POLITIKA

poskytovania dôveryhodnej služby vyhotovovania a overovania kvalifikovaných certifikátov

Disig, a.s.

Vypracoval	Ing. Peter **Miškovič**
Dátum platnosti	1.12.2017
Verzia	5.1
Typ	POLITIKA
Schválil	Ing. **Ľuboš Batěk**

Obsah

1.	Úvod	9
1.1	Prehľad	9
1.2	Názov dokumentu a jeho identifikácia	10
1.3	Účastníci PKI	11
1.3.1	Certifikačné autority	11
1.3.2	Registračná autorita	12
1.3.3	Zákazník a Držiteľ KC	12
1.3.4	Spoliehajúca sa strana	13
1.3.5	Iní účastníci	13
1.4	Použiteľnosť KC	13
1.5	Správa politiky	14
1.5.1	Organizácia zodpovedná za správu dokumentu	14
1.5.2	Kontaktná osoba	14
1.5.3	Osoba rozhodujúca o súlade CPS s certifikačnou politikou	15
1.5.4	Postupy schvaľovania CPS a externej politiky	15
1.6	Definície a skratky	15
1.6.1	Definície	15
1.6.2	Skratky	18
2.	**Zverejňovanie** informácií a úložiská	19
2.1.1	Úložiská	19
2.2	Zverejňovanie informácií o CA	19
2.3	Frekvencia zverejňovania informácií	19
2.4	Kontroly prístupu	20
3.	Identifikácia a autentifikácia	21
3.1	Mená	21
3.1.1	Typy mien	21
3.1.2	Potreba zmysluplnosti mien	21
3.1.3	Anonymita a používanie pseudonymov	21
3.1.4	Pravidlá na interpretáciu rôznych foriem mien	22
3.1.5	Jednoznačnosť mien	22
3.1.6	Rozpoznanie, autentizácia a význam obchodných značiek	22
3.2	Počiatočné overenie identity	22
3.2.1	Preukazovanie vlastníctva súkromného kľúča	22
3.2.2	Autentizácia identity právnickej osoby	23
3.2.3	Autentizácia identity fyzickej osoby	23
3.2.4	Neoverované informácie o Držiteľovi	28

3.2.5	Overovanie oprávnení	28
3.2.6	Kritériá interoperability	28
3.3	Identifikácia a autentifikácia pri vyhotovovaní následného KC	28
3.4	Identifikácia a autentifikácia pri žiadaní o zrušenie KC	29
4.	Požiadavky na životný cyklus certifikátu	30
4.1	Žiadosť o vydanie KC	30
4.1.1	Kto môže žiadať o vydanie KC	30
4.1.2	Registračný proces a zodpovednosti	30
4.1.3	Generovanie žiadosti	31
4.2	Spracovanie žiadosti o vydanie certifikátu	33
4.2.1	Vykonanie identifikácie a autentifikácie	33
4.2.2	Schválenie alebo zamietnutie žiadosti	33
4.2.3	Čas spracovania žiadosti o KC	33
4.3	Vydanie KC	34
4.3.1	Činnosť Poskytovateľa pri vyhotovovaní KC	34
4.3.2	Informovanie Držiteľa o vydaní certifikátu	34
4.4	Prevzatie vydaného certifikátu	34
4.4.1	Spôsob prevzatia certifikátu	34
4.4.2	Zverejnenie certifikátu	34
4.4.3	Oznámenie o vydaní certifikátu iným stranám	35
4.5	Kľúčový pár a používanie certifikátu	35
4.5.1	Používanie súkromného kľúča a certifikátu Držiteľom	35
4.5.2	Používanie verejného kľúča a KC Spoliehajúcou sa stranou	36
4.6	Obnova certifikátu	36
4.7	Vydanie následného KC	36
4.7.1	Podmienky vydania následného KC	36
4.7.2	Kto môže žiadať o vydanie následného KC.	36
4.7.3	Postup žiadania o vydanie následného KC	36
4.7.4	Oznámenie o vydaní následného KC	37
4.7.5	Spôsob prevzatia následného KC	37
4.7.6	Zverejňovanie následného KC	37
4.7.7	Oznámenie o vydaní následného KC iným subjektom	37
4.8	Modifikácia KC	37
4.9	Zrušenie KC	37
4.9.1	Podmienky zrušenia KC	37
4.9.2	Kto môže žiadať o zrušenie KC	38
4.9.3	Postup žiadosti o zrušenie certifikátu	39
4.9.4	Čas na podanie žiadosti o zrušenie KC	39
4.9.5	Čas na zrušenie KC	40
4.9.6	Overovanie platnosti zo strany spoliehajúcej sa strany	40
4.9.7	Frekvencia vydávania CRL	40

4.9.8	Doba publikovania CRL	41
4.9.9	Dostupnosť služby OCSP	41
4.9.10	Požiadavky na OCSP overovanie	41
4.9.11	Iné formy dostupnosti informácií o zrušení certifikátu	41
4.9.12	Špeciálne požiadavky na zmenu kľúčov po ich kompromitácii	41
4.9.13	Okolnosti pozastavenia platnosti certifikátu	42
4.9.14	Suspendovanie certifikátu	42
4.10	Služby súvisiace so stavom certifikátu	42
4.10.1	Prevádzkové požiadavky	42
4.11	Ukončenie poskytovania služieb	42
4.12	Úschova a obnova kľúčov	42
5.	Fyzické, personálne a prevádzkové **bezpečnostné** opatrenia	43
5.1	Opatrenia týkajúce sa fyzickej bezpečnosti	43
5.1.1	Priestory	43
5.1.2	Fyzický prístup	44
5.1.3	Zásobovanie elektrickou energiou a klimatizácia	44
5.1.4	Ochrana pre vodou	44
5.1.5	Ochrana pred ohňom	44
5.1.6	Úložisko médií	44
5.1.7	Nakladanie s odpadom	44
5.1.8	Zálohovanie mimo hlavnú lokalitu	45
5.2	Procedurálne bezpečnostné opatrenia	45
5.2.1	Dôveryhodné roly	45
5.2.2	Počet osôb v jednotlivých úlohách	45
5.2.3	Identifikácia a autentizácia pre každú rolu	45
5.2.4	Roly vyžadujúce oddelenie zodpovedností	45
5.3	Personálne bezpečnostné opatrenia	45
5.3.1	Požiadavky na kvalifikáciu, skúsenosti a previerky	46
5.3.2	Požiadavky na previerky	46
5.3.3	Požiadavky na školenia	46
5.3.4	Požiadavky na frekvenciu obnovy školení	46
5.3.5	Rotácia rolí	46
5.3.6	Postihy za neoprávnenú činnosť	46
5.3.7	Požiadavky na externých dodávateľov	47
5.3.8	Dokumentácia poskytovaná zamestnancom	47
5.4	Postup získavania auditných záznamov	47
5.4.1	Typy zaznamenávaných udalostí	47
5.4.2	Frekvencia spracovávania auditných záznamov	48
5.4.3	Uchovávanie logov	48
5.4.4	Ochrana auditných záznamov	48
5.4.5	Postupy zálohovania auditných logov	48

5.4.6 Systém zálohovania logov 48
5.4.7 Notifikácia subjektu iniciujúceho log záznam 48
5.4.8 Posudzovanie zraniteľností 48
5.5 Uchovávanie záznamov 48
5.5.1 Typy archivovaných záznamov 48
5.5.2 Doba uchovávania záznamov 49
5.5.3 Ochrana archívnych záznamov 49
5.5.4 Zálohovanie archívnych záznamov 49
5.5.5 Požiadavky na pridávanie časových pečiatok k záznamom 49
5.5.6 Archivačný systém 49
5.5.7 Postup získania a overenia archívnych informácií 49
5.6 Zmena kľúčov CA 49
5.7 Obnova po kompromitácii alebo havárii 50
5.7.1 Postupy riešenia incidentov a kompromitácie 50
5.7.2 Poškodenie hardvéru, softvéru alebo údajov 50
5.7.3 Postupy pri kompromitácii kľúča CA 51
5.7.4 Zachovanie kontinuity činnosti po havárii 51
5.8 Ukončenie činnosti CA resp. RA 51

6. Technické **bezpečnostné** opatrenia 53

6.1 Generovanie a inštalácia páru kľúčov 53
6.1.1 Generovanie a inštalácia páru kľúčov pre jednotlivé subjekty 53
6.1.2 Doručenie súkromného kľúča Držiteľovi certifikátu 54
6.1.3 Doručenie verejného kľúča vydavateľovi certifikátu 54
6.1.4 Poskytovanie verejných kľúčov Poskytovateľa Spoliehajúcim sa stranám 54
6.1.5 Dĺžka kľúčového páru 54
6.1.6 Parametre a kvalita verejného kľúča 55
6.1.7 Použitie kľúčov 55
6.2 Ochrana súkromného kľúča a technické opatrenia pre kryptografický modul 55
6.2.1 Štandardy a opatrenia pre kryptografický modul 55
6.2.2 Opatrenia (K z N) pre manipuláciu so súkromným kľúčom 55
6.2.3 „Key escrow“ súkromného kľúča 55
6.2.4 Zálohovanie súkromného kľúča 55
6.2.5 Archivácia súkromného kľúča 56
6.2.6 Prenos súkromných kľúčov z a do HSM modulu 56
6.2.7 Uchovávanie súkromných kľúčov v HSM module 56
6.2.8 Spôsob aktivácie súkromných kľúčov 56
6.2.9 Spôsob deaktivácie súkromného kľúča 56
6.2.10 Spôsob zničenia súkromného kľúča 56
6.2.11 Charakteristika HSM modulu 57

6.3	Ďalšie aspekty manažmentu páru kľúčov	57
6.3.1	Archivácia verejných kľúčov	57
6.3.2	Dĺžka platnosti certifikátov a použiteľnosť kľúčového páru	57
6.4	Aktivačné údaje	57
6.4.1	Vytváranie a inštalácia aktivačných údajov	57
6.4.2	Ochrana aktivačných údajov	57
6.4.3	Ostatné aspekty aktivačných údajov	58
6.5	Riadenie bezpečnosti počítačov	58
6.5.1	Špecifické požiadavky na bezpečnosť počítačov	58
6.5.2	Hodnotenie bezpečnosti informácií	58
6.6	Opatrenia v životnom cykle	59
6.6.1	Opatrenia pri vývoji systémov	59
6.6.2	Opatrenia na riadenie bezpečnosti	59
6.6.3	Bezpečnostné opatrenia v životnom cykle	59
6.7	Sieťové bezpečnostné opatrenia	59
6.8	Využívanie časovej pečiatky	59
7.	Profily KC, CRL a OCSP	60
7.1	Profil KC	60
7.1.1	Verzia	60
7.1.2	Rozšírenia certifikátu	61
7.1.3	Identifikátory použitých algoritmov	62
7.1.4	Formy mien	62
7.1.5	Obmedzenia týkajúce sa mien	66
7.1.6	Identifikátor certifikačnej politiky	66
7.1.7	Použitie rozšírení na obmedzenie politiky	66
7.1.8	Syntax a sémantika politiky	66
7.1.9	Sémantika spracovania kritických certifikačných politík	67
7.2	Profily zoznamu zrušených certifikátov	67
7.2.1	Verzia	67
7.2.2	Použité rozšírenia (CRL extensions) v CRL	67
7.3	Profil OCSP	67
7.3.1	Verzia	67
7.3.2	OCSP rozšírenia	68
8.	Audit zhody	69
8.1	Témy pokrývané auditom zhody	69
8.2	Frekvencia auditu zhody	69
8.3	Identita audítora a kvalifikačné požiadavky kladené na túto rolu	69
8.4	Vzťah audítora k Poskytovateľovi	69
8.5	Akcie vykonané na odstránenie nedostatkov	69
8.6	Zaobchádzanie s výsledkami auditu	69

9. Iné obchodné a právne záležitosti 71

9.1 Poplatky 71
9.1.1 Poplatky za vydanie certifikátu 71
9.1.2 Poplatok za prístup k certifikátu 71
9.1.3 Poplatky za zrušenie alebo overenie statusu certifikátu 71
9.1.4 Poplatky za ostatné služby 71
9.1.5 Vrátenie poplatku 72
9.2 Finančná zodpovednosť 72
9.2.1 Poistenie 72
9.2.2 Iné aktíva 72
9.2.3 Poistenie a záruky pre koncových používateľov 72
9.3 Dôvernosť 72
9.3.1 Dôverné informácie 72
9.3.2 Dôverné informácie 72
9.3.3 Informácie nepovažované za dôverné 73
9.3.4 Zodpovednosť za ochranu dôverných informácií 73
9.4 Ochrana osobných údajov 74
9.4.1 Politika ochrany osobných údajov 74
9.4.2 Informácie považované za súkromné 74
9.4.3 Informácie, ktoré nie sú považované za súkromné 75
9.4.4 Zodpovednosť za ochranu osobných údajov 75
9.4.5 Informačná povinnosť a súhlas 75
9.5 Ochrana práv duševného vlastníctva 75
9.6 Vyhlásenie a záruky 75
9.6.1 Vyhlásenia a záruky Poskytovateľa 75
9.6.2 Vyhlásenia a záruky RA 76
9.6.3 Vyhlásenie a záruky Držiteľa 77
9.6.4 Vyhlásenia a záruky Spoliehajúcej sa strany 77
9.6.5 Vyhlásenia a záruky iných strán 78
9.7 Odmietnutie poskytnutia záruky 78
9.8 Obmedzenie zodpovednosti 78
9.9 Náhrada škody 79
9.10 Doba platnosti, ukončenie platnosti 79
9.10.1 Doba platnosti 79
9.10.2 Ukončenie platnosti 80
9.10.3 Dôsledky ukončenia platnosti 80
9.11 Jednotlivé oznámenia a komunikácia s účastníkmi 80
9.12 Zmeny 80
9.12.1 Postup vykonávania zmien 80
9.12.2 Postup a periodicita oznamovania zmien 81
9.12.3 Okolnosti zmeny OID 81
9.13 Riešenie sporov 81

9.14	Rozhodné právo	82
9.15	Súlad s platnými právnymi predpismi	82
9.16	Rôzne ustanovenia	82
9.16.1	Rámcová dohoda	82
9.16.2	Postúpenie práv	82
9.16.4	Uplatnenie práv	82
9.16.5	Vyššia moc	83
9.17	Iné ustanovenia	83
10.	Odkazy	84
11.	História zmien	85

1. Úvod

Tento dokument definuje politiku (ďalej „CP“) spoločnosti Disig, a.s., so sídlom Záhradnícka 151, 821 08 Bratislava, IČO: 35975946, zapísanú v Obchodnom registri OS BA I, odd. Sa, vložka č. 3794/B, ako poskytovateľa dôveryhodných služieb (ďalej len „Poskytovateľ“) a platí pre všetky certifikačné autority, prevádzkované Poskytovateľom, prostredníctvom ktorých poskytuje kvalifikované dôveryhodné služby definované v odstavci 1.1.

Webové sídlo Poskytovateľa k poskytovaným dôveryhodným službám je dostupné na adrese:

https://eidas.disig.sk

1.1 Prehľad

Štruktúra tejto CP je v súlade s požiadavkami RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“ [1].

Táto CP sa týka poskytovania kvalifikovaných dôveryhodných služieb vyhotovovania a overovania:

- kvalifikovaných certifikátov pre elektronický podpis
  (identifikátor politiky (QCP-n) v zmysle EN 319411-2 [2]: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)),
- kvalifikovaných certifikátov pre elektronickú **pečať**
  (identifikátor politiky (QCP-l) v zmysle [2]: itu-t(0) identified-orgdodávatanization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1),
- kvalifikovaných certifikátov pre elektronický podpis, kde súkromný **kľúč** je uložený na QSCD
  (identifikátor politiky (QCP-n-qscd) v zmysle [2]: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2))
- kvalifikovaných certifikátov pre elektronickú **pečať,** kde súkromný **kľúč** je uložený na QSCD
  (identifikátor politiky (QCP-l-qscd) v zmysle [2]: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)),
- kvalifikovaných certifikátov pre autentifikáciu webového sídla
  (identifikátor politiky (QCP-w) v zmysle [2]: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (4)),

v zmysle ustanovení Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS“) [3] a zohľadnení ustanovení kapitoly 10 aktuálnej verzie dokumentu „Certifikačná politika pre koreňovú CA a dôveryhodnú službu

vyhotovovania kvalifikovaných certifikátov, ktorej kvalifikovaný štatút udelil Národný bezpečnostný úrad“ (OID politiky: 1.3.158.36061701.0.0.0.1.2.2) [4].

Mandátny certifikát, definovaný v § 8 zákona č. 272/2016 Z. z. o dôveryhodných službách [5], je kvalifikovaný certifikát (ďalej aj „KC“) pre elektronický podpis vydávaný fyzickej osobe, kde súkromný kľúč je uložený na QSCD.

KC vo všeobecnosti zväzuje verejný kľúč vlastnený fyzickou osobou, právnickou osobou, zariadením alebo webovým sídlom so súborom informácií, ktoré identifikujú entitu spojenú s používaním zodpovedajúceho súkromného kľúča.

CP je využívaná pri implementácii infraštruktúry verejných kľúčov (ďalej len „PKI“), ktorá pozostáva z produktov a služieb, ktoré poskytujú a spravujú certifikáty podľa štandardu X.509 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile) [6].

Kvalifikované dôveryhodné služby uvedené v tejto kapitole sú poskytované nasledovnými certifikačnými autoritami Poskytovateľa:

Názov	Sériové číslo certifikátu	Vydavateľ	DigitalID v SK dôveryhodnom zozname
CA Disig	00F4	KCA NBU SR 3	FX9fXwhpKsZwA6H6UWpNrI1fmFM=
CA Disig QCA	077A	KCA NBU SR 3	9FgiC3T8jAqPjDqlhZcvhFnZHyg=

Pokiaľ sa v niektorých ustanoveniach tohto dokumentu použije skratka „KC“ potom sa tieto ustanovenia týkajú všetkých typov kvalifikovaných certifikátov vyhotovovaných Poskytovateľom.

1.2 Názov dokumentu a jeho identifikácia

Názov:	Politika poskytovania dôveryhodnej služby vyhotovovania a overovania kvalifikovaných certifikátov
Skratka názvu:	CP QTSP QC*
Verzia:	5.1
Schválené dňa:	24.11.2017
Platnosť od:	1.12.2017
Tomuto CP je priradený identifikátor objektu (OID):	1.3.158.35975946.0.0.1.0.1

* - v texte tohto dokumentu sa väčšinou používa pri odkaze len skrátená forma CP

Popis použitého identifikátora objektu (OID):

1. – ISO assigned OIDs

1.3. – ISO Identified Organization

1.3.158. – Identifikačné číslo subjektu (IČO)

1.3.158.35975946. – Disig

1.3.158.35975946.0.0.1. - CA Disig – vyhotovovanie kvalifikovaných certifikátov

1.3.158.35975946.0.0.1.0.1 – CP QTSP QC

1.3 Účastníci PKI

V rámci poskytovania dôveryhodných služieb vyhotovovania a overovania KC (ďalej len „KC služby“) sú účastníkmi infraštruktúry verejného kľúča entity uvedené tejto časti.

1.3.1 Certifikačné autority

Certifikačná autorita:

- je entita, ktorá poskytuje kvalifikované dôveryhodné služby vyhotovovania a overovania KC používateľom (Zákazníci/Držitelia, Spoliehajúce sa strany),
- má celkovú zodpovednosť za poskytovanie kvalifikovaných dôveryhodných služieb špecifikovaných v časti 1.1,
- je uvádzaná vo vydaných KC ako vydavateľ a jej súkromné kľúče sú používané pri vyhotovovaní podpisu týchto KC,
- zaručuje, že všetky aspekty jej služieb, operácií a infraštruktúry zviazanej s KC vydanými podľa tejto politiky sú vykonávané v súlade s jej požiadavkami a ustanoveniami a v súlade s pravidlami na výkon certifikačných činností Poskytovateľa.

Certifikačné autority Poskytovateľa sú súčasťou hierarchickej PKI, samotné však nemajú podriadené certifikačné autority, ale sú podriadené koreňovej certifikačnej autorite KCA NBÚ. Charakter tejto podriadenosti a spôsob jej implementácie určuje NBÚ. Poskytovateľ môže prevádzkovať v rámci podriadenosti pod koreňovou KCA NBÚ viaceré certifikačné autority poskytujúce KC služby.

1.3.2 **Registračná** autorita

Registračná autorita (ďalej len „RA“) je entita, ktorá koná, na základe zmluvy, v mene Poskytovateľa, pričom vykonáva niektoré vybrané činnosti pri poskytovaní dôveryhodných služieb Poskytovateľa.

RA musí vykonávať svoje aktivity v súlade so schválenou CP a Pravidlami na výkon certifikačných činností (ďalej aj „CPS“) v aktuálnom znení.

Poskytovateľ môže zriadiť RA nasledovných typov:

- **Komerčná** RA – je určená na sprostredkovanie vybraných kvalifikovaných dôveryhodných služieb Poskytovateľa širokej verejnosti a je prevádzkovaná treťou stranou, na základe písomnej zmluvy s Poskytovateľom.
- Firemná RA – je určená na sprostredkovanie vybraných kvalifikovaných dôveryhodných služieb výhradne pre vlastné potreby konkrétnej právnickej osoby resp. pre potreby ňou prevádzkovaných systémov vyžadujúcich použitie KC a je prevádzkovaná, na základe písomnej zmluvy s Poskytovateľom, danou konkrétnou právnickou osobou.
- Interná RA – je prevádzkovaná Poskytovateľom a je určená na poskytovanie kvalifikovaných dôveryhodných služieb pre všetkých záujemcov. Táto RA nie je samostatný právny subjekt.

Poskytovateľ v súčasnej dobe zriaďuje len RA pôsobiace na území Slovenskej republiky, ktoré sú právnym subjektom so sídlom v Slovenskej republike.

1.3.3 Zákazník a **Držiteľ** KC

Zákazníkom sa rozumie fyzická osoba resp. právnická osoba, ktorá je oprávnená žiadať o KC v mene entity, ktorej meno sa objaví ako subjekt v KC – Držiteľ KC.

Držiteľom KC môže byť:

- fyzická osoba,
- fyzická osoba identifikovaná v spojení s právnickou osobou,
- právnická osoba, ktorou môže byť organizácia alebo jej jednotka resp. oddelenie,
- zariadenie alebo systém prevádzkovaný fyzickou alebo právnickou osobou alebo prevádzkovaný v mene fyzickej resp. právnickej osoby.

Niektoré požiadavky tejto CP kladené na Zákazníka sú v prípade, že Zákazník a Držiteľ KC nie sú tá istá osoba, záväzné aj pre osobu konajúcu v mene Zákazníka (Držiteľ KC).

Podmienky, ktoré musí splniť Zákazník, definuje táto CP.

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

1.3.4 Spoliehajúca sa strana

Spoliehajúcou sa stranou je fyzická alebo právnická osoba, ktorá sa pri svojom konaní spolieha na elektronickú identifikáciu alebo dôveryhodné služby Poskytovateľa.

1.3.5 Iní **účastníci**

Autorita pre správu poriadkov (Policy Management Authority - ďalej len „PMA“) je zložka Poskytovateľa ustanovená za účelom:

- dohľadu na vytváraním a aktualizáciou CP, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien,
- revízie CPS, aby sa zaručilo, že prax Poskytovateľa vyhovuje príslušnej CP,
- revízie výsledkov auditov, aby sa určilo, či Poskytovateľ zodpovedne dodržiava ustanovenia vydaných CPS,
- vydávanie odporúčaní pre Poskytovateľa týkajúcich sa nápravných a iných vhodných opatrení,
- riadenia a usmerňovania činnosti Poskytovateľa a registračných autorít (ďalej len „RA“),
- výkladu ustanovení vydaných CPS a svojich pokynov pre Poskytovateľa a RA,
- výkonu funkcie interného audítora, pričom touto činnosťou poverí samostatného zamestnanca.

PMA predstavuje vrcholovú zložku, ktorá rozhoduje s konečnou platnosťou vo všetkých záležitostiach a aspektoch týkajúcich sa Poskytovateľa a jeho činnosti.

1.4 **Použiteľnosť** KC

KC vyhotovované v zmysle tejto CP sú vyhotovované na účely identifikáciu držiteľa verejného kľúča (pozri bod 1.3.3).

KC vyhotovený pre fyzickú osobu (identifikátor politiky QCP-n) je vyhotovený za účelom podpory zdokonaleného elektronického podpisu v zmysle článkov 26 a 27 Nariadenia eIDAS [3].

KC vyhotovený pre právnickú osobu (identifikátor politiky QCP-l) je vyhotovený za účelom podpory zdokonalenej elektronickej pečate v zmysle článkov 36 a 37 Nariadenia eIDAS [3].

KC vyhotovený pre fyzickú osobu, kde súkromný kľúč sa nachádza v QSCD (identifikátor politiky QCP-n-qscd), je vyhotovený za účelom podpory kvalifikovaného elektronického podpisu v zmysle článku 3 bod 12 Nariadenia eIDAS [3].

KC vyhotovený pre právnickú osobu, kde súkromný kľúč sa nachádza v QSCD (identifikátor politiky QCP-l-qscd), je vyhotovený za účelom podpory kvalifikovanej elektronickej pečate v zmysle článku 3 bod 27 Nariadenia eIDAS [3].

KC vyhotovený pre autentifikáciu webového sídla (identifikátor politiky QCP-w) je vyhotovený za účelom podpory autentifikácie webového sídla v zmysle článku 3 bod 38 a článku 45 Nariadenia eIDAS [3].

1.5 Správa politiky

1.5.1 Organizácia zodpovedná za správu dokumentu

Tabuľka č. 1 obsahuje údaje Poskytovateľa, ktorý je zodpovedný za prípravu, vytvorenie a udržiavanie tohto dokumentu.

Tabuľka č. 1: Kontaktné údaje **Poskytovateľa**

Poskytovateľ	
spoločnosť:	Disig, a.s.
adresa:	Záhradnícka 151, 821 08 Bratislava 2
IČO:	359 75 946
telefón	+421 2 20850140
e-mail:	disig@disig.sk
webové sídlo:	http://www.disig.sk

1.5.2 Kontaktná osoba

Na účel tvorby politík má Poskytovateľ vytvorenú autoritu pre správu politík (PMA) (pozri bod 1.3.5), ktorá plne zodpovedá za jej obsah, a ktorá je pripravená odpovedať na všetky otázky týkajúce sa politík Poskytovateľa.

Tabuľka č. 2 obsahuje kontaktné údaje na zložku zodpovednú za prevádzku certifikačných autorít Poskytovateľa.

Tabuľka č. 2: Kontaktné údaje CA Disig

Certifikačná autorita CA Disig	
adresa:	Záhradnícka 151, 821 08 Bratislava 2
e-mail:	spravaca@disig.sk
telefón	+421 2 20850140
webové sídlo:	http://eidas.disig.sk

1.5.3 Osoba rozhodujúca o súlade CPS s **certifikačnou** politikou

Osobou, ktorá je zodpovedná za rozhodovanie o súlade postupov Poskytovateľa, ktoré sú uvedené v pravidlách na výkon certifikačných činností (CPS) s touto politikou je PMA (pozri bod 1.3.5).

1.5.4 Postupy **schvaľovania** CPS a externej politiky

Ešte pred začiatkom prevádzky má mať Poskytovateľ schválený svoj CP a CPS a musí spĺňať všetky jeho požiadavky. Obsah CP a CPS schvaľuje osoba menovaná do role PMA.

Po schválení zo strany PMA je príslušný dokument publikovaný v súlade s publikačnou a oznamovacou politikou.

PMA má informovať o svojich rozhodnutiach takým spôsobom, aby boli tieto informácie dobre prístupné stranám spoliehajúcim sa na KC.

1.6 Definície a skratky

1.6.1 Definície

Certifikát – elektronický dokument, ktorým vydavateľ certifikátu (certifikačná autorita) potvrdzuje, že v certifikáte uvedený verejný kľúč patrí Držiteľovi, ktorému je certifikát vydaný;

Dôveryhodná služba - elektronická služba, ktorá sa spravidla poskytuje za odplatu a spočíva:

a) vo vyhotovovaní, overovaní a validácii elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo

b) vo vyhotovovaní, overovaní a validácii certifikátov pre autentifikáciu webových sídiel, alebo

c) v uchovávaní elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia;

Držiteľ – entita identifikovaná v certifikáte ako Držiteľ súkromného kľúča prislúchajúceho k verejnému kľúču obsiahnutému v certifikáte;

Elektronický podpis - údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie;

Elektronická **pečať** - údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme s cieľom zabezpečiť pôvod a integritu týchto pridružených údajov;

Hashovacia funkcia (hash, message digest, fingerprint) – rýchlo spočítateľná funkcia, ktorá dostane na vstupe dokument ľubovoľnej dĺžky a zostrojí z neho pomerne krátku (napr. 256 bitov) charakteristiku, nazývanú hashovacia hodnota (tiež hašovacia hodnota, hash). Medzi v kryptografii najpoužívanejšie hašovacie funkcie v súčasnosti patria SHA1 a SHA2 (SHA224, SHA256, SHA384; SHA512);

Kľúčový pár – súčasť PKI systému, ktorá využíva asymetrickú kryptografiu a pozostávajúca z verejného a k nemu prislúchajúceho súkromného kľúča;

Kvalifikovaná dôveryhodná služba - je dôveryhodná služba, ktorá spĺňa uplatniteľné požiadavky stanovené v Nariadení eIDAS [3];

Kvalifikovaná elektronická pečať - je zdokonalená elektronická pečať vyhotovená pomocou kvalifikovaného zariadenia na vyhotovenie elektronickej pečate a založená na kvalifikovanom certifikáte pre elektronickú pečať;

Kvalifikované zariadenie na vyhotovenie elektronického podpisu - zariadenie na vyhotovenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílohe II Nariadenia eIDAS [3];

Kvalifikované zariadenie na vyhotovenie elektronickej **pečate** - zariadenie na vyhotovenie elektronickej pečate, ktoré primerane spĺňa požiadavky stanovené v prílohe II Nariadenia eIDAS [3];

Kvalifikované zariadenie – spoločné označenie pre kvalifikované zariadenie na vyhotovovanie elektronického podpisu a kvalifikované zariadenie na vyhotovovanie elektronickej pečate;

Kvalifikovaný certifikát pre elektronický podpis – je certifikát pre elektronický podpis, ktorý vyhotovuje kvalifikovaný poskytovateľ dôveryhodných služieb a ktorý spĺňa požiadavky stanovené v prílohe I Nariadenia eIDAS [3];

Kvalifikovaný elektronický podpis - je zdokonalený elektronický podpis vyhotovený s použitím kvalifikovaného zariadenia na vyhotovenie elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy;

Kvalifikovaný **poskytovateľ** dôveryhodných služieb - je poskytovateľ dôveryhodných služieb, ktorý poskytuje jednu alebo viacero kvalifikovaných dôveryhodných služieb a ktorému orgán dohľadu udelil kvalifikovaný štatút;

Mandátny certifikát - je kvalifikovaný certifikát pre elektronický podpis vydaný fyzickej osobe, oprávnenej zo zákona alebo na základe zákona konať za inú osobu alebo orgán verejnej moci alebo v ich mene, alebo fyzickej osobe, ktorá vykonáva činnosť podľa osobitného predpisu, alebo vykonáva funkciu podľa osobitného predpisu a obsahuje údaje uvedené v §8 zákona č. 272/2016 Z. z. [5];

Poskytovateľ dôveryhodných služieb - fyzická alebo právnická osoba poskytujúca jednu alebo viacero dôveryhodných služieb buď ako kvalifikovaný alebo nekvalifikovaný poskytovateľ dôveryhodných služieb;

Pracovník RA – zamestnanec Poskytovateľa alebo inej právnickej osoby, ktorá má s Poskytovateľom uzavretú zmluvu o poskytovaní certifikačných služieb;

Pravidlá na výkon **certifikačných činností** – postupy, ktoré Poskytovateľ používa pri vyhotovovaní certifikátov;

RFC - Postup vytvárania štandardu na Internete a zároveň označenie takto vzniknutého štandardu;

Spoliehajúca sa strana – fyzická osoba alebo právnická osoba, ktorá sa pri svojom konaní spolieha na dôveryhodné služby Poskytovateľa;

Vlastná CA – časť infraštruktúry poskytovateľa dôveryhodných služieb (obsahujúca napr. HSM modul), ktorá spolu s registračnou autoritou vyhotovuje certifikáty.

Zdokonalený elektronický podpis – je elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26 Nariadenia eIDAS [3];

Zákazník – fyzická osoba resp. právnická osoba, ktorá je oprávnená žiadať o certifikát v mene entity, ktorej meno sa objaví ako subjekt v certifikáte – Držiteľ certifikátu;

X.509 – medzinárodný štandard, ktorý okrem iného definuje aj formát certifikátu verejného kľúča.

1.6.2 Skratky

CA	-	Certifikačná autorita (Certification Authority)
CP	-	Certifikačná politika (Certification Policy)
CPS	-	Pravidlá na výkon certifikačných činnosti (Certificate Practice Statement)
CRL	-	Zoznam zrušených certifikátov (Certificate Revocation List)
HSM	-	Kvalifikované zariadenie na vyhotovenie elektronického podpisu alebo vyhotovenie elektronickej pečate; kryptografický modul, hardvérový bezpečnostný modul (Hardware Security Modul)
HW	-	Hardvér (Hardware)
KC	-	Kvalifikovaný certifikát
NBÚ	-	Národný bezpečnostný úrad
OCSP	-	Protokol určený spoliehajúcim sa stranám na potvrdenie existencie a platnosti certifikátu (OCSP – Online Certificate Status Protocol)
PKCS	-	Séria štandardov určená pre kryptografiu verejných kľúčov (Public Key Cryptography Standard)
PKI	-	Infraštruktúra verejných kľúčov (Public Key Infrastructure)
PMA	-	Autorita na správu CP (Policy Management Authority)
QSCD		Kvalifikované zariadenie určené na generovanie a uloženie páru kľúčov (súkromný, verejný) a na vyhotovovanie elektronického podpisu/pečate (Qualified electronic Signature/Seal Creation Device)
RA	-	Registračná autorita (Registration Authority)
RFC	-	Žiadosť o vyjadrenie (Request For Comment)
URL	-	Internetový ekvivalent pre web adresu (Uniform Resource Locator)

2. **Zverejňovanie** informácií a úložiská

2.1.1 Úložiská

Úložiská musia byť umiestnené tak, aby boli prístupné Držiteľom KC a Spoliehajúcim sa stranám a v súlade s celkovými bezpečnostnými požiadavkami.

Funkciu úložiska Poskytovateľa bude zastávať jeho webové sídlo. Presná URL adresa je uvedené v kapitole 1. Webové sídlo Poskytovateľa je prostredníctvom internetu verejne prístupné Držiteľom KC, Spoliehajúcim sa stranám a verejnosti vôbec.

Verejne dostupné informácie uvedené na webovom sídle Poskytovateľa majú charakter riadeného prístupu.

2.2 **Zverejňovanie** informácií o CA

Poskytovateľ musí zverejňovať, v on-line režime, úložisko, ktoré je prístupné Zákazníkom, Držiteľom KC a Spoliehajúcim sa stranám, ktoré bude obsahovať minimálne tieto informácie:

- informáciu o KC, ktoré vydal Poskytovateľ v zmysle tejto CP,
- aktuálne CRL ako aj všetky CRL vydané od začiatku činnosti vyhotovovania KC,
- vlastné certifikáty certifikačných autorít Poskytovateľa, ktoré patria k jej verejným kľúčom, ktorých zodpovedajúci súkromný kľúč je využívaný pri podpisovaní vyhotovovaných KC a CRL

Poskytovateľ musí zverejňovať v on-line režime prostredníctvom svojho webového sídla túto CP ako aj ďalšie dokumenty súvisiace s poskytovaním dôveryhodných služieb v zmysle tejto CP.

2.3 Frekvencia **zverejňovania** informácií

Informácia o vydanom KC sa musí publikovať čo najskôr po jeho vyhotovení.

Zoznam zrušených certifikátov (CRL) musí byť publikovaný ako je špecifikované v kapitole 4.9.7. Informácie o zrušenom KC musia byť dostupné na webovom sídle Poskytovateľa (pozri kapitola 1), ktorý slúži ako jeho úložisko.

Certifikačná politika a pravidlá na výkon certifikačných činností prípadne ich revízie sa musia zverejniť čo najskôr po ich schválení a vydaní.

Všetky ďalšie informácie, ktoré majú byť publikované v úložisku, sa musia publikovať podľa možnosti čo najskôr.

2.4 Kontroly prístupu

Poskytovateľ musí chrániť ľubovoľnú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozšírenie. Poskytovateľ musí vynaložiť maximálne úsilie na to, aby zaistil integritu, dôvernosť a dostupnosť dát vyplývajúcich s poskytovaných dôveryhodných služieb. Taktiež musí vykonať logické a bezpečnostné opatrenia, aby zabránil neautorizovanému prístupu k úložisku osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v úložisku.

3. Identifikácia a autentifikácia

3.1 Mená

3.1.1 Typy mien

Každá CA má byť schopná vytvárať certifikáty, ktoré obsahujú rozlišovacie mená v zmysle X.500 (X.500 Distinguished Name, ďalej ako „rozlišovacie meno“) [7], konkrétne v súlade s X.501 [8] resp. X.520 [9] a aj mená v zmysle RFC5322 Internet Message Format [10].

Zákazníci si musia zvoliť sami rozlišovacie meno, ktoré má byť uvedené v ich KC.

3.1.2 Potreba zmysluplnosti mien

Pojem **„zmysluplnosť“** znamená, že forma mena má bežne používaný tvar na určenie identity Držiteľa (fyzickej osoby, právnickej osoby, orgánu verejnej moci, webového sídla)

Používané mená musia spoľahlivo identifikovať osoby, ktorým sú priradené.

3.1.3 Anonymita a používanie pseudonymov

Namiesto mena a priezviska je možné použiť v prípade KC pre elektronický podpis vyhotovovaný pre fyzickú osobu aj pseudonym, avšak v tomto prípade poslednou časťou hodnoty tejto položky bezpodmienečne musí byť reťazec PSEUDONYM, aby bolo jednoznačné a jasné, že namiesto mena a priezviska je uvedený pseudonym a tak, aby strana spoliehajúca sa na KC nemohla byť použitím pseudonymu uvedená do omylu. Týmto nie sú dotknuté ustanovenia týkajúce sa jednoznačnej identifikácie Držiteľa takto vydaného KC.

Pseudonym nemusí byť zmysluplný, avšak Poskytovateľ má právo zamietnuť žiadosť obsahujúcu pseudonym, ktorý je z etického, rasového, náboženského alebo iného dôvodu nevhodný. Pseudonym tiež nesmie obsahovať výraz, ktorým by mohli byť poškodené práva iného subjektu (napr. neoprávnené použitie registrovanej obchodnej značky ako pseudonymu).

V zmysle ustanovení § 8 ods. 5 zákona č. 272/2013 Z. z. [5] mandátny certifikát nesmie obsahovať pseudonym.

Poskytovateľ nesmie vydať KC pre anonymného Držiteľa.

3.1.4 Pravidlá na interpretáciu rôznych foriem mien

Interpretácia jednotlivých foriem mien v KC vyhotovovaných Poskytovateľom musí byť v súlade s profilmi KC, ktoré sú popísané v kapitole 7 tejto CP.

3.1.5 **Jednoznačnosť** mien

Poskytovateľa zodpovedá za jednoznačnosť mien v rámci celej komunity Držiteľov KC.

3.1.6 Rozpoznanie, autentizácia a význam obchodných **značiek**

Poskytovateľ negarantuje žiadnej entite, že jej meno v KC bude obsahovať jej obchodnú značku (trademark) a to ani na jej výslovnú žiadosť.

V KC môžu byť použité len tie obchodné značky, ktorých vlastníctvo alebo prenájom Zákazník uspokojivo doložil. Žiadnu inú autentizáciu obchodných značiek Poskytovateľa nevykonáva

Poskytovateľ nesmie vedome vydať KC obsahujúci meno, o ktorom kompetentný súd rozhodol, že porušuje obchodnú značku iného. Poskytovateľ nemá povinnosť skúmať obchodné značky ani riešiť spory týkajúce sa obchodných značiek.

3.2 **Počiatočné** overenie identity

Táto časť obsahuje popis postupov identifikácie a autentifikácie týkajúcich sa jednotlivých subjektov (Zákazník, Držiteľ, CA, RA alebo iný účastník).

3.2.1 Preukazovanie vlastníctva súkromného **kľúča**

Kľúčový pár, na ktorý sa vyhotovuje KC pre elektronický podpis určený na vyhotovovanie kvalifikovaného elektronického podpisu resp. KC pre elektronickú pečať určený na vyhotovovanie kvalifikovanej elektronickej pečate musia byť generované priamo v kvalifikovanom zariadení na vyhotovenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílohe II Nariadenia eIDAS [3] (ďalej len „QSCD“).

Všetky žiadosti o KC, kde kľúčový pár nie je uložený v QSCD musia byť vo formáte PKCS#10, čo znamená, že žiadosť o KC bude podpísaná súkromným kľúčom patriacim k verejnému kľúču nachádzajúcemu sa v danej žiadosti o KC.

Žiadna zložka Poskytovateľa v nijakom prípade nearchivuje žiadne súkromné kľúče patriace Držiteľovi KC, ktorý vydala.

3.2.2 Autentizácia identity právnickej osoby

Právnická osoba so sídlom v Slovenskej republike musí preukázať svoju totožnosť výpisom z obchodného registra príp. iného platného registra právnických osôb. Zo strany Poskytovateľa musí byť vyžadovaný 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 musí overiť 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).

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, zriaďovacou listinou ap.

V prípade vyhotovovania KC musí právnická osoba preukázať pravdivosť identifikačného údaja uvedeného v elektronickej žiadosti o KC predložením k nahliadnutiu originálneho dokumentu preukazujúceho túto skutočnosť.

Overenie identity právnickej osoby môže byť, okrem spôsobu uvedeného vyššie, vykonané aj na diaľku, prostredníctvom certifikátu pre kvalifikovanú elektronickú pečať, ktorý bol vydaný v súlade s písmenom a) resp. b) článku 24 Nariadenia eIDAS [3].

3.2.3 Autentizácia identity fyzickej osoby

Poskytovateľ musí garantovať, že identita Držiteľa KC a jeho verejný kľúč sú zodpovedajúco previazané.

Poskytovateľ musí špecifikovať vo vydaných CPS postupy na autentizáciu identity Držiteľa KC. Poskytovateľ musí zaznamenávať tento proces pre každý KC. Dokumentácia o identifikácii musí minimálne obsahovať:

- identitu osoby, ktorá vykonáva identifikáciu,
- jednoznačné identifikačné údaje z dokladov preukazujúcich identitu autentizovanej osoby,
- dátum vykonania identifikácie.

Overenie identity musí vykonať CMA na základe dokladu, ktorý obsahujú tieto údaje Zákazníka/Držiteľa:

- celé meno a priezvisko,
- rodné číslo (osoby, ktoré ho majú pridelené),
- dátum narodenia (osoby, ktoré nemajú pridelené rodné číslo).

Zákazník/Držiteľ musí zároveň poskytnúť ešte jeden doklad, ktorý obsahuje minimálne meno a priezvisko Držiteľa a ďalší jeho osobný údaj (dátum narodenia, rodné číslo, adresu trvalého bydliska). Toto neplatí v prípade, ak ide o služobný preukaz, ale v tomto prípade ako prvý doklad totožnosti nemôže byť akceptovaný pas, keďže neobsahuje adresu trvalého bydliska Držiteľa.

Poskytovateľ musí zaznamenať aj tieto údaje z dokladov:

- číslo preukazu totožnosti,
- vydavateľa preukazu totožnosti,
- dátum platnosti preukazu totožnosti, ak je vyznačený.

Poskytovateľ musí akceptovať pri overovaní identity Držiteľa nasledovné doklady:

- občiansky preukaz,
- cestovný pas,
- vodičský preukaz,
- rodný list,
- zbrojný preukaz,
- služobný preukaz,
- preukaz poistenca verejného zdravotného poistenia.

V prípade rodného listu, zbrojného preukazu, služobného preukazu alebo preukazu poistenca verejného zdravotného poistenia sa musí poskytnúť aj jeden z týchto dokladov: občiansky preukaz, cestovný pas.

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

Súčasťou autentizácie Držiteľa KC je povinné poskytnutie zvolenej e-mailovej adresy, ktorá sa uloží spolu s jeho osobnými údajmi v IS Poskytovateľa, a ktorá bude slúžiť vyslovene na komunikáciu medzi Poskytovateľom a Držiteľom KC a nebude súčasťou vydaného KC. Poskytovateľ nebude vykonávať overenie, či uvedená e-mail adresa skutočne patrí Zákazníkovi/Držiteľovi.

Overenie identity fyzickej osoby môže byť, okrem spôsobu uvedeného vyššie, vykonané aj na diaľku, prostredníctvom certifikátu pre kvalifikovaný elektronický podpis, vydaného v súlade s písmenom a) resp. b) článku 24 Nariadenia eIDAS [3].

3.2.3.1. Autentizácia identity zariadenia alebo systému

Poskytovateľ musí garantovať aj v prípade, že KC je vyhotovovaný za účelom autentifikácie webového sídla, že identita webového sídla a jeho verejný kľúč sú zodpovedajúco previazané.

Z uvedeného dôvodu musí byť KC webového sídla priradený fyzickej osobe konajúcej v mene právnickej osoby (organizácie), ktorá má preukázateľnú kontrolu nad webovým sídlom, na ktoré je KC vyhotovený.

Táto fyzická osoba je povinná poskytnúť Poskytovateľovi tieto informácie:

- identifikáciu zariadenia/systému,
- verejné kľúče zariadenia/systému (obsiahnuté v žiadosti o KC),
- autorizáciu zariadenia/systému a jeho atribúty (ak nejaké majú byť uvedené v KC),
- kontaktné údaje, aby Poskytovateľ mohol v prípade potreby komunikovať s touto osobou,

Poskytovateľ musí autentizovať správnosť ľubovoľnej autorizácie (hodnoty položky rozlišovacieho mena), ktorá má byť uvedená v KC a bude overovať predložené údaje.

Metódy na vykonanie tejto autentizácie a kontroly údajov zahrňujú:

- overenie identity fyzickej osoby v súlade s požiadavkami bodu 3.2.3,
- overenie identity právnickej osoby, ktorej patrí daný komponent, v súlade s požiadavkami bodu 3.2.2,
- overenie oprávnenosti použitia údajov, ktoré majú byť uvedené v jednotlivých položkách KC, s dôrazom na obsah položky commonName.

> Poznámka: Typickou hodnotou tejto položky je presne stanovené meno domény (FQDN).

V prípade použitia doménového mena je podmienkou, aby príslušná doména druhej a vyššej úrovne bola pod kontrolou Zákazníka, ktorý žiada o vydanie KC pre autentifikáciu webového sídla.

Overenie toho, že Zákazník je vlastníkom domény resp. má kontrolu nad danou doménou, ktorej FQDN sa nachádza v položke CN žiadosti resp. bude uvedené v položke Subject Alternative Name (SAN), sa musí vykonať jedným z nasledovných spôsobov:

- Spoľahnutím sa na potvrdenie od oprávneného orgánu Zákazníka vo forme prehlásenia o vlastníctve domény. Prehlásenie o vlastníctve domény musí

jasne preukazovať, že pochádza od Oprávneného kontaktu domény Poskytovateľ musí overiť, že potvrdenie o vlastníctve domény:

- obsahuje dátum, ktorý je totožný alebo neskorší ako dátum kedy bola žiadosť podaná,
- údaje vo WHOIS databáze sa nezmenili pri porovnaní s údajmi, ktoré boli predložené v prehlásení o vlastníctve domény pri predchádzajúcom vyhotovovaní KC pre dané FQDN.

- Publikovaním informácie na overenie v dohodnutom adresári „/.well-known/pki-validation/“ na doméne, pre ktorú je žiadaný KC, kde informácia bude dostupná prostredníctvom HTTP/HTTPS protokolu na ich vyhradených portoch (80/443) v podobe súboru, ktorý bude obsahovať zaslanú informáciu na overenie resp. umiestnením obsahu s informáciou na overenie na predmetnom webovom sídle vo forme meta tag v index súbore hlavnej stránky.

Pokiaľ ani jednou z popísaných metód nebude možné spoľahlivo zistiť, že Zákazník danú doménu pod oprávnenou kontrolou, Poskytovateľ musí odmietnuť vydanie KC na danú žiadosť.

Rovnaké pravidlá overovania platia aj pre „wildcard“ KC, ktoré obsahujú znak hviezdička (*) na tretej a vyššej pozícii úrovne domény.

CMA musí zabezpečiť dôslednú kontrolu položky KC subject:organizationUnitName (OU), tak aby táto neobsahovala názov právnickej osoby, obchodné meno, obchodnú značku, adresu, lokalitu, alebo iný text poukazujúc na určiteľnú fyzickú alebo právnickú osobu, bez toho aby si tieto informácie hodnoverne neoverila.

3.2.3.2. Preukazovanie oprávnenia alebo postavenia

Pokiaľ je vyhotovovaný mandátny certifikát (§8 zákona č. 272/2016 Z. z.) a týka sa konania za inú osobu alebo orgán verejnej moci, musí Zákazník predložiť oprávnenie na konanie v mene zastupovanej osoby vo forme:

- dokladu preukazujúceho, že daná osoba je štatutárnym orgánom danej právnickej osoby alebo orgánu verejnej moci,
- poverenia, ak je daná fyzická osoba zamestnancom právnickej osoby, v mene ktorej koná a je s ňou v pracovnoprávnou vzťahu alebo obdobnom pracovnom vzťahu,
- notárom overenej plnej moci, ak daná fyzická osoba nie je s danou osobou v pracovnoprávnom vzťahu alebo obdobnom pracovnom vzťahu,

Pokiaľ je vyhotovovaný mandátny certifikát (§8 zákona č. 272/2016 Z. z.) a týka sa vykonávania činnosti alebo vykonávania funkcie, musí Zákazník hodnoverným spôsobom preukázať, že je orgánom verejnej moci, že vykonáva činnosť alebo funkciu podľa požiadaviek zákon č. 272/2016 Z. z. a v zmysle požiadaviek

uvedených v zozname oprávnení, pre dané oprávnenie, ktoré je zverejnené na webovom sídle NBÚ.

Poskytovateľ a jej externé registračné autority majú právo, overiť si platnosť údajov z predloženého dokumentu pomocou iných verejne dostupných zdrojov napr. notárska komora, komora exekútorov, zoznam znalcov, tlmočníkov a prekladateľov ap.

3.2.3.3. Predkladané doklady

Všetky doklady poskytované RA Zákazníkmi musia byť buď originály, alebo úradne overené kópie originálov. Nesmie v nich byť žiaden údaj doplňovaný, pozmeňovaný, prečiarknutý a podobne. Doklady, na ktorých je vyznačená doba ich platnosti, musia byť platné.

Poskytovateľ musí akceptovať aj dokumenty poskytované Zákazníkom v elektronickej podobe podpísané platným kvalifikovaným elektronickým podpisom (výpis s obchodného registra, plná moc, prehlásenie, poverenie ap.)

Na podnet Zákazníka alebo Poskytovateľa sa prípadné sporné prípady pri preukazovaní totožnosti riešia postupom podľa odstavca 9.13

3.2.3.4. Kontrola údajov na dokladoch

Na dokladoch sa musia kontrolovať najmä skutočnosti uvedené ďalej.

Osobné doklady fyzickej osoby:

- platnosť dokladu,
- súlad medzi fotografiou v osobnom doklade a vzhľadom majiteľa osobného dokladu,
- zhodnosť dokladov, t. j. či údaje na jednom doklade neodporujú údajom na inom doklade.

Výpisy z obchodného registra:

- platnosť výpisu, výpis nesmie byť starší ako 3 mesiace,
- oprávnenie fyzickej osoby (stačí jedna fyzická osoba, ak na výpise nie je uvedené inak), ktorá poskytla výpis, konať (podpisovať) za danú právnickú osobu t. j. či sú jej štatutárnymi zástupcami,
- overenie výpisu, výpis musí byť úradne overený (notárom alebo matrikou), ak nejde o originál.

Plné moci:

- overenie plnej moci, plná moc musí byť úradne overené (notárom alebo matrikou),

- údaje, uvedené v plnej moci, ktoré identifikujú zastupujúcu fyzickú resp. právnickú osobu sa musia zhodovať s údajmi uvedenými na osobných dokladoch zastupujúcej fyzickej osoby resp. s údajmi uvedenými na výpise z obchodného registra zastupujúcej právnickej osoby,
- rozsah plnej moci - t. j. či plná moc oprávňuje splnomocnenú fyzickú alebo právnickú osobu na požadovaný úkon u Poskytovateľa v mene splnomocňujúcej fyzickej alebo právnickej osoby,
- časové obmedzenie plnej moci ak existuje alebo ak obsahuje inú podmienku, či je táto splnená.

Vymenovacie dekréty, preukazy ap.,

- zhodu osobných údajov na predloženom dokumente s údajmi na identifikačných dokladoch
- zhodu postavenia, ktoré má byť uvedené v KC, s postavením v predloženom dokumente
- platnosť predloženého dokumentu, pokiaľ ju má vyznačenú

Elektronický dokument podpísaný kvalifikovaných elektronickým podpisom

- platnosť kvalifikovaného elektronického podpisu
- identitu podpisovateľa (splnomocniteľ, obchodný register, štatutár ap.)

3.2.4 Neoverované informácie o **Držiteľovi**

V priebehu prvotného vydania KC nie sú overované informácie nachádzajúce sa v žiadosti, ktoré sa týkajú položky pseudonym a organizationUnitName a u KC, ktoré neobsahujú rozšírenie emailProtection sa neoveruje e-mail adresa uvedená v elektronickej žiadosti.

3.2.5 Overovanie oprávnení

Pozri bod 3.2.5

3.2.6 Kritériá interoperability

Poskytovateľ neuplatňuje žiadne kritériá interoperability.

3.3 Identifikácia a autentifikácia pri vyhotovovaní následného KC

Vydanie následného KC znamená zmenu páru kľúčov KC – vytvorí sa nový KC, ktorý bude mať zhodné rozlišovacie meno ako pôvodný, ale nový KC bude mať odlišný

verejný kľúč (zodpovedajúci novému, odlišnému súkromné kľúču), odlišné sériové číslo (Serial Number) a môže mať zmenenú dĺžku platnosti.

Zákazník žiadajúci o následný KC sa musí podrobiť požiadavkám kladeným na prvotnú registráciu (hlavne autentizácii jeho identity). Držiteľ platného KC môže požiadať o vydanie následného KC počas posledných 30 dní platnosti svojho KC.

Po zrušení KC sa musí Držiteľ pri vyhotovovaní následného KC podrobiť požiadavkám identifikácie kladeným na prvotnú registráciu.

3.4 Identifikácia a autentifikácia pri žiadaní o zrušenie KC

Žiadosť o zrušenie KC musí byť autentizovaná, pozri odstavec 4.9.

Žiadosť o zrušenie KC môže byť autentizovaná použitím súkromného kľúča patriaceho ku KC, ktorý sa má zrušiť, bez ohľadu na to, či daný súkromný kľúč bol alebo nebol kompromitovaný.

4. Požiadavky na životný cyklus certifikátu

4.1 **Žiadosť** o vydanie KC

4.1.1 Kto môže **žiadať** o vydanie KC

Poskytovateľa môže požiadať o vydanie:

- KC pre elektronický podpis
  - fyzická osoba resp. fyzická osoba splnomocnená Držiteľom alebo konajúca na základe zákona alebo rozhodnutia príslušného orgánu
  - akákoľvek entita, s ktorou je fyzická osoba spojená napr. jej zamestnávateľ, nezisková organizácia, ktorej je členom ap.
- KC pre elektronickú pečať
  - akákoľvek entita, ktorá v zmysle platnej národnej legislatívy koná v mene danej právnickej osoby,
- KC pre autentifikáciu webového sídla
  - fyzická alebo právnická osoba prevádzkujúca zariadenie resp. systém
  - akákoľvek entita, ktorá v zmysle platnej národnej legislatívy koná v mene danej právnickej osoby,
- mandátny certifikát
  - fyzická osoba oprávnenej zo zákona alebo na základe zákona konať za inú osobu alebo orgán verejnej moci alebo v ich mene resp. alebo fyzickej osobe, ktorá vykonáva činnosť podľa osobitného predpisu (§8 ods. 1 zákona č. 272/2016 Z. z.) alebo vykonáva funkciu podľa osobitného predpisu (§8 ods. 1 zákona č. 272/2016 Z. z.).

4.1.2 **Registračný** proces a zodpovednosti

4.1.2.1. Príprava

Zákazník musí vykonať nasledovné kroky ako prípravu na návštevu Poskytovateľa:

- oboznámiť sa so Všeobecnými podmienkami poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov Disig a.s. (ďalej len „Všeobecné podmienky“) [11], ktoré musia byť v čitateľnej podobe dostupné prostredníctvo trvalého komunikačného kanálu (pozri kapitola 1),
- oboznámiť sa s týmto postupom, prípadne s princípmi a návodmi na získanie KC,

- pripraviť si hodnoty jednotlivých položiek žiadosti o KC tak, aby tieto hodnoty boli v súlade s touto CP,
- v prípade KC pre elektronický podpis, kde kľúče nebudú generované priamo v QSCD u poskytovateľa dôveryhodnej služby, si musí vygenerovať kryptografické kľúče a pripraviť elektronickú žiadosť o vydanie KC vo formáte PKCS#10,
- v prípade KC pre elektronickú pečať, kde kľúče nebudú generované priamo v QSCD u poskytovateľa dôveryhodnej služby, si musí vygenerovať kryptografické kľúče a pripraviť elektronickú žiadosť o vydanie certifikátu vo formáte PKCS#10,
- v prípade KC pre elektronickú pečať, kde kľúče budú generované priamo v QSCD (napr. HSM modul), kde QSCD nie je pod priamou kontrolou Zákazníka, pripraviť si žiadosť o vydanie certifikátu vo formáte PKCS#10, ktorú mu poskytne kvalifikovaný poskytovateľ dôveryhodnej služby, u ktorého sa dané QSCD nachádza,
- v prípade KC pre autentifikáciu webového sídla, vygenerovať si kryptografické kľúče a pripraviť elektronickú žiadosť o vydanie certifikátu vo formáte PKCS#10,
- pripraviť si zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra.
- pripraviť si, v prípade mandátneho certifikátu vyhotovovaného podľa §8 zákona č. 272/2016 Z. z., oprávnenie na konanie v mene zastupovanej osoby (prehlásenie, poverenie resp. notárom overenú plnú moc resp. dokumenty preukazujúce jeho funkciu alebo vykonávanú činnosť alebo, že je orgánom verejnej moci), tak ako sú uvedené v zozname oprávnení publikovanom na webovom sídle NBÚ.
- dohodnúť si termín návštevy.

4.1.2.2. Postup pred vydaním KC

Pred vydaním KC zamestnanec zastupujúci Poskytovateľa musí:

- informovať prítomnú fyzickú osobu o Všeobecných podmienkach,
- overiť totožnosť Zákazníka/Držiteľa prípadne osoby, ktorá ho zastupuje podľa predložených dokladov a zaznamenať všetky povinné osobné údaje do IS Poskytovateľa,
- overiť ďalšie predložené doklady podľa stanovených postupov.

4.1.3 Generovanie žiadosti

V prípade KC pre elektronický podpis, kde kryptografické kľúče sú generované v QSCD musí po overení totožnosti vygenerovať kľúčový pár v QSCD Zákazníka

a vytvoriť elektronická žiadosť o KC vo formáte PKCS#10. Obsah položiek žiadosti a povinnosť ich vyplnenia pozri Tabuľka č. 6 (hrubo vyznačené položky sú povinné).

V prípade KC pre elektronický podpis, kde kryptografické kľúče nie sú generované v QSCD musí pracovník Poskytovateľa pred overením totožnosti Zákazníka/Držiteľa skontrolovať doručenú žiadosť o KC vo formáte PKCS#10. Obsah položiek žiadosti a povinnosť ich vyplnenia pozri Tabuľka č. 6 (hrubo vyznačené položky sú povinné).

V prípade KC pre elektronickú pečať, kde kryptografické kľúče sú generované v QSCD musí pracovník Poskytovateľa po overení totožnosti v QSCD Zákazníka vygenerovať kľúčový pár a vytvoriť elektronická žiadosť o KC vo formáte PKCS#10 Obsah položiek žiadosti a povinnosť ich vyplnenia pozri Tabuľka č. 7 (hrubo vyznačené položky sú povinné).

V prípade KC pre elektronickú pečať, kde kryptografické kľúče nie sú v QSCD resp. sú uložené v QSCD, ktoré je pod kontrolou kvalifikovaného poskytovateľa dôveryhodných služieb, musí pracovník Poskytovateľa pred overením totožnosti Zákazníka skontrolovať doručenú žiadosť o KC vo formáte PKCS#10. Obsah položiek žiadosti a povinnosť ich vyplnenia pozri Tabuľka č. 7 (hrubo vyznačené položky sú povinné).

V prípade KC pre autentifikáciu webového sídla musí pracovník Poskytovateľa pred overením totožnosti Zákazníka skontrolovať doručenú žiadosť o KC vo formáte PKCS#10. Obsah položiek žiadosti a povinnosť ich vyplnenia pozri Tabuľka č. 8 (hrubo vyznačené položky sú povinné).

V prípade generovania kľúčového páru priamo u Poskytovateľa musí byť zabezpečená dôvernosť takto generovaných údajov.

Poskytovateľ musí vždy overiť, či zariadenie v ktorom sú generované kľúče, či už priamo u Poskytovateľa alebo pod kontrolou Zákazníka, je certifikované QSCD.

Žiadosť o KC resp. v nej sa nachádzajúci verejný kľúč, pre ktorý už bol vydaný KC, nemôže byť z bezpečnostných dôvodov použitá opakovane na vydanie iného KC a musí byť na RA odmietnutá!

4.1.4 Zaslanie žiadosti o certifikát

V prípade, že KC je vyhotovovaný na QSCD zariadenie, tak žiadosť musí pracovník RA vygenerovať priamo v QSCD zariadení prostredníctvom aplikácii RA Client.

Žiadosti, kde kryptografické kľúče nie sú uložené v QSCD zasiela Zákazník na RA, ktorá musí vykonať všetky procedúry súvisiace s procesom vyhotovovania certifikátu.

4.2 Spracovanie žiadosti o vydanie certifikátu

4.2.1 Vykonanie identifikácie a autentifikácie

Identifikácia a autentifikácia Držiteľa jednotlivých typov KC sa vykoná v zmysle bodov 3.2.2 a 3.2.3. Pri vydaní následného certifikátu v zmysle odstavca 3.3.

Po vykonaní autentifikácie a identifikácie Držiteľa KC a zapísaní požadovaných osobných údajov do systému Poskytovateľa musí pracovník RA vykonať zadanie údajov žiadosti o KC a v prípade použitia vopred zaslanej žiadosti vykonať jej vizuálnu kontrolu.

Kontrola vyplnenia údajov (osobné údaje a údaje v žiadosti o KC) bude zároveň vykonaná aj samotným programovým vybavením používaným pracovníkom RA, ktoré neumožní pokračovať vo vyhotovovaní KC v prípade nevyplnenej položky, ktorá je povinná resp. v prípade nesprávne vyplnenej položky.

Komunikácia externých registračných autorít s Poskytovateľom musí prebehnúť cez zabezpečený kanál a musí byť umožnená len registrovaným a autentifikovaným pracovníkom RA.

4.2.2 Schválenie alebo zamietnutie žiadosti

Poskytovateľ nesmie vydať KC, kým sa nedokončia všetky verifikácie a prípadné zmeny, ak sú potrebné.

Pokiaľ kľúčový pár Zákazníka/Držiteľa certifikátu nebol generovaný priamo u poskytovateľa musí byť vykonaná automatická kontrola, že verejný kľúč nachádzajúci sa v žiadosti zodpovedá súkromnému kľúču, s využitím ktorého bola žiadosť podpísaná.

Za preverenie údajov Zákazníka/Držiteľa v plnej miere zodpovedá Poskytovateľ.

Poskytovateľ má právo nevytvoriť KC, hoci Zákazník úspešne prešiel procesom registrácie u Poskytovateľa, ak sa dodatočne zistí závažná skutočnosť, ktorá bráni vydaniu KC (napr. chyba vo formáte žiadosti).

V prípade, že na danú žiadosť z nejakého dôvodu nie je možné vydať KC musí pracovník RA vyrozumieť Zákazníka o tejto skutočnosti.

Poskytovateľ musí vhodným spôsobom informovať Držiteľa o vydaní KC.

4.2.3 **Čas** spracovania žiadosti o KC

Po zaslaní žiadosti do systému Poskytovateľa by mal byť KC pre Zákazníka vydaný v čo najkratšom čase.

4.3 Vydanie KC

4.3.1 **Činnosť Poskytovateľa** pri vyhotovovaní KC

Po odoslaní žiadosti na vydanie KC z RA do systému Poskytovateľa musí tento vykonať overenie prijatej žiadosti za účelom overenia, či:

- bola odoslaná oprávneným pracovníkom RA,
- zodpovedá štandardu PKCS#10.

Vydanie KC na kľúčový pár generovaný priamo na RA musí byť bezpečne naviazaná na procedúru tohto generovania.

V prípade splnenia všetkých požiadaviek na vydanie KC, musí Poskytovateľ KC vydať.

Po vydaní KC na QSCD musí Poskytovateľ bezpečne doručiť súkromný kľúč Držiteľovi resp. v prípade, že spravuje kľúče v mene Držiteľa certifikátu zabezpečiť jeho výhradnú kontrolu nad jeho súkromným kľúčom.

Počas životnosti vydávajúcej CA nesmie byť jej rozlišovacie meno prenesené na inú entitu.

Poskytovateľ môže na žiadosť Zákazníka vyhotoviť v produkčnom prostredí KC na overenie a testovanie jeho funkčnosti. V takomto certifikáte musí byť v položkách rozlišovacieho mena jasne uvedené, že ide o testovací certifikát. Pri vyhotovovaní takéhoto KC musia byť splnené všetky požiadavky tejto CP týkajúce sa overenia identity Držiteľa KC.

4.3.2 Informovanie **Držiteľa** o vydaní certifikátu

Poskytovateľ musí vhodným spôsobom informovať Držiteľa o vydaní KC.

4.4 Prevzatie vydaného certifikátu

4.4.1 Spôsob prevzatia certifikátu

Poskytovateľ musí bezpečným spôsobom odovzdať vydaný certifikát jeho Držiteľovi.

4.4.2 Zverejnenie certifikátu

KC, ktoré obsahujú osobné údaje Držiteľa nesmú byť zverejňované z dôvodu ochrany osobných údajov ich Držiteľov.

4.4.3 Oznámenie o vydaní certifikátu iným stranám

O vydaní kvalifikovaného certifikátu musí Poskytovateľ v zmysle požiadaviek §6 ods. 2 zákona č. 272/2016 Z. z. informovať Národný bezpečnostný úrad.

4.5 **Kľúčový** pár a používanie certifikátu

V tejto časti sú popísané zodpovednosti týkajúce sa používania kľúčov a certifikátov.

4.5.1 Používanie súkromného **kľúča** a certifikátu **Držiteľom**

Povinnosťou Držiteľa KC vo vzťahu k súkromnému kľúču a KC je:

- pri žiadaní o vydanie certifikátu poskytnúť Poskytovateľovi presné a úplné informácie zmysle tejto CP,
- ak ide o fyzickú alebo právnickú osobu, používať kľúčový pár v súlade s obmedzeniami, ktoré sú uvedené vo Všeobecných podmienkach [11],
- neustále chrániť svoje súkromné kľúče v súlade s touto CP, Všeobecnými podmienkami [11], tak aby boli výhradne pod jeho kontrolou,
- využívať súkromný kľúč až po tom ako dostane KC k verejnému kľúču s ktorým tvorí pár,
- bezodkladne upovedomiť Poskytovateľa u KC, ktorý ešte neexspiroval o podozrení, že:
  - jeho súkromný kľúč bol stratený, odcudzený alebo kompromitovaný,
  - stratil kontrolu nad súkromným kľúčom kompromitáciou jeho aktivačných údajov (PIN),
  - nepresnostiach alebo zmenách v obsahu certifikátu,
- bezodkladne požiadať o zrušenie KC v prípade, že akýkoľvek údaj uvedený v subjekte KC sa stal neplatným,
- dodržiavať všetky termíny, podmienky a obmedzenia uložené na využívanie svojho súkromného kľúča a KC napr. ukončiť používanie súkromného kľúča po exspirácii alebo zrušení KC verejného kľúča,
- používať poskytnuté KC len na príslušné účely,
- okamžite ukončiť používanie súkromného kľúča po jeho kompromitácii,

Povinnosti Držiteľa KC sa týkajú aj fyzickej osoby, ktorá prevzala certifikáty pre ňou spravované komponenty resp. webové sídla.

4.5.2 Používanie verejného **kľúča** a KC Spoliehajúcou sa stranou

Spoliehajúce sa strany sú povinné:

- používať KC len na účel, pre ktorý bol vydaný,
- predtým, ako sa na KC spoľahnú, overovať každý KC na platnosť (tzn. overovať, že KC je v danom čase platný a že sa nenachádza na aktuálnom zozname zrušených KC vydanom Poskytovateľom),
- vytvoriť vzťah dôvery k CA, ktorá vydala daný KC, verifikovaním certifikačnej cesty v súlade so štandardom X.509 verzie 3,
- uchovávať originálne podpísané údaje, aplikácie potrebné na čítanie a spracovanie týchto údajov a kryptografické aplikácie potrebné na overovanie kvalifikovaných elektronických podpisov týchto údajov, pokiaľ môže byť potrebné overovať podpis týchto údajov.

4.6 Obnova certifikátu

Poskytovateľ nesmie vydať KC na verejný kľúč, na ktorý už bol ním v minulosti KC vydaný.

4.7 Vydanie následného KC

V tejto časti sú popísané podmienky vydania následného KC po exspirácii resp. zrušení používaného KC vydaného Poskytovateľom. Pod pojmom následný certifikát sa myslí vydanie nového KC rovnakého druhu a s rovnakým obsahom pre existujúceho Držiteľa, ktorého osobné údaje sú zavedené v systéme Poskytovateľa.

4.7.1 Podmienky vydania následného KC

Následný KC je možné vydať len v prípade, že došlo k ukončeniu platnosti predchádzajúceho certifikátu, alebo bol tento zrušený z dôvodov, pre ktoré už nemohol byť používaný napr. kompromitácia súkromného kľúča.

4.7.2 Kto môže **žiadať** o vydanie následného KC.

O vydanie následného KC môže požiadať existujúci Držiteľ, ktorému bol Poskytovateľom v minulosti vydaný, a ktorý splní požiadavky na identifikáciu a autentifikáciu v zmysle odstavca 3.2 .

4.7.3 Postup žiadania o vydanie následného KC

Následný KC musí byť vydaný rovnakým spôsobom ako bol vyhotovený pôvodný KC.

4.7.4 Oznámenie o vydaní následného KC

Poskytovateľ musí vhodným spôsobom informovať Držiteľa o vydaní následného KC.

4.7.5 Spôsob prevzatia následného KC

Pozri odstavec 4.4

4.7.6 **Zverejňovanie** následného KC

Pozri odstavec 4.4.2.

4.7.7 Oznámenie o vydaní následného KC iným subjektom

Žiadne ustanovenia

4.8 Modifikácia KC

Vydanie nového KC bez zmeny kľúčového páru z dôvodu zmien týkajúcich sa jeho obsahu Poskytovateľ nepodporuje.

4.9 Zrušenie KC

4.9.1 Podmienky zrušenia KC

KC sa musí zrušiť, keď sa väzba medzi Držiteľom a jeho verejným kľúčom v certifikáte už nepovažuje za platnú. Poskytovateľ je povinná zrušiť KC, ktorý spravuje, v týchto prípadoch:

- o zrušenie certifikátu požiada Držiteľ KC,
- zistí, že pri vydaní KC neboli splnené požiadavky Nariadenie eIDAS [3] resp. zákona č. 272/2016 Z. z. [5],
- zistí, že KC bol vydaný na základe nepravdivých údajov,
- zrušenie KC nariadi Poskytovateľovi svojím rozhodnutím súd,
- dozvie sa, že Držiteľ KC zomrel ak ide o fyzickú osobu resp. ak ide o právnickú osobu zanikol,
- zistí, že došlo ku kompromitácii súkromného kľúča patriaceho k danému KC, napr. ak prístup k súkromnému kľúču patriacemu k verejnému kľúču uvedenému v KC pozná iná osoba, než Držiteľ uvedený v KC,
- ak ide o mandátny certifikát a o zrušenie požiada:
  - mandant,

- mandatár,
- orgán verejnej moci alebo osoba, u ktorej mandatár vykonáva činnosť podľa osobitného predpisu (§8 ods. 1 zákona č. 272/2016 Z. z.) alebo vykonáva funkciu podľa osobitného predpisu (§8 ods. 1 zákona č. 272/2016 Z. z.)

- dozvie sa, že údaje uvedené v certifikáte sa stali neaktuálnymi,
- Držiteľ porušil svoje povinnosti stanovené touto CP a/alebo Všeobecnými podmienkami [11],
- dozvie sa, že sa Držiteľ stal nesvojprávnym na základe rozhodnutia súdu,
- došlo ku kompromitácii súkromného kľúča Poskytovateľa.

Vždy, keď sa Poskytovateľ dozvie o niektorej z uvedených okolností, daný KC sa zruší a musí sa dať do zoznamu zrušených certifikátov (CRL) resp. informácia o jeho musí byť dostupná prostredníctvom služby OCSP.

Zrušený KC nesmie byť za žiadnych okolností obnovený.

4.9.2 Kto môže **žiadať** o zrušenie KC

Držiteľ KC (alebo ním poverená fyzická alebo právnická osoba) môže kedykoľvek požiadať spôsobom stanoveným v tejto CP o zrušenie svojho vlastného KC a to aj bez udania dôvodu v žiadosti o zrušenie.

O zrušenie certifikátu môže tiež požiadať:

- Poskytovateľ - daný zamestnanec je povinný písomne zdokumentovať túto skutočnosť vrátane dôvodu svojho konania,
- súd prostredníctvom svojho rozsudku alebo predbežného opatrenia (k dokumentom o zrušení KC musí Poskytovateľ priložiť kópiu príslušného súdneho rozhodnutia),
- subjekt (fyzická alebo právnická osoba) na základe dedičského konania (k dokumentom o zrušení KC musí Poskytovateľ priložiť kópiu dokladov, z ktorých vyplýva právo daného subjektu žiadať o zrušenie KC),
- súdom poverená osoba, napr. poručník subjektu KC, ktorý sa má zrušiť (k dokumentom o zrušení KC musí Poskytovateľ priložiť kópiu príslušného súdneho rozhodnutia),
- orgán verejnej moci alebo osoba, u ktorej mandatár vykonával činnosť podľa osobitného predpisu (§8 ods. 1 zákona č. 272/2016 Z. z.) alebo funkciu podľa osobitného predpisu (§8 ods. 1 zákona č. 272/2016 Z. z.), mandant resp. mandatár.

4.9.3 Postup žiadosti o zrušenie certifikátu

O zrušenie KC musí požiadať oprávnená osoba osobne u Poskytovateľa. Osoba, požadujúca zrušenie KC sa musí u Poskytovateľa podrobiť rovnakému procesu autentizácie, aký je požadovaný pri prvotnej registrácii Zákazníka/Držiteľa (pozri odstavec 3.2), alebo sa musí preukázať dohodnutým heslom na zrušenie KC, ktoré Zákazník/Držiteľ dostane po vydaní KC.

Autentizácia požiadavky na zrušenie KC je dôležitá, aby sa predišlo svojvoľnému zrušeniu KC neautorizovanou stranou.

Zákazníka/Držiteľa KC môže u Poskytovateľa vo veci zrušenia KC zastupovať splnomocnená/poverená osoba. Zastupujúca osoba sa musí preukázať úradne overeným splnomocnením resp. poverením, v texte ktorého je jednoznačne vyjadrená vôľa Zákazníka/Držiteľa KC tento zrušiť.

Poskytovateľ môže odmietnuť žiadosť o zrušenie KC, ak Zákazník/Držiteľ nesplní podmienky autentizácie svojej identity.

Pracovník RA musí preveriť platnosť certifikátu, ktorý sa má zrušiť. V prípade certifikátu, ktorý už nie je platný musí odmietnuť žiadosť o jeho zrušenie, keďže nie je možné zrušiť certifikát, ktorého platnosť už vypršala alebo ktorý už bol zrušený.

V prípade oprávnenej žiadosti o zrušenie KC a úspešnom overení identity Zákazníka/Držiteľa sa musí KC čo najskôr zrušiť (pozri bod 4.9.5).

Držiteľ platného KC môže požiadať o zrušenie svojho KC tiež tak, že elektronickou poštou zašle na kontaktnú emailovú adresu Poskytovateľa uvedenú v bode 1.5.2 žiadosť, ktorá bude obsahovať správu s jednoznačne vyjadrenou vôľou zrušiť KC, konkrétne vetu "Žiadam týmto o zrušenie svojho certifikátu so sériovým číslom „*nnnnnn*" a heslo na zrušenie je: *xxxxxx*“, kde za „*nnnnnn*“ a „*xxxxxx*“ vyplní reálne údaje platné pre KC, ktorý žiada zrušiť.

Žiadosť o zrušenie certifikátu je možné podať aj písomne. Zákazník/Držiteľ musí v písomnej žiadosti uviesť sériové číslo KC, ktorého zrušenie žiada, pričom zrušenie musí autentizovať pomocou platného hesla na zrušenie daného KC.

Poskytovateľ musí po zrušení KC informovať (mailom alebo písomne) Držiteľa KC o jeho zrušení.

4.9.4 Čas na podanie žiadosti o zrušenie KC

V prípade hrozby kompromitácie súkromného kľúča musí oprávnená osoba (pozri bod 4.9.2) podať žiadosť o zrušenie CERTIFIKÁTU čo najskôr. Osobne resp. telefonicky je možné žiadať o zrušenie len v pracovnej dobe určenej jednotlivými RA, ktorých zoznam a pracovná doba je zverejnená na webovom sídle Poskytovateľa

(pozri bod 1). Pri elektronickej žiadosti je túto možné zaslať na jednotlivé RA kedykoľvek.

4.9.5 Čas na zrušenie KC

Poskytovateľ musí:

- zrušiť KC, čo najneskôr od momentu prijatia platnej žiadosti o zrušenie, najneskoršie však do 24 hodín od momentu prijatia platnej žiadosti,
- zverejňovať aktuálny zoznam zrušených KC a všetky predchádzajúce zoznamy zrušených certifikátov, tak aby boli prístupné Zákazníkom/Držiteľom a všetkým spoliehajúcim sa stranám,
- archivovať všetky CRL, ktoré vydal.
- informovať Zákazníka/Držiteľa KC o zrušení jeho KC, zaslaním e-mailu na e-mailovú adresu, ktorú poskytol Držiteľ v priebehu registrácie na RA, pričom musí uviesť aj informáciu o dôvode zrušenia daného KC,
- synchronizovať systémový čas vyžívaný ako zdroj pre údaj času zrušenia certifikátu s UTC časom minimálne každých 24 hodín.

CRL musí byť publikované do úložiska v čo najrýchlejšom čase po jeho vydaní.

4.9.6 Overovanie platnosti zo strany spoliehajúcej sa strany

Spoliehajúca sa strana je povinná pri spoľahnutí sa na KC overiť si jeho platnosť prostredníctvom dostupného zoznamu zrušených certifikátov (CRL) resp. prostredníctvom služby OCSP.

V čase medzi podaním oprávnenej žiadosti o zrušenie KC a zverejnením zrušeného KC v CRL nesie Zákazník/Držiteľ certifikátu všetku zodpovednosť za prípadné škody spôsobené zneužitím jeho KC. Po zverejnení certifikátu v CRL nesie všetku zodpovednosť za prípadné škody spôsobené použitím zrušeného KC strana, ktorá sa na daný zrušený KC spoľahla.

Neoverenie platnosti KC pomocou CRL je brané ako hrubé porušenie tejto CP.

4.9.7 Frekvencia vydávania CRL

Frekvencia vydávania zoznamu zrušených certifikátov (CRL) sa líši v závislosti na tom, či sa to týka koreňovej CA, podriadenej CA alebo certifikátu pre koncového používateľa (EE). Požiadavky na vydávanie CRL sú nasledovné:

Tabuľka č. 3: Frekvencia vydávania CRL

Vydavateľ CRL	Frekvencia vydávania	nextUpdate vs. thisUpdate
CA Disig CA Disig QCA3	12 hodín	24 hodín

4.9.8 Doba publikovania CRL

Poskytovateľ musí zabezpečiť, aby čas od vydania CRL do jeho publikovania v úložisku nepresiahol 90 sekúnd.

4.9.9 **Dostupnosť** služby OCSP

URI adresy OSCP responderov jednotlivých vydávajúcich certifikačných autorít Poskytovateľa musia byť obsiahnuté v rozšírení certifikátu Authority Information Access. V zmysle Nariadenia eIDAS musí byť služba OCSP poskytovaná bezodplatne.

4.9.10 Požiadavky na OCSP overovanie

Tretie strany, ktoré majú záujem využívať službu OCSP musia zaslať požiadavku na príslušný OCSP responder, ktorého URI je publikovaná v KC, ktorého platnosť požadujú overiť. Zaslaná žiadosť musí byť v súlade s požiadavkami RFC 6960.

4.9.11 Iné formy dostupnosti informácií o zrušení certifikátu

Overenie aktuálneho stavu certifikátu je možné vykonať manuálne prostredníctvom:

- Zoznamov aktuálnych CRL ako aj archívu všetkých vydaných CRL pre jednotlivé certifikačné autority Poskytovateľa, ktoré sú k dispozícii na adrese:
  - http://eidas.disig.sk/sk/crlinfo/ (SK verzia) resp.
  - http://eidas.disig.sk/en/crlinfo/ (EN verzia)

Poskytovateľ musí zabezpečiť odpoveď na telefonický alebo emailom zaslaný dopyt týkajúci sa stavu konkrétneho certifikátu.

4.9.12 Špeciálne požiadavky na zmenu **kľúčov** po ich kompromitácii

Žiadne ustanovenia.

4.9.13 Okolnosti pozastavenia platnosti certifikátu

Žiadne ustanovenia.

4.9.14 Suspendovanie certifikátu

Žiadne ustanovenia.

4.10 Služby súvisiace so stavom certifikátu

4.10.1 Prevádzkové požiadavky

Zoznam zrušených certifikátov musí byť dostupný na URL adrese uvedenej v bodu 4.9.11 a musí byť prístupný prostredníctvom HTTP protokolu na porte 80.

Služba OCSP musí byť dostupná na URL adrese uvedenej vo vydanom kvalifikovanom certifikáte a žiadateľ o zistenie stavu certifikátu musí zaslať žiadosť v zmysle bodu 4.9.10

4.11 **Ukončenie** poskytovania služieb

V prípade, že sa Zákazník/Držiteľ rozhodne ukončiť zmluvný vzťah s Poskytovateľom pred uplynutím doby platnosti vydaného KC musí zároveň požiadať o zrušenie certifikátu.

4.12 Úschova a obnova **kľúčov**

Poskytovateľ takúto službu neposkytuje.

5. Fyzické, personálne a prevádzkové **bezpečnostné** opatrenia

Bezpečnosť Poskytovateľa musí byť založená na súhrne bezpečnostných opatrení v oblasti fyzickej, objektovej, personálnej a prevádzkovej bezpečnosti. Tieto bezpečnostné opatrenia musia byť navrhnuté, dokumentované a aplikované na základe bezpečnostných pravidiel a schválené manažmentom Poskytovateľa.

Bezpečnostné opatrenia musia byť k dispozícii všetkým pracovníkom, ktorých sa týkajú.

Poskytovateľ musí:

- niesť plnú zodpovednosť za súlad svojej činnosti s postupmi definovanými vo svojej bezpečnostnej politike, vrátane jej dodržiavania zo strany externých registračných autorít.
- definovať zodpovednosť externých registračných autorít a zaviazať ich dodržiavaním stanovených bezpečnostných opatrení,
- mať zoznam všetkých svojich aktív s vyznačením ich klasifikácie v zmysle vykonaného posúdenia rizika.

Bezpečnostná politika Poskytovateľa a súhrn aktív týkajúci sa bezpečnosti musia byť preskúmavané v pravidelných intervaloch, prípade pri významných zmenách na zaistenie ich kontinuity, vhodnosti, dostatočnosti a účinnosti.

Všetky zmeny, ktoré môžu ovplyvniť úroveň poskytovanej bezpečnosti musia byť schválené manažmentom Poskytovateľa.

Nastavenie systémov Poskytovateľa musí byť pravidelne preskúmavané na zmeny, ktoré ohrozujú bezpečnostnú politiku Poskytovateľa.

5.1 Opatrenia týkajúce sa fyzickej **bezpečnosti**

5.1.1 Priestory

Technologické priestory, v ktorých je umiestnená základná infraštruktúra Poskytovateľa musia byť v chránených priestoroch, ktoré sú prístupné len autorizovaným osobám a od ostatných priestorov sú oddelené prostredníctvom primeraných bezpečnostných prvkov (bezpečnostné dvere, mreže, pevné múry ap.). Vybavenie Poskytovateľa má pozostávať len z vybavenia vyhradeného na poskytovanie dôveryhodných služieb a kvalifikovaných dôveryhodných služieb, nemá slúžiť na žiadne účely, ktoré sa netýkajú týchto služieb.

5.1.2 Fyzický prístup

Mechanizmy riadenia prístupu do chránených priestorov Poskytovateľa t. j. do priestorov zóny s najvyššou bezpečnosťou musia byť zabezpečené tak, že tieto priestory musia byť chránené bezpečnostným alarmom a vstup do nich môže byť umožnený len osobám, ktoré vlastnia bezpečnostný token a sú uvedené na zozname oprávnených osôb na vstup do chránených priestorov Poskytovateľa. Vybavenie Poskytovateľa musí byť neprestajne chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom. Vstup iných osôb môže byť povolený len v sprievode oprávnenej osoby a každý takýto vstup musí byť zaznamenaný.

5.1.3 Zásobovanie elektrickou energiou a klimatizácia

Priestory, v ktorých je umiestnené vybavenie Poskytovateľa, majú byť postačujúco zásobované elektrickou energiou a klimatizované na vytvorenie spoľahlivého operačného prostredia.

5.1.4 Ochrana pre vodou

Priestory, v ktorých je umiestnené vybavenie Poskytovateľa, majú byť umiestnené tak, aby nemohlo dôjsť k ich ohrozeniu vodou s akýchkoľvek zdrojov. V prípade, že to nie je úplne možné musia byť prijaté opatrenia, ktoré minimalizujú riziko ohrozenia priestorov vodou na minimum.

5.1.5 Ochrana pred **ohňom**

Priestory, v ktorých je umiestnené vybavenie Poskytovateľa musia byť spoľahlivo chránené od zdrojov priameho ohňa resp. tepla, ktoré by mohli spôsobiť požiar v priestoroch.

5.1.6 Úložisko médií

Médiá majú byť uskladnené v priestoroch, ktorú sú chránené pred náhodným, neúmyselným poškodením (vodou, ohňom, elektromagneticky). Médiá, ktoré obsahujú informácie týkajúce sa bezpečnostného auditu, archív alebo zálohované informácie majú byť uložené v lokalite oddelenej od vybavenia Poskytovateľa.

5.1.7 Nakladanie s odpadom

S odpadom vznikajúcim v súvislosti s prevádzkou Poskytovateľa musí byť nakladané tak, aby v žiadnom prípade nedošlo k znečisťovaniu životného prostredia.

5.1.8 Zálohovanie mimo hlavnú lokalitu

Pre prípad nenávratného poškodenia priestorov hlavnej lokality, v ktorých je umiestnená infraštruktúra Poskytovateľa je potrebné mať k dispozícii minimálne kópie najdôležitejších aktív Poskytovateľa zálohované mimo túto hlavnú lokalitu.

5.2 Procedurálne **bezpečnostné** opatrenia

5.2.1 Dôveryhodné roly

Poskytovateľ musí mať definované dôveryhodné roly zodpovedné za jednotlivé aspekty poskytovaných dôveryhodných služieb ako napr. systémový administrátor, bezpečnostný manažér, interný audítor, manažér politík ap.), ktoré formujú základ dôvery v celú PKI.

Zároveň musia byť definované zodpovednosti jednotlivých rolí.

Osoby vybrané na zastávanie rolí, ktoré si vyžadujú dôveryhodnosť, musia byť zodpovedné a dôveryhodné.

Všetky osoby v dôveryhodných roliach musí byť bez konfliktu záujmov na zabezpečenie nestrannosti služieb poskytovaných Poskytovateľom.

5.2.2 **Počet** osôb v jednotlivých úlohách

Pre každú úlohu musí byť identifikovaný počet jednotlivcov, ktorí sú určení na vykonávanie jednotlivých úloh (pravidlo K z N).

5.2.3 Identifikácia a autentizácia pre každú rolu

Každá rola musí mať definovaný spôsob identifikácie a autentifikácie pri prístupe k IS Poskytovateľa.

5.2.4 Roly vyžadujúce oddelenie zodpovedností

Každá rola musí mať stanovené kritériá, ktoré zohľadňujú potrebu oddelenia funkcií z hľadiska samotnej roly t. j. musia byť uvedené roly, ktoré nemôžu byť vykonávané rovnakými jednotlivcami.

5.3 Personálne **bezpečnostné** opatrenia

Pracovníci Poskytovateľa musia byť formálne menovaní do dôveryhodných rolí výkonným manažmentom zodpovedným za bezpečnosť.

5.3.1 Požiadavky na kvalifikáciu, skúsenosti a previerky

Zamestnanci v dôveryhodných rolách musia spĺňať kvalifikačné požiadavky, požiadavky na odbornú prax a musia mať bezpečnostné previerky stanovenej úrovne resp. musia byť v procese žiadania o takúto bezpečnostnú previerku.

Osoby v manažérskych funkciách musia:

- mať príslušné školenia alebo skúsenosti v oblasti dôveryhodných služieb, ktoré Poskytovateľ poskytuje,
- byť oboznámené s bezpečnostnými opatreniami pre roly zodpovedné za bezpečnosť
- mať skúsenosti s informačnou bezpečnosťou a odhadom rizika v rozsahu potrebnom na výkon manažérskej funkcie.

5.3.2 Požiadavky na previerky

Zamestnanec môže byť zaradený do dôveryhodnej roly Poskytovateľa len v prípade, že má bezpečnostnú previerku stanovenej úrovne resp. je v procese žiadania o takýto typ previerky. Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami Poskytovateľa.

5.3.3 Požiadavky na školenia

Pre niektoré dôveryhodné roly Poskytovateľa môžu byť špecifikované niektoré špeciálne požiadavky na školenia, ktoré by mali absolvovať pred zaradením prípadne v priebehu zaradenia. Témy majú obsahovať fungovanie softvéru a hardvéru CMA, prevádzkové a bezpečnostné postupy, ustanovenia tohto CP, CPS ap.

5.3.4 Požiadavky na frekvenciu obnovy školení

Pre roly, kde sú stanovené požiadavky na absolvovanie predpísaných školení je možné stanoviť potrebu ich opakovania po absolvovaní primárneho školenia.

5.3.5 Rotácia rolí

Žiadne ustanovenia.

5.3.6 Postihy za neoprávnenú činnosť

Zlyhanie akéhokoľvek zamestnanca Poskytovateľa, ktorého výsledok môže byť stav, ktorý nie je v súlade s ustanoveniami tejto CP resp. prijatých CPS, či už sa jedná o nedbanlivosť alebo zlý úmysel, musí byť predmetom zodpovedajúcich administratívnych a disciplinárnych konaní, ktoré môžu viesť až k ukončeniu zamestnaneckého pomeru, prípadne občianskym resp. trestnoprávnym postihom.

Akékoľvek neoprávnené alebo nevhodné konanie zamestnanca v dôveryhodnej role označené vedením Poskytovateľa musí viesť k bezodkladnému odvolaniu z dôveryhodnej roly až do ukončenia prebiehajúceho preskúmania manažmentom. Následne po preskúmaní manažmentom a vzájomnej diskusii alebo preskúmaní výsledkov vyšetrovania so zamestnancom, môže byť tento podľa potreby znovu pridelený do dôveryhodnej roly, alebo prepustený zo zamestnania.

5.3.7 Požiadavky na externých **dodávateľov**

Nezávislí dodávatelia, ktorí by mohli byť priradení na vykonávanie dôveryhodných rolí musia podliehať rovnakým povinnostiam a špecifickým požiadavkám na tieto roly v zmysle ustanovení bodu 5.3 a rovnako podliehajú sankciám uvedeným v bode 5.3.6.

5.3.8 Dokumentácia poskytovaná zamestnancom

Zamestnanci v dôveryhodných rolách musia mať k dispozícii dokumenty potrebné pre výkon funkcie, na ktorú sa sú priradení, vrátane kópie tejto CP resp. CPS a všetky technické a prevádzkovej dokumenty potrebné k zachovaniu integrity operácií Poskytovateľa. Tieto informácie musia zahŕňať aj dokumentáciu interného systému a bezpečnostnú dokumentáciu, politiky a postupy overovania identity a ďalšie informácie pripravené Poskytovateľom, dokumenty tretích strán resp. dokumenty dostupné prostredníctvom internetu.

5.4 Postup získavania auditných záznamov

Poskytovateľ musí zaznamenávať a mať k dispozícii počas nevyhnutnej doby, aj po ukončení činnosti, všetky dôležité informácie týkajúce sa vydaných KC.

Poskytovateľ musí v systéme na poskytovanie dôveryhodných služieb zaznamenávať presný čas. Čas zaznamenávaný pri jednotlivých udalostí musí byť synchronizovaný s UTC minimálne každých 24 hodín.

5.4.1 Typy zaznamenávaných udalosti

Poskytovateľ musí zaznamenávať a vyhodnocovať nasledovné dôležité udalosti:

- Procesy týkajúce sa životného cyklu kľúčov Poskytovateľa (generovanie, zálohovanie, obnova, likvidácia ap.)
- Procesy týkajúce sa samotného HSM modulu
- Údaje získané pri poskytovaní dôveryhodných služieb od Zákazníkov/Držiteľov,
- Systémové logy jednotlivých častí systému Poskytovateľa

5.4.2 Frekvencia spracovávania auditných záznamov

Administrátori Poskytovateľa sú povinní sledovať zasielané systémové logy priebežne, tak aby včas odhalili potenciálne nebezpečenstvo ohrozenia poskytovania služieb Poskytovateľa. Všetky zaznamenávané logy v elektronickej podobe musia byť v pravidelných intervaloch, minimálne 1 krát mesačne, ukladané na záznamové médiá, aby mohli byť k dispozícii audítorom. Rovnako musia byť audítorom k dispozícii všetky písomné auditné záznamy z procesov týkajúcich sa životného cyklu kľúčov certifikačných autorít Poskytovateľa, autorít časovej pečiatky a OCSP reponderov.

5.4.3 Uchovávanie logov

Poskytovateľ musí uchovávať auditné logy v súlade s požiadavkami aktuálne platnej legislatívy. Auditné logy musia byť zároveň uchovávané minimálne do času ukončenia nasledovného pravidelného externého auditu svojich služieb.

5.4.4 Ochrana auditných záznamov

Auditné záznamy musia byť uchovávané a chránené tak, aby nedošlo k ich znehodnoteniu najlepšie vo viacerých kópiách umiestnených v rozdielnych priestoroch.

5.4.5 Postupy zálohovania auditných logov

Žiadne ustanovenia.

5.4.6 Systém zálohovania logov

Žiadne ustanovenia

5.4.7 Notifikácia subjektu iniciujúceho log záznam

Žiadne ustanovenia.

5.4.8 Posudzovanie **zraniteľností**

Pozri bod 5.4.2.

5.5 Uchovávanie záznamov

5.5.1 Typy archivovaných záznamov

Poskytovateľ musí uchovávať všetky záznamy o vydaných KC ako aj samotné KC v zmysle požiadaviek aktuálne platnej legislatívy po dobu, ktorá je stanovená v bode 5.5.2.

Záznamy môžu byť v zmysle zákona uchovávané v papierovej forme resp. v elektronickej forme. Súčasťou uchovávaných záznamov musia byť aj všetky dokumenty, ktoré musí Zákazník predložiť k tomu, aby mu bol vydaný požadovaný typ certifikátu (napr. výpis z obchodného registra, plná moc, potvrdenie o vlastníctve domény ap.).

Poskytovateľ musí uchovávať aj všetky auditné záznamy (logy), písomné záznamy z udalostí CA (generovanie kľúčov CA, vyhotovovanie TSA certifikátov a certifikátov pre OCSP respondery ap.).

5.5.2 Doba uchovávania záznamov

Poskytovateľ musí uchovávať originály žiadosti o vydanie KC spolu s príslušnými dokumentami potvrdzujúcimi totožnosť Držiteľa v papierovej resp. elektronickej podobe po dobu 10 rokov.

5.5.3 Ochrana archívnych záznamov

Archívne záznamy Poskytovateľa musia byť uložené na bezpečnom mieste mimo prevádzkových priestorov a musia byť udržiavané spôsobom, ktorý zabraňuje ich neoprávnenej modifikácii, nahradenia alebo zničenia.

5.5.4 Zálohovanie archívnych záznamov

Žiadne ustanovenia.

5.5.5 Požiadavky na pridávanie **časových pečiatok** k záznamom

Žiadne ustanovenia.

5.5.6 **Archivačný** systém

Žiadne ustanovenia.

5.5.7 Postup získania a overenia archívnych informácií

Žiadne ustanovenia

5.6 Zmena **kľúčov** CA

Celý proces musí prebehnúť bez negatívneho vplyvu na úroveň zabezpečenia.

K zmene kľúčov Poskytovateľa môže dôjsť z nasledovných dôvodov:

- Blíži sa čas skončenia platnosti aktuálne používaných kľúčov Poskytovateľa. Toto je normálny stav - 14 dní pred uplynutím platnosti doteraz používaného páru kľúčov Poskytovateľa sa musí na webovom sídle Poskytovateľa zverejniť oznam o blížiacej sa zmene kľúčov Poskytovateľa.

Po tom, čo sa vygeneruje nový kľúčový pár a vyhotoví sa nový certifikát pre Poskytovateľa, tento sa musí zverejniť na webovom sídle Poskytovateľa.

- Je nutné vymeniť aktuálne používané kľúče Poskytovateľa z dôvodu ich kompromitácie. Toto je výnimočný, havarijný stav – Poskytovateľ musí bezodkladne oznámiť orgánu dohľadu, všetkým Držiteľom vydaných KC a verejnosti, že došlo ku kompromitácii kľúčov Poskytovateľa. Bezodkladne tiež musí zrušiť kompromitovaný certifikát, ako aj všetky platné KC podpísané kompromitovaným kľúčom. Poskytovateľa musí upozorniť prostredníctvom svojho webového sídla Držiteľov KC, ktoré boli podpísané zrušeným certifikátom Poskytovateľa ako aj Spoliehajúcim sa stranám, že zrušený certifikát Poskytovateľa sa má odstrániť z každej aplikácie, ktorú používajú Spoliehajúce sa strany a má byť nahradený novým certifikátom Poskytovateľa.
- Došlo k zmene kľúčov koreňovej certifikačnej autority, ktorá vydala certifikát certifikačnej autorite Poskytovateľa.

5.7 Obnova po kompromitácii alebo havárii

5.7.1 Postupy riešenia incidentov a kompromitácie

Na zabezpečenie integrity služieb musí Poskytovateľ implementovať postupy zálohovania údajov a ich obnovy.

Poskytovateľ musí mať vypracované havarijné postupy a plány obnovy pre poskytovanie dôveryhodných služieb.

Dôveryhodné služby by mali byť poskytované z dvoch geograficky oddelených CA systémov, z ktorých je jeden vedený ako hlavný a druhý ako záložný v prípade zlyhania alebo havárii hlavného.

Postupy v prípade havárie a obnovy musia byť pravidelne preskúmavané a testované (minimálne na ročnej báze) a mali by byť revidované a aktualizované podľa potreby.

5.7.2 Poškodenie hardvéru, softvéru alebo údajov

V prípade poškodenia alebo podozrenia z poškodenia hardvéru, softvéru alebo údajov musí Poskytovateľ použiť postupy určené k obnove poškodených aktív. Postupy musia zahŕňať aktivity, ktoré zabezpečia kompletnú obnovu prostredia.

5.7.3 Postupy pri kompromitácii **kľúča** CA

V prípade kompromitácie súkromného kľúča CA musí mať Poskytovateľ k dispozícii postupy na obnovu bezpečného prostredia, postupy distribúcie verejného kľúča koncovým používateľom a akým spôsobom budú vyhotovované nové certifikáty jednotlivým koncovým používateľom.

5.7.4 Zachovanie kontinuity **činnosti** po havárii

Poskytovateľ musí mať prijaté postupy na zabezpečenie kontinuity činnosti v prípade havárie v dôsledku napr. prírodnej katastrofy, ktoré zabezpečia jej schopnosť obnoviť svoju činnosť. Postupy musia zahŕňať miesto obnovy, postupy na ochranu aktív v mieste havárie resp. prírodnej katastrofy ap.

5.8 **Ukončenie činnosti** CA resp. RA

Pri ukončení činnosti Poskytovateľa z iných dôvodov ako sú udalosti spôsobené vyššou mocou (napr. prírodná katastrofa, vojnový stav, rozhodnutie štátnej moci a pod.) sa postupuje v súlade s bodom 5.7.

Ešte pred ukončením poskytovania služieb Poskytovateľ musí:

- vhodným spôsobom, minimálne 6 mesiacov vopred, oznámiť plánované ukončenie svojej činnosti orgánu dohľadu, Držiteľom všetkých ňou vydaných platných KC, stranám spoliehajúcim sa na KC a verejnosti,
- ukončiť všetky prípadné mandátne zmluvy, splnomocnenia a pod., na základe ktorých mohli iné osoby konať v mene Poskytovateľa (napr. poskytovať služby RA),
- pokúsiť sa uzavrieť zmluvu s iným kvalifikovaným poskytovateľom dôveryhodných služieb, ktorý by zabezpečil kontinuitu v poskytovaní jeho kvalifikovaných dôveryhodných služieb,
- pred ukončením činnosti zrušiť všetky platné KC, ak nezabezpečí kontinuitu v poskytovaní jeho služieb,
- sústrediť a archivovať všetky dokumenty Poskytovateľa,
- vykonať kontroly dodržania zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 122/2013 Z. z.“) [12],
- vyradiť z používania všetky súkromné kľúče, vrátane ich kópií takým spôsobom, že nebude možné ich žiadnym spôsobom obnoviť.

Ak je dôvodom ukončenia činnosti Poskytovateľa nejaký dôvod bez vzťahu k bezpečnosti, potom ani certifikáty vydávajúcich CA, ktoré končia činnosť a ani KC podpísané týmito CA nemusia byť zrušené.

Po ukončení svojej činnosti Poskytovateľ nesmie vydať žiadny KC a musí zabezpečiť preukázateľné znemožnenie opätovného použitia podpisových dát (súkromných kľúčov) CA.

Poskytovateľ musí mať riešenie na pokrytie všetkých nákladov spojených so splnením minimálnych požiadaviek pri ukončení činnosti v prípade bankrotu alebo inej príčiny, kedy nebude schopná pokryť náklady vlastnými prostriedkami, a to v súlade s platnou legislatívou o bankrote.

6. Technické **bezpečnostné** opatrenia

Technická časť infraštruktúry Poskytovateľa (hardvér a softvér) musí pozostávať len z bezpečných systémov a oficiálneho softvéru. Architektúru infraštruktúry Poskytovateľa musí byť navrhnutá s použitím komponentov, ktoré vyhovujú bezpečnostným štandardom na úrovni súčasných poznatkov.

Osobitná pozornosť musí byť venovaná kryptografickému modulu (HSM modulu), ktorý slúži na generovanie, úschovu a použitie súkromných kľúčov Poskytovateľa a ktorý patrí k najcitlivejším aktívam. Súkromné kľúče Poskytovateľa musia byť uložené v HSM module, ktorý je certifikovaný minimálne podľa štandardu FIPS 140-2 level 3.

Poskytovateľ musí používať na ochranu svojho súkromného kľúča kombináciu fyzických, logických a procedurálnych opatrení, ktoré zaručujú jeho bezpečnosť. Tieto opatrenia musia byť popísané napr. vo vydanom CPS.

Súčasťou systému Poskytovateľa musia byť zariadenia na nepretržitú detekciu, monitorovanie a signalizáciu neautorizovaných a neobvyklých pokusov o prístup k jej prostriedkom.

Aplikácie súvisiace s informáciou o stave certifikátu musia byť zabezpečené tak, zabezpečiť, že zabránia akýmkoľvek neoprávneným pokusom o modifikovanie informácií o stave certifikátu.

Všetky funkcie Poskytovateľa, pri ktorých sa používa počítačová sieť, musia byť zabezpečené pred neautorizovaným prístupom a inými škodlivými činnosťami.

6.1 Generovanie a inštalácia páru **kľúčov**

6.1.1 Generovanie a inštalácia páru **kľúčov** pre jednotlivé subjekty

6.1.1.1. Vydavateľ certifikátov

Generovanie a inštalácia páru kľúčov Poskytovateľa sa musí vykonávať štandardizovaným spôsobom, ktorý je podrobne popísaný v dokumentácii Poskytovateľa. Spôsob generovania musí zabezpečiť dostatočnú dôveru v postup generovania a celý proces musí byť písomne zaznamenaný. Generovanie kľúčov musia zabezpečiť zamestnanci Poskytovateľa zaradení v rolách, ktoré majú oprávnenie na účasť na ceremónii generovania. Generovanie kľúčov musí byť vykonané v bezpečnom zariadení na uchovávanie kryptografických kľúčov, ktoré spĺňa legislatívne požiadavky dané na takýto typ zariadenia..

6.1.1.2. Registračné autority

Generovanie kľúčových párov certifikátov pre registračné autority musí byť vykonávané pod kontrolou poverených zamestnancov Poskytovateľa a kľúče musia byť uložené v bezpečnom QSCD zariadení.

6.1.1.3. Koncoví používatelia

Pozri 4.1.3.

6.1.2 **Doručenie** súkromného **kľúča Držiteľovi** certifikátu

Vygenerovaný kľúčový pár obsahujúci súkromný kľúč RA musí byť bezpečným spôsobom doručený príslušnému pracovníkovi RA.

Vygenerovaný kľúčový pár koncového Držiteľa KC, ktorý je uložený v bezpečnom zariadení pre elektronický podpis musí byť odovzdaný osobne ihneď po vydaní KC.

U KC pre elektronickú pečať, kde kľúče boli generované v kvalifikovanom zariadení pre elektronickú pečať, pod kontrolou Zákazníka resp. kvalifikovaného dôveryhodného poskytovateľa služieb (napr. HSM modul), sa koncovému používateľovi musí doručiť len vydaný KC.

U KC pre autentifikáciu webového sídla Rovnako sa doručuje iba vydaný KC pre autentifikáciu webového sídla.

6.1.3 **Doručenie** verejného **kľúča vydavateľovi** certifikátu

Pokiaľ bol kľúčový pár, na ktorý má byť vydaný KC generovaný pod kontrolou Zákazníka resp. iného kvalifikovaného poskytovateľa dôveryhodných služieb musí byť verejný kľúč doručený certifikačnej autorite bezpečným spôsobom.

6.1.4 Poskytovanie verejných **kľúčov Poskytovateľa** Spoliehajúcim sa stranám

Pre Spoliehajúce sa strany musí Poskytovateľ bezpečným spôsobom poskytnúť verejné kľúče všetkých vydávajúcich certifikačných autorít Poskytovateľa, ktoré vyhotovujú KC.

6.1.5 **Dĺžka kľúčového** páru

Musí byť stanovená odporúčaná dĺžka kľúčového páru resp. minimálna dĺžka kľúčov pre všetky typy entít a všetky používané algoritmy (napr. RSA).

6.1.6 Parametre a kvalita verejného **kľúča**

Parametre a kvalitu verejných kľúčov Poskytovateľa musí určiť PMA. Počas ceremónie generovania kľúčov musia byť stanovené parametre dodržiavané. Poskytovateľ musí využívať na generovanie a uchovávanie kľúčov kryptografické hardvérové moduly spĺňajúce požiadavky FIPS 140-2 Level 3, ktoré zabezpečujú náhodné generovanie RSA kľúčov veľkosti minimálne 4096 bitov.

Pre jednotlivé typy KC vyhotovované pre koncových používateľov musí mať Poskytovateľ stanovené parametre a kvalitu verejného kľúča (dĺžka, typ) a pred samotným vydaním musí kontrolovať ich dodržanie.

6.1.7 Použitie **kľúčov**

Certifikáty certifikačných autorít Poskytovateľa musia obsahovať rozšírenia, ktoré určujú k čomu môžu byť tieto certifikáty použité.

6.2 Ochrana súkromného **kľúča** a technické opatrenia pre kryptografický modul

6.2.1 Štandardy a opatrenia pre kryptografický modul

Poskytovateľ musí využívať na ochranu súkromných kľúčov svojich vydávajúcich CA hardvérové kryptografické moduly, ktoré sú certifikované podľa štandardu FIPS 140-2 level 3. Moduly musia byť uložené v zabezpečených priestoroch, do ktorých majú prístup len osoby v dôveryhodných rolách.

Súkromné kľúče Poskytovateľa sa môžu používať výlučne na podpisovanie certifikátov a CRL vyhotovovaných Poskytovateľom.

Vybavenie CA musí byť neprestajne chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom.

6.2.2 Opatrenia (K z N) pre manipuláciu so súkromným **kľúčom**

Pri operáciách správy súkromných kľúčov Poskytovateľa (napr. generovanie, zálohovanie, zničenie) musí byť vždy prítomný príslušný počet oprávnených osôb na princípe „K“ z „N“ určených oprávnených osôb

6.2.3 „Key escrow“ súkromného **kľúča**

Žiadne ustanovenia.

6.2.4 Zálohovanie súkromného **kľúča**

Súkromné kľúče Poskytovateľa sú generované a uchovávané vo vnútri hardvérových kryptografických modulov. V prípade potreby ich prenosu pre proces zálohovania

a obnovy, musia byť súkromné kľúče prenášané vždy v zašifrovanej podobe. Prenášanie súkromných kľúčov a ich obnova v inom hardvérovom kryptografickom module môže byť vykonaná len oprávnenými zamestnancami v zmysle pravidiel uvedených v bode 6.2.2.

6.2.5 Archivácia súkromného **kľúča**

Žiadne ustanovenia.

6.2.6 Prenos súkromných **kľúčov** z a do HSM modulu

Pozri 6.2.4

6.2.7 Uchovávanie súkromných **kľúčov** v HSM module

Súkromné kľúče Poskytovateľa, ktoré sú využívané pri vyhotovovaní vydaných KC pre koncových používateľov môžu byť v samotnom HSM module uchovávané v čitateľnej forme. Všetky HSM moduly Poskytovateľa musia byť prevádzkované v zabezpečených priestoroch s režimovým prístupom.

6.2.8 Spôsob aktivácie súkromných **kľúčov**

Súkromné kľúče Poskytovateľa môžu aktivovať len oprávnené osoby v zmysle bodu 6.2.2.

Pri aktivácií musí každá oprávnená osoba z potrebného počtu oprávnených osôb vložiť do HSM modulu svoju čipovú kartu a zadať k nej heslo.

Po aktivácii sú kľúče v HSM module aktívne až do doby, kým nedôjde k ich deaktivácii. oprávnenou osobou (administrátor CA) alebo výpadkom elektrického napájania HSM modulu.

Za ochranu súkromných kľúčov ich Držiteľmi, ktorým Poskytovateľ vydal KC na príslušný verejný kľúč sú výhradne zodpovední ich Držitelia.

6.2.9 Spôsob deaktivácie súkromného **kľúča**

Deaktiváciu súkromného kľúča v HSM module môže vykonať len oprávnená osoba (administrátor CA) alebo sú kľúče deaktivované automaticky pri výpadku relácie alebo výpadkom elektrického napájania HSM modulu.

6.2.10 Spôsob **zničenia** súkromného **kľúča**

Poskytovateľ musí technickými a organizačnými opatreniami zabezpečiť, že súkromné kľúče vydávajúcich CA Poskytovateľa nebude možné po ukončení jeho životného cyklu ďalej používať. O ukončení životného cyklu súkromného kľúča CA a prijatých technických a organizačných opatreniach musí byť vykonaný záznam podpísaný všetkými prítomnými aktérmi.

6.2.11 Charakteristika HSM modulu

Pozri bod 6.2.1.

6.3 Ďalšie aspekty manažmentu páru kľúčov

6.3.1 Archivácia verejných kľúčov

Poskytovateľ musí uchovávať všetky verejné kľúče, na ktoré bol ňou vydaný certifikát v zmysle bodu 5.5.2

6.3.2 Dĺžka platnosti certifikátov a použiteľnosť kľúčového páru

Platnosť vyhotovovaných kvalifikovaných certifikátov Poskytovateľom a použiteľnosť páru kľúčov nesmie prekročiť nasledovné hodnoty:

Typ certifikátu	Platnosť (maximálne)
Vydávajúca CA	30 rokov
KC pre koncového používateľa	4 roky

6.4 Aktivačné údaje

6.4.1 Vytváranie a inštalácia aktivačných údajov

Aktivačné údaje Držiteľov KC (PIN a PUK), ktoré sa viažu ku konkrétnemu kvalifikovanému zariadeniu pre elektronický podpis resp. elektronickú pečať musia byť odovzdané Držiteľovi pri osobnom stretnutí počas vyhotovovania KC. Držiteľ musí byť poučený o potrebe a spôsobe ich zmeny a o rizikách pokiaľ uvedené zmeny nevykoná. Aktivačnú údaje môžu byť v podobe PIN, hesla alebo hesla rozdeleného na viacero častí na princípe k/n a pod.

Aktivačné údaje k používaným kryptografickým modulom CA Poskytovateľa musia byť vytvárané v zmysle bodu 6.2.2.

6.4.2 Ochrana aktivačných údajov

Za ochranu súkromných kľúčov Držiteľov sú zodpovední výhradne samotní Držitelia.

Pri vyhotovovaní KC musia byť Držitelia upozornení so strany Poskytovateľa o potrebe chrániť súkromný kľúč silným heslom, aby nemohlo dôjsť k jeho zneužitiu, počas celej doby jeho používania.

Kľúčový pár určený pre vydavateľa KC:

- musí byť generovaný v bezpečnostnom module, ktorý spĺňa minimálne požiadavky štandardu FIPS 140-2 level 2,
- akákoľvek manipulácia so súkromným kľúčom môže byť umožnená len za princípu viacnásobnej kontroly, pričom minimálny počet potrebných oprávnených osôb musí byť tri (3).

6.4.3 Ostatné aspekty **aktivačných** údajov

Musí byť zabezpečené, že sa súkromné kľúče vydávajúcich CA nikdy nedostali v nezašifrovanej forme mimo modul, kde sú uložené.

Nikto nemá mať prístup k súkromnému podpisovému kľúču okrem jeho Držiteľa.

Pass-frázy, PINy, biometrické dáta alebo iné mechanizmy ekvivalentnej autentizačnej robustnosti sa musia použiť na ochranu prístupu k použitiu súkromného kľúča.

Aktivačné dáta pre súkromné kľúče patriace k certifikátom potvrdzujúcim individuálnu identitu nesmú byť nikdy zdieľané.

Aktivačné dáta pre súkromné kľúče patriace k certifikátom potvrdzujúcim identitu organizácie majú byť známe len tým, ktorí sú v organizácii autorizovaní na použitie daných súkromných kľúčov.

6.5 Riadenie **bezpečnosti počítačov**

6.5.1 Špecifické požiadavky na **bezpečnosť počítačov**

Poskytovateľ musí vykonáva všetky funkcie kvalifikovaného poskytovateľa dôveryhodných služieb za použitia dôveryhodného systému, ktorý spĺňa požiadavky definované v bezpečnostnom projekte IS Poskytovateľa.

Poskytovateľ vyhotovujúci KC sa môže riadiť pri poskytovaní svojich služieb požiadavkami na bezpečnosť informácií, ktoré sú kladené na dôveryhodného poskytovateľa služieb a sú definované v štandarde ETSI EN 319411-2 " Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. [2]

Všetky systémy musia byť pravidelne overované na prítomnosť škodlivého kódu a chránené proti spyware a vírusom.

6.5.2 Hodnotenie **bezpečnosti** informácií

Žiadne ustanovenia.

6.6 Opatrenia v životnom cykle

6.6.1 Opatrenia pri vývoji systémov

Aplikácie Poskytovateľa pre potreby systému Poskytovateľa musia zohľadňovať opatrenie týkajúce sa bezpečnosti vývojového prostredia, personálnej bezpečnosti, bezpečnosti riadenia konfigurácie pri údržbe systémov, v rámci technických postupov vývoja softvéru, v rámci metodológie vývoja softvéru a jeho modularite a vrstvení.

6.6.2 Opatrenia na riadenie **bezpečnosti**

Poskytovateľ musí využívať nástroje a postupy, ktoré umožnia určiť, či operačné systémy využívané v rámci CA Poskytovateľa a využívané sieťové pripojenia stále zodpovedajú nastavenej úrovni bezpečnosti.

Tieto nástroje a postupy by mali zahŕňať kontrolu integrity bezpečnostného softvéru, firmvéru a hardvéru na zaistenie ich správnej funkčnosti.

6.6.3 **Bezpečnostné** opatrenia v životnom cykle

Žiadne ustanovenia.

6.7 **Sieťové bezpečnostné** opatrenia

Poskytovateľ musí mať prijaté opatrenia na zabezpečenie sieťovej bezpečnosti vrátane bezpečnosti firewalov.

6.8 Využívanie **časovej pečiatky**

Žiadne ustanovenie

7. Profily KC, CRL a OCSP

Profily KC, profily zoznamov zrušených certifikátov (CRL) a odpoveď vo forme informácie o platnosti certifikátu poskytovaná prostredníctvom OCSP protokolu musia byť stanovené centrálne PMA a ani osoby zastávajúce služobné úrovne (roly) nemôžu svojvoľne meniť štruktúru týchto profilov resp. odpovedí.

Podľa čl. 28 ods. 3 a čl. 38 ods. 3 Nariadenia eIDAS [3] kvalifikované certifikáty pre elektronické podpisy (pečate) môžu obsahovať nepovinné dodatočné osobitné atribúty. Týmito atribútmi sa neovplyvní interoperabilita a uznávanie kvalifikovaných elektronických podpisov (pečatí). Rovnako certifikát pre autentifikáciu webových sídiel môže obsahovať nepovinné dodatočné osobitné atribúty, pokiaľ sa týmito atribútmi neovplyvní interoperabilita a uznávanie týchto kvalifikovaných certifikátov.

Štruktúra KC vyhotovovaných Poskytovateľom sa môže meniť len na základe rozhodnutia povereného člena PMA.

7.1 Profil KC

7.1.1 Verzia

Táto CP povoľuje len profily KC vyhovujúce štandardu X.509 verzie 3.

Tabuľka č. 4 obsahuje základné položky KC vyhotovovaného Poskytovateľom.

Tabuľka č. 4: Základné položky KC

Názov **poľa**	Obsah
Verzia (Version)	V3 (hodnota 0x2)
Serial number (Sériové číslo)	Jedinečné číslo pridelené Poskytovateľom > 0
Issuer Signature Algorithm (Podpisový algoritmus vydávateľa)	sha256WithRSAEncryption (1 2 840 113549 1 1 11)
Issuer (Vydávateľ)	Jedinečné X.500 rozlišovacie meno Poskytovateľa
Valid from (Platný od)	Začiatok platnosti certifikátu (UTC čas)
Valid to (Platný do)	Koniec platnosti certifikátu (UTC čas)
Subject ()	*Obsah jednotlivých položiek pre jednotlivé typy KC pozri Tabuľka č. 6, Tabuľka č. 7 a Tabuľka č. 8*
Public key (verejný kľúč)	Verejný kľúč, na ktorý je vyhotovený certifikát (min veľkosť 2048 bit)
Extensions (Rozšírenia)	*Zoznam rozšírení v KC pozri Tabuľka č. 5*

7.1.2 Rozšírenia certifikátu

Tabuľka č. 5 obsahuje použité rozšírenia nachádzajúce sa vo všetkých typoch vyhotovovaných KC.

Tabuľka č. 5: Použité rozlíšenia v KC vyhotovovaných **Poskytovateľ**om

Názov rozšírenia	ASN.1 názov a OID / Popis	**Prítomnosť**	**Kritickosť**
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Určuje (http:// … p7c, certifikát alebo aj ldap://…) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.	Áno	Nie
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	Áno	Nie
authorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} Identifikátor verejného kľúča certifikačnej autority CA, ktorá vydala tento certifikát.	Áno	Nie
certificatePolicies	id-ce-certificatePolicies} {2.5.29.32} Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný.	Áno	Nie
crlDistributionPoints	{id-ce-CRLDistributionPoints} {2.5.29.31} Určuje, akým spôsobom a odkiaľ je možné získať CRL.	Áno	Nie
QCstatements	{id-pe-qcStatements} {1.3.6.1.5.5.7.1.3} Špecifické prehlásenie týkajúce sa EU kvalifikovaného certifikátu: esi4-qcStatement-1 esi4-qcStatement-2 esi4-qcStatement-4 esi4-qcStatement-5 esi4-qcStatement-6	Áno	Nie
BasicConstraints	{id-ce-basicConstraints} {2.5.29.19} Identifikuje typ certifikátu (end entity, CA).	Áno	Áno
keyUsage	{id-ce-keyUsage} {2.5.29.15} Definuje účel použitia súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno	Áno

Názov rozšírenia	Hodnota rozšírenia	Kritickosť?
SubjectAltNames OID (2.5.29.17)	{id-ce-subjectAltName} Toto rozšírenie obsahuje jedno alebo viac alternatívnych mien, s použitím ľubovoľného z celej rady foriem mien pre subjekt, ktorý je viazaný CA k verejnému kľúča.	Nie

7.1.3 Identifikátory použitých algoritmov

Algoritmus podpisu vyhotovovaných KC (Signature Algorithm)
sha256RSA
OID: 1.2.840.113549.1.1.11

7.1.4 Formy mien

U fyzickej osoby sa v KC pre elektronický podpis musí uviesť krstné meno(á) v poli givenName (GN) a priezvisko(á) v poli Surname (SN). Meno(a) a priezvisko(á) spolu v tvare, ktorý si určí Zákazník/Držiteľ sa ešte uvedú v poli commonName (CN).

U právnickej osoby sa v KC pre elektronickú pečať musí uviesť jej oficiálny názov v poli Organization a jej ďalší identifikačný údaj, ak existuje, v položke serialNumber resp. organizationIdentifier.

U webového sídla sa v KC na autentifikáciu webového sídla musí uviesť presne stanovené meno domény (FQDN) v poli CN a rovnako aj v rozšírení subjecAlternativeName.

V certifikáte vydávajúcej CA sa vždy musí uvádzať identifikátor Poskytovateľa v tvare „CA Disig“.

Štruktúra certifikátov vyhotovovaných Poskytovateľom sa môže meniť len na základe rozhodnutia PMA.

Algoritmy a dĺžky kľúčov uplatňované v KC:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, **dĺžka** je 2 048 bitov

Dĺžka platnosti
Maximálne 1460 dní

Tabuľka č. 6 obsahuje možné položky rozlišovacieho mena a ich popis v prípade KC pre elektronický podpis.

Tabuľka č. 6: Obsah položiek rozlišovacieho mena v KC pre elektronický podpis

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a maximálna **dĺžka** položky	Poznámka
Meno a priezvisko (commonName) OID (2.5.4.3)	CN	Meno a priezvisko alebo pseudonym, za ktorým je uvedený reťazec PSEUDONYM	Peter Disig alebo QWERTY-PSEUDONYM	DirectoryString (UTF8String) 64 znakov	Údaj je povinný!!!
Meno(á) (givenName) OID (2.5.4.42)	G	Všetky mená použité v položke CN okrem priezviska	Peter	DirectoryString (UTF8String) 64 znakov	Údaj je povinný, ak v položke CN nebol uvedený pseudonym. V prípade použitia pseudonymu sa v KC neuvádza.
Priezvisko (Surname) OID (2.5.4.4)	SN	Priezvisko z položky CN	Disig	DirectoryString (UTF8String) 64 znakov	
Pseudonym OID (2.5.4.65)		Pseudonym	QWERTY	DirectoryString (UTF8String) 64 znakov	Údaj je povinný pokiaľ ide o vydanie KC obsahujúce v CN pseudonym. V opačnom prípade sa v KC neuvádza
Útvar v organizácii (organizationUnitName) OID (2.5.4.11)	OU	Názov útvaru v organizácii uvedenej v položke „Organizácia“	ACA	DirectoryString (UTF8String) 64 znakov	Údaj je nepovinný
Organizácia (organizationName) OID (2.5.4.10)	O	Názov organizácie, podľa obchodného registra, kde je Držiteľ zamestnaný	Disig a.s.	DirectoryString (UTF8String) 64 znakov	
Mesto (localityName) OID (2.5.4.7)	L	Názov mesta/obce trvalého pobytu Držiteľa	Bratislava	DirectoryString (UTF8String) 128 znakov	
Názov kraja (stateOrProvinceName) OID (2.5.4.8)	ST	Názov územno-správneho celku trvalého bydliska Držiteľa	Bratislavský	DirectoryString (UTF8String) 128 znakov	
Štát (countryName) OID (2.5.4.6)	C	Dvojznaková skratka štátu – dvojmiestny kód podľa ISO 3166	SK	PrintableString 2 znaky	Údaj je povinný!!!
SerialNumber* OID (2.5.4.5)		Odkaz na identitu fyzickej osoby **	PNOSK 1234567890 Položka je súčasťou KC	PrintableString 64 znakov	Údaj je nepovinný

* Táto položka môže obsahovať špecifický identifikátor fyzickej osoby (pozri **) resp. pokiaľ je vydávaný KC bez špecifického identifikátora fyzickej osoby, tak obsahuje hodnotu, ktorá zabezpečuje jedinečnosť subjektu, ktorému je KC vydávaný

** Odkaz na identitu sa potom skladá z dvoch častí. Prvá časť pozostáva z troch úvodných znakov určujúcich typ odkazu na identitu a dvoch znakov krajiny. Tri úvodné znaky potom budú buď „IDC“ (identifikácia na základe identifikačnej karty), „PAS“ (identifikácia na základe čísla pasu), „PNO“ (identifikácia na základe rodného čísla u občanov SR, alebo cudzincov, ktorí majú pridelené rodné číslo podľa zákona o rodnom čísle 301/1995 Z. z. Nasledujúce dva znaky obsahujú kód krajiny podľa ISO 3166 (pre Slovensko „SK“). Druhá časť položky pozostáva z údajov, ktorých typ určujú prvé tri úvodné znaky a pri IDC a PAS sa uvedie séria a číslo identifikačného dokladu (napr. IDCSK SP989783 resp. PASSK P3000180) a pri rodnom čísle sa uvedie rodné číslo bez lomky (napr. PNOSK 7701011111). Upozornenie - Prvá a druhá časť sú oddelené pomlčkou!!!

Okrem položiek uvedených v tejto tabuľke môže žiadosť o KC pre elektronický podpis obsahovať ako nepovinný údaj emailovú adresu. Táto položka však nebude súčasťou rozlišovacieho mena, ale zadaná emailová adresa bude uvedená v certifikáte v jeho rozšírení SubjectAltName. Hodnota emailovej adresy sa zadáva obvyklým spôsobom (t. j. ako rfc822Name (OID 2 5 29 17).

Tabuľka č. 7 obsahuje možné položky rozlišovacieho mena a ich popis v prípade KC pre elektronickú pečať.

Tabuľka č. 7: Obsah položiek rozlišovacieho mena v KC pre elektronickú **pečať**

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a maximálna **dĺžka** položky	Poznámka
Meno, názov (commonName) OID (2.5.4.3)	CN	Označenie systému, pre ktoré je certifikát vyhotovovaný	Podateľňa	DirectoryString (UTF8String) 64 znakov	Údaj je povinný!!!
Útvar v organizácii (organizationUnitName) OID (2.5.4.11)	OU	Názov útvaru v organizácii uvedenej v položke „Organizácia“	Informačné systémy	DirectoryString (UTF8String) 64 znakov	Údaj je nepovinný
Organizácia (organizationName) OID (2.5.4.10)	O	Registrovaný názov právnickej osoby ktorej je certifikát vyhotovovaný	Disig a.s.	DirectoryString (UTF8String) 64 znakov	Údaj je povinný!!!
Mesto (localityName) OID (2.5.4.7)	L	Názov mesta/obce sídla právnickej osoby	Bratislava	DirectoryString (UTF8String) 128 znakov	Údaj je nepovinný
Názov kraja (stateOrProvinceName) OID (2.5.4.8)	ST	Názov územno-správneho celku sídla orgánu právnickej osoby	Bratislavský	DirectoryString (UTF8String) 128 znakov	Údaj je nepovinný
Štát (countryName) OID (2.5.4.6)	C	Dvojznaková skratka štátu – dvojmiestny kód podľa ISO 3166 kde právnická osoba registrovaná	SK	PrintableString 2 znaky	Údaj je povinný!!!
serialNumber* OID (2.5.4.5) alebo		Odkaz na identitu právnickej osoby	NTRSK-12345678 Položka je súčasťou KC	PrintableString 64 znakov	Údaj je nepovinný

organizationIdentifier* OID (2.5.4.97)					

* Sémantika identifikátora právnickej osoby má takúto štruktúru. Prvá časť pozostáva z troch úvodných znakov určujúcich typ odkazu na identitu a dvoch znakov krajiny (podľa ISO 3166). Tri úvodné znaky môžu byť „NTR“ (identifikácia na základe identifikačného čísla organizácie (IČO)), „VAT“ (identifikácia na základe daňového identifikačného čísla) alebo dva znaky podľa miestnej definície v určenej krajine a názov registračnej autority, pričom sa identifikuje národná schéma, ktorá sa považuje za vhodnú pre vnútroštátnu a európsku úroveň, za ktorým nasleduje znak ":" (dvojbodka). Nasledujúce dva znaky obsahujú kód krajiny podľa ISO 3166 (pre Slovensko „SK“). Druhá časť položky pozostáva z údajov, ktorých typ určujú prvé tri úvodné znaky a pri NTR, VAT a XX: sa uvedie identifikačné číslo (napr. NTRSK-12345678, VATSK-2022116976, XX:CC-nnnnnnn).

Okrem položiek uvedených v tejto tabuľke môže žiadosť o KC pre elektronickú pečať obsahovať ako nepovinný údaj emailovú adresu. Táto položka však nebude súčasťou rozlišovacieho mena, ale zadaná emailová adresa bude uvedená v certifikáte v jeho rozšírení SubjectAltName. Hodnota emailovej adresy sa zadáva obvyklým spôsobom (t. j. ako rfc822Name (OID 2 5 29 17)).

Tabuľka č. 8 obsahuje možné položky rozlišovacieho mena a ich popis v prípade KC pre autentifikáciu webového sídla.

Tabuľka č. 8: Obsah položiek rozlišovacieho mena v kvalifikovanom certifikáte pre autentifikáciu webového sídla

Názov položky	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a maximálna **dĺžka** položky	Poznámka
Meno, názov (commonName) OID (2.5.4.3)	CN	Presne stanovené meno domény (FQDN), na ktoré je certifikát vydávaný	www.disig.sk	DirectoryString (UTF8String) 64 znakov	Údaj je povinný!!!
Útvar v organizácii (organizationUnitName) OID (2.5.4.11)	OU	Názov útvaru v organizácii uvedenej v položke „Organizácia“		DirectoryString (UTF8String) 64 znakov	Údaj je nepovinný
Organizácia (organizationName) OID (2.5.4.10)	O	Registrovaný názov právnickej osoby ktorej je certifikát vyhotovovaný	Disig a.s.	DirectoryString (UTF8String) 64 znakov	Údaj je povinný!!!
Kategória podnikania (businessCategory) OID (2.5.4.15)		Kategória, v ktorej právnická osoba podniká	Business Entity	DirectoryString (UTF8String) 128 znakov	Údaj je povinný!!!
Krajina jurisdikcie právnickej osoby (jurisdictionOfIncorporation CountryName) OID (1.3.6.1.4.1.311.60.2.1.3)		Dvojznaková skratka štátu podľa ISO 3166 kde právnická osoba registrovaná	SK	PrintableString 2 znaky	Údaj je povinný!!!
Mesto (localityName) OID (2.5.4.7)	L	Názov mesta/obce sídla právnickej osoby, ktorej je certifikát vydávaný	Bratislava	DirectoryString (UTF8String) 128 znakov	Údaj je povinný!!!

Názov kraja (stateOrProvinceName) OID (2.5.4.8)	ST	Názov územno-správneho celku sídla právnickej osoby	Bratislavský	DirectoryString (UTF8String) 128 znakov	Údaj je nepovinný
Štát (countryName) OID (2.5.4.6)	C	Dvojznaková skratka štátu – dvojmiestny kód podľa ISO 3166 kde je orgán verejnej moci resp. právnická osoba registrovaný	SK	PrintableString 2 znaky	Údaj je povinný!!!
serialNumber* OID (2.5.4.5) alebo organizationIdentifier* OID (2.5.4.97)		Odkaz na identitu právnickej osoby resp. orgánu verejnej moci	NTRSK-12345678 Položka je súčasťou KC	PrintableString 64 znakov	Údaj je povinný!!!

* Sémantika identifikátora právnickej osoby má takúto štruktúru. Prvá časť pozostáva z troch úvodných znakov určujúcich typ odkazu na identitu a dvoch znakov krajiny (podľa ISO 3166). Tri úvodné znaky môžu byť „NTR“ (identifikácia na základe identifikačného čísla organizácie (IČO)), „VAT“ (identifikácia na základe daňového identifikačného čísla) alebo dva znaky podľa miestnej definície v určenej krajine a názov registračnej autority, pričom sa identifikuje národná schéma, ktorá sa považuje za vhodnú pre vnútroštátnu a európsku úroveň, za ktorým nasleduje znak ":" (dvojbodka). Nasledujúce dva znaky obsahujú kód krajiny podľa ISO 3166 (pre Slovensko „SK“). Druhá časť položky pozostáva z údajov, ktorých typ určujú prvé tri úvodné znaky a pri NTR, VAT a XX: sa uvedie identifikačné číslo (napr. NTRSK-12345678, VATSK-2022116976, XX:CC-nnnnnnn).

7.1.5 Obmedzenia týkajúce sa mien

Žiadne ustanovenia.

7.1.6 Identifikátor **certifikačnej** politiky

Pozri odstavec 1.2.

7.1.7 Použitie rozšírení na obmedzenie politiky

Toto rozšírenie nie je používané.

7.1.8 Syntax a sémantika politiky

Každý KC vydaný v zmysle tejto politiky musí obsahovať jej identifikátor v podobe OID (pozri odstavec 1.2) v rozšírení id-ce-certificatePolicies (2.5.29.32).

Každý KC vydaný v zmysle tejto politiky musí obsahovať identifikátor v podobe OID CP 1.3.158.36061701.0.0.0.1.2.2 v rozšírení id-ce-certificatePolicies (2.5.29.32), ktorým sa vyjadruje súlad požiadaviek Nariadenia eIDAS s národnou legislatívou.

Každý SSL certifikát naviac musí obsahovať identifikátor v podobe OID (2.23.140.1.2.2), že certifikát je vyhotovovaný ako SSL certifikát, kde bola overená

organizácia (právnická osoba resp. fyzická osoba), ktorá má pod kontrolou presne stanovené meno domény (FQDN) v ňom uvedené.

7.1.9 Sémantika spracovania kritických **certifikačných** politík

Žiadne ustanovenia.

7.2 Profily zoznamu zrušených certifikátov

7.2.1 Verzia

CRL vydávané Poskytovateľom musia byť CRL verzie 2.

CRL musia byť vydávané tou istou CA Poskytovateľa ako certifikát.

Vydávané CRL musia byť v súlade s RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and CRL Profile“ [6]

7.2.2 Použité rozšírenia (CRL extensions) v CRL

Tabuľka č. 9 obsahuje zoznam rozšírení uvádzaných v CRL vydávaných Poskytovateľom, povinnosť ich uvádzania a ich kritickosť.

Tabuľka č. 9: Rozšírenia vydávaného CRL

Názov rozšírenia	Vyžadované	**Kritickosť**
Authority Key Identifier (OID: 2.5.29.35)	ÁNO	NIE
CRL Number (OID: 2.5.29.20)	ÁNO	NIE
Issuing Distribution Point (OID: : 2.5.29.28)	ÁNO	ÁNO

7.3 Profil OCSP

7.3.1 Verzia

V prípade, že Poskytovateľ vydáva OCSP odpovede, tieto musia byť v zmysle RFC 6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“ [13]. Ak budú OCSP odpovede pre jednotlivé certifikačné autority Poskytovateľa, ktoré vydávajú KC, vydávané samostatnými OCSP respondermi, ich

podpisové certifikáty musia byť podpísané zodpovedajúcimi CA Poskytovateľa a musia obsahovať rozšírenie na použitie kľúča OCSP Signing (1.3.6.1.5.5.7.3.9).

7.3.2 OCSP rozšírenia

Tabuľka č. 10 obsahuje možné rozšírenia v OCSP odpovedi OCSP responderov Poskytovateľa, povinnosť ich uvádzania a ich kritickosť.

Tabuľka č. 10: Rozšírenia v OCSP odpovedi

Názov rozšírenia	Vyžadované	**Kritickosť**
id-commonpki-at-certHash (OID: 1.3.36.8.3.13)	ÁNO	NIE
id-pkix-ocsp-nonce (OID: 1.3.6.1.5.5.7.48.1.2)	NIE	NIE
id_pkix_ocsp_archive_cutoff (OID: 1.3.6.1.5.5.7.48. 1.6)	NIE	NIE

8. Audit zhody

8.1 Témy pokrývané auditom zhody

Účelom auditu je potvrdiť, že Poskytovateľ ako kvalifikovaný poskytovateľ dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytuje, spĺňajú požiadavky stanovené v Nariadení eIDAS [3].

8.2 Frekvencia auditu zhody

Poskytovateľ sa musí aspoň každých 24 mesiacov podrobiť auditu ním poskytovaných kvalifikovaných dôveryhodných služieb.

8.3 Identita audítora a **kvalifikačné** požiadavky kladené na túto rolu

Orgán posudzovania zhody a nim poverené osoby na výkon auditu musí spĺňať požiadavky ETSI EN 319 403 „Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers“ [14] minimálne vo verzii 2.2.2.

8.4 **Vzťah** audítora k **Poskytovateľovi**

Osoba vykonávajúca audit Poskytovateľa musí spĺňať kód správania sa audítora v zmysle Prílohy A ETSI EN 319 403 minimálne vo verzii 2.2.2.

8.5 Akcie vykonané na odstránenie nedostatkov

Keď audítor zistí rozpor medzi prevádzkou Poskytovateľa a platnými požiadavkami alebo ustanoveniami CP a vydaných CPS, musia sa uskutočniť tieto akcie:

- rozpor musí byť zaznamenaný,
- audítor musí upovedomiť o rozpore subjekty definované v odstavci 8.6,
- PMA musí určiť vhodné opatrenie na nápravu.

8.6 Zaobchádzanie s výsledkami auditu

Orgán posudzovania zhody musí výsledky auditu predložiť v písomnej forme auditovanému subjektu, ktorý na ich základe musí prijať a vykonať potrebné

nápravné opatrenia. Vykonanie opatrení na nápravu musí byť dané na vedomie orgánu posudzovania zhody.

Poskytovateľ je povinný predložiť výslednú správu o posúdení zhody orgánu dohľadu v lehote troch pracovných dní od jej doručenia.

9. Iné obchodné a právne záležitosti

9.1 Poplatky

Povinnosťou Poskytovateľa je vhodným spôsobom zverejniť platný cenník svojich kvalifikovaných dôveryhodných služieb resp. informáciu za akých zmluvných podmienok je možné získať kvalifikované dôveryhodné služby.

Poplatky za kvalifikované dôveryhodné služby poskytované Poskytovateľom uhrádza Zákazník.

9.1.1 Poplatky za vydanie certifikátu

Poskytovateľ zverejňuje platný cenník svojich služieb prostredníctvom svojho webového sídla (pozri kapitola 1).

Ceny certifikátov môže Poskytovateľ so Zákazníkom dohodnúť aj individuálne, napr. na základe zmluvy alebo ponuky a záväznej objednávky. V takom prípade sa na poskytnutie služieb Poskytovateľa všeobecný cenník neuplatní.

V prípade ak dôjde k vydaniu kvalifikovaných certifikátov Poskytovateľa prostredníctvom externej registračnej autority, je táto registračná autorita povinná účtovať za kvalifikovaný certifikát cenu podľa platného cenníka Poskytovateľa. Registračná autorita si môže účtovať vo svojom mene dodatočné poplatky, napr. súvisiace so sprostredkovaním služby.

9.1.2 Poplatok za prístup k certifikátu

Poskytovateľ poskytuje online prístup k informácii o vydaných kvalifikovaných certifikátoch zadarmo pre Spoliehajúce sa strany prostredníctvom svojho webového sídla (pozri kapitola 1).

9.1.3 Poplatky za zrušenie alebo overenie statusu certifikátu

Poskytovateľ poskytuje službu zrušenia certifikátov ako aj službu overenia statusu certifikátov spočívajúcu vo vydávaní CRL a OCSP odpovede pre Spoliehajúce sa strany zadarmo.

9.1.4 Poplatky za ostatné služby

Poskytovateľ môže účtovať poplatky aj za ďalšie pridružené dôveryhodné služby požadované Zákazníkom v zmysle platného cenníka alebo na základe individuálnej dohody so Zákazníkom.

9.1.5 Vrátenie poplatku

Poskytovateľ môže v odôvodnených prípadoch na základe individuálneho posúdenia vrátiť platbu za poskytnuté služby Zákazníkovi.

9.2 **Finančná zodpovednosť**

Poskytovateľ musí mať dostatočné zdroje na výkon ním poskytovaných dôveryhodných služieb a/alebo získať vhodné poistenie zodpovednosti, aby zostal solventný a bol prípadne schopný nahradiť škodu v prípade súdneho rozhodnutia resp. uzavretia zmieru, v súvislosti s poskytovaním týchto služieb.

9.2.1 Poistenie

Poskytovateľ musí byť poistený v súvislosti s možnými škodami, ktoré môžu byť spôsobené Držiteľom certifikátov resp. tretím stranám v súvislosti s poskytovaním dôveryhodných služieb.

9.2.2 Iné aktíva

Žiadne ustanovenia.

9.2.3 Poistenie a záruky pre koncových **používateľov**

Žiadne ustanovenia

9.3 **Dôvernosť**

Poskytovateľ ako aj Zákazník sú povinní pristupovať k údajom získaným v súvislosti s poskytovanými kvalifikovanými dôveryhodnými službami v súlade s príslušnými právnymi predpismi.

9.3.1 Dôverné informácie

9.3.2 Dôverné informácie

Dôvernými informáciami podliehajúcimi zodpovedajúcej ochrane sú:

- súkromný kľúč Poskytovateľa používaný na podpisovanie vyhotovovaných KC,
- súkromný kľúč autority časovej pečiatky používaný na podpisovanie vydaných časových pečiatok,

- súkromný kľúč OCSP respondera, používaný na podpisovanie odpovedí na požiadavky na potvrdenie existencie a platnosti KC,
- súkromné kľúče patriace k služobným certifikátom (napr. certifikáty patriace pracovníkom RA a pod.),
- interná infraštruktúra (napr. dokumenty, postupy, súbory, skripty, heslá, pass frázy a pod.) slúžiaca na prevádzku Poskytovateľa, vrátane jej RA,
- osobné údaje Držiteľov certifikátov podliehajúce ochrane v zmysle zákona č. 122/2013 Z. z.,

a prípadne ďalšie technické, obchodné alebo výrobné údaje alebo iné informácie, ktoré nie sú verejne prístupné a ktoré sú označené Poskytovateľom alebo Zákazníkom ako dôverné. Dôvernými informáciami môžu byť najmä, avšak nie výlučne, komerčné informácie, know-how, dáta, dokumentácie, špecifikácie, postupy a procesy, analýzy, informácie týkajúce sa na klientov alebo obchodných partnerov alebo iné informácie z informačného systému Poskytovateľa, resp. jeho Zákazníkov v akejkoľvek podobe.

So všetkými dôvernými informáciami, sa má zaobchádzať ako s citlivými informáciami a prístup k nim má byť obmedzený len na osoby, ktoré tieto informácie nevyhnutne potrebujú na výkon svojich oficiálnych povinností.

9.3.3 Informácie nepovažované za dôverné

Dôvernými informáciami nie sú, prípadne prestávajú byť informácie, ktoré:

- sú v dobe ich prijatia druhou stranou verejne dostupnými alebo sa takými stanú následne bez toho, aby druhá strana porušila povinnosti podľa tejto politiky, alebo
- boli druhej známe ich sprístupnením v súvislosti s poskytovanými dôveryhodnými službami, alebo
- boli druhou stranou preukázateľne získané od tretej osoby, ktorá je preukázateľne oprávnená šíriť takéto informácie, alebo
- boli druhou stranou nezávisle vyvinuté bez toho, aby došlo k neoprávnenej manipulácii s dôvernými informáciami alebo
- sú všeobecne známe aj napriek ich označeniu druhou stranou ako dôverné.

9.3.4 **Zodpovednosť** za ochranu dôverných informácií

Zákazník ako aj Poskytovateľ sú v prípade získania dôverných informácií alebo prístupu k nim, povinní chrániť ich pred prezradením a zdržať sa ich použitia alebo poskytnutia/prezradenia tretej strane.

V prípade, ak by mali byť tretej strane v rámci výkonu jej činnosti pre Poskytovateľa poskytnuté alebo sprístupnené dôverné informácie, Poskytovateľ uzatvorí s touto treťou stranou zmluvu o mlčanlivosti, resp. zmluvu o poskytnutí dôverných informácii, ktorej obsahom sú aj vyššie uvedené povinnosti.

Poskytovateľ môže za určitých okolností poskytnúť určité dôverné informácie tretej strane, najmä v prípade:

- povinného poskytnutia informácii orgánu dozoru,
- povinného poskytnutia informácii v trestnom konaní, občianskom súdnom konaní alebo správnom konaní,
- poskytnutia informácii na požiadanie dotknutej osoby.

9.4 Ochrana osobných údajov

9.4.1 Politika ochrany osobných údajov

Poskytovateľ musí pri spracovaní osobných údajov dodržiavať požiadavky zákona č. 122/2013 Z. z. [12] Zaväzuje sa prijať primerané technické a organizačné opatrenia pred neautorizovaným alebo nezákonným spracovaním osobných údajov a pred náhodnou stratou, zničením alebo poškodením osobných údajov a zdokumentovať ich v bezpečnostnom projekte.

Poskytovateľ zabezpečí dôvernosť a integritu osobných údajov získaných v rámci procesu v vyhotovovania kvalifikovaného certifikátu, a to aj v prípade ich prenosu medzi Poskytovateľom a Zákazníkom či medzi jednotlivými komponentmi systému Poskytovateľa.

Niektoré osobné údaje bude Poskytovateľ uchovávať, aby splnil svoje zákonné povinnosti a aby zabezpečil chod svojich podnikateľských aktivít.

9.4.2 Informácie považované za súkromné

Poskytovateľ považuje za súkromné akékoľvek osobné údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.

9.4.3 Informácie, ktoré nie sú považované za súkromné

Poskytovateľ môže v súlade so zákonom č. 122/2013 Z. z. definovať typy informácií, ktoré spracováva pri poskytovaní kvalifikovaných dôveryhodných služieb a nie sú považované za osobné údaje.

Poskytovateľ môže na základe písomného súhlasu Držiteľa certifikátu na svojom webovom sídle zverejniť alebo sprístupniť informáciu o vydaní kvalifikovaného certifikátu s menom jeho Držiteľa.

9.4.4 **Zodpovednosť** za ochranu osobných údajov

Poskytovateľ bude bezpečne uchovávať a ochraňovať osobné údaje spracúvané v súvislosti s vyhotovovaním kvalifikovaného certifikátu. Tieto údaje bude chrániť prijatím vhodných bezpečnostných opatrení, a to najmä pred neautorizovaným prístupom, zmenou alebo prezradením.

9.4.5 **Informačná povinnosť** a súhlas

Poskytovateľ je povinný pri plnení informačnej povinnosti voči dotknutým osobám a pri získavaní ich súhlasu so spracovaním osobných údajov postupovať v súlade s požiadavkami zákona č. 122/2013 Z. z.

9.5 Ochrana práv duševného vlastníctva

Poskytovateľ je nositeľom autorských práv k všetkým dokumentom, databázam, postupom, politikám, poriadkom, pravidlám, certifikátom a súkromným kľúčom, ktoré sú súčasťou infraštruktúry Poskytovateľa a ktoré boli vytvorené Poskytovateľom.

9.6 Vyhlásenie a záruky

Poskytovateľ prostredníctvom tejto CP a zmluvy o vydaní certifikátu vyjadruje právne predpoklady používania vydaných kvalifikovaných certifikátov ich Držiteľmi a spoliehajúcimi sa stranami.

9.6.1 Vyhlásenia a záruky **Poskytovateľa**

Pokiaľ ide o poskytované dôveryhodné služby Poskytovateľ neposkytuje žiadne vyhlásenia ani záruky s výnimkou prípadov uvedených v tejto CP a nadväzujúcich CPS.

Poskytovateľ si vyhradzuje právo, ak to uzná za vhodné, na zmenu týchto vyhlásení a to na základe vlastného uváženia alebo v súlade s platnou legislatívou.

Poskytovateľ v rozsahu stanovenom v jednotlivých častiach tejto CP resp. vydaných CPS deklaruje:

- dodržiavanie svojich povinností v zmysle tejto CP, vydaných CPS ako aj ďalších publikovaných politík a postupov, vrátane politiky informačnej bezpečnosti,
- plnenie svojich povinností v zmysle platnej legislatívy SR a Nariadenia eIDAS,
- zavedenie bezpečnostných mechanizmov, vrátane mechanizmov pri generovaní a ochrane súkromného kľúča, týkajúcich sa ochrany svojej PKI infraštruktúry,
- okamžité informovanie dotknutých subjektov v prípade kompromitácie svojich súkromných kľúčov v súlade s touto CP,
- dostupnosť tlačenej resp. elektronickej verzie tejto CP a ďalších publikovaných politík online,
- správnosť informácii nachádzajúcich sa vo vyhotovených kvalifikovaných certifikátoch podľa najlepšieho vedomia Poskytovateľa a súlad vydaných kvalifikovaných certifikátov s požiadavkami Nariadenia eIDAS,
- skutočnosť, že Držiteľ sa stáva resp. je vlastníkom súkromného kľúča v čase vyhotovovania kvalifikovaného certifikátu v zmysle tejto CP,
- dodržiavanie zákona č. 122/2013 Z. z. pri zaobchádzaní s osobnými údajmi Držiteľov.

9.6.2 Vyhlásenia a záruky RA

Registračné autority poskytujúce kvalifikované dôveryhodné služby Poskytovateľ na základe zmluvného vzťahu deklarujú, že:

- ich obchodné aktivity sú vykonávané s použitím vhodného hardvérového vybavenia a softvéru odporúčaného Poskytovateľom,
- vynaložia maximálnu snahu na zabezpečenie toho, že identifikačné údaje Držiteľa certifikátu uložené v IS Poskytovateľa budú správne a potvrdené v čase ich zadania,
- ich služby sú poskytované na základe postupov, ktoré sú prispôsobené tejto CP a CPS vydaným pre potreby RA,
- budú chrániť osobné údaje Držiteľov certifikátov v zmysle požiadaviek zákona č. 122/2013 Z. z.,
- súkromné kľúče pracovníkov RA budú používané v súlade s bezpečnostnými požiadavkami špecifikovanými Poskytovateľom,

- umožnia Poskytovateľovi prístup do svojich priestorov za účelom overenia, či sú všetky postupy RA vykonávané v súlade s touto CP resp. ďalšími relevantnými požiadavkami.

9.6.3 Vyhlásenie a záruky **Držiteľa**

Ak nie je v tejto CP alebo príslušnej zmluve so Zákazníkom/Držiteľom uvedené inak, Držiteľ je výlučne zodpovedný za:

- generovanie kľúčového páru súkromný kľúč/verejný kľúč v prípade, že si kľúče k žiadosti na vydanie KC generuje vo vlastnej réžii
- poskytnutie správnych a presných informácií v komunikácii s Poskytovateľom
- oboznámenie sa a súhlas so všetkými podmienkami danými v tejto CP a s ňou spojenými politikami, ktoré sú dostupné v úložisku Poskytovateľa (pozri kapitola 1)
- používanie vydaných KC len na právne účely a účely autorizácie v súlade s touto CP
- ukončenie používania KC, pokiaľ sa ukáže, že akákoľvek informácia v nich je zavádzajúca, neaktuálna alebo nesprávna.
- vyvinutie maximálneho úsilia na zabránenie kompromitácie, straty, odtajnenie, modifikácie alebo akéhokoľvek neautorizovaného použitia súkromného kľúča zodpovedajúceho verejnému kľúču, ktorý sa nachádza v KC vydanom Poskytovateľom

9.6.4 Vyhlásenia a záruky Spoliehajúcej sa strany

Spoliehajúca sa strana akceptuje, že v prípade spoliehania sa na KC vydaný Poskytovateľom, musí:

- oboznámiť sa a súhlasiť s podmienkami Poskytovateľa uvedenými v informácii pre stranu spoliehajúcu sa na certifikát, ktorá je dostupná na webovom sídle Poskytovateľa (pozri kapitola 1),
- overiť platnosť vydaného KC prostredníctvom informácií na overenie stavu certifikátu (CRL, OCSP),
- akceptovať KC len v prípade, že je platný a nebol zrušený alebo exspirovaný,
- dôverovať certifikátu vydávajúcej CA Poskytovateľa len v prípade, že je platný a nebol zrušený alebo nie je exspirovaný,
- mať na pamäti akékoľvek obmedzenie použitia KC, či už je obsiahnuté v samotnom certifikáte alebo v tejto CP resp. publikovaných CPS,

- prijať akékoľvek iné kroky na minimalizáciu rizika pri spoľahnutí sa na elektronický podpis alebo elektronickú pečať vytvorenú prostredníctvom kľúčov, kde verejný kľúč je neplatný, zrušený, exspirovaný,
- vziať do úvahy akékoľvek iné indície dôveryhodnosti resp. nedôveryhodnosti, alebo iné fakty, s ktorými je spoliehajúca sa strana oboznámená alebo bola na tieto upozornená.

9.6.5 Vyhlásenia a záruky iných strán

Žiadne ustanovenia.

9.7 Odmietnutie poskytnutia záruky

Poskytovateľ zodpovedá v zmysle čl. 13 Nariadenia eIDAS výhradne za škodu spôsobenú nesplnením svojich povinností podľa Nariadenia eIDAS.

9.8 Obmedzenie zodpovednosti

Poskytovateľ nezodpovedá za nepriame alebo podmienené straty alebo škody, ktoré Zákazníkom alebo spoliehajúcim sa stranám vznikli v súvislosti s používaním dôveryhodných služieb.

Poskytovateľ nezodpovedá za škodu (vrátane ušlého zisku), ktorá vznikla Zákazníkovi/Držiteľovi certifikátu, Spoliehajúcej sa strane príp. akýmkoľvek tretím stranám z dôvodu:

a) porušenia povinností Zákazníkom/Držiteľom certifikátu alebo Spoliehajúcou sa stranou uvedených v právnych predpisoch, zmluve, Všeobecných podmienkach alebo v politikách Poskytovateľa, vrátane povinnosti vynaložiť primeranú starostlivosť pri používaní certifikátov a pri spoliehaní sa na ne;

b) neposkytnutia potrebnej súčinnosti zo strany Zákazníka/Držiteľa certifikátu;

c) technickými vlastnosťami, konfiguráciou, nekompatibilitou, nevhodnosťou alebo inými vadami nimi použitých softvérových alebo hardvérových prostriedkov;

d) používania, resp. spoliehania sa na certifikát, ktorého platnosť uplynula alebo ktorý bol zrušený;

e) použitia certifikátu Zákazníkom/Držiteľom certifikátu v rozpore so zmluvou, Všeobecnými podmienkami alebo politikami Poskytovateľa;

f) že certifikát bol použitý v rozpore s jeho účelom, určením alebo obmedzeniami uvedenými v certifikáte, v týchto Všeobecných podmienkach resp. v politikách Poskytovateľa;

g) omeškania alebo nedoručenia požiadaviek na overenie statusu certifikátu Poskytovateľovi, z dôvodov, ktoré nie sú na strane Poskytovateľa (najmä prípady nedostupnosti alebo preťaženosti siete internet alebo vady zariadenia alebo technického vybavenia používaného overovateľom);

h) neposkytnutia niektorej z dôveryhodných služieb alebo jej nedostupnosti v priebehu plánovanej údržby alebo reorganizácie oznámenej na webovom sídle Poskytovateľa;

i) pôsobenia vyššej moci;

Poskytovateľ nezodpovedá za škody, ktoré vznikli spoliehajúcej sa strane z dôvodu, že pri spoliehaní sa na KC a dôveryhodné služby Poskytovateľa, resp. na kvalifikovaný elektronický podpis alebo pečať vyhotovené na ich základe nepostupovala podľa 10. časti Všeobecných podmienok [11] a v zmysle tejto CP.

9.9 Náhrada škody

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z tejto CP, Zmluvy a Všeobecných podmienok je povinný nahradiť škodu tým spôsobenú druhej strane, okrem prípadov kde je vylúčená zodpovednosť daného subjektu za škody. Za škodu sa považuje skutočná škoda, ušlý zisk a náklady vzniknuté poškodenej strane v súvislosti so škodovou udalosťou.

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z tejto CP, Zmluvy a Všeobecných podmienok, sa môže zbaviť zodpovednosti na náhradu škody, jedine ak preukáže, že k porušeniu povinnosti alebo akéhokoľvek záväzku, došlo v dôsledku okolností vylučujúcich zodpovednosť – vyššej moci.

9.10 Doba platnosti, ukončenie platnosti

9.10.1 Doba platnosti

Tato verzia CP platí odo dňa nadobudnutia jej platnosti t. j. 1.12.2017 až do jej nahradenia novou verziou. Podrobnosti o histórii zmien tejto CP sú uvedené na konci dokumentu v časti „História zmien“.

9.10.2 **Ukončenie** platnosti

Platnosť tejto verzie CP skončí dňom publikovania novej verzie s vyšším číslom ako je 5.1, prípadne ukončením činnosti poskytovania kvalifikovaných dôveryhodných služieb Poskytovateľom v čase jej platnosti. Všetky revízie CP a CPS ktoré sú uvedené v histórii zmien pre daný dokument musia byť k dispozícii Zákazníkom/Držiteľom resp. Spoliehajúcim sa stranám.

9.10.3 Dôsledky **ukončenia** platnosti

V prípade, že tento dokument nebude nahradený novou verziou a v čase jeho platnosti dôjde k ukončeniu poskytovania kvalifikovaných dôveryhodných služieb zo strany Poskytovateľa, musia byť dodržané všetky ustanovenia tejto CP týkajúce sa Poskytovateľa, ktoré je povinný dodržať po ukončení svojej činnosti..

9.11 Jednotlivé oznámenia a komunikácia s **účastníkmi**

Komunikácia Poskytovateľa s jednotlivých RA musí prebiehať oficiálne prostredníctvom autorizovanej e-mailovej komunikácie medzi poverenou osobou Poskytovateľa a poverenou osobou RA.

9.12 Zmeny

9.12.1 Postup vykonávania zmien

Aktualizácia CP sa vykonáva na základe jeho preskúmania, ktoré musí byť vykonané minimálne 1x ročne od schválenia aktuálne platnej verzie. Preskúmanie musí vykonať poverený pracovník Poskytovateľa, ktorý na základe výsledkov preskúmania musí spracovať písomný návrh na prípadné navrhované zmeny.

Schválenie navrhovaných zmien musí vykonať poverený člen PMA. Navrhované zmeny musia byť posúdené v lehote 14 dní od ich doručenia. Po uplynutí lehoty určenej na posúdenie návrhu na zmenu musí PMA navrhovanú zmenu prijať, prijať s úpravou alebo odmietnuť.

Chyby, požiadavky na aktualizáciu alebo navrhované zmeny CP sa musia oznámiť kontaktu uvedenému v bode 1.5.2. Takáto komunikácia musí obsahovať opis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje resp. navrhuje.

Všetky schválené zmeny CP musia byť dané na vedomie subjektom, ktorých sa týkajú, v lehote jedného týždňa pred nadobudnutím ich účinnosti, a to prostredníctvom kanálov publikačnej a oznamovacej politiky (pozri odstavec 2.2).

Každá zmenená verzia tejto CP musí byť očíslovaná a evidovaná, tak že novšia verzia musí mať vyššie číslo verzie ako tá, ktorú nahradzuje .

Opravy preklepov, gramatických a štylistických chýb sa nepovažujú za zmeny iniciujúce zmenu verzie tejto CP.

9.12.2 Postup a periodicita oznamovania zmien

Poskytovateľ musí publikovať informácie týkajúce sa aktuálnej verzie CP prostredníctvom svojho webového sídla (pozri kapitola 1).

Poverený zástupca Poskytovateľa musí informovať všetky zmluvne viazané RA Poskytovateľa o schválení novej verzie CP, zaslaním jeho verzie elektronickou poštou ešte pred nadobudnutím jeho účinnosti v zmysle bodu 9.12.1. Poskytovateľ si musí vyžiadať od RA spätnú väzbu v podobe potvrdzujúcej e-mailovej správy o prevzatí elektronickej verzie CP Poskytovateľa.

Aktuálna verzia CP musí byť k dispozícii na každej zmluvne viazanej RA Poskytovateľa minimálne v elektronickej forme. Interní zamestnanci musia byť rovnako informovaní o novej verzii tejto CP..

9.12.3 Okolnosti zmeny OID

Každá politika musí mať stanovený svoj OID Poskytovateľom. OID tejto politiky je uvedený v odstavci 1.2 a pre každú novú verziu CP zostáva nezmenený.

9.13 Riešenie sporov

Zákazník/Držiteľ má právo zaslať Poskytovateľovi sťažnosť, podnet alebo reklamáciu na poskytnutú kvalifikovanú dôveryhodnú služby emailom na radisig@disig.sk. Poskytovateľ vybaví reklamáciu najneskôr do 30 dní od jej prijatia, pokiaľ sa strany nedohodnú inak. Vybavenie reklamácie sa vzťahuje len k popisu vady uvedenej Zákazníkom.

Súdy Slovenskej republiky majú výlučnú právomoc na rozhodovanie akýchkoľvek sporov medzi Poskytovateľom a Zákazníkom/Držiteľom certifikátu. V prípade, že Zákazník/Držiteľ certifikátu je spotrebiteľom, prípadný spor môže riešiť taktiež mimosúdnou cestou.

V takomto prípade je oprávnený kontaktovať subjekt mimosúdneho riešenia sporov, ktorým je Slovenská obchodná inšpekcia alebo iná právnická osoba zapísaná v zozname subjektov alternatívneho riešenia spotrebiteľských sporov vedenom Ministerstvom hospodárstva Slovenskej republiky a dostupnom na jeho webovom sídle; Zákazník/Držiteľ má právo voľby, na ktorý z uvedených subjektov alternatívneho riešenia spotrebiteľských sporov sa obráti. Pred pristúpením k súdnemu alebo mimosúdnemu riešeniu sporu sú zmluvné strany povinné pokúsiť sa najskôr vyriešiť tento spor vzájomnou dohodou.

9.14 Rozhodné právo

Právne vzťahy medzi Poskytovateľom a Zákazníkom/Držiteľom certifikátu sa riadia právnymi predpismi Slovenskej republiky.

Práva a povinnosti zmluvných strán výslovne neupravené Všeobecnými podmienkami [11] a touto CP sa riadia najmä príslušnými ustanoveniami zákona č. 513/1991 Zb., Obchodný zákonník, v znení neskorších predpisov, zákona č. 40/1964 Zb., Občiansky zákonník v znení neskorších predpisov a ďalšími všeobecne záväznými právnymi predpismi Slovenskej republiky.

9.15 Súlad s platnými právnymi predpismi

Poskytovateľ poskytuje dôveryhodné služby v súlade s platnými právnymi predpismi platnými v Slovenskej republike.

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 Iné ustanovenia

Služby vyhotovovania KC sú dostupné prostredníctvom mobilnej registračnej autority Poskytovateľa aj osobám so zdravotným postihnutím, pokiaľ splnia všetky požiadavky VP a tejto CP.

10. Odkazy

1. RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.
2. ETSI EN 319411-2 " Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
3. Nariadenie Európskeho parlamentu a Rady (EÚ) **č.** 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES .
4. **Certifikačná** politika pre **koreňovú** CA a dôveryhodnú službu vyhotovovania kvalifikovaných certifikátov, ktorej kvalifikovaný štatút udelil Národný **bezpečnostný** úrad. s.l. : Národný **bezpečnostný** úrad.
5. Zákon **č.** 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách).
6. RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
7. X.500 Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services. *10/2012.* s.l. : ITU-T.
8. X.501 Information technology – Open Systems Interconnection – The Directory: Models. s.l. : ITU-T, 10/2012.
9. X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types. s.l. : ITU-T, 10/2012.
10. RFC5322 "Internet Message Format".
11. Všeobecné podmienky poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov Disig, a.s.
12. Zákon **č.** 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
13. RFC 6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“.
14. „Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
15. Disig, a.s. Informácia pre stranu spoliehajúcu sa na certifikát.

11. História zmien

Verzia	Dátum revízie	Popis revízie; revidoval
1.0	13.2.0007	Prvá verzia dokumentu; Miškovič
1.1	16.7.2007	Zmena názvu certifikačnej autority; Miškovič
1.5	2.1.2009	Úprava CP v súvislosti s nadobudnutím účinnosti zákona č. 214/2008 Z. z., ktorým sa novelizuje zákon č. 215/2002 Z. z. o elektronickom podpise; Miškovič
1.6	10.2.2009	Zapracovanie zmien v súvislosti s nasadením nového aplikačného rozhrania, vybudovaného nad certifikovaným produktom Disig CA Signer verzia 1.0; Miškovič
1.7	9.4.2009	Úprava CP v súvislosti s publikovaním Vyhlášok NBÚ SR č. 131 až č.136 z 26.marca 2009 v zbierke zákonov (ods. 1; 11). Spresnenie generovania kľúčov na QSCD (ods. 3.1; 3.1.5); spresnenie uvádzania odkazu na identitu fyzickej osoby (ods. 3.1.2; 4.1.1; 7.1); doplnenie definícii certifikátov na správu (1.3.1.2; 7)
1.8	10.12.2009	Úprava v súvislosti so znením §13 ods. 1) Vyhlášky NBÚ č. 135/2009 z 26. marca 2009.
2.0	18.12.2009	Zmena certifikátu akreditovanej CA Disig; zmena podpisového algoritmu; zmena profilu KC.
3.0	06.09.2010	Zapracovanie navrhnutých nápravných opatrení z auditu z 09/2009; Miškovič
3.1	29.12.2011	Zmena platnosti vydávaných KC; čiastočné úpravy textov v súvislosti so spresnením pojmov; Miškovič
3.2	30.12.2011	Revízia CP s úpravami doby platnosti TSA a OCSP certifikátu a akceptovania dokumentov podpísaných ZEP; spresnenie vydávania mandátnych certifikátov v zmysle §7 ods. 3 písm. b až d) Zákona č. 215/2002 Z. z.; Miškovič
4.0	24.11.2014	Revízia CP v súvislosti s novelou zákona o elektronickom podpise v zmysle zákona č. 305/2013 Z. z.; Miškovič
4.5	18.10.2016	Vykonané zmeny v súvislosti s Nariadením eIDAS a v súvislosti s ukončením platnosti zákona č. 215/2002 Z. z. a nadobudnutím účinnosti zákona č. 272/2016 Z. z.; Miškovič
5.0	2.5.2017	Komplexná revízia v súvislosti s nadobudnutím účinnosti Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014; Zmena štruktúry v zmysle RFC 3647; Miškovič
5.1	24.11.2017	Overovanie identity fyzickej osoby, právnickej osoby – doplnenie (3.2); Úprava profilu kvalifikovaného certifikátu pre autentifikáciu webového sídla (7.1.4); Miškovič