CERTIFIKAČNÝ PORIADOK
Disig CA External

Disig, a.s.

Vypracoval	Peter Miškovič
Dátum	22.1.2026
Verzia	1.0
Typ	CERTIFIKAČNÝ PORIADOK
Schválil	Ľuboš BatěkĽuboš BatěkĽuboš Batěk

História zmien

Verzia	Dátum	Popis revízie; revidoval
0.5	21.6.2016	Prvá verzia dokumentu; Lehotský; Miškovič
1.0	22.1.2026	Aktualizácia v súvislosti s rozšírením používania Disig CA External aj pre širší okruh zmluvných partnerov; Miškovič

Obsah

1. ÚVOD

Tento dokument definuje certifikačný poriadok (ďalej aj „CP“) certifikačnej autority Disig CA External (ďalej len „CA External“), ktorú prevádzkuje spoločnosť Disig, a.s., so sídlom Galvaniho 17/C, 821 04 Bratislava, IČO: 35975946, zapísanú v Obchodnom registri Mestského súdu Bratislava III, odd. Sa, vložka č. 3794/B, ako poskytovateľ dôveryhodných služieb (ďalej len „Poskytovateľ“).

Poriadok definuje podmienky vydávania certifikátov verzie X.509, ktoré môžu byť používané v rámci uzavretých IS zmluvných partnerov spoločnosti Poskytovateľa, alebo v rámci verejne dôveryhodných IS, ktoré sa rozhodli dôverovať certifikátom vydaných Poskytovateľom, prostredníctvom tejto CA External.

Štruktúra CP je plne v súlade s požiadavkami RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.

V dokumente sú používané technické pojmy spojené s technológiou PKI. Ak sa chcete oboznámiť s použitou terminológiu, dôrazne odporúčame, aby ste si prečítali časti dokumentu, kde sú vysvetlené skratky a uvedené potrebné definície, skôr ako budete pokračovať v čítaní dokumentu.

1.1. Prehľad

Pri odvolávaní sa na tento dokument môžu byť použité pojmy "CP", "politika" alebo CP CA External.

CP je určená na použitie v určitých situáciách a identifikuje špecifické úlohy a zodpovednosti Poskytovateľa pre:

- CA External pri vydávaní certifikátov,
- registračné autority (RA),
- držiteľov certifikátov a
- spoliehajúce sa strany,

pričom všetky tieto špecifické povinnosti sú v ňom popísané.

CA External používa jeden koreňový certifikát, ku ktorému vydáva zoznam zrušených certifikátom (CRL). Koreňový certifikát CA External musí byť k dispozícii držiteľom certifikátov prostredníctvom verejne dostupného repozitára Poskytovateľa.

Akékoľvek spory týkajúce sa kľúčov alebo manažmentu certifikátov podľa tejto CP, pokiaľ nie sú vyriešené dotknutými stranami pomocou k tomu určených mechanizmov (rokovanie, zmenové konanie, dohoda) sa môžu riešiť len v zmysle zmluvy o poskytovaní certifikačných služieb uzavretej s konkrétnou právnickou osobou.

Certifikačná autorita CA External :

- zruší platnosť certifikátu len v prípadoch, ktoré sú uvedené v tomto CP,
- je povinná viesť záznamy alebo logy spôsobom popísaným v tomto CP,
- musí zabezpečiť oddelenie kritických funkcií CA medzi najmenej tri osoby priradené do rôznych dôveryhodných rolí.

Žiadne údaje poskytnuté držiteľom pre potreby CA External nesmú byť zverejnené bez jeho súhlasu, ak to nevyžaduje zákon alebo súdny príkaz.

CA činnosti podliehajú kontrole vykonávanej Policy Management Authority (PMA) alebo jej zástupcom podľa uváženia PMA.

1.2. Identifikácia

OID tohto poriadku je registrovaný pod ISO a je {ISO assigned OIDs (1) ISO Identified Organization (3) Identification number of economic subject (IČO) (158) Disig, a.s. (35975946) CP CA External (0.0.0.4) a v certifikátoch bude uvádzaný v tvare:

1.3.158.35975946.0.0.0.4

CA External bola navrhnutá pre použitie v určitých situáciách a identifikuje konkrétne úlohy pre ich vykonanie. Certifikačná autorita (CA), registračné autority (RA), osoby zodpovedné za úložisko, držitelia certifikátov a spoliehajúce sa strany majú špecifické povinnosti, ktoré sú uvedené v tomto CP.

1.3. Účastníci PKI

Tento CP bol pripravený tak, aby spĺňala všeobecné legislatívne požiadavky na certifikát verejného kľúča a požiadavky RFC 3647.

CA External môže postúpiť povinnosti a iné zodpovednosti ustanovené v tomto CP na tretiu osobu, ktorá súhlasí s tým, že bude viazaná týmto poriadkom. CA External zostáva zodpovedná za výkon postúpených povinností a zodpovedností treťou stranou v súlade s týmto poriadkom v plnom rozsahu.

1.3.1. Autorita na správu politík

Autorita na správu politík (Policy Management Authority - PMA) je zložka ustanovená za účelom:

- dohľadu na vytváranie a aktualizáciu certifikačných politík (CP, CPS) a iných dokumentov, vrátane vyhodnocovania zmien a plánov na implementovanie prijatých zmien tak, aby sa zaručilo, že prax CA External vyhovuje príslušnej politike,
- revízie výsledkov interných auditov zhody, aby sa určilo, či CA External adekvátne dodržuje ustanovenia schválených politík,

- vydávania odporúčaní pre CA External týkajúcich sa nápravných opatrení a iných vhodných akcií,
- vydávania odporúčaní ohľadne vhodnosti certifikátov asociovaných s CP pre špecifické aplikácie riadenia a usmerňovania činnosti certifikačnej autority a registračných autorít,
- výkladu ustanovení CP a svojich pokynov pre RA a CA,
- vykonávania interného auditu CA External,
- zabezpečenia, že prijatý a schválený certifikačný poriadok je riadne a náležite realizovaný.

PMA predstavuje vrcholovú zložku, ktorá rozhoduje s konečnou platnosťou vo všetkých záležitostiach a aspektoch týkajúcich sa CA External a jej činnosti.

1.3.2. Certifikačná autorita (CA External)

CA External , ktorá vydáva certifikáty v súlade s touto politikou:

- vytvorí, podpíše, distribuuje a ruší certifikáty verejného kľúča zaväzujúce X.500 Distinguished Name žiadateľa (držiteľa) s ich súkromným kľúčom,
- poskytuje informáciu o stave certifikátov prostredníctvom zoznamu zrušených certifikátov (CRL),
- má pripravené, implementované a prevádzkuje postupy pri poskytovaní certifikačných služieb tak, aby boli adekvátne dosiahnuté požiadavky tohto poriadku.

1.3.3. Registračné autority (RA)

RA prevádzkované v zmysle tohto CP sú zodpovedné za všetky povinnosti, ktoré sú na ňu kladené zo strany vydávajúcej CA External.

1.3.4. Personalizačné pracovisko

V prípade, že u zmluvného partnera, ktorému sú vydávané certifikáty CA External, existuje, tak zabezpečuje inicializáciu a sprostredkovanie vydania certifikátov na čipové karty, dohľad nad kartami, prípadne aj potlač čipových kariet.

1.3.5. Držitelia

Zmluvným partnerom sa rozumie fyzická osoba resp. právnická osoba, ktorej Poskytovateľ poskytuje dôveryhodné služby na základe zmluvy.

V prípade, že Zákazník je zároveň Držiteľom certifikátu, je priamo zodpovedný v prípade neplnenia si povinností kladených na zákazníka aj držiteľa certifikátu.

Zodpovednosti Zákazníka a Držiteľa sú definované v dokumente Všeobecné podmienky poskytovania a používania dôveryhodnej služby vydávania a overovania

certifikátov“ (ďalej len „Všeobecné podmienky“) zverejnené na webovom sídle Poskytovateľa.

Podmienky, ktoré musí splniť Zákazník, definuje táto CP.

Formálnym Držiteľom certifikátu sa rozumie fyzická osoba, ktorá sa zaviaže, že bude používať zodpovedajúci súkromný kľúč a certifikát v súlade s touto CP.

1.3.6. Spoliehajúce sa strany

Spoliehajúce sa strany sú spravidla používatelia IS konkrétnych zmluvných partnerov, pre ktorých potreby sú certifikáty vydávané.

Akceptovaním certifikátu vydaného v súlade s ustanoveniami tohto poriadku, spoliehajúca sa strana súhlasí s tým, že bude viazaná ustanoveniami tohto poriadku.

1.4. Používanie certifikátu

1.4.1. Povolené používanie

Spoločnosť Disig nestanovuje žiadne obmedzenia na používanie certifikátov vydaných CA External, pokiaľ je ich používanie v súlade s týmto CP. Každý zmluvný partner si však môže na používanie certifikátov vydaných CA External stanoviť vlastné interné pravidlá, ktoré môžu obmedziť účely a spôsob ich používania.

1.4.2. Obmedzenie používania

Žiadne ustanovenia.

1.5. Správa politík

1.5.1. Organizácia zodpovedná za správu CP

Za správu (vypracovanie, udržiavanie, aktualizáciu) tohto CP je zodpovedný:

Disig, a. s.

Galvaniho 17/C

821 04 Bratislava

e-mail:PMA_L@disig.sk

tel.: +421 2 208 50 140

1.5.2. Kontaktná osoba

Kontaktnou osobou zodpovednou za obsah, udržiavanie a aktualizáciu CP CA External je poverený člen PMA:

e-mail: PMA_L@disig.sk

1.6. Skratky a definície

1.6.1. Skratky

CA	–	Certifikačná autorita (Certificate Authority)
ARL	–	Zoznam zrušených autorít (Authority Revocation List)
CN	–	Meno subjektu (Common Name)
CP	–	Certifikačný poriadok
CPS	–	Pravidlá na výkon certifikačných činností (Certificate Practice Statement)
CRL	–	Zoznam zrušených certifikátov (Certificate Revocation List)
DN	–	Rozlišujúce meno (Distinguished name)
ETSI	–	Európsky telekomunikačný štandardizačný úrad (European Telecommunications Standards Institute)
FIPS	–	USA štandard z oblasti informačnej bezpečnosti (Federal Information Processing Standards)
HSM	–	Hardvérový bezpečnostný modul (Hardware Security Module)
ISO	–	Medzinárodná štandardizačná organizácie (International Standard Organization)
OCSP	–	Služba okamžitého poskytovania informácie o stave certifikátu (Online Certificate Status Protocol)
OID	–	Objektový identifikátor (Object Identifier)
PIN	–	Osobné identifikačné číslo (Personal Identification Number)
PKCS	–	Kryptografické štandardy pre PKI (Public Key Cryptography Standards)
PKI	–	Infraštruktúra verejného kľúča (Public Key Infrastructure!)
PMA	–	Autorita na správu politík (Policy Management Authority)
RA	–	Registračná autorita (Registration Authority)
RFC	–	Request for Comment
RSA	–	Kryptografický algoritmus pomenovaný podľa tvorcov (Rivest, Shamir, Adleman)
SHA	–	Kryptografická funkcia na vytváranie odtlačkov (hash) elektronických informácií (Secure Hash Algorithm)

URL	—	Uniform Resource Locator

1.6.2. Definície

Sponzor	—	Fyzická osoba, ktorá ma pod patronátom zariadenie resp. systém, ktorému je vydávaný certifikát

2. Zverejňovanie informácií a úložisko

2.1. Úložisko

Úložisko Poskytovateľa je prevádzkované spoločnosťou Disig (pozri časť 1.5.1) a tvorí ho webová stránka dostupná na adrese eidas.disig.sk.

2.2. Publikovanie informácií o certifikátoch

Vydávajúca CA External musí:

- zabezpečiť sprístupnenie tejto CP všetkým dotknutým stranám (držitelia, spoliehajúce sa strany) prostredníctvom svojho úložiska,
- zabezpečiť, že operačný systém, resp. systém kontroly prístupu k úložisku bude nastavený takým spôsobom, že len oprávnené osoby môžu modifikovať takto publikovaný CP.

2.3. Čas a frekvencia zverejňovania informácií

Všetky informácie musia byť zverejnené v úložisku ihneď ako je taká informácia k dispozícii Poskytovateľovi.

2.4. Kontroly prístupu k úložisku

Poskytovateľ musí chrániť ľubovoľnú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozširovanie. Poskytovateľ vynaloží maximálne úsilie na to, aby zaistila integritu, dôvernosť a dostupnosť dát vyplývajúcich s poskytovaním certifikačných služieb. Taktiež boli vykonané logické a bezpečnostné opatrenia, aby zabránili neautorizovanému prístupu osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v repozitári.

3. Identifikácia a autentizácia

V tejto časti sú popísané postupy, ktoré používa na overenie identity a/alebo iných atribútov žiadateľa o vydanie certifikátu na príslušných RA Zákazníka alebo priamo u Poskytovateľa.

Tiež popisuje, ako sú overované strany pokiaľ požadujú opakované vydanie certifikátu, resp. zrušenie certifikátu. Táto časť rieši aj postupy týkajúce sa používaných mien, vrátane uznávania práv k ochrannej známke v niektorých menách.

3.1. Pomenovanie

3.1.1. Typy mien

Poskytovateľ je schopný vytvárať certifikáty, ktoré obsahujú rozlišovacie mená v zmysle X.500 (X.500 Distinguished Name, ďalej ako „rozlišovacie meno“). Každý držiteľ, pre ktorého je vydávaný certifikát, musí mať jasne rozoznateľný a jedinečný X.501 rozlišujúce názov (DN) v poli Subject Name. DN musí byť vo formáte X.501 printable String a nesmie byť prázdny.

3.1.2. Potreba zmysluplnosti mien

Obsah poľa obsahujúci meno držiteľa resp. názov vydavateľa certifikátu musí mať spojitosť s identifikovateľným menom osoby resp. inej entity (zariadenie, systém). V prípade fyzických osôb to môže byť výhradne kombinácia mena a priezviska držiteľa.

3.1.3. Anonymita alebo pseudonymita držiteľov

Používanie pseudonymov, prezývok, krycích mien, aliasov a podobne (tzv. nicknames) v certifikátoch je dovolené len v prípade, že je v položke CN jednoznačne definované, že sa jedná o pseudonym uvedením textu „PSEUDONYM“ v položke CommonName (napr. CN= alias – PSEUDONYM“) a v X.501 Name v položke pseudonym (OID 2.5.4.65) . Týmto nie sú dotknuté ustanovenia týkajúce sa jednoznačnej identifikácie držiteľa takto vydaného certifikátu.

3.1.4. Pravidlá pre interpretáciu rôznych foriem mien

Žiadne ustanovenia.

3.1.5. Jedinečnosť mien

V prípade potreby rozlíšenia rovnakých rozlišovacích mien sa použije atribút serialNumber v DN certifikátu, ktorý bude jedinečný pre daného držiteľa certifikátu. Jeho obsah bude priradený CA alebo inou autoritou.

3.2. Prvotné overenie identity

3.2.1. Spôsob preukazovania vlastníctvo súkromného kľúča

V prípade, že generovanie súkromného kľúča uskutoční Poskytovateľ priamo na čipovú kartu, nie je potrebné zo strany žiadateľa preukazovanie jeho vlastníctva. V prípade generovania žiadosti samotným žiadateľom bude potrebné preukázať vlastníctvo súkromného zaslaním podpísanej žiadosti o vydanie certifikátu vo formáte PKCS#10 na adresu Poskytovateľa (radisig@disig.sk).

3.2.2. Overenie identity právnickej osoby

U Zákazníka/Držiteľa, ktorý žiada o certifikát pre právnickú osobu RA kontroluje predložené doklady dokazujúce existencie danej právnickej osoby, čo je spravidla výpis z obchodného registra resp. iný rovnocenný výpis z iného oficiálneho platného registra právnických osôb.

Predložené doklady musia byť buď originál alebo úradne overená kópia originálu, nie starší/ia ako tri mesiace. Doklad musí obsahovať úplné obchodné meno alebo názov, identifikačný údaj (spravidla IČO), sídlo, meno/á osoby/osôb konajúcej/ich za právnickú osobu a spôsob konania a podpisovania za danú právnickú osobu.

V prípade, že právnická osoba nemá sídlo na území Slovenskej republiky, jej totožnosť sa overuje rovnakým spôsobom ako je uvedené vyššie. Výpis z platného registra právnických osôb musí byť úradne preložený do slovenského jazyka (okrem organizácií so sídlom v Českej republike).

Fyzické osoby, ktoré na základe predloženého výpisu z obchodného registra konajú na RA za danú právnickú osobu vo veci získania certifikátu, musia preukázať svoju totožnosť podľa časti 3.2.3.

V mene právnickej osoby môže na RA konať len oprávnená osoba používateľa t. j. osoba, ktorá je jej štatutárom (alebo viac takýchto osôb súčasne, ak to vyžaduje predložený výpis z obchodného registra), prípadne sa právnická osoba môže nechať zastupovať fyzickou alebo inou právnickou osobou.

Ak sa právnická osoba nechá zastupovať na RA, zastupujúca fyzická alebo právnická osoba musí vždy predložiť k nahliadnutiu overený výpis z obchodného registra zastupovanej právnickej osoby nie starší ako tri mesiace.

Ak sa právnická osoba nechá zastupovať na RA fyzickou osobou, táto zastupujúca fyzická osoba musí preukázať svoju totožnosť podľa časti 3.2.3 a navyše sa musí preukázať úradne overenou (notárom alebo matrikou) plnou mocou, z textu ktorej je jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou právnickou osobou konať v danej veci v jej mene.

Ak sa právnická osoba nechá zastupovať na RA inou právnickou osobou, táto zastupujúca právnická osoba okrem príslušnej plnej moci (viď predošlý odsek) musí

preukázať svoju totožnosť rovnakým spôsobom ako zastupovaná právnická osoba, ako je to požadované vyššie.

Subjekt (fyzická alebo právnická osoba), ktorý zastupuje právnickú osobu, sa vo veci právnickej osoby, ktorú zastupuje, v žiadnom prípade nemôže nechať zastupovať iným subjektom.

V prípade, že právnická osoba nemôže preukázať svoju totožnosť výpisom z obchodného registra (platí pre nepodnikateľské subjekty ako sú napr. obec, cirkev, občianske združenie, nadácia, štátny orgán a podobne), musí takáto právnická osoba písomne preukázať okrem svojej totožnosti aj legálnosť (resp. „dôvod“) svojej existencie (s využitím a poukázaním na zákon alebo iný predpis, ktorý o subjekte daného typu pojednáva, zriaďovaciu listinu ap.).

3.2.3. Overenie identity fyzickej osoby, zariadenia a systému.

Fyzickou osobou môže byť plnoletý občan Slovenskej republiky alebo cudzí štátny príslušník.

Fyzická osoba musí preukázať svoju totožnosť dvomi z týchto osobných dokladov:

- občiansky preukaz,
- cestovný pas,
- vodičský preukaz,
- rodný list,
- povolenie na prechodný pobyt (resp. trvalý pobyt) v prípade cudzinca
- zbrojný preukaz
- služobný preukaz

Požaduje sa pritom, aby aspoň jeden z predkladaných dokladov bol dokladom, ktorého súčasťou je fotografia danej osoby. V prípade predloženia rodného listu, zbrojného preukazu alebo služobného preukazu sa musí predložiť aj jeden z týchto dokladov: občiansky preukaz alebo cestovný pas.

Ak fyzická osoba zastupuje na RA inú fyzickú osobu, musí sa navyše preukázať úradne overenou (notárom alebo matrikou) plnou mocou, z textu ktorej je jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou fyzickou osobou konať v danej veci v jej mene.

Ak právnická osoba zastupuje fyzickú osobu, okrem plnej moci (viď predošlý odsek) musí splnomocnená právnická osoba preukázať svoju totožnosť podľa časti 3.2.2.

Subjekt (fyzická alebo právnická osoba), ktorý zastupuje fyzickú osobu, sa vo veci fyzickej osoby, ktorú zastupuje, v žiadnom prípade nemôže nechať zastupovať iným subjektom.

3.2.4. Neoverované údaje o žiadateľovi

Nie sú definované žiadne podmienky.

3.2.5. Overovanie právomocí

V rámci overovania právomocí Poskytovateľ, resp. RA vykoná formálnu kontrolu, či žiadateľ o certifikát má oprávnenie na vydanie požadovaného typu certifikátu.

3.2.6. Kritériá pre interoperabilitu

Nie sú definované žiadne podmienky.

3.3. Identifikácia a autentizácia pri obnove certifikátu

Obnova certifikátu znamená rutinnú výmenu kryptografických kľúčov pred exspiráciou certifikátu alebo výmenu kľúčov po zrušení platného certifikátu.

3.3.1. Obnova certifikátu

Držiteľ certifikátu môže požiadať o jeho obnovu 30 dní pred uplynutím platnosti aktuálneho certifikátu za podmienok splnenia overení podľa tohto CP. Nový certifikát bude vydaný na novú dvojicu vygenerovaných kryptografických kľúčov.

Žiadosť o obnovu certifikátu môže byť zaslaná elektronicky prostredníctvom digitálne podpísaného e-mailu za podmienok použitia pôvodných kryptografických kľúčov.

Žiadosť o obnovu môže byť vykonaná iba entitou, na ktorej meno boli vydané pôvodná kľúče. Poskytovateľ musí overiť všetky žiadosti o obnovu tak, že následná odpoveď musí byť potvrdená žiadajúcou entitou. Žiadajúca entita môže potvrdiť svoju žiadosť platným elektronickým podpisom. V prípade, že došlo k exspirácii certifikátu vydaného na pôvodné kľúče musí byť žiadateľ o obnovu certifikátu overený rovnakým spôsobom ako pri prvej vydávaní.

V prípade dohody so zmluvným partnerom môže byť poskytnutá aj služba automatickej obnovy certifikátu. Spôsob automatickej obnovy bude potom definovaný v zmluve s daným zmluvným partnerom.

3.3.2. Obnova certifikátu po jeho zrušení

Ak sa informácie obsiahnuté v certifikáte zmenili alebo je známe alebo existuje podozrenie kompromitácie súkromného kľúča, musí Poskytovateľ pred obnovou certifikátu overiť identitu žiadateľa rovnakým spôsobom, ako pri prvotnej registrácii. Poskytovateľ alebo RA oprávnená konať v jeho mene musia overiť akúkoľvek zmenu informácií obsiahnutých v žiadosti ešte pred jeho vydaním.

3.3.3. Identifikácia a autentifikácia žiadosti o zrušenie certifikátu

Poskytovateľ alebo RA konajúca v jeho mene, musí preskúmať žiadosť o zrušenie platnosti certifikátu. Poskytovateľ musí vytvoriť a sprístupní verejnosti postup s podmienkami zrušenia certifikátu a opatrenia, ktorými overí platnosť žiadosti o zrušenie. Všetky žiadosti o zrušenie certifikátu musia byť zaznamenané. Žiadosť o zrušenie certifikátu môže byť autentizovaná použitím súkromného kľúča patriaceho k certifikátu bez ohľadu na to, či daný súkromný kľúč bol alebo nebol kompromitovaný.

4. Prevádzkové požiadavky

4.1. Žiadanie o certifikát

Poskytovateľ musí zabezpečiť, že všetky postupy a požiadavky kladené na žiadosť o vydanie certifikátu sú popísané v tomto CP.

4.1.1. Žiadatelia o certifikát

Žiadateľom o certifikát môže byť fyzická osoba resp. sponzor, ktorá je zamestnancom zmluvného partnera, a ktorá splnila požiadavky dané týmto CP.

4.1.2. Postup žiadania a zodpovednosti

Žiadateľ o certifikát vyplní žiadosť o certifikát spôsobom, ktorý je definovaný v tomto CP a túto doručí Poskytovateľovi prostredníctvom v zmysle časti 3.2.1.

RA a následne Poskytovateľ musia zabezpečiť, že každá doručená žiadosť bude sprevádzaná:

- overením splnenia náležitostí týkajúcich sa overenia identity a autenticity žiadateľa (pozri časť 4.2.1),
- overením súladu údajov na zaslanej žiadosti s údajmi v systéme Poskytovateľa.

Zaslaním žiadosti nevzniká Poskytovateľovi automatická povinnosť na vydanie certifikátu.

4.2. Spracovanie žiadosti o certifikát

4.2.1. Spôsob overenia identity a autenticity žiadateľa

Overenie identity a autenticity žiadateľa vykoná Poskytovateľ resp. RA vystupujúca v jej mene na základe žiadosti o vydanie certifikátu a na základe údajov požadovaných pri overení identity v tejto CP.

4.2.2. Schválenie alebo zamietnutie žiadosti

Pokiaľ overenie identity a autenticity vykonané RA resp. Poskytovateľom bude úspešné a všetky ostatné náležitosti žiadosti sú v poriadku bude žiadosť postúpená Poskytovateľovi na vydanie certifikátu. Pokiaľ pri overenie identity a autenticity preukáže nezrovnalosti v predložených údajoch resp. žiadosti, vydanie certifikátu bude Poskytovateľom zamietnuté.

4.2.3. Spracovanie žiadosti o vydanie certifikátu

Po postúpení žiadosti certifikačnej autorite Poskytovateľa táto pristúpi k procedúre vydania bez zbytočného zdržania.

4.3. Vydanie certifikátu

4.3.1. Činnosť Poskytovateľa pri vydaní certifikátu

Po úspešnom overení identity a obsahu žiadosti pracovník RA prostredníctvom aplikácie RA Client iniciuje proces vydania certifikátu odoslaním ním podpísanej žiadosti spolu s osobnými údajmi držiteľa do systému Poskytovateľa.

4.3.2. Notifikácia žiadateľa o vydaní certifikátu

Poskytovateľ zašle žiadateľovi informáciu o vydaní certifikátu e-mailom spolu s informáciou o nevyhnutných krokoch na jeho inštaláciu.

4.4. Prevzatie certifikátu

4.4.1. Spôsob prevzatia certifikátu

Poskytovateľ doručí vydaný certifikát žiadateľovi (e-mail, osobné prevzatia na RA ap.), v čo najkratšom čase po jeho vydaní spolu s informáciou o spôsobe jeho inštalácie.

4.4.2. Publikovanie certifikátu Poskytovateľom

Certifikáty vydávané Poskytovateľom sú verejne dostupné pre tretie strany prostredníctvom úložiska Poskytovateľa (pozri časť 2.1).

4.4.3. Notifikácia o vydaní certifikátu iným entitám

Žiadne ustanovenia.

4.5. Kľúčový pár a používanie certifikátu

4.5.1. Súkromný kľúč držiteľa a používanie certifikátu

Držiteľ certifikátu je povinný používať svoj súkromný kľúč a certifikát len v v súlade s týmto CP resp. vnútornými predpismi zmluvného partnera. V prípade, že bol certifikát zrušený resp. skončila doba jeho platnosti je používanie jemu zodpovedajúceho súkromného kľúča zakázané.

4.5.2. Používanie certifikátu a verejného kľúča spoliehajúcou sa stranou

Žiadne ustanovenia.

4.6. Obnova certifikátu na pôvodné kľúče

Obnova certifikátu bez zmeny žiadateľovho/držiteľovho kľúčového páru (verejný kľúč a súkromný kľúč) nie je možná.

4.7. Obnova certifikátu na nové kľúče

Pod obnovou certifikátu sa rozumie jeho vydanie na novo vygenerované kľúče za podmienok, že nedôjde k zmene údajov v predmetnej časti v porovnaní s pôvodným certifikátom.

4.7.1. Okolnosti obnovy certifikátu na nové kľúče

Obnova certifikátu s vygenerovaním nového kľúčového páru sa uskutoční v prípade:

- jeho exspirácie,
- jeho zrušenia na základe kompromitácie súkromného kľúča resp. iných okolností vedúcich k jeho zrušeniu.

4.7.2. Kto môže žiadať o obnovu certifikátu na nové kľúče

O obnovu certifikátu na nové kľúče môže požiadať len oprávnený držiteľ pôvodného certifikátu (fyzická osoba, sponzor).

4.7.3. Postup žiadania o obnovu certifikátu

Obnova certifikátu po jeho zrušení z akéhokoľvek dôvodu resp. po jeho exspirácii je možná len rovnakým spôsobom ako bolo vykonané prvotné vydanie certifikátu.

4.7.4. Notifikácia o vydaní obnoveného certifikátu

Informácia o vydaní certifikátu po jeho obnove je zasielaná rovnakým spôsobom ako pri jeho prvotnom vydaní.

4.7.5. Spôsob prevzatia obnoveného certifikátu

Prevzatie obnoveného certifikátu sa vykoná rovnakým spôsobom ako pri jeho prvotnom vydaní.

4.7.6. Zverejnenie obnoveného certifikátu

Vykoná sa rovnakým spôsobom ako pri jeho prvotnom vydaní.

4.7.7. Notifikácia o vydaní obnoveného certifikátu spoliehajúcim sa stranám

Vykoná sa rovnakým spôsobom ako u prvotného vydania.

4.8. Zmena údajov v certifikáte

V prípade, že u držiteľa dôjde z akéhokoľvek dôvodu k zmene údajov, ktoré sú uvedené v certifikáte (napr. zmena priezviska pri vydaji) a tieto sa týmto stanú neaktuálne je potrebné požiadať o vydanie certifikátu s novými údajmi. Vydanie nového certifikátu sa vykoná rovnako ako v prípade vydanie pôvodného certifikátu.

4.9. Zrušenie certifikátu

4.9.1. Okolnosti zrušenia certifikátu

Certifikát je možné zrušiť v nasledovných prípadoch:

- držiteľ certifikátu alebo iná oprávnená strana požiada o zrušenie certifikátu,
- je podozrenie, že bol kompromitovaný súkromný kľúč (zodpovedajúci verejnému kľúču v certifikáte), alebo certifikát bol iným spôsobom zneužitý,
- ukázalo sa, že držiteľ certifikátu nedodržuje svoje povinnosti držiteľa certifikátu, ktoré ho zmluvne viažu,
- identifikačné informácie alebo pričlenené prvky ľubovoľných mien v certifikáte sa stanú neplatnými,
- je podozrenie, že certifikát nebol vydaný v súlade s týmto CP,
- zistilo sa, že niektorá z informácií uvedených v certifikáte je chybná alebo nesprávna,
- Poskytovateľ ukončí z akéhokoľvek dôvodu svoju činnosť a zmluvne nezaisti u inej CA, aby poskytovala informácie o zrušených certifikátoch v mene Poskytovateľa,
- skončili okolnosti, ktoré vyžadovali vydanie certifikátu (testovanie, overovanie aplikácií ap.),
- došlo ku strate súkromného kľúča,
- technické parametre alebo formát certifikátu by mohli viesť k neakceptovateľnému riziku z pohľadu dodávateľov softvéru alebo spoliehajúcich sa strán (zmena kryptografických algoritmov na podpisovanie, dĺžka kryptografických kľúčov ap.),
- smrť držiteľa certifikátu,
- došlo ku kompromitácii súkromného kľúča vydávajúcej CA Poskytovateľa,
- právoplatný rozsudok alebo predbežné opatrenie súdu.

4.9.2. Kto môže žiadať o zrušenie certifikátu

Držiteľ certifikátu (alebo ním poverená fyzická alebo právnická osoba) môže kedykoľvek požiadať o zrušenie svojho vlastného certifikátu a to aj bez udania dôvodu žiadosti o zrušenie certifikátu.

O zrušenie certifikátu môže tiež požiadať:

- pracovník RA Poskytovateľa alebo RA konajúcej v jej mene Poskytovateľa, pričom daný pracovník je povinný písomne zdokumentovať túto skutočnosť vrátane dôvodu svojho konania,

- Právnická osoba, ktorej zamestnancovi bol, na základe zmluvy s Poskytovateľom, vydaný certifikát a v certifikáte je táto skutočnosť preukázateľne uvedená.
- Člen PMA ak sa zistí závažnú skutočnosť na zrušenie certifikátu (pozri časť 4.9.1.)

4.9.3. Procedúra žiadosti o zrušenie certifikátu

Žiadosť o zrušenie certifikátu možno podať:

- osobne v sídle Poskytovateľa resp. v sídle RA konajúcej v jeho mene,
- prostredníctvom elektronickej pošty – zaslaním elektronickej poštovej správy, podpísanej súkromným kľúčom súvisiacim s certifikátom, o zrušenie ktorého sa žiada resp. nepodpísanej správy obsahujúcej dohodnuté tajomstvo známe len držiteľovi certifikátu.
- prostredníctvom poštovej zásielky spolu so zadaním tajomstva známeho len držiteľovi certifikátu zaslanej Poskytovateľovi resp. RA konajúcej v jeho mene,
- telefonicky na telefónnom čísle patriacom Poskytovateľovi resp. RA konajúcej v jeho mene.

4.9.4. Lehota na zaslanie žiadosti o zrušenie certifikátu

Držiteľ certifikátu musí požiadať o jeho zrušenie okamžite ako nastane niektorá zo skutočnosti uvedená v časti 4.9.1.

4.9.5. Čas na zrušenie certifikátu

Poskytovateľ je povinný zrušiť certifikát čo najskôr po prevzatí žiadosti o jeho zrušenie za podmienky, že boli splnené zo strany držiteľa resp. inej oprávnenej osoby všetky náležitosti týkajúce sa zrušenia certifikátu. Zrušenie sa musí uskutočniť najneskoršie do 48 hodín od prevzatia žiadosti o zrušenie

4.9.6. Povinnosti overovania stavu certifikátu zo strany spoliehajúcich sa strán

Spoliehajúce sa strany sú povinné pred tým ako sa spoľahnú na elektronický podpis resp. inú skutočnosť zviazanú s vydaným certifikátom overiť jeho platnosť použitím aktuálneho vydaného zoznamu zrušených certifikátov (CRL).

4.9.7. Frekvencia zverejňovania CRL

Zoznam zrušených certifikátov (CRL) je vydávaný s frekvenciou minimálne 1 krát za 24 hodín.

4.9.8. Čas zverejnenia vydaného CRL

Vydaný zoznam zrušených certifikátov je publikovaný v úložisku Poskytovateľa bezodkladne pričom čas od vydania CRL do jeho publikovania v úložisku nesmie prekročiť 120 sekúnd.

4.9.9. Overovanie stavu certifikátu prostredníctvom OCSP

Poskytovateľ u CA External nemá k dispozícii službu OCSP.

4.9.10. Požiadavky na overenie stavu certifikátu prostredníctvom OCSP

Pozri časť 4.9.9.

4.9.11. Pozastavenie platnosti certifikátu

Pozastavenie certifikátu nie je zo strany Poskytovateľa podporované.

4.10. Služby overovania stavu certifikátu

4.10.1. Charakteristika služby

Poskytovateľ poskytuje službu overovania stavu certifikátu prostredníctvom zverejňovania zoznamu zrušených certifikátov (CRL)

4.10.2. Dostupnosť služby

Aktuálny zoznam publikovaný spoločnosťou Disig je dostupný na v úložisku poskytovateľa – Zoznamy CRL.

Vydávané CRL obsahuje všetky zrušené certifikáty vrátane už exspirovaných zrušených certifikátov.

4.11. Ukončenie zmluvného vzťahu

Certifikáty pre potreby zamestnancov zmluvného partnera sú vydávané na základe zmluvy medzi spoločnosťou Disig a zmluvným partnerom. V tejto zmluve je uvedená aj doba platnosti jednotlivých certifikátov, ktorá je spravidla v rozmedzí 1 až 3 roky. Počas trvania zmluvného vzťahu sú zmluvnému partnerovi poskytované kompletné certifikačné služby (vydávanie certifikátov, ich rušenie, poskytovanie CRL). V prípade, že sa tento zmluvný vzťah ukončí, tak v rámci dohody o ukončení sa stanovia pravidlá týkajúce sa existencie vydaných certifikátov.

U certifikátov pre jednotlivé fyzické osoby resp. fyzické osoby zamestnancov právnických osôb sa predpokladá existencia rámcovej zmluvy o poskytovaní dôveryhodnej služby vydávania certifikátov, kde sú presne uvedené podmienky ukončenia zmluvného vzťahu.

4.12. Obnova kľúčov z depozitu alebo zálohy

Poskytovateľ nepodporuje uchovávanie súkromných kľúčov držiteľov certifikátov.

5. Manažérske, prevádzkové a fyzické bezpečnostné opatrenia

5.1. Fyzické bezpečnostné opatrenia

5.1.1. Umiestnenie, priestory a prístup

Umiestnenie infraštruktúry Poskytovateľ, ktoré tvorí infraštruktúru CA Disig External musí zabezpečiť že:

- priestory CA sú nepretržite fyzicky alebo elektronický monitorované proti neoprávnenému vniknutiu,
- samostatný prístup k serverom CA budú mať len osoby nachádzajúce sa na zozname oprávnených osôb s právom prístupu,
- osoby, ktoré nie sú na zozname oprávnených osôb na vstup budú vstupovať do priestorov CA len pod dohľadom oprávnenej osoby,
- záznamy o vstupe do priestorov sú udržiavané a kontrolované pravidelne,
- všetky vymeniteľné médiá a dokumenty obsahujúce citlivé informácie sú uložené v zabezpečených kontajneroch.

Poskytovateľ zabezpečí prevádzku RA tak, že zaistí primeranú bezpečnosť kryptografickému modulu s podpisovými kľúčmi CA a systémovému softvéru.

Držitelia by nemali ponechať svoje pracovné stanice bez dozoru, pokiaľ sú kryptografické kľúče používané, t. j. keď PIN alebo heslo už boli zadané. Pracovné stanice, ktoré majú uložený súkromný kľúč na pevnom disku musia byť fyzicky zabezpečené alebo chránené vhodným produktom riadenie prístupu.

Certifikáty pracovníkov RA, ktoré sú umiestnené na bezpečnom hardvérovom zariadení musia byť chránené fyzicky. To môže byť vykonané napríklad tým, že je zariadenie je prechovávané u jeho držiteľa.

5.1.2. Dodávka energie a klimatizácia

Poskytovateľ musí zabezpečiť že zdroj elektrickej energie a klimatizácia bude postačujúca k bezproblémovému chodu systému CA.

5.1.3. Ohrozenie vodou

Poskytovateľ musí zabezpečiť, že CA systém je chránený pred ohrozením vodou.

5.1.4. Protipožiarna ochrana

Poskytovateľ musí zabezpečiť, že CA systém je chránený protipožiarnym systémom.

5.1.5. Uchovávanie médií

Poskytovateľ musí zabezpečiť, že uchovávané média používané v systéme CA sú chránené pred nepriaznivými účinkami okolitého prostredia ako sú teplota, vlhkosť a elektromagnetické žiarenie. Záložné kópie musia byť uchovávané v oddelených priestoroch chránených pred zničením požiarom resp. vodou.

5.1.6. Nakladanie s odpadom

Všetky média používané na uchovávanie informácií ako sú kľúče, aktivačné údaje alebo súbory CA musia byť pred vyhodením do odpadu odstránené a fyzicky zničené.

5.1.7. Záložné pracovisko

Poskytovateľ musí zabezpečiť, že záložné pracovisko, ak existuje, musí mať rovnakú úroveň bezpečnosti ako primárne pracovisko CA.

5.2. Procedurálne bezpečnostné opatrenia

5.2.1. Dôveryhodné roly

5.2.1.1. Dôveryhodné roly CA

Poskytovateľ musí zabezpečiť rozdelenie povinností pre kritické funkcie CA, aby sa zabránilo, že jedna osoba môže zneužiť systém CA bez možnosti zistenia. Každý prístup užívateľa do systému by mal byť prístup obmedzený len na tie akcie, ktoré sú potrebné na vykonanie pri plnení ich povinností.

Poskytovateľ musí mať minimálne tieto odlišné roly v rámci PKI, ktoré oddelia každodennú správu systému CA, manažment a auditu tejto správy a manažment podstatných zmien v požiadavkách na systém, vrátane politiky, poriadkov, postupov a personálu.

5.2.1.2. Dôveryhodné roly RA

Poskytovateľ musí zabezpečiť, aby pracovníci RA pochopili svoju zodpovednosť za identifikáciu a overovanie žiadateľov a vykonávanie nasledovných funkcií:

- prijatie žiadosti, zmena certifikátu, rušenie certifikátu,
- overenie identity a autenticity žiadateľa,
- prenos informácie o žiadateľovi k CA,
- overovanie všetkých ostatných informácií súvisiacich s vydaním certifikátu

Poskytovateľ môže povoliť vykonávanie všetkých povinností funkcie RA jednou osobou.

5.2.2. Počet osôb potrebný na výkon úloh

Generovanie kľúčov CA External si vyžaduje prítomnosť najmenej troch pracovníkov Poskytovateľa zaradených v dôveryhodných rolách. Pracovníci môžu samostatne vykonávať všetky prevádzkové povinnosti spojené s ich rolou u Poskytovateľa.

Poskytovateľ musí zabezpečiť, že ktorýkoľvek zavedený overovací proces poskytne celkový prehľad všetkých aktivít vykonaný pracovníkmi v dôveryhodných rolách.

5.2.3. Identifikácia a autentizácia jednotlivých rolí

Všetky zamestnanci Poskytovateľa sa musia podrobiť overeniu identity a oprávnení pred tým, ako:

- sú priradení na zoznam s oprávnením prístupu do chránených priestorov CA Poskytovateľa,
- sú priradení na zozname s oprávnením fyzického prístupu do chránených priestorov CA Poskytovateľa,
- im je pridelený certifikát na výkon roly v rámci CA Poskytovateľa
- im je pridelený účet v systéme CA Poskytovateľa.

Každý z týchto certifikátov a účtov (s výnimkou podpisových certifikátov Poskytovateľa):

- musí byť priamo priradený fyzickej osobe,
- nemôže byť zdieľaný,
- musí mať obmedzený rozsah oprávnení na oprávnenia danej roly v CA softvéri, operačnom systéme a riadení procesov.

CA operácie musia byť, pri prístupe cez zdieľanú sieť, zabezpečené použitím mechanizmov, akými sú silná autentifikácia a šifrovanie s využitím hardvérových tokenov.

5.3. Personálne opatrenia

Poskytovateľ musí zabezpečiť, že všetci zamestnanci vykonávajúci povinnosti v súvislosti s prevádzkou CA alebo RA musia:

- byť písomne menovaní,
- byť viazaný zmluvou alebo štatútom k podmienkach a pravidlám pre danú pozíciu, ktoré musia plniť,
- absolvovať komplexné školenie s ohľadom na povinnosti, ktoré majú plniť,
- byť viazaný zákonom alebo zmluvou k mlčanlivosti o citlivých skutočnostiach týkajúcich sa Poskytovateľa alebo držiteľov certifikátov,

Zamestnanci nesmú mať pridelené povinnosti, ktoré môžu vyvolať konflikt záujmov s ich CA alebo RA povinnosťami.

5.3.1. Vzdelanie, kvalifikácia, skúsenosti a vôľové požiadavky

Poskytovateľ musí formulovať a dodržiavať personálnu a manažérsku politiku dostatočnú na to aby poskytla primeranú istotu o dôveryhodnosti a kompetentnosti svojich zamestnancov a viedla k uspokojivému plneniu ich povinností v súlade s týmto CP.

5.3.2. Postupy overovania

Poskytovateľ vykoná zodpovedajúce preskúmanie všetkých pracovníkov, ktorí sú zaradení v dôveryhodných rolách (pred ich zamestnaním a potom v pravidelných intervaloch podľa potreby) na overenie ich dôveryhodnosti a kompetencie v súlade s požiadavkami tohto poriadku a postupov personálnej práce CA alebo ekvivalentných požiadaviek. Všetci pracovníci, ktorí neuspejú v rámci počiatočného alebo pravidelného preskúmavania nesmú ďalej pôsobiť, alebo pokračovať v pôsobení v dôveryhodnej role. PMA môže stanoviť dodatočné požiadavky v súlade s národnou legislatívou.

5.3.3. Požiadavky na školenie

Poskytovateľ musí zabezpečiť, že všetci zamestnanci plniaci si povinnosti v súvislosti s prevádzkou CA alebo RA musia dostať komplexné školenie v oblasti:

- bezpečnostných pravidiel a mechanizmov platných pre CA/RA,
- všetkých verzií PKI softvéru v systéme CA,
- všetkých povinnosti v rámci PKI, ktorých plnenie sa očakáva,
- postupov obnovy po havárii a postupov obnovy činnosti (business continuity).

5.3.4. Frekvencia preškoľovania a požiadavky

Žiadne ustanovenia.

5.3.5. Obmena pozícií

Žiadne požiadavky

5.3.6. Sankcie za neoprávnené zásahy

V prípade reálneho alebo údajného výkonu neoprávneného zásahu osobou vykonávajúcou povinnosti v súvislosti s prevádzkou CA alebo RA, môže CA pozastaviť jeho/jej prístup k systému CA.

5.3.7. Zamestnanci na zmluvu

Žiadne ustanovenia.

5.3.8. Dokumentácia poskytovaná zamestnancom

Poskytovateľ musí sprístupniť všetkým pracovníkom CA External certifikačný poriadok a ostatné špecifické nariadenia, politiky alebo zmluvy týkajúce sa ich pozície.

5.4. Postupy zaznamenávania auditných logov

5.4.1. Typy zaznamenávaných udalostí

Poskytovateľ by mal zaznamenať do auditných log súborov všetky udalosti týkajúce sa bezpečnosti systému CA.

Všetky záznamy, či už elektronické alebo manuálne, by mal obsahovať dátum a čas udalosti, a totožnosť subjektu, ktorý udalosť spôsobil.

5.4.2. Frekvencia spracovávania auditných log záznamov

Poskytovateľ musí zabezpečiť, že pracovníci CA preskúmavajú pravidelne svoje audit log záznamy a všetky významné udalosti sú vysvetlené v súhrnom zázname s preskúmavania. Postup hodnotenia zahŕňa overovanie, či nedošlo k manipulácii so záznamami, krátkeho prezretia všetkých položiek log záznamov s dôkladnejším preskúmaním akýchkoľvek upozornení alebo nepravidelností v záznamoch. Všetky prijaté opatrenia prijaté na základe týchto hodnotení musia byť dokumentované.

5.4.3. Doba uchovávanie auditných log záznamov

Poskytovateľ musí zachovať svoju auditné log záznamy k dispozícii najmenej dva mesiace a následne archivovať v zmysle časti 4.6.

5.4.4. Ochrana auditných log záznamov

Systém zaznamenávanie auditných log záznamov musí zahŕňať mechanizmy na ochranu log súborov proti neoprávnenému prezeraniu, úprave a vymazaniu. Manuálne log záznamy musia byť chránené pred neoprávneným prezeraním, úpravou a zničením.

5.4.5. Postup zálohovania auditných log záznamov

Auditné log záznamy a súhrnné reporty musia byť zálohované alebo kopírované manuálne.

5.4.6. Systém získavania auditných záznamov

Poskytovateľ musí identifikovať spôsob získavania auditných záznamov v interných predpisoch.

5.4.7. Upozornenie pôvodcu na udalosť

Pokiaľ je zaznamenaná udalosť systémom zaznamenávania auditných logov nemusí dôjsť k upozorneniu jedinca, organizácie, zariadenia alebo aplikácie, ktorá ju zapríčinila.

5.4.8. Zraniteľnosti

V rámci zaznamenávania auditných logov sú tieto zaznamenávané aj z dôvodu monitorovania zraniteľnosti systému. Poskytovateľ musí zabezpečiť, aby bolo vykonávané hodnotenie zraniteľnosti, ich preskúmavanie a revízia, po ich dôkladnej analýze

5.5. Uchovávanie záznamov

5.5.1. Typy uchovávaných záznamov

Nasledujúce dáta a súbory musia byť archivované Poskytovateľom alebo v jeho mene:

- zmluvné záväzky,
- žiadosti o certifikát,
- žiadosti o zrušenie certifikátu,
- osobné údaje držiteľa certifikátu,
- všetky vydané a/alebo zverejnenie certifikáty,
- zmena kľúčov CA,
- všetky CRL vydané a/alebo zverejnené,
- všetky auditné log záznamy.

5.5.2. Doba uchovávanie archívnych záznamov

Archív kľúčov a informácie o certifikáte sa musia uchovávať po dobu najmenej 5 rokov. Archív auditných log záznamov musí byť uchovávaný po dobu najmenej šiestich (6) mesiacov.

5.5.3. Ochrana archívnych záznamov

Archívne médiá musí byť chránené len fyzickými bezpečnostnými opatreniami alebo kombináciou fyzických bezpečnostných opatrení a kryptografickej ochrany.

5.5.4. Požiadavky na archiváciu záznamov autority časovej pečiatky

Žiadne ustanovenia.

5.5.5. Archívny systém

Žiadne ustanovenia.

5.5.6. Postup získania a overenia archívnych informácií

Žiadne ustanovenia.

5.6. Zmena kľúčov

Držiteľ môže požiadať o obnovu jeho/jej kľúčového páru v priebehu 30 dní pred exspiráciou kľúčov, ak predchádzajúci certifikát nebol zrušený. Proces obnovy môže začať držiteľ, Poskytovateľ alebo RA.

Držitelia bez platného certifikátu musia byť znovu overení Poskytovateľom alebo externou RA rovnakým spôsobom ako pri prvej registrácii.

V prípade, že držiteľov certifikát bol zrušený v dôsledku nedodržania jeho povinností, musí Poskytovateľ overiť, že všetky dôvody pre nedodržania povinností boli odstránené k jej spokojnosti ešte pred obnovou certifikátu.

5.7. Kompromitácia a obnova po havárii

5.7.1. Postupy dokumentovania a riadenia incidentov a kompromitácií

Poskytovateľ musí prijať postupy dokumentovania a riadenia incidentov a kompromitácií v zmysle ktorých bude vykonávaná obnova jej činnosti.

5.7.2. Poškodený hardvér, softvér, a/alebo údaje

Poskytovateľ musí prijať postupy obnovy s definovanými krokmi pre prípad, že dôjde k poškodeniu alebo strate hardvéru, softvéru a/alebo údajov. V prípade, že úložisko nie je pod kontrolou Poskytovateľa, musí Poskytovateľ zaistiť súhlas s poskytovateľom úložiska, aby postupy obnovy boli prijaté a dokumentované poskytovateľom.

5.7.3. Kompromitácia súkromného kľúča CA

Poskytovateľ musí mať zavedený vhodný plán pre prípad kompromitácie kľúčov, ktorý rieši postupy, ktoré budú nasledovať v prípade kompromitácie súkromného podpisového kľúča používaného na podpisovanie CA External vydávaných certifikátov pre koncových používateľov. Takýto plán musí obsahovať postupy na zrušenie všetkých dotknutých certifikátov a postupu na bezodkladné informovanie všetkých držiteľov týchto certifikátov a spoliehajúcich sa strán.

V prípade potreby zrušenia podpisového certifikátu CA External musí Poskytovateľ bezodkladne informovať:

- PMA,

- všetky jeho RA,
- všetkých držiteľov,
- všetkých zmluvných partnerov, ktorým sú vydávané certifikáty CA External

Poskytovateľ musí tiež:

- zverejniť sériové číslo zrušeného certifikátu vo vhodnom CRL,

Po vyriešení skutočností, ktoré viedli k zrušeniu, môže Poskytovateľ:

- vygenerovať nový kľúčový pár CA,
- obnoviť certifikáty všetkým subjektom a zabezpečiť, aby všetky zoznamy CRL a ARL boli podpísané prostredníctvom nových kľúčov.

5.7.4. Pokračovanie v poskytovaní služieb po havárii

Poskytovateľ musí zabezpečiť poskytovanie nevyhnutných služieb (napr. vydávanie CRL) v prípade havárie spôsobenej prírodnou alebo inou katastrofou. K pokračovaniu poskytovania služieb musí mať k dispozícii vzdialené miesto obnovy, kde je možné obnoviť poskytovanie služieb.

5.8. Ukončenie činnosti CA

V prípade, že Poskytovateľ ukončí prevádzku Disig CA External, musí to okamžite oznámiť všetkým zmluvným partnerom, ktorým sú touto CA vydávané certifikáty.

Všetky platné certifikáty vydané touto certifikačnou autoritou v zmysle tohto CP budú zrušené skôr ako dôjde k ukončeniu činnosti. Všetky aktuálne a archivované dokumenty CA musia byť odovzdané PMA (alebo inej určenej osobe) počas 48 hodín po ukončení činnosti CA a v súlade s týmto CP.

6. Technické bezpečnostné opatrenia

6.1. Generovanie kľúčového páru a jeho inštalácia

6.1.1. Generovanie kľúčov

Generovanie kľúčových párov pre koncového užívateľa zmluvného partnera sa uskutočňuje buď na RA (SSCD; QSCD) resp. môže byť generované priamo v PC koncového používateľa.

6.1.2. Doručenie privátneho kľúča držiteľovi

Súkromné kľúče budú doručené držiteľovi bezpečným spôsobom ich prevzatím priamo na RA pri vydávaní na SSCD/QSCD. V prípade generovania kľúčového páru v PC koncového držiteľa je privátny kľúč vždy výhradne pod jeho kontrolou a chránený ním zvoleným silným heslom.

6.1.3. Doručenie verejného kľúča Poskytovateľovi

Doručenie verejného kľúča Poskytovateľovi sa uskutoční v prípade jeho generovania na PC používateľa v zmysle postupu dohodnutého s jednotlivými zmluvnými partnermi resp. žiadateľmi o certifikát, zvyčajne zaslaním linky na stiahnutie certifikátu z úložiska Poskytovateľa.

6.1.4. Veľkosť kľúčov

Poskytovateľ musí zabezpečiť, že kľúčová páry pre všetky subjekty v rámci PKI zmluvných partnerov, ktorým sú touto CA vydávané certifikáty budú mať dĺžku najmenej 2048 bit RSA.

6.1.5. Parametre generovania kľúčov a kontrola kvality

Žiadne požiadavky.

6.1.6. Účel použitia kľúčov

Kryptografické kľúče koncových používateľov sú určené hlavne na:

- autentifikáciu držiteľa,
- vytváranie elektronického podpisu a
- end-2-end šifrovanie údajov.

Polia určujúce možnosti použitia certifikátu musia byť použité v súlade s požiadavkami RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“.

Podpisové kľúče CA External sú jediné kľúče určené na podpisovanie vydávaných certifikátov a CRL. V podpisovom certifikáte CA External musia byť prítomné nasledovné hodnoty „Key Certifikát Sign a CRL Sign“.

6.2. Ochrana súkromného kľúča a využívanie kryptografických hardvérových modulov (HSM)

Poskytovateľ musí uchovávať kryptografické kľúče vydávajúca CA External, určené na podpisovanie certifikátov koncových používateľov, v kryptografickom bezpečnostnom module (HSM).

6.2.1. Štandardné požiadavky na HSM

HSM modul musí byť uložený v bezpečných priestoroch bez prístupu neoprávnených osôb. HSM modul musí spĺňať ochranu pred odchytávaním elektromagnetického vyžarovania, podporovať funkciu self test, poskytovať funkciu key recovery.

6.2.2. Práca so súkromných kľúčom

Súkromný kľúč certifikačnej autority musí byť generovaný a obnovovaný pod kontrolou viacerých osôb podľa princípu *n* z *m*. U CA External sú tieto hodnoty n=4 a m=7.

6.2.3. Obnova súkromných kľúčov z depozitu

Súkromný kľúč CA External nie je uložený v depozite u tretej osoby.

6.2.4. Zálohovanie súkromných kľúčov

Súkromný kľúč CA External je zálohovaný pri vytváraní pravidelných záloh servera certifikačnej autority, nakoľko sa v zašifrovanej podobe nachádza na pevnom disku servera CA s pripojeným HSM modulom. Obnova kľúča je možná len v jednom konkrétnom prostredí HSM (Security world) a s použitím príslušného počtu operátorských kariet (princíp *n* z *m*).

6.2.5. Archivácia súkromných kľúčov

Pozri časť 6.2.4.

6.2.6. Prenos súkromného kľúča do alebo z kryptografického modulu

Súkromný kľúč je štandardne uložený v zašifrovanej podobne na pevnom disku počítača, ku ktorému je pripojený HSM modul. Do HSM modulu sa prenáša pri spustení operácia aktivácie kľúčov za použitia príslušného počtu operátorských kariet (princíp *n* z *m*).

6.2.7. Uchovávanie súkromného kľúča v HSM module modulu

Súkromný kľúč v HSM module je uložený vo forme plain textu. Mimo HSM modulu je uložený v zašifrovanej podobe a chránený príslušným počtom operátorských kariet (princíp n z m) t.j. heslo na dešifrovanie je možné získať len použitím predpísaného počtu operátorských kariet. U CA External je počet operátorských kariet n=2 a m=5.

6.2.8. Spôsob aktivácie súkromného kľúča

Oprávnené osoby musia byť overené kryptografickým modulom pred aktiváciou súkromného kľúča. Toto overenie môže byť vo forme hesla. Pri deaktivácii, musí byť súkromný kľúč uchovávaný iba v šifrovanej podobe.

6.2.9. Spôsob deaktivácia súkromného kľúča

Pri deaktivácii musí byť kľúč vymazaný z pamäte HSM modulu. Každý priestor na disku, v ktorom boli uložené kľúče musí byť prepísaný pokiaľ sa uvoľní na použitie pre operačný systém. Kryptografický modul musí automaticky vypnúť súkromný kľúč po uplynutí prednastavenej doby nečinnosti.

6.2.10. Spôsob zničenia súkromného kľúča

Po ukončení používania súkromného kľúča, všetky kópie súkromného kľúča v pamäti počítača a na zdieľanom diskovom priestore musia byť bezpečne zlikvidované jeho prepísaním Spôsob prepísania musí byť schválený PMA.

6.2.11. Charakteristika HSM modulu

Žiadne ustanovenia.

6.3. Ďalšie aspekty manažmentu kľúčového páru

6.3.1. Archivácia verejného kľúča

Pozri časť 4.6

6.3.2. Doba platnosti certifikátov a použiteľnosti kľúčového páru

Doba platnosti certifikátov vydaných na kľúče s minimálnou veľkosťou 2048 bit je maximálne 5 rokov. Kľúčový pár je použiteľný len po dobu platnosti naň vydaného certifikátu.

6.4. Aktivačné údaje

6.4.1. Generovanie aktivačných údajov a ich inštalácia

Všetky aktivačný údaje musia byť jedinečné a nepredvídateľné. Aktivačné údaje, v spojení s niektorým iným overovaním prístupu, musia mať primeranú úroveň sily

v závislosti na kľúčoch alebo údajoch, ktoré majú byť chránené. Tam, kde sa používajú heslá, musí mať subjekt možnosť zmeniť jeho heslo kedykoľvek.

6.4.2. Ochrana aktivačných údajov

Údaje použité pre inicializáciu entity musia byť chránené pred neoprávneným použitím kombinácie mechanizmov kryptografického a fyzického riadenia prístupu.

Súkromné kľúče subjektov musia byť chránené pred neoprávneným použitím kombinácie mechanizmov kryptografického a fyzického riadenia prístupu. Úroveň ochrany musí byť dostatočná, tak aby odradila motivovaného útočníka s dostatočnými prostriedkami. Ak je možné používať heslo opakovane, mechanizmus by mal zahŕňať možnosť dočasne zablokovať účet po vopred určenom počte pokusov o prihlásenie.

6.4.3. Ďalšie aspekty aktivačných údajov

Žiadne požiadavky.

6.5. Počítačové bezpečnostné opatrenia

6.5.1. Špecifické technické požiadavky z oblasti počítačovej bezpečnosti

Každý server certifikačnej autority musí umožňovať nasledovnú funkcionalitu:

- riadenie prístupu k službám CA a PKI rolám,
- vynucovať oddelenie zodpovedností pre PKI roly,
- identifikáciu a autentizáciu PKI rolí a s nimi súvisiace identity,
- použitie kryptografie pri komunikácii v rámci session a zabezpečenie databázy,
- interný audit udalostí súvisiacich s bezpečnosťou,
- self-test CA služieb vzťahujúcich sa k bezpečnosti,
- dôveryhodnú cestu k identifikácii PKI rolí a súvisiacich identít,
- mechanizmus obnovy kľúčov a systému CA.

Táto funkcia môže byť poskytovaná operačným systémom, alebo v kombinácii operačného systému, PKI CA softvéru a fyzickej ochrany.

6.5.2. Hodnotenie počítačovej bezpečnosti

Žiadne požiadavky.

6.6. Životný cyklus riadenia bezpečnosti

6.6.1. Riadenie vývoja systému

Žiadne ustanovenia.

6.6.2. Riadenie manažmentu bezpečnosti

Žiadne ustanovenia

6.7. Riadenie sieťovej bezpečnosti

Servery CA External musia byť chránené pred napadnutím z ľubovoľnej otvorenej alebo internej siete, do ktorej sú pripojené. Táto ochrana musí byť riešená prostredníctvom inštalácie zariadení nakonfigurovaný tak, že budú prístupné len protokoly a príkazy potrebné pre prevádzku CA.

6.8. Využívanie časovej pečiatky

Žiadne požiadavky.

7. Profily certifikátov a CRL

7.1. Profily certifikátov

7.1.1. Podporovaná verzia

CA External vydáva X.509 verzie 3 certifikáty v zmysle RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“.

7.1.2. Použite rozšírenia v certifikátoch

Softvér CA External musí podporovať všetky základné X.509 definované položky:

Podpis (Certificate Signature)	**Podpis CA na autentifikáciu certifikátu**
Algoritmus podpisu (Certificate Signature Algorithm)	*Použitý algoritmus podpisu*
Vydavateľ (Issuer)	*Meno CA*
Platnosť (Validity)	*Dátum začiatku a konca platnosti*
Subjekt (Subject)	*Rozlišovacie meno držiteľa*
Informácie o verejnom kľúči subjektu (Subject Public Key Information)	*ID algoritmu, kľúč*
Verzia (Certificate Version)	*Verzia X.509 certifikátu, verzia 3*
Sériové číslo (Serial NUmber)	*Jedinečné sériové číslo certifikátu*

Žiadne rozšírenie nesmie modifikovať alebo podkopať dôveru použitia týchto základných položiek.

Každý používaný softvér zmluvného partnera, pre ktorého sú certifikáty vydávané musí korektne spracovávať rozšírenia definované v časti 4.2.1 a 4.2.2 RFC 5280.

7.1.3. Identifikácia kryptografických algoritmov

Žiadne ustanovenia.

7.1.4. Menná konvencia

Žiadne ustanovenia.

7.1.5. Obmedzenia týkajúce sa mena

DN subjektu a vydavateľa musí byť prítomné v každom certifikáte a musí spĺňať požiadavky RFC 5280.

7.1.6. Aplikované OID certifikačného poriadku

Poskytovateľ musí zabezpečiť, že OID tohto certifikačného poriadku je zahrnutý v certifikátoch, ktoré vydáva.

7.1.7. Použitie rozšírenia „policy constraints“

Žiadne požiadavky.

7.1.8. Syntax a sémantika CP

Žiadne ustanovenia.

7.1.9. Sémantika spracovanie kritických rozšírení CP

Kritické rozšírenia musia byť interpretované spôsobom definovaným v RFC 5280.

7.2. Profil CRL

7.2.1. Podporovaná verzia

Poskytovateľ musí publikovať CRL vo verzii X.509 verzia 2 v súlade s požiadavkami RFC 5280.

7.2.2. CRL a CRL rozšírenia

Každý softvér používaný zmluvným partnerom musí správne spracovať všetky rozšírenie CLR definované v RFC 5280. Poskytovateľ môže vymedziť použitie akýchkoľvek rozšírenie podporovaných CA, jeho RA a koncovým držiteľom certifikátov.

7.3. OCSP profil

7.3.1. Používaná verzia

Poskytovateľ neposkytuje službu OCSP pre Disig CA External.

7.3.2. Rozšírenia OCSP

Žiadne ustanovenia.

8. Audit súladu a iné posudzovanie

Audit súladu určuje, či Poskytovateľ spĺňa štandardy a stanovené požiadavky tohto CP.

Autorita zodpovedná za správu tohto CP musí vymedziť špecifické požiadavky pre audit súladu.

Účelom tohto auditu musí byť overenie, že CA a ňou poverené strany majú zavedený systém, na zabezpečenie kvality poskytovaných služieb CA, tak, že Poskytovateľ a jeho CA sú v súlade so všetkými požiadavkami tohto poriadku,

8.1. Frekvencia auditu alebo iného hodnotenia

Audit súladu certifikačnej autority CA External Poskytovateľa musí byť vykonaný minimálne 1 krát ročne a vždy pokiaľ tak rozhodne PMA ako následok potenciálneho resp. aktuálneho porušenia bezpečnosti.

Audit sa vykoná formou interného auditu.

8.2. Rozsah auditu a použité metódy

Audit CA External bude zameraný na splnenie požiadaviek v aktuálnej verzii dokumentu ETSI EN 319 411-1 „Electronic Signatures and Trust Infrastructures (ESI);Policy and security requirements for Trust Service Providers issuing certificates;Part 1: General requirements“.

8.3. Identita a kvalifikácia audítora

Interný audítor musí mať skúsenosti s PKI a kryptografickými technológiami ako aj prevádzkou príslušného PKI softvéru, ktorý je definovaný PMA.

8.4. Vzťah audítora a hodnoteného subjektu

Audítor nemusí byť nezávislý od Poskytovateľa.

8.5. Možné opatrenia prijaté na základe výsledkov auditu

Výsledky auditu musia byť predložené PMA. Ak sa zistia nezrovnalosti, musí zodpovedná osoba Poskytovateľa predložiť správu PMA, aké nápravné opatrenia uskutoční ako reakciu na správu o audite.

8.6. Výsledok auditu a jeho zverejnenie

Poskytovateľ musí poskytnúť členom PMA kópiou výsledkov auditu zhody.

9. Ostatné obchodné a legislatívne otázky

9.1. Poplatky

9.1.1. Poplatok za vydanie a obnovu certifikátu

Poplatok za všetky poskytované PKI služby bude určený zmluvou medzi spoločnosťou Disig a zmluvným partnerom resp. držiteľom certifikátu.

Cenník služieb je dostupný v cenníku publikovanom na web stránke Poskytovateľa.

Poskytovateľ sa nesmie požadovať poplatky za poskytnutie CP na čítanie.

9.2. Finančná zodpovednosť

Žiadne ustanovenia.

9.3. Dôvernosť obchodných informácií

9.3.1. Rozsah dôverných informácií

Žiadne ustanovenia.

9.3.2. Informácie, ktoré nie sú dôvernými informáciami

Žiadne ustanovenia.

9.3.3. Zodpovednosť za ochranu dôverných informácií

Žiadne ustanovenia.

9.4. Ochrana osobných údajov

9.4.1. Požiadavky na ochranu osobných údajov

Poskytovateľ musí spracovávať osobné údaje Zákazníkov/Držiteľov certifikátov, resp. nimi splnomocnených osôb v súlade s požiadavkami predpisov o ochrane osobných údajov Informácia o spracúvaní osobných údajov, Disig, a.s.

9.4.2. Informácie, ktoré nie sú považované za osobné

Za osobné údaje v rámci poskytovaných služieb nie sú považované vydané certifikáty verejného kľúča a certifikáty vydávajúcej CA External. Rovnako publikované zoznamy zrušených certifikátov.

9.4.3. Zodpovednosť za ochranu osobných údajov

Všetci držitelia certifikátov musia v maximálne možnej miere zabezpečiť bezpečnosť svojich súkromných kľúčov a informácií, ktoré chránia ich použitie (PIN, heslá).

9.4.4. Súhlas so spracovaním osobných údajov

Súčasťou zmluvy spoločnosti Disig so zmluvným partnerom resp. držiteľom certifikátu, ktorým sú poskytované certifikačné služby Poskytovateľa musia byť ustanovenia týkajúce sa spracovania osobných údajov.

9.4.5. Podmienky zverejnenia osobných údajov

Poskytovateľ nezverejní žiadne informácie týkajúce sa žiadateľa o certifikát alebo držiteľa certifikátu žiadnej tretej strane, pokiaľ to nie je povolené týmto CP, požadované zákonom alebo príkazom kompetentného súdu resp. je to predmetom zmluvy medzi Poskytovateľom a jej partnerom. Každá požiadavka na uvoľnenie informácií má byť autentizovaná a zadokumentovaná.

Poskytovateľ nesmie poskytnúť osobné údaje žiadnej tretej strane s výnimkou subjektov, ktoré zo zákona majú právo kontrolovať činnosť Poskytovateľa a kompetentných štátnych orgánov ako sú polícia, súdy, prokuratúra.

9.5. Právo duševného vlastníctva

Súkromný kľúč musí byť považovaný za výslovný majetok oprávneného držiteľa zodpovedajúceho verejného kľúča identifikovaného v certifikáte.

Táto CP a jeho OID sú majetkom Disig a môžu byť použité len pre potreby CA External v súlade s ustanoveniami uvedenými v tomto CP. Akékoľvek iné použitie tohto CP a jeho OID bez výslovného písomného súhlasu Poskytovateľa je výslovne zakázané.

9.6. Vyhlásenia a záruky

9.6.1. Záruky Poskytovateľa

Všetky informácie uvedené v certifikáte musia byť presné a správne do takej miery ako sú poskytnuté žiadateľom o certifikát v procese jeho identifikácie a autentifikácie. Záruky poskytované zo strany Poskytovateľa musia byť uvedené v zmluve uzavretej s držiteľom certifikátu, ktorý je ňou vydaný

9.6.2. Záruky RA

RA poskytujúca služby v mene Poskytovateľa musí poskytovať záruky v súlade s poskytovanými zárukami Poskytovateľa.

9.7. Odmietnutie záruky

Podmienky odmietnutia záruky musia byť uvedené v zmluve uzavretej so zmluvným partnerom, ktorého zamestnancom sú vydávané certifikáty resp. s držiteľom certifikátu.

9.8. Obmedzenie zodpovednosti

Žiadne požiadavky.

9.9. Náhrady

Žiadne požiadavky

9.10. Doba platnosti a jej ukončenie

9.10.1. Doba platnosti

Táto verzia CP zostáva v platnosti pokiaľ nie je nahradená novšou verziou. Nová verzia tohto dokumentu bude v plnej miere nahrádzať predchádzajúcu verziu.

9.10.2. Ukončenie doby platnosti

Pozri časť 9.10.1.

9.10.3. Následky ukončenia platnosti

Poskytovateľ je povinný uchovávať jeden exemplár z každej platnej verzie CP pre archívne účely a to buď v tlačenej alebo elektronickej forme. Pokiaľ sú dokumenty uchovávané v elektronickej forme, musí byť zachovaná ich integrita.

9.11. Notifikácia a komunikácia s držiteľmi

Poskytovateľ musí definovať spôsob komunikácie s držiteľmi ňou vydaných certifikátov resp. inými subjektmi. Spôsob komunikácie môže zahŕňať využívanie elektronicky podpísaných e-mailových správ, listovú komunikáciu, priamu komunikáciu na k tomu určených miestach.

9.12. Zmeny a prílohy CP

9.12.1. Postup zmeny dokumentácie

PMA má právo posúdiť a prípadne revidovať toto CP. Chyby, požiadavky na aktualizáciu alebo navrhované zmeny tohto CP sa majú oznámiť kontaktu uvedenému v časti 1.4. Takáto komunikácia musí obsahovať popis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje.

Po uplynutí doby určenej na posúdenie má PMA navrhovanú zmenu prijať, prijať s úpravou alebo odmietnuť.

9.12.2. Notifikácia o zmene dokumentácie

Všetky zmeny CP motivované PMA majú byť dané na vedomie subjektom, ktorých sa týkajú v perióde aspoň jedného mesiaca.

9.13. Riešenie sporov

Pre potreby interpretácie CP a zmluvy alebo riešenia sporov sa možno obrátiť na PMA. PMA rozhoduje s konečnou platnosťou v prípade akýchkoľvek sporov o interpretácii alebo použiteľnosti tohto CP a zmluvy.

Žiadnym rozhodnutím PMA nie je dotknuté právo sťažovateľa postúpiť sťažnosť nezávislému súdu.

9.14. Uplatňované právne predpisy

Pri rozhodovaní v súdnych sporoch sa uplatňuje právo Slovenskej republiky.

9.15. Súlad s platnými zákonmi

Žiadne ustanovenia

9.16. Rôzne ustanovenia

9.16.1. Rámcová dohoda

Žiadne ustanovenia.

9.16.2. Postúpenie práv

Zákazník/Držiteľ nesmie svoje práva, povinnosti ako aj pohľadávky z tejto CP, Zmluvy alebo Všeobecných podmienok postúpiť alebo previesť (ani s nimi akokoľvek inak obchodovať) tretej osobe bez písomného súhlasu Poskytovateľa.

9.16.3. Salvatórska klauzula

Pokiaľ akékoľvek ustanovenie tejto CP je alebo sa stane neplatným alebo nevymáhateľným, nespôsobí to neplatnosť alebo nevymáhateľnosť celej CP, ak je úplne oddeliteľným od ostatných ustanovení tejto CP. Poskytovateľ bezodkladne nahradí neplatné alebo nevymáhateľné ustanovenie CP novým platným a vymáhateľným ustanovením, ktorého predmet bude v najvyššej možnej miere zodpovedať predmetu pôvodného ustanovenia a zároveň bude zachovaný účel tejto CP a obsah jednotlivých ustanovení tejto CP.

9.16.4. Uplatnenie práv

V prípade, že určité právo počas trvania zmluvného vzťahu medzi zmluvnými stranami nie je uplatňované, toto právo z titulu jeho neuplatňovania nezaniká, pokiaľ nie je inde uvedené inak.

Zánikom zmluvného vzťahu medzi zmluvnými stranami nie sú zmluvné strany zbavené povinnosti plniť všetky dovtedy vzniknuté záväzky z uplatnených práv a uskutočniť všetky nevyhnutné právne úkony, ktoré neznesú odklad a ktoré sú nevyhnutne potrebné na zabránenie vzniku škody.

9.16.5. Vyššia moc

Poskytovateľ, Zákazník a Držiteľ nie sú zodpovední za omeškanie so splnením svojich záväzkov spôsobené okolnosťami vylučujúcimi zodpovednosť (vyššou mocou).

Okolnosťou vylučujúcou zodpovednosť je prekážka, ktorá nastala nezávisle na vôli povinnej strany a bráni jej v splnení jej povinnosti, ak je nemožné rozumne predpokladať, že by povinná strana túto prekážku alebo jej následky odvrátila alebo prekonala a ďalej, že by v čase vzniku prekážku predvídala, či mohla alebo mala predvídať.

Ak okolnosti vylučujúce zodpovednosť nastanú, potom je strana, u ktorej táto skutočnosť nastane, povinná bezodkladne informovať druhú stranu o povahe, začiatku a konci trvania takejto prekážky, ktorá bráni splneniu jej povinností. Poskytovateľ, Zákazník a Držiteľ sa zaväzujú vyvinúť maximálne úsilie na odvrátenie a prekonanie okolností vylučujúcich zodpovednosť.

Zodpovednosť však nie je vylúčená v prípade, keď takáto okolnosť vznikla až v čase, keď povinná strana bola v omeškaní s plnením svojej povinnosti, alebo ak predmetná strana nesplní svoju povinnosť bezodkladne informovať druhú stranu o povahe a začiatku trvania prekážky, alebo ak vznikla z jej hospodárskych pomerov. Účinky vylučujúce zodpovednosť sú obmedzené len na obdobie, kým trvá prekážka, s ktorou sú tieto účinky spojené.

9.17. Ostatné dojednania

Žiadne požiadavky