcs és a tanúsítvány használata

A Végfelhasználó

- a tanúsítványához tartozó magánkulcsát kizárólag a tanúsítványban jelölt felhasználási célnak megfelelően használhatja fel ("kulcshasználat" és "kiterjesztett kulcshasználat" mezők szerint);
- Az autentikációs tanúsítvány eszköz használata esetén PKI algoritmus használatával többfaktoros bejelentkezésre/felhasználóazonosításra használhatja.
- Az autentikációs tanúsítvány eszköz használata esetén PKI algoritmus használatával tanúsítványos bejelentkezésre/felhasználóazonosításra használhatja.
- Az titkosító tanúsítványt titkosított állományok, üzenetek FOGADÁSÁRA/DEKÓDOLÁSÁRA használhatja, a dekódolást csak a magánkulcs birtokában lehet elvégezni.
- A weboldal hitelesítő tanúsítványok esetében (DVCP) a tanúsítványt kizárólag weboldal hitelesítésre használhatja.
- A kriptográfiai eszközre generált magánkulcsot (lásd 6.1) kizárólag a kriptográfiai eszközön alkalmazza.
- lejárt érvényességű, visszavont, vagy felfüggesztett tanúsítványhoz tartozó

magánkulcsot nem használhat fel;

- köteles gondoskodni magánkulcsának és az aktiváló adatának megfelelő védelméről, elkerülve azok illetéktelen használatát;
- amennyiben a magánkulcsról másolatot készít, akkor azt ugyanolyan gondossággal kell kezelje, mint az eredeti példányt;
- azonnal értesíti a szolgáltatót, amennyiben az alábbi esetek valamelyike bekövetkezik a tanúsítvány érvényességének vége előtt, s egyúttal azonnal beszünteti a magánkulcs alkalmazását, kivéve az adatvisszafejtés műveletet:
 - a magánkulcs elvesztése, ellopása, kompromittálódása,
 - a magánkulcs feletti kizárólagos kontroll elvesztése, pl. az aktiválási adat kompromittálódása miatt,
 - a tanúsítványban feltüntetett adatok pontatlansága vagy változása;
- a szolgáltatói kulcs kompromittálódása esetén beszünteti a magánkulcs és a tanúsítvány alkalmazását;
- a magánkulcshoz tartozó tanúsítvány érvényessége végén vagy visszavonása esetén a magánkulcsot, s annak bármilyen másolatát visszaállíthatatlan módon törli.

A magánkulcs a Végfelhasználó kizárólagos befolyása alatt kell álljon.

A használat során be kell tartani az 1.4. fejezetben leírt korlátozásokat.

4.5.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata

A Szolgáltatónak a szolgáltatási szabályzatában közzé kell tennie azokat az eljárásokat és feltételeket, amelyek követésével és betartásával az Érintett Felek megbízhatnak a tanúsítványokban.

4.6 Tanúsítványmegújítás

Szolgáltatónak a tanúsítványok egyszerűsített kiadása érdekében Tanúsítványmegújítási szolgáltatást kell nyújtania.

Tanúsítványmegújítást a Szolgáltató saját hatáskörben is végrehajthat, valamint az Ügyfél is kezdeményezheti. Az Ügyfél jogosult tanúsítványa megújítását igényelni, amennyiben annak lejáratára 30 napon belül esedékes.

4.6.1. A tanúsítványmegújítás körülményei

Az eljárás - Ügyfél igénylése esetén - egy az eljárásra vonatkozó igény Szolgáltatóhoz történő beérkezésével kezdődő és egy új végfelhasználói tanúsítvány kibocsátásával, illetve nem megfelelő igénylés esetén az igénylés visszautasításával záródó folyamat.

Amennyiben a Szolgáltató az új tanúsítványt eltérő szabályzatok szerint vagy eltérő kiadóval adja ki, mint amivel az eredeti tanúsítvány készült, akkor intézkedni kell, hogy minden új vagy szigorúbb elvárásnak is megfeleljen az újonnan kiadott tanúsítvány.

A megújított tanúsítvány kibocsátásakor a Szolgáltatónak a kezdeti tanúsítványkibocsátás

során alkalmazott módon kell eljárnia a Tanúsítvány előállítása, közzététele, az Ügyfél és az érintett felek értesítése során.

Az új tanúsítvány kiadását követően a Szolgáltató az eredeti tanúsítványt visszavonhatja, az eljárás idejére az eredeti tanúsítványt felfüggesztheti.

4.6.2. Ki igényelheti a tanúsítványmegújítást?

A Tanúsítványmegújítás a Tanúsítványigénylés benyújtásával igényelhető a Szolgáltatónál. Az igénylésre az jogosult, aki a kezdeti tanúsítványigénylésre is jogosult. Az igénylés teljesítését megelőzően az Igénylőt azonosítani kell a 3.3. fejezetben megadottak szerint és tájékoztatni kell a Tanúsítvány használatával kapcsolatos kikötésekről és feltételekről, amiket el kell fogadnia.

A tanúsítvány megújítási igénylésben az Igénylőnek nyilatkoznia kell, hogy a Tanúsítványban szereplő adatok még érvényben vannak.

4.6.3. A tanúsítványmegújítási igénylések feldolgozása

A Szolgáltatónak meg kell győződni az Ügyfél által benyújtott Tanúsítványigénylés feldolgozásakor, hogy

- a benyújtott igénylés hiteles (elektronikusan aláírt igénylés esetén érvényes aláírással rendelkezik);
- Igénylő jogosult igénylés benyújtására az Előfizető nevében (kivéve, ha az érintett tanúsítványhoz tartozó magánkulccsal van aláírva az igénylés);
- az igénylés teljes (minden kötelező adata kitöltött) és hibátlan;
- az érintett tanúsítvány egyértelműen azonosítható;
- az aktuálisan elérhető információk alapján a kiadandó Tanúsítvány tervezett érvényessége alatt a felhasznált kriptográfiai algoritmusok még használhatók lesznek;
- a tanúsítvány még érvényes (nem járt le, nincs felfüggesztve vagy visszavonva);
- a tanúsítványhoz tartozó magánkulcs nem kompromittálódott (ügyfélnyilatkozat);
- a tanúsítvány igénylése során az adatok ellenőrzésére használt dokumentumok még érvényesek;
- a szolgáltatási szerződés még hatályos;
- a művelet végrehajtható.

Amennyiben a fenti elvárások nem teljesülnek, akkor az igénylést a Szolgáltatónak vissza kell utasítania, az Ügyfél pedig a kezdeti tanúsítványigénylési eljárásban tud új tanúsítványt igényelni.

A szolgáltató korlátozhatja az ugyanazon tanúsítványra vonatkozó megújítások számát, illetve további elvárásokat határozhat meg a megújítás feltételeként.

4.6.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A 4.3.2 fejezet alkalmazandó.

4.6.5. A megújított tanúsítvány elfogadása

A 4.4.1 fejezet alkalmazandó.

4.6.6. A megújított tanúsítvány közzététele

A 4.4.2 fejezet alkalmazandó.

4.6.7. További szereplők értesítése a tanúsítvány kibocsátásáról

A 4.4.3 fejezet alkalmazandó.

4.7 Kulcscsere

Szolgáltatónak a tanúsítványok érvényességi idején belül történő alkalmazhatósága érdekében Kulcscsere szolgáltatást kell nyújtania.

Kulcscserét a Szolgáltató saját hatáskörben is végrehajthat, valamint az Ügyfél indoklás nélkül is kezdeményezheti. A Szolgáltatónak hivatalból kell kezdeményeznie a kulcscserét, amennyiben a tanúsítványban szereplő nyilvános kulcs nem felel meg a hatályos jogszabályi követelményeknek, az irányadó szabványleírásoknak vagy a Bizalmi Felügyelet vonatkozó hatályos határozatának.

Kulcscserére sor kerülhet érvényes és érvénytelen (pl. kulcskompromittálódás miatt visszavonásra került) Tanúsítvány esetén egyaránt.

A kulcscsere során kiállított új Tanúsítványban a Végfelhasználó nyilvános kulcsa mellett változnak (például tanúsítvány sorozatszám és érvényességi idő eleje), illetve opcionálisan változhatnak további adatok is (például egyes Szolgáltatói adatok, mint az CRL és OCSP hivatkozások vagy a Tanúsítvány aláírására használt szolgáltatói kulcs), de az Ügyfél a kulcson kívül nem igényelheti más adat módosítását.

A szolgáltatói kulcsok cseréjével kapcsolatosan lásd az 5.6 fejezetet.

4.7.1. A kulcscsere körülményei

A 4.6.1 fejezet alkalmazandó.

4.7.2. Ki igényelheti a kulcscserét

A 4.6.2 fejezet alkalmazandó.

4.7.3. A kulcscsere igénylések feldolgozása

A 4.6.3 fejezet alkalmazandó, azzal a különbséggel, hogy az érintett tanúsítvány érvényessége, illetve a hozzá tartozó magánkulcs kompromittálódás-mentessége nem elvárás (kivéve, ha az igénylés azzal lett aláírva).

Amennyiben a Szolgáltatónak a kulcscsere eljárás során jut tudomására, hogy a kulcs

kompromittálódott, akkor azonnal intézkednie kell annak visszavonásáról, és ennek megfelelően elbírálni az igénylést.

4.7.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A 4.6.4 fejezet alkalmazandó.

4.7.5. A kulcscserével megújított tanúsítvány elfogadása

A 4.6.5 fejezet alkalmazandó.

4.7.6. A kulcscserével megújított tanúsítvány közzététele

A 4.6.6 fejezet alkalmazandó.

4.7.7. További szereplők értesítése a tanúsítvány kibocsátásáról

A 4.6.7 fejezet alkalmazandó.

4.8 Tanúsítványmódosítás

Szolgáltatónak a tanúsítványok folyamatosan hiteles adattartalma és alkalmazhatósága érdekében tanúsítványmódosítási szolgáltatást kell nyújtania.

Tanúsítványmódosítást a Szolgáltató saját hatáskörben is végrehajthat, valamint az Ügyfél is kezdeményezheti.

A Szolgáltatónak hivatalból kell kezdeményeznie a Tanúsítványmódosítást, amennyiben tudomására jut a Tanúsítványban szereplő adatokban bekövetkezett valamilyen változás, beleértve a Tanúsítványban szereplő valamely saját adatának vagy bármely más tanúsítványadat megváltozását (pl. jogszabály-, szabvány- vagy szabályzatváltozás következtében). A Szolgáltató jogosult a végfelhasználói tanúsítványok módosítására, ha a Tanúsítványkibocsátáshoz használt szolgáltatói aláíró kulcsát le kell cserélnie.

A tanúsítványmódosítást az Ügyfél akkor igényelheti, ha a tanúsítványban szereplő adatai megváltoznak.

4.8.1. A tanúsítványmódosítás körülményei

A 4.6.1 fejezet alkalmazandó.

4.8.2. Ki igényelheti a tanúsítványmódosítást

A 4.6.2 fejezet alkalmazandó, azzal a különbséggel, hogy az Alany adatok változatlan voltáról szóló nyilatkozat értelemszerűen nem vonatkozik a megváltozott adatokra.

4.8.3. A tanúsítványmódosítási igénylések feldolgozása

A 4.6.3 fejezet alkalmazandó.

A Szolgáltatónak az új Alany adatok valódiságának ellenőrzése során a 3.2 fejezetben ismertetett Kezdeti azonosítási eljárás szerint kell eljárnia.

4.8.4. Az Ügyfél értesítése az új tanúsítvány kibocsátásáról

A 4.6.4 fejezet alkalmazandó.

4.8.5. A módosított tanúsítvány elfogadása

A 4.6.5 fejezet alkalmazandó.

4.8.6. A módosított tanúsítvány közzététele

A 4.6.6 fejezet alkalmazandó.

4.8.7. További szereplők értesítése a tanúsítvány kibocsátásáról

A 4.6.7 fejezet alkalmazandó.

4.9 Visszavonás és felfüggesztés

A Szolgáltatónak az általa kibocsátott tanúsítványok érvényességének kezelésére állapotváltoztatási (tanúsítvány-visszavonási, -felfüggesztési és -aktiválási) szolgáltatásokat kell nyújtania. E műveleteket a Szolgáltató saját hatáskörben is végrehajthatja, valamint az Ügyfél és Bíróság vagy hatóság is kezdeményezheti. Az Ügyféligenyek fogadására a Szolgáltatónak folyamatos (7*24 órás) lehetőséget kell biztosítani.

Szolgáltatónak gondoskodni kell arról, hogy a visszavont és felfüggesztett tanúsítványok nyilvántartásában szereplő adatokat az arra jogosult harmadik személyek értelmezni tudják.

Weboldal-hitelesítő tanúsítványok (DVCP) esetén tanúsítványfelfüggesztési és -aktiválási szolgáltatás nem nyújtható.

4.9.1 A visszavonást és a felfüggesztést indukáló körülmények

A végfelhasználói tanúsítványok visszavonását vagy felfüggesztését az alábbi körülmények indukálhatják. Az alábbi esetekben a Szolgáltatónak az Igény beérkezését követő legfeljebb 24 órán belül vissza kell vonnia vagy fel kell függesztenie a tanúsítványt:

- Ügyfél szabályos igénylése (Állapotváltoztatási ügyféligeny);
- Ügyfél jelzi a szolgáltatónak, hogy az eredeti tanúsítványigénylés nem volt engedélyezett és azt utólag sem engedélyezi;
- Ügyfél kötelezettségeinek be nem tartása;
- Harmadik fél bejelentése talált ügyféleszközzel;
- a szolgáltató szabályzatai és az ÁSZF által meghatározott egyéb körülmény;

- a tanúsítványban lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódása;
- a tanúsítványt hitelesítő szolgáltatói magánkulcs kompromittálódása;
- jogszerűtlen név- vagy adathasználat,
- a tanúsítványban hibásan rögzített adatok vagy az adatok valótlanúsága, megváltozása, félrevezetésre alkalmassága;
- Ügyfél nem kérte a tanúsítvány aktiválását a felfüggesztési időn belül;
- a tanúsítvány rosszhiszemű felhasználása;
- bíróság vagy hatóság erre vonatkozó jogerős és végrehajtható határozata;
- a tanúsítvány műszaki jellemzői a mértékadó szakmai ajánlások alapján az elfogadhatónál nagyobb kockázatot jelentenek bármely félnek (pl. kulcshossz ajánlottnál kisebb mérete);
- a szolgáltatási szerződés megszűnése vagy megszűnése;
- a tanúsítvány nem a vonatkozó szabályzatok szerint lett kibocsátva;
- a szolgáltató tudomására jut, hogy a tanúsítványban szereplő valamely név (pl. FQDN) használatára az Ügyfél nem jogosult;
- a szolgáltató tudomására jut a tanúsítványban feltüntetett képviseleti jogosultság megszűnése;
- amennyiben a tanúsítványra vonatkozó érvényességi információk szolgáltatások fenntartása megszűnik;
- a szolgáltatás megszűnése, kivéve, ha a Szolgáltató korábban gondoskodott az általa kibocsátott tanúsítványok vonatkozásában a CRL és OCSP szolgáltatások fenntartásáról;
- jogszabály teszi kötelezővé.

A tanúsítványok felfüggesztésének lehetséges okai:

- a tanúsítvány kiadását követő kezdeti felfüggesztés a szállítás biztonságának növelésére;
- a tanúsítvány visszavonását indukáló bármely körülményre vonatkozó alapos vélelem.

Weboldal-hitelesítő tanúsítványok (DVCP) esetén tanúsítványfelfüggesztési és -aktiválási szolgáltatás nem újítható.

A Szolgáltató legfeljebb 7 napon belül köteles intézkedni a Szolgáltató tanúsítványának visszavonásáról az alábbi esetekben:

- a Hitelesítő Egység szabályos, írásbeli igénylése (kihelyezett kiadó esetén);
- a Hitelesítő Egység jelzi a szolgáltatónak, hogy az eredeti kiadó tanúsítványigénylés nem volt hiteles és azt utólag sem hitelesíti, illetve engedélyezi (kihelyezett kiadó esetén);
- a tanúsítványban lévő nyilvános kulcshoz tartozó magánkulcs kompromittálódása;
- a tanúsítványt hitelesítő szolgáltatói magánkulcs kompromittálódása;
- a tanúsítvány rosszhiszemű felhasználása;
- a tanúsítványban hibásan rögzített adatok vagy az adatok valótlanúsága, megváltozása, félrevezetésre alkalmassága;
- amennyiben a tanúsítványra vonatkozó érvényességi információk szolgáltatások fenntartása megszűnik;

- a tanúsítvány műszaki jellemzői a mértékadó szakmai ajánlások alapján az elfogadhatónál nagyobb kockázatot jelentenek bármely félnek (pl. kulcshossz ajánlottnál kisebb mérete);
- bíróság vagy hatóság erre vonatkozó jogerős és végrehajtható határozata;
- a szolgáltatás megszűnése;
- jogszabály teszi kötelezővé;
- a szolgáltató szabályzatai által meghatározott egyéb körülmény.

4.9.2 Állapotváltoztatási ügyféligenyre jogosultak

A tanúsítványokra vonatkozó állapotváltozási igény benyújtására az alábbi felek jogosultak:

- Ügyfél;
- Regisztrációs egység;
- Szolgáltató;
- ésszerű ok esetén bármely harmadik fél.

Tanúsítványaktiválást Ügyfél abban az esetben jogosult igényelni, amennyiben a felfüggesztést Igénylő vagy Előfizető igényelte és az igényt indukáló körülmények már nem állnak fenn. Amennyiben Szolgáltató saját hatáskörben függesztette fel a végfelhasználói tanúsítványt, a felfüggesztést indukáló körülmények megszűnésével haladéktalanul köteles a tanúsítványt aktiválni.

4.9.3 A visszavonási, felfüggesztési és aktiválási eljárás

A Szolgáltatónak lehetőséget kell biztosítania az Ügyfelek számára a végfelhasználói tanúsítványok visszavonására illetve felfüggesztésére. A Szolgáltató szabályzatainak tartalmaznia kell a visszavonási, felfüggesztési és a aktiválási folyamat leírását, a tanúsítványállapot-változtatási igénylésére pedig folyamatos (7x24) lehetőséget kell biztosítania.

A Szolgáltató tájékoztatni kell az Ügyfeleket a magánkulcs kompromittálódására, és tanúsítvánnyal való visszaélésre vagy más típusú csalásokra vonatkozó bejelentések módjáról.

A visszavonás vagy felfüggesztés vonatkozhat egy végfelhasználói tanúsítványra vagy a szolgáltató valamely köztes Kiadójára; az aktiválás csak felfüggesztett állapotú tanúsítványra vonatkozhat.

A Szolgáltató nem vonhat vissza vagy függeszthet fel egy tanúsítványt a visszavonás vagy felfüggesztés közzétételét megelőző időre.

A Szolgáltató a szabályzataiban vagy szolgáltatási szerződésben rendelkezik a tanúsítvány eredeti érvényességének lejártá előtti visszavonásának illetve felfüggesztésének jogkövetkezményeiről.

A tanúsítvány új státuszának az intézkedést követően haladéktalanul be kell kerülnie a tanúsítványtárba (ún. tanúsítványállapot-adatbázisba), ezzel lehetővé téve a valós idejű tanúsítványállapot ellenőrzést. A végfelhasználói tanúsítvány visszavonását vagy

felfüggesztését követő legkésőbb 1 órán belül új visszavonási lista (CRL) kiadására is sor kerül, mely ugyancsak tartalmazza a tanúsítvány megváltozott státuszát.

A Szolgáltató valamely Kiadója magánkulcsának kompromittálódása esetén tegyen meg minden ésszerű erőfeszítést annak érdekében, hogy az eseményről értesítse az Érintett feleket. A szolgáltatói tanúsítványok állapotváltozását hozza nyilvánosságra a honlapján.

4.9.4 Az igénylések feldolgozása

A Szolgáltatónak a tanúsítványállapot-változtatási igények feldolgozását átvételük után azonnal el kell kezdenie, s haladéktalanul, minden más típusú tevékenysége (így különösen tanúsítvány előállítás vagy kibocsátása) előtt feldolgozni, és az arra jogosult által benyújtott kérelmeket teljesíteni.

A Szolgáltatónak meg kell győződni az Állapotváltoztatási ügyféligény feldolgozásakor, hogy

- a benyújtott igénylés hiteles (elektronikusan aláírt igénylés esetén érvényes aláírással rendelkezik, kivéve, ha az érintett tanúsítványhoz tartozó magánkulccsal van aláírva az igénylés);
- Igénylő jogosult igénylés benyújtására az Előfizető nevében;
- az igénylés teljes (minden kötelező adata kitöltött) és hibátlan;
- az érintett tanúsítvány egyértelműen azonosítható;
- a művelet végrehajtható.

Az igénylésre való jogosultság ellenőrzése a *3.4. Azonosítás és hitelesítés tanúsítvány felfüggesztési és visszavonási igénylés esetén* fejezetben leírtak szerint történik.

Amennyiben a fenti elvárások nem teljesülnek, akkor az igénylést a Szolgáltatónak vissza kell utasítania, egyébként további mérlegelés nélkül intézkednie kell a tanúsítvány visszavonása, felfüggesztése vagy aktiválása érdekében.

A visszavonási igényt a visszavonást indukáló körülmény vélelemének tisztázása céljából a Szolgáltató ideiglenesen a tanúsítvány felfüggesztésével is kezelheti.

A Szolgáltató minden végrehajtott és visszautasított felfüggesztési, visszavonási és tanúsítványaktiválási igénylésről e-mailben értesíti az Igénylőt és az Előfizetőt.

4.9.5 Állapotváltozási igények feldolgozásának maximális ideje

Az érvényes tanúsítványvisszavonás-igényeket azok kézhezvételét követő 24 órán belül rögzíteni kell és közzé kell tenni a tanúsítvány visszavont státuszát.

Visszavonás vagy felfüggesztés esetén az igény végrehajtását követően a tanúsítvány visszavont vagy felfüggesztett státusza haladéktalanul bekerül a tanúsítványtárba, valamint az igénylést követő legkésőbb 1 órán belül új visszavonási lista (CRL) kiadására is sor kerül, melyen a tanúsítvány státusza

- felfüggesztés esetén "onHold" státusszal jelenik meg;
- visszavonás esetén a végleges visszavonás okát tartalmazza megjelölésként az RFC 5280 szerint

Felfüggesztett állapotú tanúsítványra vonatkozó aktiválási igény esetén, amennyiben a

Szolgáltató meggyőződött arról, hogy a felfüggesztést indukáló körülmények megszűntek, az aktiválási igényt haladéktalanul végrehajtja és a tanúsítvány érvényes státusza haladéktalanul bekerül a tanúsítványtárba, valamint az aktiválási igénylést követő legkésőbb 1 órán belül új visszavonási lista (CRL) kiadására is sor kerül, melyen a tanúsítvány már nem szerepel.

4.9.6 Javasolt eljárás az tanúsítványállapot ellenőrzésére

A Tanúsítványban foglalt információk elfogadását és felhasználását megelőzően a Szolgáltató által garantált biztonsági szint megtartásához szükséges, hogy az Érintett felek megfelelően gondosan járjanak el, így különösen javasolt ellenőrizniük az érvényességi láncban található valamennyi Tanúsítvány érvényességét a vonatkozó műszaki szabványoknak megfelelően.

Az ellenőrzés terjedjen ki a Tanúsítványok érvényességének ellenőrzésére, a szabályzatok és a kulcshasználat megkötéseire, az egyes Tanúsítványokban hivatkozott CRL vagy OCSP alapú visszavonási státusz információk ellenőrzésére.

4.9.7 A visszavonási lista kibocsátás gyakorisága

A Szolgáltató legalább naponta egyszer bocsásson ki új tanúsítványvisszavonási listát a végfelhasználói Tanúsítványokat kibocsátó Kiadóra. Az ilyen kibocsátott tanúsítványvisszavonási listák érvényességi ideje legfeljebb 24 óra lehet. A kereszthitelesített kiadók esetén 31 naponta kell tanúsítványvisszavonási listát kibocsátani.

A Szolgáltató legalább évente egyszer, de visszavonás esetén 24 órán belül bocsásson ki új tanúsítványvisszavonási listát a köztes Kiadóra. Az ilyen kibocsátott tanúsítványvisszavonási listák érvényességi ideje legfeljebb 12 hónap lehet.

A visszavonási listának tartalmaznia kell az öt követő visszavonási lista kibocsátásának tervezett időpontját, a Szolgáltató ugyanakkor ezen időpontot megelőzően is kiadhat új visszavonási listát. A visszavonási listákat a Szolgáltatónak saját elektronikus aláírásával kell hitelesítenie.

4.9.8 A visszavonási lista előállítása és közzététele közötti idő maximális hossza

A tanúsítvány visszavonása vagy felfüggesztése a visszavonási vagy felfüggesztési igénylés teljesítésével egyidejűleg jelenjen meg a CRL-ben.

4.9.9 Tanúsítványállapot szolgáltatás rendelkezésre állása

A Szolgáltatónak online (valós idejű) tanúsítványállapot szolgáltatást (OCSP) kell nyújtania a szolgáltatások keretében kibocsátott tanúsítványok állapotának ellenőrzéséhez.

Lásd a [4.10 fejezet](#)et.

4.9.10 Tanúsítványállapot szolgáltatásra vonatkozó követelmények

A Szolgáltató által kibocsátott OCSP válaszoknak meg kell felelniük az RFC 6960 és/vagy a RFC5019 ajánlásnak. Az OCSP válaszokat alá kell írnia

- az ellenőrizendő tanúsítványt kibocsátó Kiadónak, vagy
- egy OCSP válaszdónak, amelynek a tanúsítványát az a Kiadó írta alá, mely az ellenőrizendő tanúsítványt kibocsátotta. (Ebben az esetben az RFC 6960 alapján az OCSP-t aláíró tanúsítványnak tartalmaznia kell egy "id-pkix-ocsp-nocheck" típusú kiterjesztést³.)

A Szolgáltatónak támogatnia kell a GET metódusú OCSP kéréseket⁴.

A Szolgáltató által kibocsátott OCSP válasz csak az adott Kiadó által aláírt, a Szolgáltató Tanúsítványtárában szereplő Tanúsítványokra vonatkozóan tartalmazhat "good" állapotinformációt. Egy még ki nem bocsátott tanúsítványra vonatkozó OCSP válasz nem tartalmazhat "good" állapotinformációt. Az OCSP kéréseket a Szolgáltatónak a 6.5 Informatikai biztonsági előírások fejezetben foglaltaknak megfelelően kell ellenőriznie.

A 7.1.5 Névhasználati megkötések fejezetben írtaknak nem megfelelő Kiadó tanúsítványára vonatkozó OCSP válasz nem tartalmazhat "good" állapotinformációt.

4.9.11 A visszavonási hirdetmények egyéb formái

A Szolgáltató egyes szolgáltatások keretében a visszavonási információkat egyéb módokon is közzéteheti, amennyiben ezt szabályzataiban rögzíti.

4.9.12 A kulcs kompromittálódásra vonatkozó speciális követelmények

Szolgáltató dolgozzon ki megoldást arra, hogy tájékoztassa Ügyfeleit, amennyiben magánkulcsuk veszélybe került (pl. Új sérülékenység felfedezése esetén vagy Szolgáltató saját megállapítása alapján). Amennyiben kulcs kompromittálódás nem vitatott, akkor az érintett Szolgáltatói vagy végfelhasználói tanúsítvány visszavonásáról késedelem nélkül intézkedni kell.

Magánkulcs kompromittálódása esetén az ahhoz tartozó nyilvános kulcs tanúsítványát a 4.9 A visszavonást és a felfüggesztést indukáló körülmények fejezetben írtak szerint a Szolgáltatónak fel kell függesztenie vagy vissza kell vonnia.

Szolgáltatói kulcs kompromittálódás esetére lásd az 5.7.3 fejezetet.

³ Ez a kiterjesztés azt jelenti, hogy az OCSP válaszdó tanúsítványa érvényesség ellenőrzése nem szükséges.

⁴ Lásd HTTP (HyperText Transfer Protocol) protokoll leírását

4.9.13 A felfüggesztés maximális ideje

A felfüggesztett állapot időtartama legfeljebb 30 naptári nap (720 óra lehet). Az időtartam elteltét követően a Szolgáltató külön értesítés nélkül jogosult a felfüggesztett tanúsítvány visszavonására. A felfüggesztési időtartam alatt az Igénylő és Előfizető jogosult a tanúsítvány aktiválását igényelni (lásd még 4.9.2 Állapotváltoztatási ügyféligényre jogosultak).

Weboldal-hitelesítő tanúsítványok (DVCP) esetén a tanúsítványfelfüggesztés nem támogatott.

4.10 Visszavonási nyilvántartások

A Szolgáltatónak biztosítania kell az általa kibocsátott tanúsítványok állapotának (érvényes, felfüggesztett vagy visszavont) ellenőrzését biztosító szolgáltatásokat.

4.10.1 Működési jellemzők

Szolgáltatónak tájékoztatnia kell az Érintett feleket az általa kibocsátott tanúsítványok érvényességéről vagy visszavont státusáról. Ennek az információnak – legalább tanúsítványonként – megbízható, ingyenes és hatékony automatizált formában bármikor, a tanúsítvány érvényességi idejének lejártát követően is elérhetőnek kell lennie.

A szolgáltatási szabályzatban ismertetni kell az érvényességi információk elérésének a módját, beleértve az érvényességi időn túli elérés lehetőségeit.

A visszavonási nyilvántartások működtetése során a Szolgáltatónak az alábbi követelményeket kell teljesítenie:

- A tanúsítványállapot-információkat folyamatosan, napi 24 órában, heti 7 napban kell elérhetővé tenni.
- A tanúsítványállapot-információk elérését akadályozó külső vagy belső meghibásodások esetén a szolgáltatónak el kell követni mindent annak érdekében, hogy az információk elérhetőek legyenek a szolgáltatási szabályzatban jelzett maximális kiesési időn belül.
- Biztosítani kell a tanúsítványállapot-információk sértetlenségét és hitelességét.
- A visszavonási információt legalább a tanúsítvány eredeti érvényességi idejéig kell szerepeltetni a tanúsítványállapot-információk között.
- Tanúsítványvisszavonási listát és tanúsítványállapot szolgáltatást egyaránt nyújtani kell;
- A CRL és az OCSP szolgáltatásoknak egymással összhangban kell működniük, egy tanúsítvány állapotának változásáról szóló információnak mindkét szolgáltatásban elérhetőnek kell lennie.
- A tanúsítványvisszavonási információknak nyilvánosnak és nemzetközileg is elérhetőnek kell lenniük.
- A weboldal-hitelesítő tanúsítványokra (DVCP) vonatkozó visszavonási listának 3 másodpercen belül letölthetőnek kell lenni analóg telefonvonal esetén.⁵

⁵ 20MBit/sec ADSL kapcsolatot feltételezve

4.10.2 Szolgáltatások elérhetősége és rendelkezésre állása

Szolgáltatónak biztosítani kell a Tanúsítványtár, a Tanúsítványállapot szolgáltatás és a visszavonás-kezelés éves szinten számított legalább 99%-os rendelkezésre állását. Egy eseti szolgáltatás kiesés időtartama nem haladhatja meg a három órát.

A Szolgáltatónak továbbá biztosítani kell az általa kibocsátott Tanúsítványok használatára vonatkozó kikötések és feltételek folyamatos (7X24) elérhetőségét, éves szinten legalább 99%-os rendelkezésre állással.

Weboldal-hitelesítő tanúsítványok esetén a visszavonási nyilvántartások válaszideje normál terhelés esetén legfeljebb 10 másodperc lehet.

Lásd továbbá a 4.9.9 Tanúsítványállapot szolgáltatás rendelkezésre állása fejezetet.

4.10.3 További lehetőségek

Nincs előírás.

4.11 A szolgáltatási szerződés megszűnése

Nincs előírás.

4.12 Kulcsletét és kulcshelyreállítás

A végfelhasználói magánkulcs másolatára ugyanolyan szintű biztonsági előírások vonatkozik, mint az eredeti magánkulcsra. A végfelhasználói magánkulcsokról legfeljebb annyi másolatot szabad készíteni, ami elégséges a szolgáltatás fenntartásához.

4.12.1 A kulcsletét és -helyreállítás rendje és szabályai

Autentikációs és weboldal-hitelesítő tanúsítványok magánkulcsai esetében a szolgáltató nem biztosíthat kulcsletét szolgáltatást.

4.12.2 Szimmetrikus rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

Nincs előírás.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

A Szolgáltatónak gondoskodnia kell arról, hogy az elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, illetve az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazzon.

A Szolgáltatónak meg kell felelnie az alábbi követelményeknek:

- Rendszeresen elvégzett kockázatelemzéssel kell rendelkeznie (ennek részleteit lásd az 5.4.8-ban)
- Menedzsment által elfogadott, dokumentált, implementált és karbantartott információbiztonsági szabályozással kell rendelkeznie, beleértve a biztonsági kontrollok és műveleti eljárásokat a Szolgáltató létesítményei, rendszerei és információs eszközei számára, melyek a szolgáltatásnyújtást biztosítják. A Szolgáltató az információbiztonsági szabályozást minden érintett minden munkavállalójával.
- Szolgáltató felelősséget visel az információbiztonsági szabályozásában meghatározott eljárások betartásáért, akkor is, ha azokat nem szolgáltató saját személyzete végzi. Szolgáltatónak meg kell határoznia e közreműködők felelősségét, és biztosítania kell, hogy az előírt eljárásokat betartják.
- Az információbiztonsági szabályozást és vagyonnyilvántartást rendszeres időközönként vagy ha jelentős változások történnek felül kell vizsgálni, hogy biztosított legyen azok folyamatos alkalmazhatósága, megfelelősége és eredményessége. Minden változtatást, amely hatással van a biztonsági szintre, jóvá kell hagynia a Szolgáltató menedzsmentjének. A Szolgáltatói rendszerek konfigurációját rendszeresen ellenőrizni kell a biztonsági előírásokat sértő változások kiszűrése érdekében.

5.1 Fizikai óvintézkedések

A Szolgáltató gondoskodjon arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen, és a kritikus szolgáltatások eszközeinek fizikai kockázatát minimalizálják.

A Szolgáltató biztosítsa az értékek elvesztésének, sérülésének, és kompromittálódásának, valamint a működési tevékenységek megzavarásának elkerülését.

A Szolgáltató óvintézkedéseket valósítson meg az információ és az információ feldolgozó berendezések kompromittálódásának, illetve ellopásának elkerülése érdekében.

5.1.1 Telephely felépítése

A telephely kiépítése és a környezeti biztonság kezelése során szolgáltatónak figyelembe kell venni a tűz és vízvédelemre, a folyamatos áramellátásra, a légkondicionálásra, a fizikai behatolás megakadályozására, a biztonságos zónák kialakítására és a telekommunikációs hálózatok elérhetőségére és a sugárzás elleni védelemre vonatkozó ajánlásokat és előírásokat.

5.1.2 Fizikai hozzáférés

A Szolgáltató biztosítson egy egyértelműen meghatározott és fizikailag lehatárolt biztonsági területet a biztonságos működéséhez kritikus komponensei számára, amelyet a behatolás ellen fizikailag véd, ahova a bejutást ellenőrzi, az illetéktelen behatolást észleli és riasztani képes. Bármely más szervezettel, szervezeti egységgel megosztott rész e körleten kívül essen. Ugyanezen biztonsági területen belül más tevékenységek abban az esetben végezhetők, ha a területre belépési jogosultsággal rendelkezők azt el tudják végezni.

E kritikus szolgáltatások fizikai- és környezetbiztonsági programjai foglalkozzanak a fizikai hozzáférés szabályozásával, a természeti katasztrófa elleni védelemmel, a villámvédelem és tűzbiztonság tényezőivel, a támogató eszközök (ezen belül az áram és klíma berendezések) meghibásodásával, az építmény összeomlásával, vízvezeték szivárgással, talajvíz elleni védelemmel, lopás, betörés és behatolás elleni védelemmel, katasztrófa utáni helyreállítással.

Szolgáltató óvintézkedéseket valósítson meg

- a fizikai és környezetbiztonsági rendszererőforrások, illetve a működésük támogatására használt berendezések megvédése érdekében;
- annak megakadályozására, hogy az elektronikus aláírással kapcsolatos szolgáltatáshoz szükséges berendezés, információ, adathordozó vagy szoftver elveszen, megsérüljön vagy jogosulatlanul elvigyék a helyszínről.

A Szolgáltató a kritikus szolgáltatásaival kapcsolatos eszközökhöz történő fizikai hozzáférést megfelelően felhatalmazott egyénekre korlátozza, s az eszközöket olyan környezetben működtesse, amely fizikailag megvédi a szolgáltatásokat attól, hogy a rendszerekhez, illetve adatokhoz történő jogosulatlan hozzáféréseken keresztül kompromittálódjanak.

A biztonsági körletbe való belépéseket felügyelni kell, a nem jogosult személyek csak jogosult személyek felügyeletével tartózkodhatnak a körletben. A belépéseket és kilépéseket azok időpontjával és a tartózkodásának céljával együtt naplózni kell.

A szolgáltató gyökér kulcsok a normál operációtól elkülönített módon tárolhatók, a hozzáférést csak a bizalmi munkatársakra korlátozva.

5.1.3 Áramellátás, légkondicionálás

A Szolgáltató szolgáltatási helyszíneire olyan szünetmentes áramellátást kell biztosítani, amely megfelelő teljesítménnyel rendelkezik a rendszerek áramellátásához, rövid idejű kimaradás esetén, és tartós áramszünet esetén saját áramtermelő berendezés segítségével biztosított a rendszerek további működése.

A szolgáltatási helyszínrre bejutó levegő tisztaságát megfelelő szűrőrendszerrel kell biztosítani, amely kiszűri a levegőből a különféle szennyeződések, tovább biztosítja a szolgáltató munkatársai részére szükséges levegőt. A keringetett levegő nedvesség tartalmát és hőmérsékletét az informatikai rendszerek számára megfelelően kell beállítani.

A légkondicionáló rendszer teljesítménye olyan kell legyen, hogy képes legyen a szükséges hűtést biztosítani az IT rendszerek számára.

5.1.4 Beázás és elárasztódás veszélyeztetettsége

A Szolgáltató szolgáltatási helyszíneit védeni kell a beázástól és az elárasztódástól.

5.1.5 Tűzmegelőzés és tűzvédelem

A Szolgáltató szolgáltatási helyszíneit védeni kell a tűztől.

Az aktuális tűzvédelmi szabályzásoknak megfelelő tűz és füstérzékelőket, kézi és automata oltó berendezéseket kell felszerelni, jelezni kell a kézi oltó berendezések helyét, a menekülési útvonalat.

5.1.6 Adathordozók kezelése

A Szolgáltató az adathordozó eszközöket biztonságosan kezelje a sérülés, ellopás és jogosulatlan hozzáférés és az avulás elleni védelem érdekében. A Szolgáltató az összes adathordozó eszközt biztonságosan kezelje az adat-minősítési rendszer követelményeinek megfelelően. A média avulását és sérülését meg kell akadályozni az adatok teljes megőrzési idejében.

A Szolgáltató az érzékeny adatokat tartalmazó adathordozó eszköztől biztonságosan váljon meg, amennyiben azokra már nincs szükség. A selejtezett eszközök tartalmát - széles körben elfogadott módszerek alapján – véglegesen törölni kell, vagy az eszközt egyéb módon helyreállíthatatlanul tönkre kell tenni.

A Szolgáltatónak a kritikus adatokról több mentési példánnyal kell rendelkeznie, és egy példányt a szolgáltatói helyszíntől eltérő olyan külső helyszínen kell tárolni, melyben a mentések védelmének szintje azonos a szolgáltatási helyszínével.

5.1.7 Hulladékelhelyezés

Informatikai eszközeinek selejtezése esetén a szolgáltatónak biztonságosan és helyreállíthatatlanul törölnie kell az azon tárolt adatokat, vagy ha ez nem lehetséges legalább az ilyen elemet hordozó alkatrészt fizikai tönkretétellel megsemmisíti, ami annak olvashatóságát megakadályozza.

Iratok selejtezése esetén a személyes adatot tartalmazó iratokat megfelelő eljárással olvashatatlaná kell tenni.

Szolgáltatónak követni kell a hulladékról szóló 2012. évi CLXXXV. törvényt és a hivatkozott kormányrendeletet az elektronikai hulladékok megsemmisítése tekintetében.

5.1.8 Mentés külső helyszínen

A szolgáltatónak az üzemmenet folytonossága és az adatvesztés elkerülése érdekében mentéseket kell végeznie, és biztosítani kell az informatikai rendszer egészének szükség esetén való helyreállíthatóságát. A mentéseket védeni kell a jogosulatlan módosítástól, törléstől, megsemmisüléstől és a jogosulatlan hozzáféréstől. A rendkívüli helyzetekre való felkészülés magában foglalja a kidolgozott tervek adott esetekre történő alkalmazását és tesztelését is.

A megőrzendő adatok biztonságos tárolását a szolgáltató elvégezheti csak írható médiával, távoli helyen tárolt mentéssel, vagy több tárolási helyen történő távoli párhuzamos tárolással.

5.2 Eljárásrendi biztonsági intézkedések

Szolgáltatónak gondoskodnia kell rendszerei biztonságos, szabályszerű, a meghibásodás minimális kockázata melletti üzemeltetéséről. Ennek érdekében elegendő számú és megfelelő képzettséggel, műszaki tudással, tapasztalattal rendelkező személyzetet kell alkalmaznia.

A Szolgáltató a jogszabályoknak és szabályzatainak megfelelő és naprakész belső irányítási és ellenőrzési eljárásrendet és kapcsolódó felelősségi rendszert kell működtessen. A rendszer megfelelő működését a független rendszervizsgáló ellenőrzési tevékenységének kell biztosítani.

A Szolgáltatónak külső, független rendszervizsgáló által folyamatosan ellenőrzött minőségirányítási és információbiztonsági irányítási rendszerrel kell rendelkeznie.

A Szolgáltatónak a szolgáltatás nyújtása során létrejövő és kezelt adatot a jogszabályok és a szolgáltatási szabályzatban meghatározott kockázatelemzés alapján biztonsági osztályba kell sorolnia, és gondoskodnia kell azok megfelelő nyilvántartásáról, ellenőrzéséről, védelméről, valamint az ehhez szükséges felelősségi rendszer működtetéséről.

5.2.1 Bizalmi munkakörök

A Szolgáltatónál bizalmi munkakört csak olyan személy tölthet be, akinek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét, szakértelmét a szolgáltató szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

Az informatikai rendszerért általánosan felelős munkakört olyan személynek kell betöltenie, aki szakirányú felsőfokú végzettséggel⁶ és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik.

A szolgáltató a bizalmi munkakört betöltő személyt munkaviszonyban köteles foglalkoztatni, és a bizalmi munkakört betöltő személynek függetlennek kell lennie minden olyan érdektől, amely hátrányosan érintheti a szolgáltatás megbízhatóságát és biztonságát. A szolgáltatónak gondoskodnia kell arról, hogy a szolgáltatások nyújtásával kapcsolatban álló személy a szükséges és megfelelően naprakész tudással és tapasztalattal rendelkezzen. A szolgáltató valamennyi bizalmi munkakör betöltését köteles biztosítani, és a bizalmi munkaköröket nevesítenie kell.

Bizalmi munkaköröknek kell tekinteni a következőket:

- Biztonsági tisztviselő: A szolgáltatás biztonságáért általánosan felelős személy.
- Rendszeradminisztrátor: A szolgáltató informatikai rendszer telepítését, konfigurálását, karbantartását végző személy.

⁶ szakirányú felsőfokú végzettség a matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség

- Rendszerüzemeltető: A szolgáltató informatikai rendszerének folyamatos üzemeltetését, mentését és helyreállítását végző személy.
- Független rendszervizsgáló: A szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy
- Regisztrációs felelős: a tanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy

Bizalmi munkakört kizárólag a Szolgáltatóval munkaviszonyban álló munkatárs tölthet be, a Szolgáltató felső vezetésének formális kinevezését követően. Bizalmi munkakör megbízási szerződés alapján nem tölthető be.

A bizalmi munkakörökről naprakész nyilvántartást kell vezetni, változás esetén a változás tényét haladéktalanul be kell jelenteni a Bizalmi Felügyeletnek.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám

Szolgáltató Gyökér- és Köztes kiadóihoz tartozó kulcsok generálását (lásd 6.1.1) valamint e tanúsítványok magánkulcsainak mentését, megőrzését és visszaállítását fizikailag védett környezetben legalább kettő arra kijelölt és a műveletre közvetlen felhatalmazással rendelkező bizalmi munkatárs együttes fizikai jelenlétével kell elvégezni.

5.2.3 Az egyes szerepkörökhöz tartozó azonosítás és hitelesítés

Szolgáltató köteles az informatikai rendszerének minden felhasználóját és az adminisztratív folyamatok minden szereplőjét személy szerint azonosítani, kivéve a nyilvános adatszolgáltatásához kizárólag olvasási jogosultsággal rendelkező felhasználókat.

Szolgáltató informatikai rendszereihez csak az arra felhatalmazott személyek férhetnek hozzá. A szolgáltatónak adminisztrálnia kell a rendszeradminisztrátorok, rendszerüzemeltetők és Független rendszervizsgálók rendszerhozzáférést, beleértve a felhasználói fiók kezelését, alkalmi módosítását és adott esetben a hozzáférés megszüntetését.

Az egyes alkalmazásokhoz való hozzáféréseknek szolgáltató szabályozása szerint korlátozhatónak kell lennie. A rendszernek el kell tudnia különíteni az egyes bizalmi munkaköröket, így különösen a rendszeradminisztrátori és rendszerüzemeltető hozzáféréseket.

A személyzetet azonosítani és hitelesíteni kell a szolgáltatások szempontjából kritikus alkalmazások használata előtt, s tevékenységükkel kapcsolatban elszámoltathatónak kell lenniük.

5.2.4 Egyes szerepkörök összeférhetetlensége

A szolgáltatói eszközökben, rendszerekben végrehajtott azonosítatlan vagy nem szándékolt módosítások illetve más visszaélések lehetőségének csökkentése érdekében a Szolgáltatónak az egymást kizáró feladatokat és felelősségi területeket el kell különíteni.

A feladatkörök elhatárolása végett

- a biztonsági tisztviselő nem láthatja el a független rendszervizsgáló, a Rendszeradminisztrátor és az informatikai rendszerért általánosan felelős vezető feladatait, valamint
- a független rendszervizsgáló nem láthatja el a Regisztrációs felelős, a Rendszeradminisztrátor és az informatikai rendszerért általánosan felelős vezető feladatait.

A szolgáltatónak törekednie kell a bizalmi munkakörök teljes személyi elválasztására. A fentiekben túl az alábbi feladatköröket is el kell választania:

- a Biztonsági Tisztviselő nem láthatja el a Rendszeradminisztrátor feladatait, és
- a Független Rendszervizsgáló nem láthatja el a Regisztrációs felelős és a Rendszeradminisztrátor feladatait.

Szolgáltatónak biztosítani kell a regisztrációs feladatok elkülönítését, azaz, hogy a regisztrációs folyamat során a tanúsítvány kibocsátásához szükséges adatok ellenőrzését, érvényesítését és tanúsítványkibocsátás jóváhagyását ne ugyanaz a bizalmi munkatárs végezze. Az ellenőrzési eljárásoknak auditálhatónak kell lenniük.

5.3 Személyzeti biztonsági intézkedések

A Szolgáltató gondoskodjon arról, hogy alkalmazottai és szerződéses partnerei támogassák a szolgáltatások megbízhatóságát. A Szolgáltató bizalmi munkakörben foglalkoztatott személyzetének minden olyan összeférhetetlenségtől mentesnek kell lennie, amely a szolgáltatások nyújtásában végzett tevékenységének pártatlanságát sértheti

A személyzetnek az informatikai biztonsági eljárásokkal összhangban kell végrehajtani az adminisztrációs és menedzsment eljárásokat.

Az információbiztonsági szabályzatban azonosított biztonsági munkaköröket és felelőségeket munkaköri leírásokban vagy más az érintett felek számára elérhető dokumentációban dokumentálni kell. A bizalmi munkaköröket világosan meg kell határozni, be kell tölteni, és a megbízást el kell fogadnia a menedzsmentnek és az érintett személynek egyaránt.

A személyzetnek (beleértve az állandóan és ideiglenesen foglalkoztatottakat egyaránt) olyan munkaköri leírásokkal kell rendelkezni, amelyek a feladatok szétválasztása és legkevesebb jogosultság elvéből indulnak ki, s a pozíció bizalmas jellegének meghatározása a feladatok, a hozzáférési szintek, a háttér szűrés és az alkalmazott képzése és tudatossága alapján történik.

5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények

A Szolgáltató valamennyi munkatársának rendelkeznie kell a munkaköre ellátásához szükséges végzettséggel, gyakorlattal, megbízhatósággal és szakmai ismeretekkel, tapasztalattal. A Szolgáltató bizalmi munkakörben csak büntetlen előélettel rendelkező alkalmazottakat foglalkoztathat, amit a felvételi eljárás során 3 hónapnál nem régebbi erkölcsi

bizonyítvánnyal kell igazolni.

A szolgáltatónál bizalmi munkakört csak olyan személy tölthet be, akinek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét, szakértelmét a szolgáltató szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

Az informatikai rendszerért általánosan felelős munkakört olyan személynek kell betöltenie, aki a 24/2016 BM rendelet által elfogadott szakirányú felsőfokú végzettséggel és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik.

Szolgáltató a bizalmi munkatársakat munkaviszonyban köteles foglalkoztatni. Szolgáltatónak a bizalmi munkakörre jelölt személy foglalkoztatásának megkezdése előtt meg kell győződnie arról jelölt független minden olyan érdektől, amely hátrányosan érintheti a szolgáltatás megbízhatóságát és biztonságát.

Szolgáltatónak gondoskodnia kell arról, hogy a szolgáltatások nyújtásával kapcsolatban álló személy a szükséges és megfelelően naprakész tudással és tapasztalattal rendelkezzen (lásd 5.3.3 és 5.3.4).

Szolgáltató köteles biztosítani valamennyi bizalmi munkakör betöltését, és a bizalmi munkaköröket a szolgáltatási szabályzatban nevesítenie kell.

A szolgáltató menedzsmentjének megfelelő tapasztalattal kell bírnia a szolgáltató által nyújtott szolgáltatások területén, valamint informatikai biztonsági és kockázatkezelési területeken, valamint a biztonságért felelős menedzsereknek a biztonsági eljárások területén, annak érdekében, hogy menedzsment feladataikat elláthassák.

A Regisztrációs felelős számára Szolgáltatónak biztosítania kell a munkaköre ellátásához szükséges ismereteket biztosító tréninget. Szolgáltatónak vizsgáztatnia kell a Regisztrációs felelősöket a szabályzataiban meghatározott regisztrációs követelmények ismeretéből.

A Szolgáltató köteles olyan munkatársakat és adott esetben olyan alvállalkozókat alkalmazni, akik megbízhatóak, rendelkeznek a szükséges szakértelemmel, tapasztalattal és képesítésekkel, valamint megfelelő képzésben részesültek a biztonságra és a személyes adatok védelmére vonatkozó szabályokkal kapcsolatban, továbbá köteles olyan igazgatási és ügyvezetési eljárásokat alkalmazni, amelyek megfelelnek az európai és nemzetközi szabványoknak.

5.3.2 Ellenőrzési eljárások

A Szolgáltatónak a bizalmi munkakörben foglalkoztatandó személyek esetében (a szerződéses viszonytól függetlenül) meg kell győződnie e személyek személyazonosságáról fizikai jelenlétük során vagy fényképes személyazonosító okmányaik ellenőrzésével. Valamint meg kell győződnie e személyek megbízhatóságáról, ami magában foglalja a korábbi munkahelyekre, releváns végzettségekre és szakmai referenciákra vonatkozó információk ellenőrzését. Az ellenőrzések lefolytatását megelőzően nem kaphatnak hozzáférést a szolgáltató rendszereihez.

5.3.3 Képzési követelmények

A szolgáltatónak meg kell bizonyosodni arról, hogy a bizalmi munkakörben dolgozó személyek

rendelkeznek a feladataik ellátásához szükséges tudással. Ennek érdekében vizsgát kell tenniük a szükséges ismeretek birtoklását igazolandó. A Szolgáltató szolgáltatást nyújtó rendszereihez hozzáférési jogosultságot csak a sikeres vizsgát tevő személyek kaphatnak. A vizsga megtörténtét dokumentálni kell. A szolgáltatónak a vizsgát megelőzően az érintett személyek számára szükség szerinti mértékben támogatni kell a hiányzó ismeretek megszerzését a feladatuk ellátásához szükséges mértékben. A vizsgának és a képzésnek a következőket kell felölelnie:

- PKI alapismeretek;
- hitelesítés és ellenőrzési szabályok és eljárások;
- Biztonsági és adatvédelmi szabályok;
- általános fenyegetések az információhitelesítési eljárásokra (beleértve az adathalászt és egyéb social engineering taktikákat);
- jelen Szolgáltatási Rend, a Szolgáltatási Szabályzat és egyéb szabályzatok előírásai;
- egyes tevékenységük jogi következményei;
- Szolgáltató informatikai rendszerének sajátosságai és kezelésének módja;

5.3.4 Továbbképzési gyakoriságok és követelmények

A Szolgáltatónak gondoskodnia kell róla, hogy a bizalmi munkakört ellátó személyek folyamatosan rendelkezzenek a feladataik ellátásához szükséges tudással, így szükség esetén továbbképzést, vagy ismétlő jellegű képzést kell tartania. Így továbbképzést kell tartania, amennyiben a szabályzataiban vagy informatikai rendszerében olyan változás áll be, ami érinti e munkakörök tevékenységét. Legalább 12 havonta tájékoztatni kell a személyzetet - minden munkatársat a munkakörének megfelelő mértékben - az előző 12 hónapban ismertté vált esetleges új fenyegetettségekről és az aktuális biztonsági eljárásokról.

A továbbképzést megfelelően dokumentálni kell, amelyből utólag is megállapítható a továbbképzés tematikája és a résztvevők személye.

5.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága

Nincs előírás.

5.3.6 Jogosulatlan tevékenységek büntető következményei

A Szolgáltatónak megfelelő fegyelmi szankciókat kell alkalmazni szolgáltatói rendszerének nem engedélyezett használata vagy a szolgáltatás nyújtása közben elkövetett hibák, mulasztások, károkozások esetére az azt okozó alkalmazottak vagy közreműködő természetes és jogi személyek esetében. A lehetséges szankciókról a velük kötött szerződésben rendelkezni kell.

5.3.7 Szerződéses közreműködőkre vonatkozó követelmények

A Szolgáltató által szerződéses viszonyban közreműködő személyekre ugyanúgy vonatkoznak a szabályzatok elvárásai, mint az alkalmazottaira.

5.3.8 A személyzet számára biztosított dokumentációk

A Szolgáltatónak folyamatosan biztosítani kell a szolgáltatásnyújtásban közreműködő személyek részére a szerepkörük ellátásához szükséges aktuális szabályzatok és dokumentációk elérhetőségét.

5.4 Naplózási eljárások

A szolgáltatónak minden, az informatikai rendszerével és a szolgáltatás nyújtásával kapcsolatos eseményt, illetve az általa vagy számára kibocsátott adatokra vonatkozó összes lényeges információt - az üzemmenet folytonossága, az adatvesztés elkerülése, bizonyítékok bírósági eljárások során történő bemutatása, valamint az informatikai biztonság biztosítása érdekében - folyamatosan naplózni kell. A naplózott adatállománynak a szolgáltatás nyújtásának teljes folyamatát át kell fognia, és alkalmasnak kell lennie a szolgáltatással kapcsolatos minden esemény rekonstruálására a valós helyzetek megítéléséhez szükséges mértékben.

A naplózott adatállománynak a naplózott esemény bekövetkeztének naptári napját és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat és az eseményt előidéző felhasználó vagy más személy nevét kell tartalmaznia.

A naplózott adatállomány minden bejegyzését védeni kell a módosítástól és a jogosulatlan hozzáféréstől. A naplót úgy kell kezelni, hogy kizárható legyen a napló megsemmisítése, a napló bejegyzéseinek törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása, s hogy ezen védelmek a szolgáltató tevékenységeinek beszüntetését követő időszakra is kiterjedjenek. A szolgáltató a naplóról rendszeres mentést készít.

A szolgáltatónak gondoskodnia kell a naplóadatok folyamatos értékeléséről és ellenőrzéséről. Szolgáltatónak dokumentálni kell a naplózott információk elérésének módját és megőrzési idejét.

A Szolgáltatónak rögzíteni és egy meghatározott ideig folyamatosan hozzáférhetővé kell tenni - a tevékenységének megszűnése utáni időszakban is - minden lényeges információt beleértve a kiadott és fogadott adatokat, különösen a bírósági eljárásokban bizonyítékként való felhasználás érdekében, valamint a szolgáltatásfolyamatosság biztosítása céljából és a megfelelőségértékelés számára.

A naplóbejegyzések mellett el kell tárolni

- az bejegyzés (és ha eltér az esemény) dátumát és időpontját;
- az esemény típusát;
- az eseményvégrehajtás sikerességét illetve sikertelenségét;
- a felhasználó vagy rendszer azonosítóját, aki/amely az eseményt kiváltotta.

Amennyiben naplózó és naplóelemző rendszer működésében komoly rendellenesség lép fel, a Szolgáltató működését fel kell függeszteni az üzemzavar elhárításáig.

Az események mellett rögzített időinformációt legalább naponta szinkronizálni kell hiteles időforrással.

5.4.1 A tárolt események típusai

Az automatikusan és manuálisan rögzített naplóállományokban az alábbi eseményeket el kell tárolni:

1. Biztonsági események
 - a. Biztonsági profil változások
 - b. Rendszer indítása és leállítása
 - c. Tűzfal és router tevékenységek
 - d. Szolgáltatói rendszer hozzáférési kísérletek módja és eredménye (sikeres és sikertelen)
 - e. Szolgáltatói létesítménybe történő belépések és kilépések
2. Szolgáltatói rendszer beállításai
 - a. Rendszer telepítése
 - b. Rendszerkonfiguráció változásai (pl. frissítések, foltozások, beállítások)
 - c. Tanúsítvány és CRL profil megváltoztatása;
 - d. Rendszer vagy rendszeradatok mentése és visszaállítása
3. Szolgáltatói és végfelhasználói kulcsok életciklus műveletei
 - a. Kulcsgenerálás, másolatkészítés, tárolás, visszaállítás, archiválás és megsemmisítés
 - b. Kriptográfiai eszközök életciklus műveletei
4. Tanúsítványok életciklus műveletei
 - a. Igénylések, megújítások, kulcscserék, felfüggesztés, aktiválás, visszavonás
 - b. Életciklus műveleteket érintő ellenőrzési események
 - c. Igénylések elfogadása és visszautasítása
 - d. Tanúsítványkibocsátások
 - e. Visszavonási listák generálása
5. Pontos időt érintő események
 - a. Óraszinkronizációs események
 - b. Előírt időpontossági küszöb túllépése
6. Naplózási események
 - a. Naplózó rendszer leállítása, újraindítása;
 - b. Naplózási beállítás módosítása
 - c. Naplózási adatok archiválása-törlése;
7. Felhasználó menedzsment műveletek (Szolgáltatói rendszerek tekintetében)
 - a. Felhasználók felvétele, törlése
 - b. Szerepkörök vagy jogosultságok kiosztása, visszavonása
 - c. Státuszváltozások (pl. zárolás, tiltás, engedélyezés)
 - d. Előírt azonosítási módszer beállításai
 - e. Hitelesítési adat (pl. jelszó) cseréje
8. Rendellenes vagy veszélyt jelentő események
 - a. Rendszerösszeomlás és a hardver hibák;
 - b. Bármilyen szoftverművelet hibája;
 - c. Szoftverintegritás hiba;
 - d. Hálózati támadási kísérletek;
 - e. Elektromos hálózati üzemzavar;

- f. Szünetmentes tápegység hiba;
- g. Kommunikációs üzemzavar.

Az ügyféligenylések és tanúsítvány műveletek kapcsán az alábbi információk rögzítése szükséges:

- A műveletek dátuma és pontos ideje;
- A bemutatott dokumentumok típusai és azonosító adatai
- A bemutatott dokumentumok és az aláírt szolgáltatási szerződés vagy másolataik és ezek tárolási helye
- Az ügyfél által végzett bármilyen választás a szolgáltatás tekintetében (pl. szolgáltatási szerződésben)
- Az Ügyféligenlyt feldolgozó személy azonosítója
- A dokumentumok ellenőrzésének módszere - amennyiben több módszer is alkalmazható
- A feldolgozásban közreműködő hitelesítői és regisztrációs egységek azonosítói;
- Az ellenőrzés ideje, az ellenőrzéshez felkeresett személy adatai (pl. telefonszáma)

5.4.2 A naplófájl feldolgozásának gyakorisága

A Szolgáltatónak biztosítania kell a keletkezett naplóállományok rendszeres kiértékelését. A naplóállományokban rögzített bejegyzéseket a keletkezésüktől számított legkésőbb 1 héten belül ki kell értékelni a megfelelő szakértelemmel és jogosultságokkal rendelkező Független rendszervizsgálónak. A kiértékeléshez szoftvereszközök is igénybe vehetők.

A kiértékelés során meg kell győződni a vizsgált naplóállományok hitelességéről és sértetlenségéről.

A kiértékelés során elemezni kell

- a rendszerek által generált hibaüzeneteket,
- a forgalmi adatokban bekövetkezett jelentős változásokat,
- a szokványostól eltérő bármilyen rendkívüli mintákat,
- gyanús aktivitásokat.

A kiértékelés tényét, eredményeit és az esetlegesen feltárt problémák és kockázatok elhárítása érdekében meghozott intézkedéseket dokumentálni kell.

Az automatikus kiértékelő eljárásoknak riasztani kell a személyzetet a biztonságilag kritikusnak tűnő események észlelése esetén.

5.4.3 A naplófájl megőrzési időtartama

A naplóállományokban rögzített információkat meg kell őrizni az érintett tanúsítványok megőrzési idejéig, de legalább 10 évig (a Szolgáltatói rendszerben vagy archivált formában).

A Független rendszervizsgáló számára bármikor elérhetővé kell tenni a naplózott információkat.

5.4.4 A naplófájl védelme

Gondoskodni kell arról, hogy a naplóállományok, illetve a benne rögzített információk ne legyenek egyszerűen törölhetők vagy megsemmisíthetők. A rögzített információk bizalmasságát és integritását (beleértve a még nem és már archivált eseményeket is) fenn kell tartani a megőrzési idő végéig. A naplóállományokhoz csak az arra jogosultak – elsősorban a Független rendszervizsgálók – férhessenek hozzá. Jogi eljárás esetén az érintett információkat elérhetővé kell tenni az eljárásban érintett és erre feljogosított személyek számára.

5.4.5 A naplófájl mentési eljárásai

A naplóállományokat 2 példányban, fizikailag elkülönülő helyeken kell tárolni. Amennyiben a naplóbejegyzés egy helyen keletkezik, akkor legkésőbb 24 órán belül gondoskodni kell arról, hogy egy másik helyszínen is létrejöjjön róla másolat. Lásd az 5.1.6 Adathordozók kezelése és 5.1.8. Mentés külső helyszínen fejezeteit.

5.4.6 A naplózás adatgyűjtési rendszere

Nincs előírás.

5.4.7 Az eseményeket kiváltó Ügyfelek értesítése

Nincs előírás.

5.4.8 Sebezhetőség felmérése

A Szolgáltatónak legalább negyedévente sebezhetőségi felmérést kell végeznie, amely segítségével

- azonosítja az előrelátható belső és külső fenyegetettségeket, amelyek lehetővé tehetik a tanúsítványadatok vagy a Tanúsítványkibocsátási, tanúsítványkezelési és állapotváltoztatási folyamatok jogosulatlan elérését, nyilvánosságra hozatalát, megváltoztatását megsemmisítését vagy más visszaélést;
- feltérképezi e fenyegetettségek bekövetkezésének valószínűségét és a bekövetkezés esetén várható kárt is;
- értékeli a feltárt fenyegetettségek elhárítására alkalmazott folyamatok, védelmi intézkedések és informatikai rendszerek megfelelőségét.

5.5 Adatok archiválása

A Szolgáltató az egyes tanúsítványokkal kapcsolatosan rendelkezésére álló adatokat - ide értve a személyes adatokat is köteles megőrizni (időtartamot lásd az [5.5.2 fejezetben](#)). A Szolgáltatónak a megőréssel együtt olyan eszközt is biztosítania kell, amellyel a kibocsátott tanúsítvány tartalma megállapítható.

A Szolgáltatónak az archivált adatállomány minden bejegyzését védenie kell a jogosulatlan módosítástól, törléstől, megsemmisüléstől és jogosulatlan hozzáféréstől. Az elektronikus

formában tárolt archivált adatállományt legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel, és időbélyegzővel kell ellássa. A szolgáltató köteles biztosítani, hogy mindaddig, amíg az adatokat őrzi, azok hitelesek, az arra jogosult személyek számára hozzáférhetők és értelmezhetők legyenek.

5.5.1 Az archiválandó adatok típusa

A Szolgáltatónak az egyes tanúsítványokkal kapcsolatosan rendelkezésre álló információkat - beleértve az azok előállításával összefüggőket is - és az ahhoz kapcsolódó személyes adatokat meg kell őriznie. Így például:

- a tanúsítványigénylési eljárás során bekért és beszerzett információkat és dokumentációt (4.1 Tanúsítványigénylés);
- a tanúsítványállapot-változtatási eljárás során közzétett információkat (4.9.3 A visszavonási, felfüggesztési és aktiválási eljárás);
- a jelen Szolgáltatási rend szerint naplózott információkat (5.4 Naplózási eljárások).

5.5.2 Archiválási időtartam

A Szolgáltató a jelen Szolgáltatási rend szerint az egyes tanúsítványokkal kapcsolatban archivált adatokat az alábbi időtartamokig köteles megőrizni:

- a tanúsítvány érvényességének lejáratától számított 10 évig;
- a tanúsítványba foglalt adat valódiságával vagy érvényességével kapcsolatosan megindult jogvita esetén a jogvita jogerős lezárásáig.

A Szolgáltató az egyéb naplózott adatokat a keletkezésüktől, a szolgáltatási szabályzatot és annak módosításait pedig hatályon kívül helyezésétől számított 10 évig köteles megőrizni, vagy megőrzéséről gondoskodni.

5.5.3 Az archívum védelme

Az [5.4.4. A naplófájl védelme](#) fejezetben írtak szerint kell eljárni.

5.5.4 Az archívum mentési folyamatai

Az [5.4.5. A naplófájl mentési eljárásai](#) fejezetben írtak szerint kell eljárni.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Szolgáltatónak az archiválandó adatokat időadattal, vagy időbélyeggel kell ellátnia.

5.5.6 Az archívum gyűjtési rendszere

Nincs előírás.

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

Nincs előírás.

5.6 Kulcscsere

Szolgáltatónak le kell cserélnie kulcsát amennyiben valamely saját szolgáltatói tanúsítványa lejár, illetve, amennyiben alkalmazott kulcsai elavulnak, továbbá saját belátása szerint egyéb esetben is dönthet kulcscsere mellett.

Az új kulccsal kiállított új tanúsítvány esetében annak profilját és adatait az aktuális előírásokhoz és legjobb gyakorlathoz kell igazítani.

5.7 Katasztrófaelhárítás és helyreállítás

Szolgáltatónak megfelelő technikai és szervezeti intézkedéseket kell végrehajtani az általuk nyújtott szolgáltatások biztonságát fenyegető kockázatok kezelése érdekében. Ezen intézkedésekkel – figyelembe véve a legújabb technológiai fejleményeket – biztosítani kell, hogy a biztonsági szint arányos legyen a kockázat mértékével. Intézkedéseket kell végrehajtani különösen a biztonsági események megelőzése és azok hatásának minimálisra csökkentése, valamint az érdekeltek bármely esemény káros hatásairól való tájékoztatása érdekében.

Szolgáltatónak indokolatlan késedelem nélkül, de minden esetben az esetről való értesüléstől számított 24 órán belül értesíteni kell a felügyeleti szervet és adott esetben más érintett szerveket, például az információbiztonságért felelős nemzeti szervet vagy az adatvédelmi hatóságot a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről, amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra.

Amennyiben a biztonság megsértése vagy az adatok sértetlenségének megszűnése vélhetőleg hátrányosan érintheti azt a természetes személyt vagy szervezetet, aki szolgáltatást vett igénybe, a Szolgáltató a természetes személyt és szervezetet is indokolatlan késedelem nélkül értesíti a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről.

5.7.1 Incidens- és kompromittálódáskezelési eljárások

Az informatikai rendszerekbe való belépésekre, azok felhasználóira és a szolgáltatásigénylésekre vonatkozó rendszertevékenységeket a Szolgáltatónak folyamatosan ellenőriznie kell, az alábbi szempontokat figyelembe véve:

1. A tevékenységek ellenőrzésénél figyelemmel kell lenni a begyűjtött és elemzett adatok érzékenyégére.
2. A potenciális biztonsági sérülésre utaló rendellenes rendszertevékenységet (beleértve a szolgáltatói hálózatba való behatolást is), a Szolgáltatónak azonosítani és jelentenie kell.

3. A szolgáltatói informatikai rendszereknek az alábbi eseményeket kell ellenőriznie:
 - a. a naplózási funkciók indítását és leállítását;
 - b. a szolgáltatások rendelkezésre állását és működőképességét.
4. A Szolgáltatónak rövid időn belül és összehangoltan kell eljárnia a káreseményre való minél gyorsabb reagálás és a biztonsági sérülés hatásainak korlátozása érdekében. A Szolgáltatónak meg kell jelölnie azon riasztásokat és potenciálisan kritikus eseményeket, melyeket a bizalmi személyzetnek nyomon kell követnie és melyekről a belső szabályzatok szerint jelentést kell tennie.
5. Szolgáltató eljárásokat határoz meg az érintett felek értesítése érdekében a biztonságát vagy integritását sértő azon eseményekről, melyek jelentős hatással vannak a szolgáltatásra vagy az abban kezelt személyes adatokra.
6. Szolgáltató egy korábban nem ismert kritikus sebezhetőséget a felfedezése után 48 órán belül kezeli. Ha ez nem lehetséges, akkor létrehoz és életbe léptet egy tervet, amivel a kritikus sebezhetőség veszélyét enyhítheti, vagy tényszerűen dokumentálja, hogy a biztonsági rés nem igényel ilyen lépéseket.
7. Incidensjelentési és reagálási eljárásokat léptet életbe, melyekkel a biztonsági incidensek és zavarok okozta károk minimálisra csökkenthetők.

A Szolgáltatónak rendelkeznie kell Incidenskezelési és Katasztrófa-helyreállítási tervvel.

A Szolgáltató az üzletfolytonossági és katasztrófa-helyreállítási tervében dokumentálja azokat az eljárásokat, amivel értesíti és - lehetőség szerint - megvédi az Ügyfeleket és az érintett feleket katasztrófa, biztonsági kompromittálódás vagy üzleti kudarc esetén. Szolgáltató nem köteles nyilvánosságra hozni üzletfolytonossági és katasztrófa-helyreállítási tervét, de elérhetővé teszik őket a Független rendszervizsgálók kérésre. Szolgáltatónak évente tesztelni, felülvizsgálni, és frissítenie kell ezeket az eljárásokat.

Az üzletfolytonossági tervnek tartalmaznia kell:

1. A tervben foglalt intézkedések aktiválásának feltételei,
2. Vészhelyzeti eljárások,
3. Üzemszüneti eljárások,
4. Újraindulási eljárások,
5. A terv karbantartási ütemezése,
6. Tudatosító és oktatási követelményeknek,
7. Egyéni felelősségek,
8. Helyreállítási idő célkitűzés (RTO),
9. A készenléti tervek rendszeres vizsgálata,
10. Szolgáltató terve az üzleti tevékenységének fenntartására vagy helyreállítására kritikus üzleti folyamatainak sérülése vagy megszakadása esetén,
11. A kritikus kriptográfiai eszközök (kulcsok, kulcstároló eszközök, aktiváló kódok) eltérő helyen való tárolása;
12. Elfogadható kiesési és helyreállítási idő
13. A fontos üzleti információkról és szoftverekről történő biztonsági másolatotok készítésének gyakorisága,
14. A helyreállító létesítmények távolsága az elsődleges üzletviteli helyszíntől,
15. A berendezések biztosítására szolgáló eljárások katasztrófa után és a helyreállítás

előtt az eredeti, vagy egy távoli helyszínen.

5.7.2 IT erőforrások, szoftverek és/vagy adatok meghibásodása

A Szolgáltató informatikai rendszereit megbízható hardver és szoftver komponensekből kell felépíteni.

A kritikus funkciókat redundáns rendszerelemek alkalmazásával kell megvalósítani úgy, hogy azok egy elem meghibásodása esetén is képesek legyenek a további működésre.

A Szolgáltató olyan gyakorisággal készítsen teljes rendszermentést, amely biztosítja, hogy abból katasztrófa esetén a teljes szolgáltatás helyreállítható legyen.

A Szolgáltató üzletfolytonossági terve tartalmazzon előírásokat a kritikus rendszerelemek meghibásodása esetén végrehajtandó feladatokra.

A Szolgáltató a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leghamarabb indítsa újra a szolgáltatásait. A helyreállítása során elsőbbséget kell élvezzenek a tanúsítványállapot-információkat szolgáltató rendszerelemeknek.

Adatmentés és helyreállítás

- Szolgáltató működésének helyreállításához szükséges adatokat menteni szükséges, és biztonságos, lehetőleg távoli helyen kell tárolni, ami alkalmas arra, hogy lehetővé tegye a Szolgáltató működésének helyreállítását incidens vagy katasztrófa esetén.
- A fontos üzleti információkról és szoftverekről rendszeresen biztonsági másolatot kell készíteni. Megfelelő biztonsági mentési eszközöket kell biztosítani annak érdekében, hogy minden lényeges információt és szoftvert helyre lehessen állítani katasztrófa vagy médiasérülés után. A mentési rendszert rendszeresen tesztelni kell az üzletfolytonossági tervnek való megfelelés biztosítása érdekében.
- A biztonsági mentési és helyreállítási funkciókat 5.3 pontban meghatározott, releváns megbízható szerepkörrel rendelkező személyzetnek kell elvégezni.
- Amennyiben az előírások kettős kontrollt követlenek meg az adat kezeléséhez, akkor ezek helyreállításához is kettős kontrollt kell alkalmazni.

5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás

Végfelhasználói kulcs kompromittálódás

Lásd a 4.9.12 A kulcs kompromittálódásra vonatkozó speciális követelmények fejezetet.

Szolgáltatói kulcs kompromittálódás

- Szolgáltató üzletfolytonossági tervének (vagy katasztrófa-helyreállítási tervének) ki kell térni a Szolgáltatói kulcs kompromittálódás vagy annak gyanúja - mint katasztrófahelyzet - esetére, és tervezett folyamatokkal kell készülnie erre a helyzetre.
- A katasztrófát követően Szolgáltatónak lépéseket kell tennie a katasztrófa megismétlődésének elkerülése érdekében.

Szolgáltatói kulcs kompromittálódása esetén a Szolgáltatónak legalább:

- Tájékoztatnia kell az Ügyfeleit, Szolgáltatói partnereit és az Érintett feleket.

- Jeleznie kell, hogy az érintett szolgáltatói kulccsal kibocsátott tanúsítványok és tanúsítványállapot-információ már nem érvényesek; és
- Vissza kell vonni az érintett Szolgáltatói tanúsítványt.

Amennyiben bármelyik algoritmus (vagy a kapcsolódó paraméterek) - amiket a Szolgáltató vagy a Végfelhasználók alkalmaznak - nem felel meg az elvárásoknak a fennmaradó tervezett felhasználási időtartamra, akkor a Szolgáltató köteles:

- Tájékoztatnia kell az Ügyfeleit, Szolgáltatói partnereit és az Érintett feleket; és
- Vissza kell vonnia mindegyik érintett tanúsítványt.

5.7.4 A működés folytonosságának fenntartása katasztrófaesemény után

A szolgáltatónak rendelkeznie kell üzletfolytonossági tervvel, amit katasztrófa esetén életbe léptethet. Katasztrófa bekövetkezte esetén - beleértve valamely szolgáltatói aláíró magánkulcs vagy más hitelesítő adatának kompromittálódását is - szolgáltató normál működése a tervben foglalt időszakon belül helyreállítandó, s egyúttal gondoskodni kell az ismételten bekövetkező hibák megelőzéséről is.

Katasztrófa esetén (beleértve a Szolgáltatói kulcs vagy hitelesítési adat kompromittálódását vagy a szolgáltató rendszer kritikus elemeinek meghibásodását) a normál üzletmenet a lehető leghamarabb helyreállítandó.

A Szolgáltatónak a szolgáltatás folytonosságának biztosítása érdekében a rendkívüli üzemeltetési helyzetek esetére olyan eljárással kell rendelkeznie, amely lehetővé teszi a szolgáltatás mielőbbi helyreállítását. A visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása rendkívüli üzemeltetési helyzet bekövetkezése esetén minden más szolgáltatás vagy tevékenység helyreállítását megelőzi.

5.8 A Hitelesítő vagy Regisztrációs egység vagy a szolgáltatás megszűnése

Amennyiben Szolgáltató meg kívánja szüntetni szolgáltatásának nyújtását, erről legkésőbb a megszüntetést megelőzően hatvan nappal értesítenie kell Ügyfeleit, Szolgáltatói partnereit, az Érintett feleket. Ezt követően Szolgáltató nem bocsáthat ki az adott szolgáltatás kapcsán új tanúsítványt.

Szolgáltatónak a szolgáltatás megszüntetésekor teljesítenie kell a szabványokban megfogalmazott követelményeket.

A Szolgáltatás leállítása kapcsán a Szolgáltatónak az alábbi minimum intézkedéseket kell megtennie:

- A tervezett leállásról a szolgáltatási szabályzatban meghatározottak szerint értesítenie kell az Ügyfeleket és az Érintett feleket.
- Szolgáltatónak minden ésszerű erőfeszítést meg kell tennie annak érdekében, hogy egy erre alkalmas szolgáltató a nyilvántartásait és szolgáltatási kötelezettségeit legkésőbb a szolgáltatás leállításáig átvegye tőle.
- Szolgáltatónak kötelessége visszavonni a szolgáltatói tanúsítványokat, a hozzájuk

tartozó magánkulcsokat pedig meg kell semmisítenie.

- Szolgáltatónak a szolgáltatás leállítása után közvetlenül egy teljes rendszermentést és archiválást kell végeznie;
- a rendszermentést és az archivált adatokat pedig át kell adnia a szolgáltatást átvevő szolgáltatónak.

A Szolgáltatás megszűnéséből fakadó esetleges zavarokat minimalizálnia kell a Szolgáltatónak. Ennek érdekében:

- Rendelkeznie kell egy naprakész tervvel a szolgáltatás megszüntetésére vonatkozóan, a szolgáltatás folytonosságának biztosítása érdekében;
- A szolgáltatói magánkulcsokat (beleértve azok biztonsági mentéseit is) visszaállíthatatlan módon meg kell semmisítenie.
- A megszüntetés költségeinek a fedezetét Szolgáltatónak biztosítani kell arra az esetre is, amennyiben csődbe menne vagy egyéb okok miatt nem tudná fedezni a költségeket önerőből.
- Meg kell szüntetnie minden Szolgáltatói partnerének a felhatalmazását, ami a Tanúsítványkibocsátási tevékenységben való közreműködésre vonatkozik.
- Köteles gondoskodni kötelezettségeinek ellátásáról és a tanúsítványok ellenőrzéséhez szükséges adatok folyamatos elérhetőségéről, és a tárolt adatainak kezeléséről - beleértve a regisztrációs adatokat és a napló állományokat - ezt követően is (saját maga vagy szolgáltatónak átadva azokat).
- A tevékenység megszüntetését legalább húsz nappal megelőzően köteles az általa kibocsátott és még vissza nem vont tanúsítványokat visszavonni.
- Tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel ellátott mentést kell készítenie. A mentett adatállományokat védenie kell a jogosulatlan módosítástól, és a jogosulatlan hozzáféréstől, s biztosítania kell, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára legyenek csak hozzáférhetők és értelmezhetők.

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

Szolgáltató köteles megfelelő intézkedéseket hozni az adathamisítás és az adatlopás ellen; ennek érdekében meg kell győződnie arról, hogy a szolgáltatásnyújtáshoz - elsősorban a kriptográfiai kulcsok és aktiváló adataik kezeléséhez - alkalmazott rendszerek és termékek a teljes életciklus alatt megbízhatóak és védettek a módosítás ellen.

6.1 Kulcspár generálás és telepítés

A Szolgáltatónak megfelelő biztonsági kontrollokat kell alkalmazni a kriptográfiai kulcsok és eszközök kezelésére, azok teljes életciklusában.

Amennyiben az eszköz tanúsítása érvényességét vesztené, akkor szolgáltatónak megfelelő intézkedéseket kell hoznia az adott eszközre kiadott tanúsítványokkal kapcsolatosan, melyeket szolgáltatási szabályzatában dokumentálnia kell.

6.1.1. Kulcspár előállítása

Szolgáltatónak a kulcsokat védett módon kell generálni és a magánkulcsok bizalmasságáról gondoskodnia kell.

A szolgáltatói kulcsok generálására vonatkozóan az alábbiakat kell követni:

- A szolgáltatói kulcsok generálását és a nyilvános kulcs tanúsítását fizikailag védett környezetben kell megvalósítani legalább két bizalmi munkakört betöltő személy együttes részvételével. E műveletre feljogosított munkatársak számát a minimumon kell tartani és a tevékenységnek a szabályzatokkal összhangban kell zajlani.
- A szolgáltatói kulcsok generálásánál csak olyan algoritmus és kulcshosszúság használható, amely megfelel az adott felhasználási célra vonatkozó szabványoknak, illetve a Nemzeti Média- és Hírközlési Hatóság engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának a tanúsítvány érvényességi ideje alatt.
- A szolgáltatói kulcsok generálására csak olyan kriptográfiai modulok alkalmazhatók, amelyek megfelelnek a szolgáltató szabályzataiban nyilvánosságra hozott műszaki és egyéb követelményeknek. A kulcsok nem importálhatók olyan eszközökbe, amelyek az alkalmazásra vonatkozó elvárásokat nem teljesítik.
- A ténylegesen alkalmazott algoritmusokat a Szolgáltatási szabályzatban fel kell tüntetni.
- A végfelhasználói tanúsítványok aláírását ellátó szolgáltatói tanúsítványok lejáratát megelőzően a szolgáltatónak új tanúsítványt kell generálnia, s mindent el kell követnie annak érdekében, hogy a tanúsítvány cseréje ne okozzon zavart az érintett felek számára.
- Ezeket a műveleteket úgy kell elvégezni, a megfelelő időtartam álljon rendelkezésre minden szolgáltatói partner és érintett fél számára az átállási feladatok végrehajtására. Ez nem vonatkozik arra az esetre, amikor a Szolgáltató befejezi a tevékenységét.
- Szolgáltatónak dokumentált eljárásokkal kell rendelkeznie a szolgáltatói kulcsok generálására, aminek legalább a következőket kell tartalmaznia:

- Munkakörök, akik részt vesznek az eljárásban (akár belső, akár külső résztvevőről van szó);
- A munkakörök által végrehajtandó feladatok az egyes fázisokban;
- Felelősségek az eljárás során és azt követően;
- Az eljárás során végrehajtandó adminisztrációs feladatok (amik bizonyítékul is szolgálnak a későbbiekben a megfelelésre).
- A szolgáltatónak az eljárás során egy olyan riportot kell előállítania, ami bizonyítja, hogy az megfelelt a szabályozásnak, és a kulcspár integritása és bizalmassága biztosított volt. A riportot alá kell írnia:
 - Gyökér Kiadó esetén az a bizalmi munkakört betöltő személynek, aki felelős a kulcsgenerálásért és egy a szolgáltató menedzsmentjétől független auditornak, aki az eljárást követve biztosítja, hogy a riport hűen dokumentálja a végrehajtott eljárást.
 - Köztes Kiadó esetén az a bizalmi munkakört betöltő személy, aki felelős a kulcsgenerálásért és aki az eljárást követve biztosítja, hogy a riport hűen dokumentálja a végrehajtott eljárást.

Amennyiben a végfelhasználói kulcsokat a szolgáltató vagy a végfelhasználó állítja elő:

- A szolgáltatói által generált végfelhasználói kulcsok esetén olyan algoritmusok alkalmazhatók, amelyek a tanúsítvány érvényességi ideje alatt megfelelnek a hitelesítési rend szerinti felhasználási célra.
- A végfelhasználói kulcsok generálásánál csak olyan algoritmus és kulcshosszúság használható, amely megfelel a hitelesítési rend szerinti felhasználási célra vonatkozó szabványoknak, illetve a Nemzeti Média- és Hírközlési Hatóságnak engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának a tanúsítvány érvényességi ideje alatt.
- Amennyiben a végfelhasználói tanúsítványban feltüntetésre kerülő másodlagos hitelesítési rend OID-ja szerint a kulcs kriptográfiai eszközre kerül generálásra (lásd az 1.2.1 fejezetet), a kulcsokat Kriptográfiai eszközben kell generálni. A szolgáltatónak vissza kell utasítani azon igényléseket, amelyek nem felelnek meg a 6.1.5 és 6.1.6 fejezetekben közzétett kulcselvárásoknak.
- A szolgáltatói által generált végfelhasználói kulcsokat biztonságos módon kell előállítani és megőrizni, amíg a szolgáltató kezelésében vannak.

A szolgáltató kulcsokat egy biztonságos kriptográfiai modulban kell generálni, ami megfelel 6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások fejezetben ismertetett elvárásoknak.

A Szolgáltató új Gyökér Kiadó kulcsainak előállítását egy minősített auditornak is meg kell figyelni, ellenőrizve a fenti követelményeknek való megfelelést, illetve a kulcspár integritását és bizalmasságát. Az auditornak egy igazolást kell kiállítani, arról hogy a szolgáltató:

- A Gyökér Kiadó kulcselőállítási és védelmi eljárásait dokumentálta szabályzataiban;
- A kulcselőállító eljárás megfelelő részletezettségű;
- Hatékony kontrollokkal gondoskodott arról, hogy a kulcsgenerálás az előírásokkal összhangban megfelelő biztonsági szinten történjen meg;
- A kulcselőállító eljárás valamennyi eljárását végrehajtotta.

6.1.2. Magánkulcs eljuttatása Végfelhasználóhoz

A végfelhasználó magánkulcsa olyan módon juttatandó el a végfelhasználó eszközére, illetve a Szolgáltatóhoz, aki azt kezelni fogja, ami biztosítja a bizalmasságát és integritását. Amennyiben a magánkulcs nem annak Átvevőjéhez kerülne eljuttatásra, akkor a magánkulcshoz tartozó összes tanúsítványt vissza kell vonnia Szolgáltatónak.

Szolgáltatónak a végfelhasználói magánkulcs minden példányát törölnie kell az Átvevőhöz való eljuttatást követően, kivéve a 4.12 Kulcsletét és kulcshelyreállítás fejezetben megadott eseteket.

Szolgáltatónak gondoskodnia kell az Ügyféleszközök biztonságáról annak elkészítése, tárolása és Átvevőhöz juttatása során.

6.1.3. A nyilvános kulcs eljuttatása a tanúsítványkibocsátóhoz

Amennyiben a végfelhasználó állította elő a kulcspárt és a tanúsítvány kérelmet, a kérelem szolgáltatóhoz eljuttatásával (mely technikailag igazolja a kulcspár mindkét tagjának birtoklását) igazolja, hogy rendelkezésre áll.

6.1.4. A szolgáltatói nyilvános kulcs közzététele

A szolgáltatónak a szolgáltatói nyilvános kulcsot egy szolgáltatói tanúsítványa részeként Interneten elérhetővé kell tennie az érintett felek számára.

6.1.5. Kulcsméretek

A 6.1.1 fejezetben megfogalmazottak az alábbiakkal egészülnek ki a weboldal-hitelesítő tanúsítványoknak (DVCP) esetében A használt algoritmusoknak az alábbiak valamelyikén kell alapulnia:

Lenyomatoló algoritmus: SHA-256, SHA-384, SHA-512

Kódoló algoritmus: RSA-2048, DSA-2048-224, DSA-2048-256 vagy NIST P-256 / P-384 / P-521 ECC.

6.1.6. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A kulcsok előállításának paraméterei az Algoritmus határozatnak megfelelő értékeket vesznek fel.

6.1.7. A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)

A Gyökér Kiadó kulcsa kizárólag a következő célokra alkalmazható:

- Gyökér Kiadó tanúsítványának aláírása (Önaláírt tanúsítvány)
- Köztes Kiadó tanúsítványának aláírása és keresztthitelesítés

- Belső Szolgáltatói tanúsítványok aláírása (pl. OCSP válaszadó)
- Tesztelési célra, amennyiben az Éles felhasználáshoz a Gyökér Kiadó aláírása szükséges

6.2 Magánkulcs védelem és kriptográfiai modul előírások

Szolgáltatónak olyan fizikai és logikai védelmeket kell implementálni, amelyek megakadályozzák a jogosulatlan tanúsítványkibocsátást.

A Szolgáltatónak a magánkulcsát biztonságos módon kell tárolnia. Meg kell akadályoznia, hogy a szolgáltatói magánkulcshoz jogosulatlan személy hozzáférhessen, és a kulcsot arra jogosulatlan személy használhassa.

A szolgáltató a tanúsítványok előállításához, a kibocsátott tanúsítványt tartalmazó nyilvántartáshoz és a visszavonási nyilvántartáshoz használt szolgáltatói magánkulcsokat csak fizikailag védett környezetben, az adott kulcsra meghatározott rendeltetési célra használhatja fel.

A hardveres kriptográfiai eszközök kezelése során a használatból kivont eszközökben tárolt magánkulcsokat olyan módon kell törölni, hogy azok visszaállítása ne legyen lehetséges.

Ha a szolgáltató a titkosításra, vagy autetnikációra használt adat előállításáról és annak eszközben való elhelyezéséről maga gondoskodik, akkor:

- a titkosításra, vagy autetnikációra használt adat előállítását fizikailag védett környezetben köteles végezni, kizárólag bizalmi munkakört betöltő személyek részvételével;
- a titkosításra, vagy autetnikációra használt adatot csak a tanúsítvány alany ügyféleszközében tárolhatja. Ha a titkosításra, vagy autetnikációra használt adatot a titkosításra, vagy autetnikációra használt eszközön kívül hozzák létre, a titkosításra, vagy autetnikációra használt adat a titkosításra, vagy autetnikációra használt eszközön kívüli minden másolatát azonnal törölnie kell - oly módon, hogy a törölt másolat további használata lehetetlenné váljon -, amint a titkosításra, vagy autetnikációra használt adat a titkosításra, vagy autetnikációra használt eszközbe kerül;
- biztosítja, hogy a titkosításra, vagy autetnikációra használt adathoz mások ne férhessenek hozzá;
- a titkosításra, vagy autetnikációra használt eszköz használatához szükséges, a tanúsítvány alany hozzáférési jogosultságát ellenőrző adatot (így különösen PIN-kódot) csak abból a célból rögzítheti, hogy azt a tanúsítvány alany számára - másolat megőrzése nélkül - átadhassa;
- a titkosításra, vagy autetnikációra használt eszközt, valamint a végfelhasználó hozzáférési jogosultságát ellenőrző adatot csak közvetlenül az Ügyfél vagy az általa feljogosított természetes személy (Átvevő) - számára adhatja át, naplózva az átadás időpontját is.

6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

A szolgáltatói magánkulcs tárolásának és felhasználásának egy biztonságos kriptográfiai eszközön kell megvalósulni, amely:

- Legalább EAL4 tanúsítással rendelkezik az ISO/IEC 15408 vagy azzal ekvivalens IT biztonsági elvárásrendszer szerint; vagy
- Megfelel az ISO/IEC 19790 vagy a FIPS PUB 140-2 [12] elvárásainak 3. szinten.

A Szolgáltatónak elkülönítve kell kezelni és működtetni

- a minősített szolgáltatás nyújtásához használt bizalmi szolgáltatást megvalósító terméket az egyéb tevékenységeihez használt termékektől;
- a minősített szolgáltatások nyújtásához használt bizalmi szolgáltatást megvalósító termékeit a nem minősített szolgáltatásokhoz használt bizalmi szolgáltatást megvalósító termékektől.

A szolgáltató egyéb tevékenységeihez használt termékek nem befolyásolhatják a bizalmi szolgáltatást megvalósító termék megbízható üzemeltetését.

A nem-minősített szolgáltatónak a bizalmi szolgáltatást megvalósító termékeit a szolgáltatási szabályzatban meghatározott kockázatelemzések alapján biztonsági osztályokba kell sorolnia, és ezekről nyilvántartást vezetnie.

Mielőtt a szolgáltató a szolgáltatás nyújtásához használt szolgáltatást megvalósító termékeit a saját maga által végzett szolgáltatásnyújtáson kívüli célokra használja fel, meg kell bizonyosodnia arról, hogy a termék nem tartalmaz olyan adatot, amely bizalmi szolgáltatáshoz fűződik, valamint arról, hogy az ilyen adatot nem lehet visszaállítani. E vizsgálatot és a vizsgálat eredménye alapján végrehajtott intézkedést a szolgáltatónak naplóznia kell.

6.2.2. Magánkulcs többszereplős (n-ből m) használata

Szolgáltató belső Biztonsági Szabályzatának részletes leírást kell tartalmaznia a többszereplős magánkulcskezelés módjáról. Amennyiben jelen Szolgáltatási Rend vagy a Szolgáltatási Szabályzat egy magánkulcs többszereplős kezelését írja elő, az adott művelet végzésére felhatalmazott bizalmi munkatársaknak ezen leírás szerint kell eljárniuk.

6.2.3. Magánkulcs letétbe helyezése

Lásd a 4.12 fejezetet.

6.2.4. Magánkulcs mentése

Szolgáltatói magánkulcsairól Szolgáltatónak biztonsági másolatokat kell készítenie. A szolgáltatói magánkulcsok mentését (másolását), tárolását és helyreállítását Szolgáltatónak fizikailag védett környezetben, a többszereplős magánkulcskezelés szabályai szerint kell megvalósítania legalább két bizalmi munkakört betöltő személy együttes részvételével. E műveletre feljogosított munkatársak számát a minimumon kell tartani és a tevékenységnek a szabályzatokkal összhangban kell zajlani.

A szolgáltatói magánkulcs biztonsági mentéséből/mentéseiből legalább egy példányt a szolgáltatás nyújtásától eltérő helyszínen kell tárolni.

A szolgáltatói magánkulcs számára a kriptográfiai eszközön kívül is az eszköz által biztosított védelmi szintet kell biztosítani. A kulcs titkosítása során olyan algoritmust és kulcsméretet kell alkalmazni, ami annak teljes hátralévő idejében biztosítja a védelmet. A szolgáltatói magánkulcs nem üzemben lévő másolatait legalább a produktív kulccsal azonos szintű biztonsági eljárásokkal kell védeni.

6.2.5. Magánkulcs archiválása

Nincs előírás

6.2.6. Magánkulcs bejuttatása kriptográfiai modulba, vagy onnan történő exportja

A szolgáltatói magánkulcsok kriptográfiai modulba juttatását Szolgáltatónak fizikailag védett környezetben, a többszereplős magánkulcskezelés szabályai szerint kell megvalósítani legalább két bizalmi munkakört betöltő személy együttes részvételével.

6.2.7. Magánkulcs tárolása kriptográfiai modulban

Amennyiben a szolgáltatói magánkulcs egy dedikált kriptográfiai eszközön kerül tárolásra, akkor gondoskodni kell arról, hogy a kulcsok ne legyenek elérhetők az eszközön kívül.

A kriptográfiai eszköz esetében gondoskodni kell a hamisítás elleni védelemről a szállítás és a tárolás során is, és biztosítani kell a helyes működését.

6.2.8. A magánkulcs aktiválásának módja

A szolgáltatói magánkulcsok aktiválását Szolgáltatónak fizikailag védett környezetben, a többszereplős magánkulcskezelés szabályai szerint kell megvalósítani legalább két bizalmi munkakört betöltő személy együttes részvételével.

A végfelhasználói magánkulcs használatához, amennyiben annak tárolása eszközön történik, az eszközhöz/szolgáltatáshoz tartozó aktiváló kód megadása szükséges.

6.2.9. A magánkulcs deaktiválásának módja

Nincs előírás

6.2.10. A magánkulcs megsemmisítésének módja

A lejárt vagy használaton kívül helyezett szolgáltatói magánkulcsok minden (éles, mentett vagy archivált) példányát meg kell megsemmisíteni, olyan módon hogy az ne legyen visszaállítható, illetve használható.

Kriptográfiai eszköz megsemmisítése esetén gondoskodni kell a rajta tárolt magánkulcsok megsemmisítéséről (ez az előírás nem vonatkozik a kulcs összes példányára, csak az

eszközön lévőre).

A végfelhasználói tanúsítványok magánkulcsait végfelhasználónak (aláírási szolgáltatás esetén a Szolgáltatónak) visszaállíthatatlan módon meg kell semmisítenie amennyiben a tanúsítvány visszavonásra kerül vagy érvényessége lejár és a magánkulcshoz tartozó nyilvános kulccsal újabb tanúsítvány nem kerül kiadásra.

6.2.11. A kriptográfiai modulok értékelése

Lásd a 6.2.1 fejezetet.

6.3 A kulcspárkezelés további szempontjai

A Szolgáltatónak megfelelő módon kell használnia szolgáltatói kulcsokat, s nem használhatja őket az érvényességük végét követően.

- A tanúsítványokat és érvényességi információkat szolgáltatói kulcsok nem használhatók semmilyen más célra.
- A tanúsítványok szolgáltatói kulcsokait csak fizikailag védett helyszínen használhatók.
- A Szolgáltatói magánkulcsnak kompatibilisnek kell lenni a 6.1.1 fejezettel összhangban a tanúsítványok aláírására alkalmazott lenyomat és aláíró eljárásokkal és kulcshosszakkal.
- Amennyiben a Szolgáltató önaláírt tanúsítványt bocsát ki, a tanúsítvány attribútumainak az ITU-T X.509 szerint meg kell felelni a meghatározott kulcshasználatnak.

A szolgáltatási szerződés lejárátát követően a végfelhasználót törölni kell.

Az aláírásszolgáltatás részeként a tanúsítványszolgáltatásra vonatkozóan rögzített végfelhasználói adatokat (tanúsítványigénylés adatai) Szolgáltató nem tárolhatja az aláírásszolgáltatás keretén belül, a tanúsítványszolgáltatás felé pedig változatlan formában kell továbbítania.

- meg kell semmisítenie a végfelhasználói tanúsítvány visszavonása esetén (lásd a 6.2.10 fejezetet);
- aláírás vagy bélyegző létrehozására nem használhatja fel.

6.3.1 Nyilvános kulcs archiválása

Nincs előírás

6.3.2 Tanúsítvány és kulcspár használati idő

A weboldal-hitelesítő végfelhasználói tanúsítványok (DVCP) érvényességi ideje nem lehet 398 napnál hosszabb.

A nem eIDAS tanúsítványok (NCP és NCP+) érvényességi ideje nem haladhatja meg azt az időt, amely időpontig az alkalmazott kriptográfiai algoritmusok biztonságosan felhasználhatók, de legfeljebb a szabványban megadott élettartamot (kibocsátástól számított 2 évet).

A teszttanúsítványok érvényességi ideje legfeljebb 2 év(24 hónap) lehet, amit Szolgáltató

tetszőleges mértékben korlátozhat.

6.4 Aktiváló adat

Az aktiváló adattal kapcsolatos kérdéseket az alábbi fejezetek írják le.

A Szolgáltatói kulcspár telepítése és helyreállítása a kriptográfiai eszközön kizárólag bizalmi munkakörben foglalkoztatott munkatársak legalább kettős kontrollja alatt valósulhat meg.

A Szolgáltatónak biztosítani kell az Ügyféleszköz aktiváló adatának megváltoztatását az aktuális aktiváló adat ismeretében. A végfelhasználói aktiváló adatot a Szolgáltató semmilyen körülmények között nem tárolhatja, kivéve az aláírási munkafolyamat idejére a memóriában való tárolás esetét.

6.4.1 Aktiváló adat generálás és telepítés

Az Aktiváló adat előállításának biztonságosan kell megvalósulni és az Ügyféleszköztől, illetve a magánkulcstól külön szabad csak Végfelhasználó részére eljuttatni.

6.4.2 Aktiváló adat védelme

A végfelhasználói aktiváló adatát kizárólag a végfelhasználó ismerheti meg.

6.4.3 Egyéb aktiváló adattal kapcsolatos előírások

Az Ügyféleszközök aktiválásának és deaktiválásának biztonságosan kell megvalósulni.

6.5 Informatikai biztonsági előírások

A szolgáltatónak a rendszerei elérését csak az arra jogosult személyek számára kell korlátozni. Ennek érdekében

- Tűzfalakkal védi a belső zónák határát a jogosulatlan hozzáférés megakadályozása érdekében (beleértve az Ügyfelek és Érintett felek általi eléréseket is).
- Az érzékeny adatokat (beleértve a regisztrációs adatokat) védeni kell az adathordozók újrafelhasználása során történő feltárástól.

Az egyes tevékenységekre a következő követelmények vonatkoznak:

Tanúsítvány generálás

- A helyi hálózati eszközöknek fizikailag és logikailag is biztonságos helyre kerülni, konfigurációjukat rendszeresen felül kell vizsgálni az Szolgáltatói előírásaival szemben.

Közzététel

- A tanúsítványtárhoz tanúsítványok hozzáadása, törlése és a kapcsolódó információk módosítása csak az arra jogosultak számára legyen lehetséges.

Tanúsítvány visszavonás

- A visszavonási információk módosítása csak az arra jogosultak számára legyen lehetséges.

Tanúsítvány kiadás és állapotváltoztatás

- A szolgáltató folyamatosan monitorozó és riasztó eszközöket biztosítson annak érdekében, hogy észlelhesse, rögzíthesse és időben reagálhasson bármilyen az erőforrásait érintő jogosulatlan vagy szokatlan hozzáférési próbálkozásra.

6.5.1. Speciális informatikai biztonsági műszaki követelmények

Szolgáltatónak multifaktoros azonosítást kell megkövetelnie minden Tanúsítványkibocsátásra jogosult felhasználó esetében.

6.5.2. Az informatikai biztonság értékelése

Nincs megkötés.

6.6 Életciklusra vonatkozó biztonsági előírások

6.6.1 Rendszerfejlesztési előírások

A biztonsági követelmények elemzését el kell végezni a - Szolgáltató által vagy az ő megbízásából végzett - rendszerfejlesztési projektek tervezési és követelmény meghatározási szakaszában, annak érdekében, hogy a biztonság be legyen építve az informatikai rendszerekbe.

Változáskezelési eljárásokat kell alkalmazni a Szolgáltatói szoftver új verzióinak kiadásai, a szoftvermódosítások és szoftverjavítások esetén, valamint a konfigurációváltozásokra, amelyek a Szolgáltató biztonsági szabályait érintik. Az eljárások között szerepelni kell a dokumentáció aktualizálásának is.

Szolgáltatónak biztosítania kell a szolgáltatás nyújtásához a szabályozott változáskezelést és a megbízható üzemeltetést, továbbá az üzemeltetés elválasztását a fejlesztéstől.

6.6.2 Biztonságkezelési előírások

A Szolgáltatónak megbízható rendszereket és termékeket kell használnia, amelyek védettek változtatásokkal szemben, és biztosítják az általuk támogatott eljárások technikai biztonságát és megbízhatóságát.

- A Szolgáltatói rendszereket és információkat védeni kell a vírusok, a rosszindulatú és a nem engedélyezett szoftverektől.
- Eljárásokat kell megállapítani és végrehajtani az összes megbízható és adminisztratív szerepkörre, amelyek hatással vannak a szolgáltatások nyújtására.
- Szolgáltatónak eljárásokat kell meghatározni és alkalmazni biztosítandó, hogy:
 - a biztonsági javítások ésszerű időn belül (legfeljebb 6 hónapon belül) alkalmazásra kerülnek, miután azok megjelentek;

- A biztonsági javítások nem alkalmazhatók, ha azok olyan plusz biztonsági réseket tartalmaznak vagy instabilitást okozhatnak, amelyek hátrányosabbak, mint a kínált javítás; és a nem alkalmazás okai dokumentálásra kerültek.

Szolgáltatónak megbízható rendszereket kell használni a számára szolgáltatott adatok ellenőrizhető formában történő tárolására, olyan módon, hogy:

- az adatok kizárólag annak a személynek a hozzájárulásával legyenek nyilvánosan kereshetők, akire az adatok vonatkoznak;
- kizárólag arra feljogosított személyek végezhesenek bejegyzéseket és változtatásokat a tárolt adatokon;
- ellenőrizhető legyen az adatok hitelessége.

6.6.3 Életciklusra vonatkozó biztonsági előírások

Szolgáltatónak figyelemmel kell követnie az erőforrások igénybevételét és előrejelzéseket kell készítenie a jövőbeni kapacitásszükségletek várható alakulásáról, annak érdekében, hogy elegendő teljesítmény és tárterület álljon rendelkezésre a Szolgáltatás stabil működtetéséhez.

Szolgáltatónak gondoskodnia kell a szolgáltatásnyújtás során felhasznált kriptográfiai hardvereszközök védelméről azok teljes életciklusa alatt, valamint gondoskodnia kell az alábbiakról:

- Az alkalmazott kriptográfiai hardvereszköznek megfelelő érvényes tanúsítással kell rendelkeznie teljes életciklusa alatt.
- A kriptográfiai hardvereszköz átvételekor Szolgáltatónak meg kell róla győződnie arról, hogy a szállítás során biztosított volt a kriptográfiai hardvereszközök feltörés elleni védelem.
- Szolgáltatónak biztosítania kell a kriptográfiai hardvereszközök feltörés elleni védelmét a tárolás során.
- Szolgáltatónak gondoskodnia kell a kriptográfiai hardvereszköz üzemeltetése során az eszköz dokumentációjában és a tanúsítási jelentésben szereplő követelmények folyamatos betartásáról.
- A használatból kivont kriptográfiai hardvereszközökben tárolt magánkulcsokat a 6.2.10. A magánkulcs megsemmisítésének módja pont szerint visszaállíthatatlan módon kell törölni.

6.7 Hálózati biztonság

A Szolgáltatónak a következő hálózati biztonsági feltételeknek kell megfelelni:

- A szolgáltatói rendszereknek legalább biztonságos zónán belül kell elhelyezkednie, s a szolgáltatónak biztonsági eljárással kell szavatolnia e rendszerek valamint a nagy biztonságú zónával való kommunikáció biztonságát.
- A szolgáltatói rendszerek esetében a szolgáltatásnyújtáshoz nem használt felhasználói fiókokat, alkalmazásokat szolgáltatásokat, kapcsolatokat, protokollokat és portokat tiltani kell vagy el kell távolítani. A meghatározott szabályokat rendszeresen felül kell vizsgálni.
- A szolgáltató a biztonságos zónához és a nagy biztonságú zónához csak megbízható szerepkörrel rendelkező munkatársnak adhat hozzáférést.
- A szolgáltatónak kockázatértékelés alapján különböző hálózatokba vagy zónákba kell

szegmentálnia a rendszereit, figyelembe véve a megbízható rendszerekkel és szolgáltatásokkal való funkcionális logikai és fizikai kapcsolatokat.

- A szolgáltatói rendszerek számára külön hálózatot kell biztosítani. Az információbiztonsági szabályzat érvényesítésére használt rendszereket más célra nem szabad használni. A produktív rendszereknek el kell különülni a fejlesztési, teszt és egyéb felhasználású rendszerektől.
- A különböző megbízható rendszerek közötti kommunikációnak megbízható csatornán kell folynia, ami logikailag elkülönül az egyéb kommunikációs csatornáktól, s biztosítja a végpontok megbízható azonosítását és a forgalmazott adatok bizalmasságát és sértetlenségét.
- Amennyiben a szolgáltatáshoz nagy rendelkezésre állású külső elérés szükséges, akkor a hálózati kapcsolatnak redundánsnak kell lennie, hogy biztosítsa a szolgáltatás elérését amennyiben valamelyik kapcsolat kiesik.
- Szolgáltatónak rendszeresen sebezhetőségi ellenőrzést kell végeznie a nyilvános és privát IP címein és rögzítenie kell annak bizonyítékait, hogy a vizsgálatot olyan független, a megfelelő ismeretekkel, tapasztalattal és eszközökkel bíró személy vagy szervezet végezte, amely megbízható riportot eredményez. Az ellenőrzést negyedévente vagy szignifikáns hálózati változás esetén kell elvégezni.
- A szolgáltatói rendszeren rendszeresen betörési ellenőrzést kell végezni és rögzítenie kell annak bizonyítékait, hogy a vizsgálatot olyan független, a megfelelő ismeretekkel, tapasztalattal és eszközökkel bíró személy vagy szervezet végezte, amely megbízható riportot eredményez. Az ellenőrzést évente vagy szignifikáns infrastrukturális változás, alkalmazásmódosítás esetén kell elvégezni.

6.8 Időbélyegzés

Szolgáltatónak a tanúsítványkiadás szolgáltatás nyújtása keretében minősített bizalmi szolgáltató által kibocsátott időbélyegzőket kell használnia, amennyiben szükség van időbélyegzésére.

Szolgáltatónak a rendszerei időforrásait legalább naponta egyszer UTC időforráshoz kell szinkronizálnia.

7 TANÚSÍTVÁNY-, CRL- ÉS OCSP- ÉS PROFILOK

7.1. Tanúsítványprofil

A Szolgáltató által kibocsátott Tanúsítványok feleljenek meg az RFC 5280, RFC 6818 és az ITU-T X.509 specifikációknak.

A szolgáltató a kibocsátott nem eIDAS tanúsítvány felhasználását a tanúsítványban meghatározott tárgyi, időbeli, földrajzi vagy egyéb korlátok szerint korlátozhatja, ha a korlátozás a tanúsítványból egyértelműen kitűnik. A korlátozásról és ennek következményeiről a szolgáltató köteles a tanúsítvány alanyt megfelelően tájékoztatni.

7.1.1. Verzió szám(ok)

A Szolgáltató az X.509 specifikáció szerinti "V3" tanúsítványokat bocsásson ki.

7.1.2. Tanúsítvány kiterjesztések

A Szolgáltató az X.509 specifikáció szerinti tanúsítvány kiterjesztéseket használhat, a kritikus mezők szükség szerinti jelzésével.

7.1.3. Az algoritmus objektum azonosítója

A tanúsítványban jelezni kell annak az algoritmusnak a megnevezését és paramétereit, amellyel a tanúsítvány hitelesítésre került.

7.1.4. Névformák

Az Alany névformái tekintetében lásd a 3.1.1. Névtypusok fejezetet.

A tanúsítvány "Issuer" mezőjében szereplő értéknek meg kell egyeznie a kibocsátó Kiadó tanúsítványának "Subject" mezőjében szereplő értékkel.

7.1.5. Névhasználati megkötések

A Szolgáltatónak az alkalmazott névhasználati megkötéseket a "nameConstraints" mezőben kell jeleznie, a mezőt kritikusnak megjelölve.

7.1.6. A Hitelesítési rendek azonosítói

A Szolgáltatónak a jelen Szolgáltatási rendek alapján kibocsátott Tanúsítványokba fel kell vennie a nem kritikus Hitelesítési Rend kiterjesztést, jelezve benne az alkalmazott Hitelesítési rend OID alapú azonosítóját (lásd 1.2.1 Hitelesítési Rendek).

7.1.7. A szabályzati korlátozás kiterjesztés használata

Nincs megkötés.

7.1.8. Szabályzatminősítő szintaxis és szemantika

A Szolgáltató a Hitelesítési rend (Certificate Policy) kiterjesztés Szabályzatminősítő (Policy Qualifier) mezőjében rövid információt helyezhet el a Tanúsítvány felhasználhatóságával kapcsolatban. A mezőnek tartalmaznia kell a Szolgáltatási szabályzat on-line elérhetőségét is (URI).

7.1.9. A kritikus Hitelesítési rend kiterjesztés feldolgozása

Nincs megkötés.

7.2. Tanúsítványvisszavonási profil

7.2.1. Verziószám(ok)

A Szolgáltató által kibocsátott tanúsítványvisszavonási listák feleljenek meg az RFC 5280 és ITU-T X.509 specifikáció szerinti "V2" verziójú tanúsítványvisszavonási listának.

7.2.2. Tanúsítványvisszavonási lista kiterjesztések

A Szolgáltató a CRL sorozatszám (CRL number) nem kritikus visszavonási lista kiterjesztést támogassa a visszavonási listák egyesével növekvő sorozatszámának megadásával.

7.3. Tanúsítványállapot-szolgáltatás profilok

A Szolgáltatónak az RFC 6960 szerinti tanúsítványállapot-szolgáltatást kell üzemeltetnie.

7.3.1. Verziószám(ok)

A Szolgáltató az RFC 6960 szerinti "V1" verziójú tanúsítványállapot kéréseket és válaszokat támogassa.

7.3.2. OCSP kiterjesztések

Nincs megkötés.

8 A MEGFELELŐSÉG VIZSGÁLATA

A Szolgáltatónak tevékenységét összhangban kell végeznie

- a vonatkozó és hatályos Európai Unió és hazai szabályozással,
- jelen Szolgáltatási rend követelményeivel, valamint
- az ETSI 319411-1 szabvánnyal

A Szolgáltatónak tevékenységét külső megfelelőségértékelő szervezettel értékeltetnie kell a vonatkozó szabványoknak megfelelően.

A Szolgáltató külső megfelelőségértékeléséhez végzett vizsgálat során az alábbiakat kell betartani:

- figyelembe kell venni Szolgáltató összes értékelendő nem eIDAS szolgáltatás sajátosságát;
- biztosítani kell, hogy a vizsgálat tárgyához tartozó minden szolgáltatói tevékenységet lefedjen a vizsgálat;
- a vizsgálatot vonatkozó szabványok, nyilvánosan hozzáférhető specifikációk és/vagy releváns jogszabályi követelmények alapján kell végezni.
 - ETSI 319411-1
 - ETSI 319412
 - ETSI 319403
 - ETSI 319401

8.1. Az ellenőrzések körülményei és gyakorisága

A Szolgáltató köteles folyamatosan ellenőrizni jelen Szolgáltatási rendjében és Szolgáltatási szabályzataiban foglalt betartását valamint szigorú ellenőrzés alatt kell tartania szolgáltatásai minőségét önellenőrzések végrehajtásával. E cél megvalósulása érdekében a Szolgáltatónak évente egyszer belső audit kell tartania.

Amíg a Szolgáltató tanúsítványszolgáltatást nyújt, legalább évente köteles a vonatkozó szabványoknak való megfelelőséget belső auditok és külső megfelelőségértékelés elvégzésével vizsgálni.

A Szolgáltatónak legalább évente ellenőriznie kell a Kihelyezett Regisztrációs Egységek működését is, kivéve, ha a Kihelyezett Regisztrációs Egység a vonatkozó szabványoknak való megfelelőséget igazoló éves külső audit jelentéssel rendelkezik. A Kihelyezett Regisztrációs Egységekre ugyanazon követelmények vonatkoznak, mint a Szolgáltató belső Regisztrációs egységére.

A Szolgáltatónak szigorúan kontrollálnia kell a weboldal-hitelesítő (DVCP) tanúsítványszolgáltatása minőségét. Ennek érdekében az előző önellenőrzés óta általa kibocsátott weboldal-hitelesítő tanúsítványok - véletlenszerű mintavétellel kiválasztott - legalább 3%-át negyedévente ellenőriznie kell.

8.2 Az értékelő és szükséges képesítése

A Szolgáltató a belső auditokat a független rendszervizsgáló szerepkörrel felruházott

alkalmazottai segítségével is elvégezheti.

A külső megfelelőségértékeléseket olyan természetes vagy jogi személynek avagy természetes személyek csoportjának kell végeznie, aki vagy amely rendelkezik egy EU tagállam nemzeti akkreditációs szervezetétől megfelelő felhatalmazással, valamint:

- képes a 8 A megfelelőség vizsgálata fejezetben megadott szabványokra vonatkozó audit elvégzésére;
- megfelel a 8.3 Az auditor és az auditált entitás kapcsolata fejezetben megadott követelménynek;
- megfelelő jártassággal bír vagy bírnak a Publikus Kulcsú Infrastruktúra (PKI), az IT illetve IT biztonsági megoldások, technológiák és auditok terén valamint Kihelyezett Regisztrációs Egységnél végzett audit során annak funkcióival kapcsolatban;
- ETSI szabványok alapján végzett auditok esetén rendelkezik vagy rendelkeznek
 - az ETSI EN 319 403 szerinti akkreditációval, vagy
 - egy ezzel egyenértékű nemzeti szabvány szerinti akkreditációval, vagy
 - a Nemzeti Akkreditációs Hatóság által ISO 27001 szerint végrehajtott ISO 27006 szerinti akkreditációval;
- WebTrust audit végzése esetén rendelkezik vagy rendelkeznek WebTrust audit elvégzéséhez szükséges engedéllyel;
- tevékenységét vagy tevékenységüket jogszabályok vagy szakmai etikai kódex szabályozza;
- rendelkezik az auditor tevékenység végzéséből eredő mulasztások, hibák esetére szóló, legalább egymillió USD fedezetű biztosítással.

8.3 Az auditor és az auditált entitás kapcsolata

A külső megfelelőségértékeléseket olyan értékelő végezheti, aki vagy amely a Szolgáltató tulajdonosi körétől, vezetőségétől, üzemeltetésétől független.

8.4. Az értékelés által lefedett területek

Szolgáltató belső megfelelőségértékelésének az alábbi területeket kell lefednie:

- szabályzatok hatályos jogszabályoknak és szabványoknak való megfelelése;
- az alkalmazott folyamatok szabályzatoknak való megfelelése.

Külső megfelelőségértékelés esetén a megfelelőségértékelőnek az adott értékelési rendszer által meghatározott követelmények és kritériumok teljesülését kell értékelnie.

8.5. A hiányosságok kezelése

A külső megfelelőségértékelések eredményét egy értékelésjelentésben kell összefoglalni. A jelentésben – amennyiben vannak – rögzíteni kell a vizsgálat során feltárt eltéréseket és az elhárításukra kitűzött határidőket.

8.6. Az eredmények közzététele

A Szolgáltató nem köteles a belső megfelelőségértékelés-jelentés publikálására, az abban foglaltakat bizalmas információként kezelheti.

A Szolgáltatónak az auditidőszakot követő három (3) hónapon belül nyilvánosságra kell hoznia a külső megfelelőségértékelési jelentést. A Szolgáltató nem köteles nyilvánosságra hozni az auditjelentés azon általános megállapításait, melyek nincsenek hatással az audit eredményére.

9. EGYÉB ÜZLETI ÉS JOGI TUDNIVALÓK

9.1. Díjak

A Szolgáltató nyilvános árlistán köteles elérhetővé tenni az Előfizetők részére a szolgáltatások kapcsán alkalmazott díjakat.

A Szolgáltató az alábbi szolgáltatások szabályzatokban leírt módon való igénybevételéért nem számíthat fel díjat:

- tanúsítványtár használata;
- tanúsítványállapot-információk elérése (CRL és OCSP).

9.1.1 Tanúsítványszolgáltatás díjai

A Szolgáltató a tanúsítványszolgáltatás igénybevételéért a nyilvános árlista alapján számíthat fel díjat Előfizető részére, illetve attól Előfizetővel való előzetes egyeztetés alapján eltérhet.

A tanúsítványszolgáltatás díjának magában kell foglalnia a tanúsítvány kiadását, a teljes érvényességi időre való nyilvántartását (tanúsítványtárban és visszavonási nyilvántartásokban) és a jogszabályok szerinti archiválását.

A tanúsítványigénylési és –kezelési eljárásokhoz kapcsolódóan a tanúsítványszolgáltatáshoz kötődő további opcionális szolgáltatásokért szolgáltató díjat számíthat fel Előfizető részére.

9.1.2 Tanúsítvány-hozzáférési díjak

A Szolgáltató a tanúsítványtár szabályzatokban leírt módon való on-line igénybevételéért nem számíthat fel díjat az Érintett felek felé.

9.1.3 Tanúsítványállapot változtatás és a tanúsítványállapot-információk díjai

A Szolgáltató a tanúsítványállapot változtatásáért és a tanúsítványállapot-információk szabályzatokban leírt módon való igénybevételéért nem számíthat fel díjat az Érintett felek felé.

9.1.4 Egyéb szolgáltatások díjai

A Szolgáltató a tanúsítványszolgáltatás igénybevételéhez kapcsolódó egyéb szolgáltatások (pl. opcionális szolgáltatások) igénybevételéért a nyilvános árlista vagy egyedi megállapodás alapján számíthat fel díjat.

9.1.5 Visszatérítési politika

Nincs megkötés.

9.2. Pénzügyi felelősség

A Szolgáltató a mindenkor hatályos polgári törvénykönyvben meghatározott szerződésszegésért való felelősség szabályai szerint meghatározott mértékig; s a szolgáltatási szabályzatában, általános szerződési feltételeiben és a tanúsítványba foglaltaknak megfelelően felel a szolgáltatásaival okozott károkért.

A szolgáltató korlátozhatja a felelősségvállalása értékét, az Ügyfeleket és Érintett feleket a weboldalán keresztül vagy a tanúsítványban tájékoztatva.

9.2.1 Biztosítási fedezet

A Szolgáltató köteles megbízhatóság érdeklében felelősségbiztosítással rendelkezni. A felelősségbiztosításnak ki kell terjedni a szolgáltató által nyújtott szolgáltatásokkal összefüggésben okozott károkra és költségekre:

- a szolgáltatási ügyfélnek a szolgáltatási szerződés megszegésével összefüggésben okozott károkra,
- a szolgáltatási ügyfélnek és harmadik személynek szerződésen kívüli okozott károkra,

A szolgáltatónak biztosítania kell, hogy az általa kötött biztosítási szerződés kifejezetten nevesítse, hogy a szerződés kiterjed a fentiekre.

A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként nem lehet alacsonyabb, mint 3 000 000 (hárommillió) forint.

Az DVCP hitelesítési rend szerinti kibocsátott weboldal-hitelesítő tanúsítványokra vonatkozóan rendelkeznie kell a szolgáltatónak az DV előírásokban meghatározott mértékű biztosítással.

9.2.2 Egyéb eszközök

A Szolgáltató a szolgáltatás megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében

- legalább huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával kell rendelkeznie VAGY
- pénzügyi intézménynél óvadékot kell alapítania legalább huszonötmillió forint értékben VAGY
- egy legalább százmillió forint jegyzett tőkéjű, az Európai Gazdasági Térségben letelepedett vállalkozás készfizető kezességével kell rendelkeznie legalább huszonötmillió forintig terjedően.

9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák

Szolgáltató tegye közzé, hogy az általa nyújtott garanciák és biztosítások mennyiben terjednek ki más felek által okozott károkra.

9.3. Bizalmas üzleti információk kezelése

A Szolgáltató köteles az információs önrendelkezési jogról és az információszabadságról szóló jogszabály rendelkezéseinek megfelelően tárolni és kezelni a birtokába jutott bizalmas adatokat.

9.3.1 A bizalmas információk köre

A Szolgáltatónak bizalmas információnak kell tekintenie minden az egyes Ügyfelekre vonatkozó adatot, amik nem szerepelnek a 9.3.2 fejezetben.

9.3.2 A bizalmas információk körén kívül eső adatok

A Szolgáltatónak nem kell bizalmas információnak tekintenie azon adatokat, amiket személyes jellegűtől megfosztott (pl. anonimizálással), valamint azokat, amelyeket a szolgáltatása részeként hoz nyilvánosságra a tanúsítványtárán keresztül:

- a tanúsítványban szereplő adatokat, valamint
- a tanúsítvány állapotával kapcsolatos adatokat.

A nem bizalmas adatokat Szolgáltató nyilvánosságra hozhatja, megoszthatja partnereivel, illetve nyilvánosságra kerülésükért nem tartozik felelősséggel.

9.3.3 A bizalmas információk védelme

A Szolgáltató felelősséggel tartozik az általa kezelt bizalmas adatok védelméért. Ezeket az adatokat csak azon munkatársai és partnerei ismerhetik meg, amelyek munkájához ezen adatok ismerete szükséges. Más személyek hozzáférését ki kell zárni jogi úton és lehetőség szerint műszaki-biztonsági óvintézkedésekkel.

Minden, a bizalmas adathoz hozzáférő személyt szerződésben vagy titoktartási nyilatkozat aláírásával kell kötelezni a bizalmasság megőrzésére.

Szolgáltatónak az alábbi esetekben kötelessége átadnia a birtokában lévő bizalmas adatokat az adatszolgáltatást kérő jogszabályban meghatározott hatóságnak vagy más szervnek:

- jogszabályilag megalapozott kötelező adatszolgáltatás bűncselekmények felderítése vagy megelőzése céljából, vagy nemzetbiztonsági érdekből a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak,
- jogszabályilag megalapozott kötelező adatszolgáltatás polgári peres, illetve nemperes eljárás során.

A Szolgáltatónak a Szolgáltatási szabályzatában kell tételesen meghatároznia a fenti adatszolgáltatások módját.

9.4. Személyes adatok kezelése

Szolgáltatónak az Ügyfelek személyes adatait – a 9.3.2 fejezetben foglalt kivételekkel – a 9.3.1 fejezet szerinti bizalmas információként, ennek megfelelő védelem (9.3.3. fejezet) mellett a 9.4.1 fejezet szabályait betartva kell kezelnie.

9.4.1 Adatkezelési szabályok

Szolgáltatónak az Ügyfelek személyes adatait a jelen szolgáltatási rend, a vonatkozó szolgáltatási szabályzatok valamint a szabályzatban részletezett, adatkezelésre vonatkozó, hatályos jogszabályi előírások rendelkezéseit betartva kell kezelnie.

A Szolgáltató köteles biztosítani, hogy bármely adat rendelkezésére bocsátása esetén ezen adatokhoz illetéktelen személyek ne férhessenek hozzá.

A Szolgáltató köteles a hatályos jogszabályoknak megfelelően a tanúsítványokkal kapcsolatos információkat – beleértve az azok előállításával összefüggőket is – és az ahhoz kapcsolódó személyes adatokat a tanúsítvány érvényességének lejártától számított 10 évig, illetőleg az elektronikus aláírással/bélyegzővel, vagy az azzal ellátott elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig megőrizni, valamint ugyanezen határidőig olyan eszközt biztosítani, mellyel a kibocsátott tanúsítvány tartalma megállapítható.

Szolgáltatónak a tanúsítványok állapotinformációit minden esetben nyilvánosságra kell hoznia illetve az Ügyfél írásbeli hozzájárulása/kérése esetén a tanúsítvány Alanyadatait és magát a tanúsítványt nyilvános tanúsítványtárában közzé kell tennie.

A Szolgáltatónak rendelkeznie kell adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a bizalmas és személyes információk kezelésére. Az adatkezelési szabályzat által lefektetett adatkezelési gyakorlatról Szolgáltatónak weboldalán (lásd 1.1.2) külön tájékoztatást kell közzétennie.

9.4.2. Személyes adatok

Szolgáltatónak személyes adatként kell kezelnie minden olyan birtokába kerülő adatot,

- mely alapján természetes személy beazonosítható - különös tekintettel a természetes személy nevére vagy hatóság által nyilvántartott azonosítójára -, vagy
- ami természetes személlyel kapcsolatba hozható, vagy
- melyből a természetes személyre vonatkozó következtetés levonható, és
- amely nem sorolható egyúttal a 9.4.3 fejezet szerinti adatok közé.

A Szolgáltató csak olyan személyes adatokat kezelhet, amely az adatkezelés céljának megvalósuláshoz elengedhetetlen, a cél elérésre alkalmas, s melyek kezeléséről az érintett feleket tájékoztatja. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

A Szolgáltatónak bizalmas adatként kell kezelnie minden személyes adatot, kivéve a 9.3.2-ben és 9.4.3-ban megadott személyes adatokat.

9.4.3. Személyes adatnak nem minősülő információk

A 9.4.2 pontban meghatározott adatok körén kívül eső adatokat Szolgáltató nem tekinti személyes adatnak.

9.4.4. Személyes adatok védelme

A Szolgáltató köteles a vonatkozó előírásoknak megfelelően (lásd 9.4.1) biztonságosan tárolni és védeni a tanúsítványkibocsátással kapcsolatos és a tanúsítványban nem szereplő személyes adatokat. Az adatokat megfelelő intézkedésekkel védeni kell a jogosulatlan hozzáférés és a megváltoztatás ellen, különösen az Ügyfél és a szolgáltató egyes egységei között történő továbbítás során. Továbbá védeni kell őket, az adatvesztés, a károsodás és a nem engedélyezett feldolgozás ellen is. Lásd még az 5.3.1, 5.5.1, 5.7.1, 5.7.4 és 9.3.3 fejezeteket.

9.4.5. Személyes adatok felhasználása

A Szolgáltató csak a tanúsítványban szereplő személyes adatokat hozhatja nyilvánosságra az Ügyfél előzetes írásbeli hozzájárulása/kérése alapján.

A Szolgáltató a személyes adatokat csak a vonatkozó mindenkor jogszabályi előírásokra tekintettel illetve olyan módon és mértékben használhatja fel, amely a tanúsítvánnyal kapcsolatos (például: kiadási, állapotváltoztatási, megújítási, módosítási vagy kulcscsere) műveletek elvégzéséhez szükséges.

9.4.6. Adatkezelés

A Szolgáltató személyes adatokat – az érintett részletes tájékoztatását követően – jogszabályi előírásból fakadó kötelezettség teljesítése céljából vagy a Szolgáltató és az érintett jogos érdekéből és az érintett előzetes – tájékoztatáson alapuló és konkrét – hozzájárulása alapján kezelhet.

Szolgáltatónak a személyes adatokat a 9.4.1. pontban felsorolt rendelkezésekre figyelemmel és az 5. fejezet vonatkozó eljárási szabályainak megfelelően kell tárolnia és kezelnie, melyeket kizárólag a 9.3.3 pontban felsorolt, jogszabályok által meghatározott esetekben adhat át a jogszabályok szerinti harmadik feleknek.

9.4.7. Egyéb adatvédelmi követelmények

Szolgáltató az általa nyújtott szolgáltatások felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, vagy nemzetbiztonsági érdekből - az érintett személyazonosságát igazoló, valamint egyeztetett adatok tekintetében - az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén díjmentesen adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét rögzíteni kell, az adatátadásról a Szolgáltató az érintett Ügyfelet nem tájékoztathatja (lásd 9.3.3).

9.5 Szellemi tulajdonhoz fűződő jogok

A Szolgáltató által ügyfelei részére kibocsátott magán- és nyilvános kulcstulajdonosa az Előfizető, teljes jogú felhasználója pedig a Végfelhasználó. A Szolgáltató által ügyfelei részére kibocsátott tanúsítvány tulajdonosa a Szolgáltató, teljes jogú felhasználója pedig a Végfelhasználó.

A Szolgáltató az általa kibocsátott végfelhasználói tanúsítványokat a benne szereplő nyilvános kulccsal és egyéb adatokkal együtt közzéteheti, sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti.

A Szolgáltató tulajdonát képezi a tanúsítványvisszavonási lista és állapotinformáció, amit nyilvánosságra hozhat. A Szolgáltató által az Ügyfelek részére kibocsátott egyedi azonosító (OID) a szolgáltató tulajdonát képezi.

A jelen Szolgáltatási rend és szolgáltató további szabályzatai és dokumentációi a NETLOCK kizárólagos tulajdonát képezi. Az Ügyfelek, Végfelhasználók és egyéb Érintett felek e dokumentumokat csak jelen előírásoknak megfelelően jogosultak felhasználni, minden egyéb (pl. kereskedelmi) célú felhasználás szigorúan tilos. A nyilvános dokumentumok szabadon terjeszthetők, de csak változatlan formában, teljes terjedelemben és az eredet feltüntetésével.

A Szolgáltatási rendben, szolgáltató további szabályzataiban és dokumentációiban, valamint a tanúsítványokban található védett nevek felett a jogtulajdonosuk rendelkezik. Az itt hivatkozott művek (szabványok, jogi források) szerzői joga a jog tulajdonosáé. A Szolgáltató működése során nem sértheti meg harmadik személyek szellemi tulajdonjogait.

A szolgáltatási tevékenység során alkalmazott szoftver és hardver komponensek a Szolgáltató tulajdonát képezik vagy azokat jogszerűen használja.

9.6 Felelősség és garanciák

A Szolgáltató felelős jelen Szolgáltatási Rend és a Szolgáltatási szabályzata előírásainak betartásáért, abban az esetben is, ha egyes tevékenységeit kiszervezi.

9.6.1 A Hitelesítő Egység felelőssége

A Hitelesítő Egységnek garantálnia kell, hogy a kibocsátott tanúsítvány a jelen Szolgáltatási rendnek és a vonatkozó Szolgáltatási szabályzatnak megfelelően kerül kiállításra.

9.6.2 A Regisztrációs Egység felelőssége

A Szolgáltató megköveteli a vele együttműködő Kihelyezett Regisztrációs Egységektől a jelen Szolgáltatási rend és a vonatkozó Szolgáltatási szabályzat előírásainak maradéktalan betartását.

A Regisztrációs Egység felelőssége:

- az Igénylők és az Alanyként feltüntetett entitások (személy-) azonosságának megállapítása, a szolgáltató rendelkezésére bocsátott adatok ellenőrzése;
- a Képviselt szervezet szervezeti azonosságának, a Képviselt szervezet nevében eljáró személy személyazonosságának és képviseleti jogosultságának megállapítása, ellenőrzése;
- a felvett regisztrációs adatok valóságának garantálása;
- a szolgáltatási szerződés megkötését megelőzően Ügyfél tájékoztatása a Szolgáltatási Rend és a Szolgáltatási Szabályzat tartalmáról és elérhetőségéről, a szolgáltatás igénybevételének feltételeiről;

- a tanúsítvány állapotváltoztatási igények végrehajtása;
- általános kötelezettségeinek maradéktalan betartása.

9.6.3 Ügyfelek felelőssége és kötelezettségei

Az Ügyfél további kötelezettségeit és felelősségét az Általános szerződési feltételek, valamint a Szolgáltatási szabályzat határozzák meg.

Ügyfél köteles:

- a Szolgáltatóval szolgáltatási szerződést kötni, vagy az általános szerződési feltételekkel megegyező megállapodást kötni;
- valós adatokat megadni a tanúsítvány igényléskor, valamint haladéktalanul tájékoztatni a Szolgáltatót a következő adatok változásáról: az azonosításához szükséges, a tanúsítványban feltüntetett személyazonosító adatok, más személy képviseletével összefüggésben kiállított tanúsítvány esetén a képviseletre jogosult személy és a képviselt személy adatai, a tanúsítványban feltüntetett egyéb adatok;
- a tanúsítványhoz tartozó kulcspárt jelen Szolgáltatási rendnek valamint Szolgáltatási szabályzatnak megfelelően felhasználni, biztonságosan kezelni (lásd a 4.5.1 fejezeteket);
- ellenőrizni a kiadott tanúsítványban foglalt adatokat;
- haladéktalanul tájékoztatni a Szolgáltatót a szolgáltatással vagy a tanúsítvánnyal kapcsolatban észlelt, a külön jogszabályban, szolgáltatási szerződésben illetve szolgáltatási szabályzatban meghatározott rendellenességről vagy más, a szolgáltatást érintő eseményről, így különösen arról, ha a szolgáltatás használatához szükséges, a Szolgáltató által biztosított Ügyféleszközt, illetve magánkulcsot jogosulatlan személy használhatta;
- a tanúsítvány módosítását, kulcscseréjét vagy visszavonását kezdeményezni, ha
 - kompromittálódott, elveszett a tanúsítványhoz tartozó magánkulcs,
 - pontatlan vagy helytelen adatokat tartalmaz a tanúsítvány,
 - a tanúsítványban feltüntetett képviseleti jogosultság megszűnik,
 - amennyiben a bélyegző tanúsítvány végfelhasználójának képviseleti/eljárási jogosultsága megszűnik;
- haladéktalanul tájékoztatni a Szolgáltatót a szolgáltatással kapcsolatos jogvita megindulásáról.

A tanúsítványokat végfelhasználóik csak a tanúsítványban feltüntetett felhasználási célokra vehetik igénybe, a benne jelzett korlátozásoknak megfelelően. A teszttanúsítványokhoz tartozó magánkulcsok valódi kötelezettségvállalásra nem vehetők igénybe.

9.6.4 Érintett felek felelőssége

Az Érintett feleknek a tanúsítványok elfogadása és felhasználása során a tanúsítványban feltüntetett felhasználási célok és egyéb információk és korlátozások szerint kell eljárni. Ezen túl a saját belátásuk és/vagy szabályzataik alapján dönthetnek a tanúsítványok elfogadásáról. Az érvényesség vizsgálata során a Szolgáltató által garantált biztonsági szint megtartásához szükséges, hogy az Érintett fél megfelelő körültekintéssel járjon el.

A teszttanúsítványok valódi kötelezettség vállalás elfogadására nem alkalmazhatók.

9.6.5 Egyéb résztvevők felelőssége

Amennyiben a szervezet képviselője nem személyesen jár el a tanúsítvány igénylése során, úgy a képviselt szervezet felelősséggel tartozik az általa kiadott igazolásokért, különös tekintettel azon igazolásokra, amelyben azt igazolja, hogy az Igénylő jogosult a Szervezet nevét is tartalmazó Tanúsítvány igénylése, állapotváltoztatása, megújítása stb. kapcsán eljárni.

9.7 Szavatosság kizárása

A Szolgáltató kizárja a szavatosságot, amennyiben:

- az Érintett fél nem körültekintően jár el a tanúsítványok felhasználása vagy ellenőrzése során, azaz nem a jelen Szolgáltatási rend, a Szolgáltatási szabályzat vagy a hatályos jogszabályok szerint jár el;
- az Ügyfelek nem tartják be az Ügyféleszköz illetve a kulcs kezelésével kapcsolatos előírásokat;
- az Érintett felek vagy mások által kibocsátott szabályzatok nem felelnek meg a jelen Szolgáltatási rendnek vagy a Szolgáltatási szabályzatnak;
- a Szolgáltató az Internet, vagy egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a Felügyeleti szerv által jóváhagyott kriptográfia algoritmusok hibájából, illetve gyengeségeiből ered.

9.8 Felelősség korlátozása

A Szolgáltató kártérítési felelősségét a Szolgáltatási Szabályzatának 9.2 pontja szerint korlátozhatja.

9.9 Kártérítés, kártalanítás

Szolgáltatónak a jelen Szolgáltatási Rend alapján nyújtott szolgáltatásokkal, a kapcsolatos kártérítési, kártalanítási kötelezettségének részletes szabályait az jelen Szolgáltatási Rend alapján készült Szolgáltatási Szabályzatban kell ismertetnie. Szolgáltató kártérítési, kártalanítási kötelezettségével kapcsolatos további kikötéseket az ÁSZF, a szolgáltatási szerződések és/vagy az Ügyfelekkel kötött más típusú szerződések és megállapodások is tartalmazhatnak.

A Szolgáltató felelős minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okozott a vállalt kötelezettségének megszegéséből eredően. Amennyiben a Szolgáltató előzetesen megfelelően tájékoztatja ügyfeleit az általuk nyújtott szolgáltatások igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek számára felismerhetők, a Szolgáltató nem felelős a szolgáltatások igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért.

Minden egyéb esetben a mindenkor hatályos polgári törvénykönyv vonatkozó rendelkezései

az irányadóak.

9.10 A Szolgáltatási rend hatálya

A Szolgáltatási rend aktuális verziójának időbeli hatálya a fedlapon jelzett hatálybalépés dátumával kezdődik és visszavonásig hatályos.

A Szolgáltatási rend személyi hatálya a Szolgáltatóra, annak a Szolgáltatásokban közreműködő munkatársaira, valamint az Ügyfelekre terjed ki.

A Szolgáltatási rend tárgyi hatálya kiterjed a Szolgáltató által nyújtott Szolgáltatásokra, illetve ezek keretében kibocsájtott tanúsítványokra, valamint Szolgáltatónak a fenti Szolgáltatásokkal kapcsolatban álló összes objektumára és tárgyi eszközére.

9.10.1 Érvényesség

A Szolgáltatási rend adott verziója hatályba lépésének napja a dokumentum fedlapján kerül meghatározásra.

9.10.2 Megszűnés

A Szolgáltatási rend érvényessége megszűnik egy újabb Szolgáltatási Rend verzió hatályba lépésével vagy a szolgáltatási tevékenység beszüntetésekor.

9.10.3 A megszűnés következményei

A Szolgáltatási rend visszavonása esetén a Szolgáltató honlapján teszi közzé a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket.

A Szolgáltató vállalja, hogy a Szolgáltatási rend visszavonása esetén is érvényben maradnak a mindenkor hatályos vonatkozó jogszabályokban meghatározott bizalmas adatok védelmére vonatkozó előírások.

9.11 Egyedi értesítések és a résztvevők közti kommunikáció

A Szolgáltató az Ügyfelekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát, telefonos ügyfélszolgálatot működtet.

9.12 Módosítások

A Szolgáltató a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén megváltoztatja a Szolgáltatási rendjét, a vonatkozó szabályzatait.

A szabályzatok egymásnak és a vonatkozó szabványoknak való megfelelés vizsgálatát legalább évente egy alkalommal el kell végezni. A szabályzatok rendkívüli felülvizsgálata és módosítása a szabványkörnyezet változása esetén is szükséges. Szolgáltatónak a működése

során szerzett gyakorlati tapasztalatok alapján is folyamatosan felül kell vizsgálnia Szolgáltatási Rendjét és Szabályzatát.

A módosított rendet és szabályzatot Szolgáltató legkorábban a közzététele napján léptetheti hatályba, de rendkívüli esetben a változások azonnali hatállyal is életbe léptethetők.

Lásd még az 1.5 és 2.1 fejezetet.

9.12.1 A módosítási eljárás

Szolgáltató a szabályzatváltoztatási igényeket gyűjti (lásd 1.5), a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz, s a változtatásokat életbe lépteti.

Szolgáltató a változtatási igényeket előzetesen megvizsgálja a Szolgáltatási Rendszerben meghatározott tartalmi követelményeknek valamint a szabvány elvárásoknak való megfelelés szempontjából. Amennyiben egyikkel kapcsolatban sem merül fel kifogás, a módosítási igényt elfogadja és megkezdí annak kidolgozását.

A változtatásokat gyűjtve a Szabályzatelfogadó Egységnek belső, nem nyilvános munkaváltozatokat kell létre hoznia a szabályzatokból, melyeknek a közzététel előtt belső felülvizsgálaton kell átesniük. Szolgáltatónak a változásokat – lehetősége szerint – kötegelve kell új szabályzati változattá szerkeszteni, törekedve arra, hogy új szabályzatot csak a lehető legtrikábban kelljen kibocsátania.

A kidolgozott módosításokat a Szabályzat jóváhagyójának (lásd 1.5) kell elfogadnia, melyet megelőzően szintén meg kell vizsgálnia a fenti tartalmi és formai követelményeket. Ezt követően kerülhet sor az Ügyfelek és az Érintett felek értesítésére (lásd 9.12.2). A Szabályzat jóváhagyására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik.

A módosított Szolgáltatási rend és szabályzatok változatai – a nyilvános tervezetek is – mindig új verziószámmal kerülnek nyilvánosságra.

9.12.2 Az értesítések módja és határideje

Nincs megkötés.

9.12.3 A dokumentumazonosító változása

Szolgáltatónak a Szolgáltatási Rend és Szabályzat újabb nyilvános változatait – a tervezeteket is – mindig új verziószámmal kell nyilvánosságra hoznia, vagyis a két eltérő tartalmú dokumentumnak nem lehet azonos OID azonosítója.

A dokumentum azonosítója a következő elemekből épül fel – az egyes elemeket pontok választják el egymástól: szolgáltatói OID (1.3.6.1.4.1.3555), nyilvános dokumentumok jelölése (1), dokumentumtípus megjelölése, jóváhagyás dátuma, azaz:

- jelen szolgáltatási rend esetén: 1.3.6.1.4.1.3555.1.65.jóváhagyás dátuma;
- a szolgáltatási szabályzat esetén: 1.3.6.1.4.1.3555.1.49.jóváhagyás dátuma.

A módosított rend és szabályzat csak a hatálybalépésüket követően, újonnan kibocsátásra kerülő tanúsítványokra vonatkozhat (de a már kibocsátottakra nem).

9.13 Vitás kérdések rendezése

A Szolgáltató köteles biztosítani a panaszok bejelentésének elérhetőségét, a panaszok kezelését, valamint köteles tájékoztatni a szolgáltatással összefüggő jogviták peres és peren kívüli kezdeményezésének lehetőségéről, annak feltételeiről, a békéltető testülethez való fordulás jogalapjáról, az eljárásra jogosult hatóságok és békéltető testület vagy más vitarendező szervezetek megnevezéséről, elérhetőségeiről.

9.14 Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar és európai uniós jogszabályoknak megfelelően végzi. A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

9.15 A hatályos jogszabályoknak való megfelelés

Szolgáltatónak szolgáltatásait a mindenkor hatályos európai uniós és magyarországi szabályozásnak megfelelően kell nyújtania. A vonatkozó jogszabályokat és az azoknak való megfelelés módját Szolgáltató szolgáltatási szabályzataiban adja meg.

A nem eIDAS szolgáltatásokra nem felétlenül terjednek ki az alábbi jogszabályok, azonban a szolgáltató az egyenbiztonság miatt jellemzően meg felel ezen feltételeknek a nem eIDAS szolgáltatások esetében is, értelemszerűen a különbségek és lehetőségek figyelembe vételével.

A jelen Szolgáltatási Rend hatálybalépésekor hatályos jogszabályok:

- a Polgári Törvénykönyvről szóló 2013. évi V. törvény
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI) General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 V1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 412-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-4 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Nincs megkötés.

9.16.2 Átruházás

A jelen Szolgáltatási rendnek megfelelően működő szolgáltató csak a Szolgáltató előzetes írásbeli engedélyével adhatják tovább jogosultságukat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3 Részleges érvénytelenség

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

9.16.4 Igényérvényesítés

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

9.16.5 Vis maior

A Szolgáltató nem felelős a Szolgáltatási rendben és a Szolgáltatási szabályzatban megfogalmazott követelmények hibás vagy késedelmes teljesítéséért, ha a hiba vagy késedelem oka a Szolgáltató ellenőrzési körén kívül eső, előre nem látható körülmény volt.

9.17 Egyéb rendelkezések

A Szolgáltató tanúsítvány előállításával és állapotváltoztatással foglalkozó egységeinek (hitelesítő és regisztrációs egységek) függetlennek kell lennie más szervezetektől a tanúsítványok szabályzatoknak megfelelő kezelése tekintetében. Ezen egységeknek dokumentált felépítésének kell lennie, amely megakadályozza a részrehajló működését.

A vezető munkatársaknak függetlennek kell lenni minden olyan üzleti, pénzügyi és más befolyástól, ami hátrányosan hathat a szolgáltatásokba vetett bizalomra.