



Pravidlá

poskytovania dôveryhodnej služby
vyhotovovania a overovania TLS certifikátov -
časť: RA



Disig, a.s.

Vypracoval	Disig, a.s.
Dátum platnosti	10. 1. 2025
Verzia	6.3
Typ	PRAVIDLÁ
Schválil	Ing. Ľuboš Batěk

Obsah

1.	ÚVOD	10
1.1	Prehľad	10
1.2	Identifikácia	10
1.2.1	História zmien	11
1.3	Komunita a použiteľnosť	13
1.3.1	Certifikačné authority	13
1.3.2	Registračné authority	13
1.3.3	Zákazník a Držiteľ certifikátu	13
1.3.4	Strany spoliehajúce sa na certifikáty	13
1.3.5	Iní účastníci	14
1.4	Použiteľnosť certifikátov	14
1.4.1	Vhodné použitie certifikátov	14
1.4.2	Nedovolené použitie certifikátov	14
1.5	Správa pravidiel	14
1.5.1	Organizácia zodpovedná za správu pravidiel	14
1.5.2	Kontaktná osoba	14
1.5.3	Osoba rozhodujúca o súlade CPS s CP	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	15
1.6.3	Odkazy	15
2.	ZVEREJŇOVANIE INFORMÁCIÍ A ÚLOŽISKO	17
2.1	Úložiská	17
2.2	Zverejňovanie informácií o CA/RA	17
2.3	Frekvencia zverejňovania informácií	17
2.4	Kontroly prístupu	17
3.	IDENTIFIKÁCIA A AUTENTIZÁCIA	18
3.1	Mená	18
3.1.1	Typy mien	18
3.1.2	Potreba zmysluplnosti mien	18
3.1.3	Anonymita a používanie pseudonymov	18
3.1.4	Pravidlá na interpretáciu rôznych foriem mien	18
3.1.5	Jedinečnosť mien	18
3.1.6	Rozpoznanie, autentizácia a rola obchodných značiek	18
3.2	Počiatočné overenie identity	18
3.2.1	Preukazovanie vlastníctva súkromného kľúča	18

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 2/53

3.2.2	Autentizácia identity právnickej osoby a identity domény	18
3.2.3	Autentizácia identity fyzickej osoby	22
3.2.4	Neoverované informácie o Držiteľovi	25
3.2.5	Overovanie oprávnení	26
3.2.6	Kritériá interoperability	26
3.3	Identifikácia a autentifikácia pri vydávaní následného certifikátu	26
3.3.1	Identifikácia a autentifikácia pri rutinnom vydávaní následného certifikátu po zrušení predchádzajúceho	26
3.3.2	Identifikácia a autentifikácia pri vydávaní následného certifikátu po zrušení predchádzajúceho	26
3.4	Identifikácia a autentifikácia pri žiadaní o zrušenie certifikátu	26
4.	POŽIADAVKY NA ŽIVOTNÝ CYKLUS CERTIFIKÁTU	27
4.1	Žiadanie o certifikát	27
4.1.1	Kto môže žiadať o vydanie certifikátu	27
4.1.2	Registračný proces a zodpovednosti	27
4.2	Spracovanie žiadosti a vydanie certifikátu	27
4.2.1	Vykonanie identifikácie a autentifikácie	27
4.2.2	Schválenie alebo zamietnutie žiadosti o certifikát	28
4.2.3	Doručenie verejného kľúča vydavateľovi certifikátu	28
4.3	Vydanie certifikátu	29
4.3.1	Činnosť CA pri vydávaní certifikátu	29
4.3.2	Informovanie Držiteľa o vydaní certifikátu	29
4.4	Prevzatie certifikátu	29
4.4.1	Spôsob prevzatia certifikátu	29
4.4.2	Zverejňovanie certifikátu	29
4.4.3	Oznámenie o vydaní certifikátu iným subjektom	29
4.5	Kľúčový pár a používanie certifikátu	29
4.5.1	Používanie súkromného kľúča a certifikátu Držiteľom	29
4.5.2	Používanie verejného kľúča a certifikátu Spoliehajúcou sa stranou	29
4.6	Obnova certifikátu	29
4.6.1	Okolnosti pre obnovenie certifikátu	29
4.6.2	Kto môže požiadať o obnovenie	30
4.6.3	Spracovanie žiadostí o obnovenie certifikátu	30
4.6.4	Oznámenie o vydaní nového certifikátu držiteľovi	30
4.6.5	Spôsob prevzatia obnoveného certifikátu	30
4.6.6	Zverejňovanie obnoveného certifikátu zo strany Poskytovateľa	30
4.6.7	Oznámenie o vydaní obnoveného certifikátu iným subjektom	30
4.7	Vydanie certifikátu na nové kľúče	30
4.7.1	Podmienky vydania certifikátu na nové kľúče	30
4.7.2	Kto môže žiadať o vydanie certifikátu na nové kľúče	30
4.7.3	Postup žiadania o vydanie certifikátu na nové kľúče	30

4.7.4	Oznámenie o vydaní certifikátu na nové kľúče Držiteľovi	30
4.7.5	Spôsob prevzatia certifikátu vydaného na nové kľúče	30
4.7.6	Zverejňovanie certifikátov zo strany Poskytovateľa	30
4.7.7	Oznámenie o vydaní certifikátu CA iným subjektom	31
4.8	Modifikácia certifikátu	31
4.8.1	Okolnosti pre modifikovanie certifikátu	31
4.8.2	Kto môže požiadať o modifikáciu certifikátu	31
4.8.3	Spracovanie žiadostí o modifikáciu certifikátu	31
4.8.4	Oznámenie o vydaní nového certifikátu držiteľovi	31
4.8.5	Spôsob prevzatia modifikovaného certifikátu	31
4.8.6	Zverejňovanie modifikovaného certifikátu zo strany Poskytovateľa	31
4.8.7	Oznámenie o vydaní modifikovaného certifikátu iným subjektom	31
4.9	Zrušenie a suspendovanie certifikátu	31
4.9.1	Podmienky zrušenia certifikátu	31
4.9.2	Kto môže žiadať o zrušenie certifikátu	31
4.9.3	Postup žiadosti o zrušenie certifikátu	32
4.9.4	Čas na podanie žiadosti o zrušenie certifikátu	32
4.9.5	Čas na spracovanie žiadosti o zrušenie certifikátu	32
4.9.6	Overovanie platnosti zo strany spoliehajúcej sa strany	33
4.9.7	Frekvencia vydávania CRL	33
4.9.8	Doba publikovania CRL	33
4.9.9	Dostupnosť služby OCSP	33
4.9.10	Požiadavky na OCSP overovanie	33
4.9.11	Iné formy dostupnosti informácií o zrušení certifikátu	33
4.9.12	Špeciálne požiadavky na zmenu kľúčov po ich kompromitácii	33
4.9.13	Okolnosti pozastavenia platnosti certifikátu	33
4.9.14	Suspendovanie certifikátu	33
4.9.15	Postup pre pozastavenie platnosti certifikátu	33
4.9.16	Limity pre obdobie pozastavenia	33
4.10	Služby súvisiace so stavom certifikátu	33
4.10.1	Prevádzkové charakteristiky	33
4.10.2	Dostupnosť služieb	34
4.10.3	Doplňkové funkcie	34
4.11	Ukončenie poskytovanie služieb	34
4.12	Uchovávanie a obnova kľúčov	34
4.12.1	Politika a postupy uchovávania a obnovy kľúčov	34
4.12.2	Politika a postupy ochrany „session key“	34
5.	FYZICKÉ, PROCEDURÁLNE A PERSONÁLNE BEZPEČNOSTNÉ OPATRENIA	35
5.1	Opatrenie týkajúce sa fyzickej bezpečnosti	35
5.1.1	Priestory	35
5.1.2	Fyzický prístup	35
5.1.3	Zásobovanie elektrickou energiou a klimatizácia	35

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 4/53

5.1.4	Ochrana pre vodou	35
5.1.5	Ochrana pred ohňom	35
5.1.6	Úložisko médií	35
5.1.7	Nakladanie s odpadom	36
5.1.8	Zálohovanie off-site	36
5.2	Procedurálne bezpečnostné opatrenia	36
5.2.1	Dôveryhodné role	36
5.2.2	Počet osôb v jednotlivých rolách	36
5.2.3	Identifikácia a autentizácia pre každú rolu	36
5.2.4	Role vyžadujúce oddelenie zodpovedností	37
5.3	Personálne bezpečnostné opatrenia	37
5.3.1	Požiadavky na kvalifikáciu, skúsenosti a previerky	37
5.3.2	Požiadavky na previerky	37
5.3.3	Požiadavky na školenia	37
5.3.4	Požiadavky na frekvenciu obnovy školení	37
5.3.5	Rotácia rolí	38
5.3.6	Postihy za neoprávnenú činnosť	38
5.3.7	Požiadavky na externých dodávateľov	38
5.3.8	Dokumentácia dodávané pre personál	38
5.4	Postupu získavania auditných záznamov	38
5.4.1	Typy zaznamenávaných udalostí	38
5.4.2	Frekvencia spracovávaní auditných záznamov	38
5.4.3	Uchovávanie logov	39
5.4.4	Ochrana auditných záznamov	39
5.4.5	Postupy zálohovania auditných logov	39
5.4.6	Systém zálohovania logov	39
5.4.7	Notifikácia subjektu iniciujúceho log záznam	39
5.4.8	Posudzovanie zraniteľností	39
5.5	Uchovávanie záznamov	39
5.5.1	Typy archivovaných záznamov	39
5.5.2	Doba uchovávaní záznamov	39
5.5.3	Ochrana archívnych záznamov	39
5.5.4	Zálohovanie archívnych záznamov	39
5.5.5	Požiadavky na pridávanie časových pečiatok k záznamom	40
5.5.6	Archivačný systém	40
5.5.7	Postup získania a overenia archívnych informácií	40
5.6	Zmena kľúčov pracovníka RA	40
5.7	Obnova po kompromitácii alebo havárii	40
5.7.1	Postupy riešenia incidentov a kompromitácie	40
5.7.2	Poškodenie hardvéru, softvéru alebo údajov	40
5.7.3	Postupy pri kompromitácii kľúča CA	40
5.7.4	Zachovanie kontinuity činnosti po havárii	40
5.8	Ukončenie činnosti RA	40

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 5/53

6.	TECHNICKÉ BEZPEČNOSTNÉ OPATRENIA	41
6.1	Generovanie a inštalácia páru kľúčov	41
6.1.1	Generovanie a inštalácia páru pre jednotlivé subjekty	41
6.1.2	Doručenie súkromného kľúča držiteľovi certifikátu	41
6.1.3	Doručenie verejného kľúča vydavateľovi certifikátu	41
6.1.4	Doručenie verejného kľúča CA spoliehajúcim sa stranám	41
6.1.5	Dĺžky kľúčov	41
6.1.6	Parametre a kvalita verejného kľúča	42
6.1.7	Použitie kľúčov	42
6.2	Ochrana súkromného kľúča a technické opatrenia pre kryptografický modul	42
6.2.1	Štandardy a opatrenia pre kryptografický modul	42
6.2.2	Opatrenia (K z N) pre manipuláciu so súkromným kľúčom	42
6.2.3	„Key escrow“ súkromného kľúča	42
6.2.4	Zálohovanie súkromného kľúča	42
6.2.5	Archivácia súkromného kľúča	42
6.2.6	Prenos súkromných kľúčov z a do HSM modulu	42
6.2.7	Uchovávanie súkromných kľúčov v HSM module	42
6.2.8	Spôsob aktivácie súkromných kľúčov	42
6.2.9	Spôsob deaktivácie súkromného kľúča	42
6.2.10	Spôsob zničenia súkromného kľúča	43
6.2.11	Charakteristika HSM modulu	43
6.3	Ďalšie aspekty manažmentu kľúčového páru	43
6.3.1	Archivácia verejných kľúčov	43
6.3.2	Dĺžka platnosti certifikátov a použiteľnosť kľúčového páru	43
6.4	Aktivačné údaje	43
6.4.1	Vytváranie a inštalácia aktivačných údajov	43
6.4.2	Ochrana aktivačných údajov	43
6.4.3	Ostatné aspekty aktivačných údajov	43
6.5	Riadenie bezpečnosti počítačov	43
6.5.1	Špecifické požiadavky na bezpečnosť počítačov	43
6.5.2	Hodnotenie bezpečnosti informácií	44
6.6	Opatrenia v životnom cykle	44
6.6.1	Opatrenia pri vývoji systémov	44
6.6.2	Opatrenia na riadenie bezpečnosti	44
6.6.3	Bezpečnostné opatrenia v životnom cykle	44
6.7	Sietové bezpečnostné opatrenia	44
6.8	Využívanie časovej pečiatky	44
7.	PROFILY CERTIFIKÁTOV A ZOZNAMOV ZRUŠENÝCH CERTIFIKÁTOV	45
7.1	Profily certifikátov	45
7.1.1	Verzia	45

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 6/53

7.1.2	Obsah a rozšírenia certifikátu	45
7.1.3	Identifikátory použitých algoritmov	45
7.1.4	Kódovanie názvov	45
7.1.5	Obmedzenia týkajúce sa mien	45
7.1.6	Identifikátor pravidiel CPS	45
7.1.7	Použitie rozšírení na obmedzenie politiky	45
7.1.8	Syntax a sémantika politiky	45
7.1.9	Sémantika spracovania kritických certifikačných politík	45
7.1.10	Ostatné ustanovenia	45
7.2	Profily zoznamov zrušených certifikátov	46
7.2.1	Verzia	46
7.2.2	Použité rozšírenia (CRL extensions) v CRL vydávanom Poskytovateľom	46
7.3	Profil OCSP	46
7.3.1	Verzia	46
7.3.2	OCSP rozšírenia	46
8.	AUDIT ZHODY	47
8.1	Frekvencia auditu zhody pre danú entitu	47
8.2	Identita audítora a kvalifikačné požiadavky na neho	47
8.3	Vzt'ah audítora k auditovanému subjektu	47
8.4	Témy pokryté audiom	47
8.5	Akcie vykonané na odstránenie nedostatkov	47
8.6	Zaobchádzanie s výsledkami auditu	47
8.7	Interný audit	47
9.	INÉ OBCHODNÉ A PRÁVNE ZÁLEŽITOSTI	48
9.1	Poplatky	48
9.1.1	Poplatky za vydanie certifikátu	48
9.1.2	Poplatok za prístup k certifikátu	48
9.1.3	Poplatky za služby vydávania CRL a OCSP	48
9.1.4	Poplatky za ostatné služby	48
9.1.5	Vrátenie platby	48
9.2	Finančná zodpovednosť	48
9.2.1	Poistenie	48
9.2.2	Iné aktíva	48
9.2.3	Poistenie a záruky pre Zákazníkov	48
9.3	Dôvernosc'	49
9.3.1	Typy informácií, ktoré sa majú chrániť	49
9.3.2	Nechránené informácie	49
9.3.3	Zodpovednosť za ochranu dôverných informácií	49
9.4	Ochrana osobných údajov	49

9.4.1	Politika ochrany osobných údajov	49
9.4.2	Informácie považované za osobné údaje	49
9.4.3	Informácie, ktoré nie sú považované za osobné údaje	49
9.4.4	Zodpovednosť za ochranu osobných údajov	49
9.4.5	Súhlas so spracovaním osobných údajov	49
9.4.6	Zverejnenie na základe súdneho alebo správneho procesu	49
9.4.7	Ďalšie okolnosti zverejňovania informácií	50
9.5	Práva duševného vlastníctva	50
9.6	Vyhlásenie a záruky	50
9.6.1	Vyhlásenia a záruky Poskytovateľa	50
9.6.2	Vyhlásenia a záruky RA	50
9.6.3	Vyhlásenie a záruky Držiteľa	50
9.6.4	Vyhlásenia a záruky spoliehajúcej sa strany	50
9.6.5	Vyhlásenia a záruky iných strán	50
9.7	Odmietnutie poskytnutia záruky	50
9.8	Obmedzenie zodpovednosti	50
9.9	Náhrada škody	51
9.10	Doba platnosti, ukončenie platnosti	51
9.10.1	Doba platnosti	51
9.10.2	Ukončenie platnosti	51
9.10.3	Dôsledky ukončenia platnosti	51
9.11	Jednotlivé oznámenia a komunikácia s účastníkmi	51
9.12	Zmeny	51
9.12.1	Postup vykonávania zmien	51
9.12.2	Postup a periodicita oznamovania zmien	52
9.12.3	Okolnosti zmeny OID	52
9.13	Riešenie sporov	52
9.14	Rozhodné právo	52
9.15	Súlad s platnými právnymi predpismi	52
9.16	Rôzne ustanovenia	52
9.16.1	Rámcová dohoda	52
9.16.2	Postúpenie práv	52
9.16.3	Salvátorská klauzula	52
9.16.4	Uplatnenie práv	53
9.16.5	Vyššia moc	53
9.17	Iné ustanovenia	53

Obchodné meno	Disig, a.s.
Sídlo	Galvaniho 17/C, 821 04 Bratislava
Zapísaná v OR	Mestského súdu Bratislava III, odd. Sa 3794/B
Telefón	+ 421 2 208 50 140
Fax	+ 421 2 208 50 141
E-mail	disig@disig.sk

Všetky práva vyhradené.

© Disig, a.s.

Informácie v tomto dokumente nesmú byť menené bez písomného súhlasu Disig, a.s.

Tento dokument neprešiel jazykovou úpravou.

Ochranné známky

Mená produktov uvádzané v tomto dokumente môžu byť registrované ochranné známky príslušných firiem.

1. Úvod

Tento dokument definuje pravidlá poskytovania dôveryhodnej služby vyhotovovania a overovania TLS certifikátov - časť: RA (Certificate Practice Statement, ďalej len „CPS“) pre registračné authority (ďalej len „RA“) spoločnosti Disig ako poskytovateľa dôveryhodných služieb (ďalej len „Poskytovateľ“). CPS vychádzajú z dokumentu „Politika poskytovania dôveryhodnej služby vyhotovovania a overovania TLS certifikátov“ (OID=1.3.158.35975946.0.0.0.1.1) [1] Poskytovateľa (ďalej len „CP CA Disig“). Aktuálna verzia CP CA Disig, na ktorú sa viažu tieto CPS je verzia 6.3 s platnosťou od 10. 1. 2025.

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

<http://eidas.disig.sk>

1.1 Prehľad

CPS boli vytvorené na základe materiálov Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework (RFC3647) [2]; Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (RFC5280) [3], Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [4], „), požiadavkami jednotlivých programov pre koreňové certifikáty distribuované spoločnosťami Microsoft [5], Mozilla [6], Apple [7], Google [8] a Nariadenia Európskeho parlamentu a Rady EÚ č. 910/2014 [9].

Poskytovateľ potvrdzuje, že v týchto CPS sú zohľadnené všetky požiadavky aktuálnej verzie dokumentu [4], ktorý je publikovaný na stránke <http://www.cabforum.org>. V prípade akýchkoľvek rozporuplností medzi týmito požiadavkami a týmito CPS, majú prednosť požiadavky dané aktuálnou verziou dokumentu [4].

Tieto pravidlá sú štruktúrované v súlade s RFC 3647 [2].

1.2 Identifikácia

Názov:	Pravidlá Poskytovania dôveryhodnej služby vyhotovovania a overovania TLS certifikátov - časť: RA
Skratka názvu:	CPS RA CA Disig
Verzia:	6.3
Schválené dňa:	30. 12. 2024
Platnosť od:	10. 1. 2025
Tomuto dokumentu je priradený identifikátor objektu (OID):	1.3.158.35975946.0.0.0.1.3

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 10/53

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, a. s.

1.3.158.35975946.0.0.0.1.- CA Disig

1.3.158.35975946.0.0.0.1.3. - CPS RA CA Disig

Tieto CPS sa týkajú verejne dôveryhodných certifikátov pre autentizáciu webového sídla (TLS certifikát) vydávaných Poskytovateľom.

Pokiaľ v pravidlách nie je vyslovene uvedené, že sa to týka certifikátu koreňovej certifikačnej autority resp. podriadenej certifikačnej autority, tak slovo „certifikát“ znamená TLS certifikát koncovej entity.

1.2.1 História zmien

Verzia	Dátum revízie	Popis revízie; revidoval
1.0	25.03.2006	Prvá verzia dokumentu; Miškovič
1.5	20.12.2006	Formálne úpravy textu dokumentu - formátovanie, opravy odkazov, úpravy textu v kapitole 4 „Prevádzkové požiadavky“; Miškovič
3.0	19.03.2008	Celková revízia CP vzhľadom k jednotlivým typom certifikátov; Ďurišová, Miškovič.
3.1	24.06.2008	Pridanie nového typu certifikátu; Miškovič
3.2	10.11.2008	Zrušenie prevádzky na Záhradníckej 153.
3.3	25.11.2008	Úprava znenia: ods. 3.1.9 - overovanie vlastníctva domény ods. 4.1.1, 4.1.2, - overovanie platnosti e-mail adresy žiadateľa
3.4	02.06.2009	Úprava v súvislosti s požiadavkou na minimálnu dĺžku verejného kľúča, na ktorý CA Disig vydá certifikát (ods.5.1.3; 6.1.2); Zmena umiestnenia e-mail adresy v profile certifikátu (ods. 3.1.2; 6.1.2); Miškovič
4.0	14.10.2009	Úprava v súvislosti s požiadavkami Mozilla Foundation pri uchádzaní sa o umiestnenie certifikátu CA Disig do Mozilla Root Certificate Store
4.1	11.05.2010	Zapracovanie navrhnutých nápravných opatrení z auditu zo dňa 13.11.2009 (audit podľa ETSI TS 102042 V1.3.4); Miškovič
4.2	11.03.2011	Zmena dĺžky platnosti certifikátov; zapracovanie požiadaviek novej bezpečnostnej politiky Mozilla Foundation a požiadaviek Microsoft (code signing); formálne úpravy tabuliek a textov; Miškovič

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 11/53

4.3	25.01.2012	Doplnenie možnosti vydávania podriadených CA a pravidelná ročná revízia obsahu; Miškovič
4.4	22.06.2012	Zpracovanie požiadaviek dokumentu „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0, ktorý vydala CA/Browser Forum; Miškovič
4.5	15.08.2012	Spresnenie profilu certifikátov koreňových certifikačných autorít CA Disig a ostatných vydávaných typov certifikátov; Miškovič
4.6	21.06.2013	Spresnenie OID dokumentu - vypustenie verzie dokumentu z OID (kap. 1.2); drobné úpravy textov v kapitole 3.1.9; Miškovič
4.7	16.03.2015	Zpracovanie požiadaviek aktuálnej verzie dokumentu „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.2.3; Zmena certifikátu vydávaného právnickej osobe na systémový certifikát pre elektronický pečať (3.1.2); Miškovič
4.8	22.05.2015	Overovanie CAA záznamov (4.1.3)
4.9	21.11.2016	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.; Zmeny v profiloch vydávaných certifikátov; Zpracovanie požiadaviek Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, do verzie 1.4.1; Miškovič
5.0	25.9.2017	Konverzia CP do formátu v zmysle RFC 3647; Zpracovanie požiadaviek nariadenia eIDAS [9] a zpracovanie požiadaviek aktuálnej verzie Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.5.2; Miškovič
5.1	23.5.2018	Nadobudnutie účinnosti Nariadenia č. 2016/679 - GDPR; Zmena znenia bodu 3.2.2.4 (nový spôsob overenia); doplnenie kapitoly 4.2.2 (gTLD); Miškovič
5.2	17.5.2019	Revízia dokumentu a modifikácia v zmysle požiadaviek [4], zmeny v bodoch 4.9.3; 5; 5.2; 5.3; 5.4 and 5.5; Miškovič
5.3	2.12.2019	Revízia dokumentu; Zmena názvov dokumentov súvisiacich s vydávaním certifikátov (4.2.1.2); Miškovič
5.4	1.9.2020	Spresnenie overovania vlastníctva domény 4.2.2.4); Aktualizácia odkazov (1.6.3); Miškovič
5.5	20.5.2021	Doplnenie zodpovednej osoby za hlásenie incidentov (2.2); Miškovič

5.6	18.6.2021	Aktualizácia znenia časti 3.2.2.4; Miškovič
5.7	20.5.2022	Zmena označenia typu certifikátu TLS/SSL na TLS; Doplnenie a úpravy v časti 5.4 týkajúce sa uchovávanía záznamov; Miškovič
5.8	1. 10. 2022	Zmena v súvislosti s požiadavkou zverejnenia dôvodu zrušenia v CRL pri zrušení vydaných TLS certifikátov (4.9.3); Miškovič
5.9	1. 9. 2023	Zmeny v súvislosti s nadobudnutím účinnosti „Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates“; Miškovič
6.0	1. 2. 2023	Vyčlenenie CPS výhradne pre politiku vyhotovovanie verejne dôveryhodných TLS certifikátov; Miškovič
6.1	18. 7. 2024	Zmena sídla spoločnosti Disig, a.s.; Miškovič
6.2	15. 8. 2024	Rozšírenie metód na overenie domény o metódu Zmena DNS v zmysle TLS Baseline Requirements časť 3.2.2.4.7; Miškovič
6.3	10. 1. 2025	Zmena používaných metód na overovania domény k 15.1.2025 (3.2.2.4); Multiperspektívne potvrdenie vydania (3.22.2.9); Miškovič

1.3 Komunita a použiteľnosť

1.3.1 Certifikačné authority

Tieto CPS sa týkajú poskytovania dôveryhodných služieb podriadenými certifikačnými autoritami, ktoré patria pod koreňovú certifikačnú autoritu CA Disig Root R2 - pozri časť 1.4.1 aktuálnej verzie CP CA Disig.

1.3.2 Registračné authority

Zložkou Poskytovateľa, o ktorej detailne pojednávajú tieto pravidlá sú:

■ Interná registračná autorita

Spoločný termín pre CA a RA je authority na správu certifikátov (Certificate Management Authority, ďalej len „CMA“). Termín CMA sa bude používať, keď funkciu možno priradiť buď CA alebo RA, prípadne keď sa požiadavka týka súčasne CA aj RA.

1.3.3 Zákazník a Držiteľ certifikátu

Pozri časť 1.3.3 CP CA Disig.

1.3.4 Strany spoliehajúce sa na certifikáty

Pozri časť 1.3.4 CP CA Disig.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 13/53

1.3.5 Iní účastníci

Pozri časť 1.3.5 CP CA Disig

1.4 Použiteľnosť certifikátov

1.4.1 Vhodné použitie certifikátov

Pozri časť 1.4.1 CP CA Disig.

1.4.2 Nedovolené použitie certifikátov

Pozri časť 1.4.2 CP CA Disig.

1.5 Správa pravidiel

1.5.1 Organizácia zodpovedná za správu pravidiel

Poskytovateľ	
Spoločnosť:	Disig, a.s.
Adresa sídla:	Galvaniho 17/C, 821 04 Bratislava
IČO:	359 75 946
telefón	+421 2 20850140
fax:	+421 2 20828141
e-mail:	disig@disig.sk
webové sídlo:	http://www.disig.sk

1.5.2 Kontaktná osoba

Kontaktná osoba zodpovedná za prevádzku registračných autorít Poskytovateľa je:

Registračná autorita	
Adresa:	Galvaniho 17/C, 821 04 Bratislava
e-mail:	radisig@disig.sk
telefón	+421 2 20850140
fax:	+421 2 20850141
webové sídlo:	http://eidas.disig.sk/
oznamovanie incidentov	tspnotify@disig.sk viac pozri: https://eidas.disig.sk/pdf/incident_reporting.pdf

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 14/53

1.5.3 Osoba rozhodujúca o súlade CPS s CP

Pozri časť 1.5.3 CP CA Disig.

1.5.4 Postupy schvaľovania CPS a externej politiky

Tieto CPS sú schválené osobou, ktorá je menovaná do role PMA.

CPS sú publikovaný v súlade s publikačnou a oznamovacou politikou na webovom sídle Poskytovateľa (pozri časť 1).

1.6 Definície a skratky

1.6.1 Definície

Zmluvný partner - právnická osoba, s ktorou ma s Poskytovateľom uzatvorenú písomnú zmluvu o poskytovaní dôveryhodných služieb.

1.6.2 Skratky

CP	-	Politika poskytovania dôveryhodnej služby vyhotovovania a overovania TLS certifikátov
CPS	-	Pravidlá poskytovania dôveryhodnej služby vyhotovovania a overovania TLS certifikátov
CA	-	Certifikačná autorita (Certification Authority)
OID	-	Identifikátor objektu (Object Identifier)
PKI		Infraštruktúra verejných kľúčov (Public Key Infrastructure)
PMA	-	Autorita pre správu CP (Policy Management Authority)
RA	-	Registračná autorita (Registration Authority)
CRL	-	Zoznam zrušených certifikátov (Certification Revocation List)
HSM	-	Hardware Security Modul
CMA	-	Autorita pre správu certifikátov (Certificate Management Authority)
IČO	-	Identifikačné číslo organizácie
TLS	-	Je nasledovníkom SSL protokolu (Transport Layer Security)
SWACA	-	Softvér certifikačnej autority Poskytovateľa

1.6.3 Odkazy

[1] Politika poskytovania dôveryhodnej služby vyhotovovania a overovanie certifikátov. s.l. : Disig, a.s.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 15/53

- [2] RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. November 2003.
- [3] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Máj 2008.
- [4] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v. 2.1.2.
- [5] Program Requirements - Microsoft Trusted Root Program. s.l. : <https://learn.microsoft.com/en-us/security/trusted-root/program-requirements>.
- [6] Mozilla Root Store Policy, Version 2.9, Effective September 1, 2023.
- [7] Apple Root Certificate Program platný od 15.8.2023. s.l. : https://www.apple.com/certificateauthority/ca_program.html.
- [8] Chrome Root Program Policy, Version 1.5. s.l. : <https://www.chromium.org/Home/chromium-security/root-ca-policy/>.
- [9] 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 v znení Nariadenie EK a Rady (EÚ) č. 1183/2024.
- [10] Informácia o spracúvaní osobných údajov, Disig, a.s.
- [11] Všeobecné podmienky poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov Disig, a.s.
- [12] Mozilla Root Store Policy version 2.9. s.l. : <https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/>.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 16/53

2. Zverejňovanie informácií a úložisko

2.1 Úložiská

Funkciu úložiska Poskytovateľa zastáva jej webové sídlo, ktorého URL adresa je uvedená v časti 1. Úložisko je verejne prístupný držiteľom certifikátov, stranám spoliehajúcim sa na certifikáty a verejnosti vôbec.

2.2 Zverejňovanie informácií o CA/RA

Pozri časť 2.2 CP CA Disig.

Pokiaľ dôjde k nedodržaniu podmienok stanovených aktuálnou politikou „Mozilla Root Store Policy“ [6], tak za hlásenie vzniknutého incidentu je zodpovedný manažér certifikačnej autority Poskytovateľa menovaný do roly PMA.

2.3 Frekvencia zverejňovania informácií

Certifikát sa publikuje ihneď po jeho vydaní a okamžite je možné jeho prevzatie Zákazníkom/Držiteľom certifikátu. Informácie o vydanom certifikáte sú dostupné v úložisku Poskytovateľa - pozri časť 2.1.

CRL sa publikuje ako je špecifikované v časti 4.9.8. Informácie o zrušenom certifikáte možno nájsť v úložisku Poskytovateľa.

Všetky informácie v úložisku sú publikované čo možno najskôr po ich vzniku (vydanie, zrušenie ap.).

2.4 Kontroly prístupu

Poskytovateľ prostredníctvom technických a prijatých organizačných opatrení chráni ľubovoľnú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozšírenie. K tomuto účelu má vypracované presné pravidlá zahrnuté v bezpečnostnom projekte Poskytovateľa a s ním súvisiacich smerniciach.

Verejne dostupné informácie uvedené v repári Poskytovateľa majú charakter riadeného prístupu.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 17/53

3. Identifikácia a autentizácia

3.1 Mená

CA Disig prijíma len tie žiadosti o certifikát, ktoré vyhovujú štandardu PKCS #10 alebo SPKAC a sú vo formáte PEM, ak nebolo so zákazníkom vopred dohodnuté inak.

3.1.1 Typy mien

Žiadne ustanovenia.

3.1.2 Potreba zmysluplnosti mien

Žiadne ustanovenia.

3.1.3 Anonymita a používanie pseudonymov

Žiadne ustanovenia.

3.1.4 Pravidlá na interpretáciu rôznych foriem mien

Pozri časť 3.1.4 aktuálnej verzie CP CA Disig.

3.1.5 Jedinečnosť mien

Žiadne ustanovenia.

3.1.6 Rozpoznanie, autentizácia a rola obchodných značiek

Žiadne ustanovenia.

3.2 Počiatočné overenie identity

3.2.1 Preukazovanie vlastníctva súkromného kľúča

Žiadne ustanovenia.

3.2.2 Autentizácia identity právnickej osoby a identity domény

3.2.2.1 Autentizácia identity

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

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

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 18/53

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

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

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

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

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

Ak sa právnická osoba nechá zastupovať na RA inou právnickou osobou, táto zastupujúca právnická osoba okrem príslušnej plnej moci (viď predošlý odsek) musí preukázať svoju totožnosť rovnakým spôsobom ako zastupovaná právnická osoba, ako je to požadované vyššie.

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

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

3.2.2.2 DBA/Obchodné meno

Ak je obsahom certifikátu DBA/Obchodné meno, tak pracovník RA overuje, či má Zákazník/Držiteľ právo použiť dané TBA/Obchodné meno na základe preloženia jedného z dokladov uvedených v časti 3.2.2.2 aktuálnej verzie CP CA Disig.

3.2.2.3 Overenie krajiny Zákazníka/Držiteľa

U položky subjektu certifikátu *countryName* overuje pracovník RA oprávnenosť spojenia uvedeného kódu krajiny so Zákazníkom/Držiteľom na základe informácií poskytovaných registrátorom domény resp. na základe iných predkladaných dokumentov - pozri časť 3.2.2.1 týchto CPS.

3.2.2.4 Overenie oprávnenia k doméne alebo kontroly nad doménou

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 19/53

Pracovník RA vykoná overenie oprávnenia k doméne alebo kontroly nad doménou metódou, ktorá je uvedená v dokumente [4] v časti 3.2.2.4.2 resp. v prípade, že nie je možné využiť túto metódu, tak alternatívne použije metódu, ktorá je uvedená v dokumente [4] v časti 3.2.2.4.15. Metódu uvedenú v dokumente [4] v časti 3.2.2.4.2 resp. v časti 3.2.2.4.15 môže použiť len do 15.1.2025.

Od 15.1.2025 na overenie oprávnenia k doméne alebo kontroly nad doménou použije miesto metódy uvedenej v dokumente [4] v časti 3.2.2.4.2 resp. časti 3.2.2.4.15 jednu z metód uvedených v dokumente [4] v časti 3.2.2.4.13 resp. 3.2.2.4.14.

V prípade overenia v zmysle časti 3.2.2.4.2 [4] pracovník RA prostredníctvom softvérovej aplikácie KeePass vygeneruje náhodný textový reťazec s minimálnou dĺžkou 20 znakov, ktorý bude obsahovať veľké a malé písmená, čísla a špeciálne znaky. Takto vygenerovanú hodnotu zašle prostredníctvom emailu na emailovú adresu identifikovanú ako oprávnený kontakt pre danú doménu v registri oprávneného registrátora pre danú doménu (napr. pre doménu najvyššej úrovne „.sk“ je to whois.sk-nic.sk). Náhodne vygenerovaná hodnota musí byť zaslaná spolu s potvrdením oprávnenosti žiadosti o vydanie TLS certifikátu v spätne zaslanej emailovej správe z emailovej adresy, na ktorú bol overovací email zaslaný. Náhodná hodnota musí byť pre každú odoslanú emailovú správu jedinečná. Ak prebehne úspešná validácia oprávnenosti použitia FQDN týmto spôsobom, tak Poskytovateľ môže vydať aj iné TLS certifikáty, ktoré končia rovnakým FQDN na druhej a vyššej úrovni. Pracovník RA potom archivuje príslušnú emailovú komunikáciu k vydaným TLS certifikátom v elektronickej podobe. Túto metódu je možné použiť aj na validáciu žiadosti o vydanie „wildcard“ TLS certifikátu.

V prípade overenia v zmysle časti 3.2.2.4.15 [4] pracovník RA overí oprávnenosť žiadosti o vydanie TLS certifikátu zo strany Zákazníka telefonicky, tak že zavolá na telefónne číslo oprávneného kontaktu, ktoré je uvedené ako oprávnený kontakt pre danú doménu v registri oprávneného registrátora pre danú doménu (napr. pre doménu najvyššej úrovne „.sk“ je to whois.sk-nic.sk). Ak prebehne úspešná validácia oprávnenosti použitia FQDN týmto spôsobom, tak Poskytovateľ môže vydať aj iné TLS certifikáty, ktoré končia rovnakým FQDN na druhej a vyššej úrovni. V prípade, že na telefonickom kontakte bude iná osoba ako kontakt uvedený pre danú doménu, musí pracovník RA požiadať o spojenie s osobou, ktorá je daným kontaktom. V prípade, že na telefonickom kontakte bude záznamník, tak pracovník RA zanechá na záznamníku informáciu s obsahom náhodne vygenerovanej hodnoty (pozri postup podľa metódy 3.2.2.4.2 [4]) a overovanú ADN (Authorization Domain Name). Pracovník RA vykoná záznam v elektronickej podobe o telefonickom rozhovore s vyznačením telefónneho čísla, na ktoré bolo vykonaný a menom osoby, ktorá potvrdila oprávnenosť žiadosti o vydanie TLS certifikátu prípadne zaznamená náhodne vygenerovanú hodnotu, ak na telefónnom čísle bol záznamník a rovnako zaznamená odpoveď na takto zanechaný odkaz. Túto metódu je možné použiť aj na validáciu žiadosti o vydanie „wildcard“ TLS certifikátu.

V prípade overenia v zmysle časti 3.2.2.4.13 [4] pracovník RA prostredníctvom softvérovej aplikácie KeePass vygeneruje náhodný textový reťazec s minimálnou dĺžkou 20 znakov, ktorý bude obsahovať veľké a malé písmená, čísla a špeciálne znaky. Takto vygenerovanú hodnotu zašle prostredníctvom emailu na emailovú adresu identifikovanú ako doménový kontakt pre danú doménu získanú z DNS CAA

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 20/53

záznamu pre doménu (položka CAA záznamu „*contactemail*“), ktorá sa overuje. Náhodne vygenerovaná hodnota musí byť zaslaná spolu s potvrdením oprávnenosti žiadosti o vydanie TLS certifikátu v spätne zaslanej emailovej správe z emailovej adresy, na ktorú bol overovací email zaslaný. Náhodná hodnota musí byť pre každú odoslanú emailovú správu jedinečná. Ak prebehne úspešná validácia oprávnenosti použitia FQDN týmto spôsobom, tak Poskytovateľ môže vydať aj iné TLS certifikáty, ktoré končia rovnakým FQDN na druhej a vyššej úrovni. Pracovník RA potom archivuje príslušnú emailovú komunikáciu k vydaným TLS certifikátom v elektronickej podobe. Túto metódu je možné použiť aj na validáciu žiadosti o vydanie „wildcard“ TLS certifikátu.

V prípade overenia v zmysle časti 3.2.2.4.14 [4] pracovník RA prostredníctvom softvérovej aplikácie KeePass vygeneruje náhodný textový reťazec s minimálnou dĺžkou 20 znakov, ktorý bude obsahovať veľké a malé písmená, čísla a špeciálne znaky. Takto vygenerovanú hodnotu zašle prostredníctvom emailu na emailovú adresu identifikovanú ako doménový kontakt pre danú doménu - položka DNS TXT na subdoméne „_validation-contactemail“ overovanej domény. Náhodne vygenerovaná hodnota musí byť zaslaná spolu s potvrdením oprávnenosti žiadosti o vydanie TLS certifikátu v spätne zaslanej emailovej správe z emailovej adresy, na ktorú bol overovací email zaslaný. Náhodná hodnota musí byť pre každú odoslanú emailovú správu jedinečná. Ak prebehne úspešná validácia oprávnenosti použitia FQDN týmto spôsobom, tak Poskytovateľ môže vydať aj iné TLS certifikáty, ktoré končia rovnakým FQDN na druhej a vyššej úrovni. Pracovník RA potom archivuje príslušnú emailovú komunikáciu k vydaným TLS certifikátom v elektronickej podobe. Túto metódu je možné použiť aj na validáciu žiadosti o vydanie „wildcard“ TLS certifikátu.

Rovnako je k dispozícii automatizovaná metóda overovania vlastníctva a kontroly nad doménou v zmysle časti 3.2.2.4.7 [4], kedy je systémom používaným na vyhotovovanie TLS certifikátov zaslaná jedinečná náhodne vygenerovaná hodnota pre každú FQDN ktorá sa očakáva, že sa bude nachádzať v SAN vydaného TLS certifikátu, s tým, že táto jedinečná hodnota musí byť zapísaná v DNS TXT zázname pre každú FQDN a zároveň musí byť zapísaná aj pre všetky nižšie úrovne, až po druhú úroveň, z daných FQDN. Následne systém CA automaticky skontroluje prítomnosť hodnoty TXT v DNS záznamoch. Overenie náhodne vygenerovanej jedinečnej hodnoty pre dané FQDN sa použije na overenie maximálne do 30 dní od jej zaslania. Údaje o overení získané použitím tejto metódy (3.2.2.4.7 [4]) môžu byť použité na overenie vlastníctva a kontroly nad rovnakou FQDN ak nie sú staršie ako 398 dní.

3.2.2.5 Autentifikácia IP adresy

Žiadne ustanovenia.

3.2.2.6 Validácia domény obsahujúcej „wildcard“ znak

Pracovník RA vykoná validáciu žiadosti o vyhotovenie „wildcard“ TLS certifikátu, tým spôsobom, že skontroluje, či v položke CN resp. SAN sa wildcard znak hviezdička („*“) nachádza na prvej pozícii zľava, a či za ním ihneď nasleduje znak bodka („.“). Zároveň skontroluje, či je „wildcard“ TLS certifikát vydávaný pre doménu tretej a vyššej úrovne, kde prvá úroveň môže byť len úroveň národnej

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 21/53

domény „.sk“ t. j. akceptovateľná žiadosť musí mať tvar „wildcard“ doménového mena pre tretiu úroveň „*.názovdomény.sk“. Overenie oprávnenia k doméne sa vykoná v zmysle bodu 3.2.2.4.

3.2.2.7 Presnosť zdroja údajov

Pracovník RA musí pred použitím akéhokoľvek zdroja ako dôveryhodného zdroja postupovať v zmysle časti 3.2.2.7 aktuálnej verzie CP CA Disig.

3.2.2.8 CAA záznam

Pracovník RA musí pred vydaním TLS certifikátu skontrolovať publikovaný CAA záznam. Ak zistí, že takýto záznam existuje nesmie vydať certifikát pokiaľ sa nepotvrdí, že žiadosť o certifikát je v súlade s príslušnou množinou záznamov v CAA.

Overovanie záznamu sa vykonáva pre každé FQDN uvedené v CN žiadosti resp. to, ktoré má byť uvedené v SAN takým spôsobom, že sa postupuje v mennom strome od ľavej strany až po pravú napr. pre kontrolu CAA záznamu žiadosti, ktorá obsahuje FQDN v tvare X.Y.X sa kontrola vykoná v poradí X.Y.X -> Y.Z -> Z, pokiaľ Z nie je národná úroveň napr. „.sk“.

O vykonaní kontroly CAA záznamu sa vytvorí písomný záznam obsahujúci všetky kontrolované FQDN aj s výsledkom kontroly.

3.2.2.9 Multiperspektívne potvrdenie vydania

Pozri časť 3.2.2.9 aktuálnej verzie CP CA Disig.

3.2.3 Autentizácia identity fyzickej osoby

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

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

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

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

Ak fyzická osoba zastupuje na RA inú fyzickú osobu, musí sa navyše preukázať úradne overenou (notárom alebo matrikou) plnou mocou, z textu ktorej je

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 22/53

jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou fyzickou osobou konať v danej veci v jej mene.

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

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

3.2.3.1 Autentizácia identity komponentu

CMA musí garantovať aj v takomto prípade, že identita komponentu a jeho verejný kľúč sú zodpovedajúco previazané.

Hardvérový alebo softvérový komponent, ktorý bude používať certifikáty, bude predmetom certifikácie a je možné vytvoriť preň certifikát. V takom prípade komponent musí byť priradený fyzickej alebo právnickej osobe (organizácii), ktorá ho spravuje.

Táto osoba alebo organizácia je povinná poskytnúť RA tieto informácie:

- identifikáciu zariadenia (názov softvérového komponentu),
- verejný kľúč zariadenia (obsiahnutý v žiadosti o certifikát),
- autorizáciu zariadenia a jeho atribúty (ak nejaké majú byť uvedené v certifikáte),
- kontaktné údaje, aby CMA mohla v prípade potreby komunikovať s touto osobou,

RA musí autentizovať správnosť ľubovoľnej autorizácie (hodnoty položky rozlišovacieho mena), ktorá má byť uvedená v certifikáte a overuje predložené údaje.

Metódy na vykonanie tejto autentizácie a kontroly údajov zahŕňujú:

- overenie identity danej osoby v súlade s požiadavkami časti 3.2,
- overenie identity organizácie, ktorej patrí daný komponent, v súlade s požiadavkami časti 3.2.2,
- overenie oprávnenosti použitia údajov, ktoré majú byť uvedené v jednotlivých položkách certifikátu, s dôrazom na obsah položky commonName.

Typickou hodnotou tejto položky bude úplné doménové meno.

RA vykoná overenie všetkých položiek nachádzajúcich sa v subjekte certifikátu.

3.2.3.2 Predkladané doklady

3.2.3.2.1 Všeobecne

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

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 23/53

Ak má pracovník RA pochybnosti o totožnosti potenciálneho zákazníka (napr. zjavný nesúlad medzi fotografiou v predloženom osobnom doklade a vzhľadom zákazníka, rozpornosť dvoch predložených dokladov a podobne), môže odmietnuť jeho registráciu.

Prípadné predložené doklady v cudzom jazyku (okrem češtiny) musia byť preložené do slovenského jazyka úradným prekladateľom - znalcom.

Na žiadosť potenciálneho zákazníka alebo RA sa prípadné sporné prípady pri preukazovaní totožnosti riešia postupom podľa časti 9.13.

Pri predkladaní dokladov sa vyžaduje, aby na pobočke RA boli predložené originály týchto dokladov slúžiacie k nahliadnutiu a kópie originálov (nemusia byť overené), okrem osobných dokladov identifikujúcich totožnosť žiadateľa resp. splnomocnenej osoby, slúžiacie na archiváciu pre potreby Poskytovateľa. Predloženie výpisu z obchodného registra resp. živnostenského registra získaného z Internetu, zo strany žiadateľa, nie je postačujúce, nakoľko tento má len informatívny charakter a nie je použiteľný na právne úkony.

3.2.3.2.2 Fyzická osoba

Pozri časť 3.2.3 a časť 3.2.3.3.2 aktuálnej verzie CP CA Disig.

3.2.3.2.3 Fyzická osoba - zamestnanec

Pozri časť 3.2.3.3.4 aktuálnej verzie CP CA Disig.

3.2.3.2.4 Právnická osoba

V tomto prípade žiadateľ o certifikát predkladá doklady uvedené v časti 3.2.3.2.2. Súčasne musí predložiť doklad podľa časti 3.2.2.

3.2.3.3 Zariadenie alebo systém

Pozri časť 3.2.3.1.

3.2.3.4 Kontrola údajov na predložených dokladoch

V prípade ľubovoľných odôvodnených pochybností o totožnosti potenciálneho zákazníka môže RA jeho registráciu odmietnuť. Pracovník RA kontroluje na predložených dokladoch najmä nasledovné:

- Osobné doklady fyzickej osoby:
 - platnosť predloženého dokladu - v prípade neplatného osobného dokladu sa postupuje ako pri chýbajúcom osobnom doklade - RA registráciu odmietne
 - plnoletosť fyzickej osoby (t. j. vek 18 rokov) - RA odmietne registráciu neplnoletých osôb pričom za neplnoleté osoby má právo konať ich zákonný zástupca (obvykle rodič).
 - či nie je zjavný nesúlad medzi fotografiou v osobnom doklade a vzhľadom držiteľa osobného dokladu - v prípade, že áno, RA môže odmietnuť registráciu.
 - rozpornosť predložených dokladov, t. j. či údaje na jednom doklade neodporujú údajom na inom doklade

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 24/53

- Výpisy z obchodného registra:
 - či výpis nie je starší ako 3 mesiace
 - či majú fyzické osoby (stačí jedna fyzická osoba, ak na výpise nie je uvedené inak), ktoré predložili daný výpis, právo konať (podpisovať) za danú právnickú osobu (t. j. či sú jej štatutárnymi zástupcami)
 - či je výpis úradne overený (notárom alebo matrikou), ak sa nejedná o originál
- Plné moci:
 - či je plná moc úradne overená (notárom alebo matrikou)
 - či sa údaje, uvedené v plnej moci, ktoré definujú zastupujúcu fyzickú resp. právnickú osobu, zhodujú 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 k požadovanému úkonu na RA v mene splnomocňujúcej fyzickej alebo právnickej osoby
 - či plná moc nie je časovo obmedzená alebo ak obsahuje inú podmienku, či je táto splnená
- Čestné prehlásenia:
 - oprávnenie na podpis - či osoba podpisujúca prehlásenie je oprávnená zastupovať právnickú osobu. Oprávnenosť sa kontroluje podľa výpisu z OR resp. iného registra právnických osôb. Pokiaľ podpisujúca osoba nie je zapísaná v tomto výpise, musí predložiť iný doklad, na základe ktorého môže konať za spoločnosť (spravidla notárom overená plná moc)

Druh predložených dokladov (napr. občiansky preukaz, pas) a príslušné údaje z nich zaznamenaná pracovník RA elektronicky do informačného systému CA.

V prípade zistených nedostatkov na predložených dokladoch, resp. predložení neúplných dokladov, musí pracovník RA registráciu žiadateľa odmietnuť. Služba vydania certifikátu bude v tomto prípade zamietnutá.

Pracovník RA musí akceptovať aj dokumenty predkladané žiadateľom v elektronickej podobe podpísané platným ZEP (výpis s obchodného registra, plná moc, prehlásenie, poverenie ap.)

3.2.3.5 Prvotná registrácia RA

Prvotná registrácia osoby v role RA sa vykoná za rovnakých, vyššie popísaných podmienok ako v prípade zákazníka - žiadateľa o osobný certifikát. Vlastné overenie identity pracovníkov RA vykonajú pracovníci Poskytovateľa, pokiaľ nie je zmluvne dohodnutý iný mechanizmus.

3.2.4 Neoverované informácie o Držiteľovi

Pozri časť 3.2.4 aktuálnej verzie CP CA Disig.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 25/53

3.2.5 Overovanie oprávnení

Pozri časť 3.2.3.

3.2.6 Kritériá interoperability

Žiadne ustanovenia.

3.3 Identifikácia a autentifikácia pri vydávaní následného certifikátu

Žiadne ustanovenia.

3.3.1 Identifikácia a autentifikácia pri rutinnom vydávaní následného certifikátu po zrušení predchádzajúceho

Po zrušení certifikátu musí žiadateľ o následný certifikát podrobiť všetkým požiadavkám prvej registrácie.

3.3.2 Identifikácia a autentifikácia pri vydávaní následného certifikátu po zrušení predchádzajúceho

Žiadne ustanovenia.

3.4 Identifikácia a autentifikácia pri žiadaní o zrušenie certifikátu

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 26/53

4. Požiadavky na životný cyklus certifikátu

4.1 Žiadanie o certifikát

4.1.1 Kto môže žiadať o vydanie certifikátu

Pozri časť 4.1.1 aktuálnej verzie CP CA Disig.

4.1.2 Registračný proces a zodpovednosti

4.1.2.1 Príprava

Pozri časť 4.1.2.1 aktuálnej verzie CP CA Disig.

4.1.2.2 Generovanie žiadosti

Pozri časť 4.1.2.2 aktuálnej verzie CP CA Disig.

4.1.2.3 Zaslanie žiadosti o certifikát

Pozri časť 4.1.2.3 aktuálnej verzie CP CA Disig.

4.2 Spracovanie žiadosti a vydanie certifikátu

4.2.1 Vykonanie identifikácie a autentifikácie

4.2.1.1 Detailný postup na získanie certifikátu

4.2.1.1.1 Príprava na návštevu na RA

Zákazník vykoná nasledovné kroky:

- oboznámi sa s týmto postupom, prípadne s princípmi a návodmi na získanie certifikátu,
- pomocou svojho softvéru (typicky napr. Microsoft IIS alebo Apache/Openssl) si vygeneruje žiadosť o certifikát a túto odošle elektronicky na RA (radisig@disig.sk) a zároveň si ju uloží z dôvodov zálohy na vhodné prenosné médium,

Poznámky a upozornenia: Upozorňujeme, že žiadosť o certifikát resp. v nej sa nachádzajúci verejný kľúč, na ktorý už bol vydaný certifikát, nemôže byť z bezpečnostných dôvodov použitá opakovane na vydanie iného certifikátu a bude na RA odmietnutá! Žiadosť o certifikát musí povinne obsahovať vhodne vyplnenú položku subject:commonName (tzv. názov entity). Jednotlivé položky je potrebné vyplniť tak, aby zadané hodnoty boli v súlade s požiadavkami uvedenými v časti 3.1.2 CP CA Disig, a aby jednoznačne identifikovali entitu, ktorá bude používať daný certifikát (typicky úplné doménové meno (FQDN)).

Použitie špeciálnych znakov (napr. čiarka, pomlčka, =, / a iné) treba obmedziť na minimálnu nutnú mieru, odporúčame prípadne tieto znaky použiť až po dohode s Poskytovateľom, v opačnom prípade si Poskytovateľ vyhradzuje právo odmietnuť takúto žiadosť o certifikát.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 27/53

- pripraví si zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra (odporúčame overiť platnosť dokladov) podľa ustanovení časti 3.

Poznámka: Je potrebné, aby si zákazník pripravil kópie (nemusia byť overené) všetkých dokladov (okrem osobných dokladov fyzických osôb), ktoré mieni predložiť na RA (napr. výpis z obchodného registra a iné doklady o právnickej osobe, splnomocnenie, ak sa dá zastupovať na RA), aby ich mohol odovzdať na RA. Predloženie výpisu z obchodného registra získaného z Internetu, zo strany žiadateľa, nie je postačujúce, nakoľko tento výpis má len informatívny charakter a nie je použiteľný na právne úkony.

Odporúča sa, aby si zákazník na RA ešte pred návštevou RA overil a vyjasnil prípadné pochybnosti a problémy, najmä tie, ktoré týkajú vhodnosti hodnôt jednotlivých položiek v žiadosti o certifikát.

- dohodne si termín návštevy RA (telefonicky, e-mailom).

4.2.1.2 Postup RA pred vydaním certifikátu

Na základe vopred zaslanej žiadosti pracovník RA vykoná overenie vlastníctva domény v zmysle ods. 3.2.2.4 a zároveň skontroluje úplnosť a správnosť prijatej žiadosti o certifikát. Ak má pracovník RA vážne podozrenie na neoprávnené použitie niektorého FQDN Zákazníkom, má právo požadovať, aby Zákazník dôveryhodným spôsobom dokladoval oprávnenosť použitia daného FQDN, v opačnom prípade môže RA odmietnuť prijať danú žiadosť o TLS certifikát.

4.2.2 Schválenie alebo zamietnutie žiadosti o certifikát

Žiadosť o vydanie certifikátu začne pracovník RA spracovávať ihneď po jej prijatí v zmysle postupov uvedených v časti 4.2.1 a ak sú splnené všetky podmienky na vydanie, tak certifikát vydá, ak ide o žiadosť zaslanú elektronicky. V prípade potreby osobnej účasti Zákazníka/Držiteľa sa vydanie uskutoční pri jeho osobnej účasti za predpokladu predloženia všetkých požadovaných dokumentov.

Pracovník RA zamietne žiadosť o vydanie certifikátu v prípade, že má odôvodnenú pochybnosť o totožnosti zákazníka a tiež v prípade, že zistí nedostatky v identifikačných dokladoch, poskytnutí neúplných informácií alebo v prípade, že v minulosti už bol Poskytovateľom vydaný certifikát na daný verejný kľúč.

Pokiaľ najvyššia doména (gTLD) uvedená v zaslanej žiadosti na vydanie certifikátu (napríklad „.ipsum“) je pre pracovníka neznáma, musí si overiť či sa nachádza v databáze „Root Zone Database“, ktorú vedie Internet Assigned Numbers Authority (IANA) (<https://www.iana.org/domains/root/db>). Ak zistí, že daná gTLD sa v zozname nenachádza, tak odmietne vydať certifikát.

Pracovník RA nevydá TLS certifikát na žiadosť obsahujúcu názov domény, ak pri overovaní CAA DNS záznamu (pozri časť 3.2.2.8 CP CA Disig) zistil, že takýto záznam existuje a Poskytovateľ nie je v zmysle jeho obsahu autorizovaný na vydávanie TLS certifikátov t. j. záznam neobsahuje autorizáciu v tvare „disig.sk“.

4.2.3 Doručenie verejného kľúča vydavateľovi certifikátu

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 28/53

4.3 Vydanie certifikátu

4.3.1 Činnosť CA pri vydávaní certifikátu

Pozri časť 4.3.1 aktuálnej verzie CP CA Disig.

4.3.2 Informovanie Držiteľa o vydaní certifikátu

Držiteľ je upozornený na vydanie certifikátu zaslaním e-mailovej správy priamo zo systému CA na e-mailovú adresu uvedenú v osobných údajoch Držiteľa certifikátu.

4.4 Prevzatie certifikátu

4.4.1 Spôsob prevzatia certifikátu

Certifikát je k dispozícii na prevzatie prostredníctvom úložiska Poskytovateľa na adrese:

<https://eidas.disig.sk/sk/poskytovatel/certifikacna-autorita/vyhľadavanie-certifikatov/>,

resp. je mu poskytnutý prostredníctvom mailovej správy alebo jeho odovzdaním na prenosnom médiu.

4.4.2 Zverejňovanie certifikátu

Každý vydaný certifikát je zverejňovaný v úložisku Poskytovateľa ihneď po vydaní, pokiaľ so Zákazníkom/Držiteľom nebolo dohodnuté jeho nezverejňovanie.

4.4.3 Oznámenie o vydaní certifikátu iným subjektom

Žiadne ustanovenia.

4.5 Kľúčový pár a používanie certifikátu

4.5.1 Používanie súkromného kľúča a certifikátu Držiteľom

Žiadne ustanovenia.

4.5.2 Používanie verejného kľúča a certifikátu Spoliehajúcou sa stranou

Žiadne ustanovenia.

4.6 Obnova certifikátu

Žiadne ustanovenia.

4.6.1 Okolnosti pre obnovenie certifikátu

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 29/53

4.6.2 Kto môže požiadať o obnovenie

Žiadne ustanovenia.

4.6.3 Spracovanie žiadostí o obnovenie certifikátu

Žiadne ustanovenia.

4.6.4 Oznámenie o vydaní nového certifikátu držiteľovi

Žiadne ustanovenia.

4.6.5 Spôsob prevzatia obnoveného certifikátu

Žiadne ustanovenia

4.6.6 Zverejňovanie obnoveného certifikátu zo strany Poskytovateľa

Žiadne ustanovenia.

4.6.7 Oznámenie o vydaní obnoveného certifikátu iným subjektom

Žiadne ustanovenia.

4.7 Vydanie certifikátu na nové kľúče

Žiadne ustanovenia.

4.7.1 Podmienky vydania certifikátu na nové kľúče

Žiadne ustanovenia

4.7.2 Kto môže žiadať o vydanie certifikátu na nové kľúče

Žiadne ustanovenia.

4.7.3 Postup žiadania o vydanie certifikátu na nové kľúče

Žiadne ustanovenia.

4.7.4 Oznámenie o vydaní certifikátu na nové kľúče Držiteľovi

Žiadne ustanovenia.

4.7.5 Spôsob prevzatia certifikátu vydaného na nové kľúče

Žiadne ustanovenia.

4.7.6 Zverejňovanie certifikátov zo strany Poskytovateľa

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 30/53

4.7.7 Oznámenie o vydaní certifikátu CA iným subjektom

Žiadne ustanovenia.

4.8 Modifikácia certifikátu

4.8.1 Okolnosti pre modifikovanie certifikátu

Žiadne ustanovenia

4.8.2 Kto môže požiadať o modifikáciu certifikátu

Žiadne ustanovenia.

4.8.3 Spracovanie žiadostí o modifikáciu certifikátu

Žiadne ustanovenia.

4.8.4 Oznámenie o vydaní nového certifikátu držiteľovi

Žiadne ustanovenia.

4.8.5 Spôsob prevzatia modifikovaného certifikátu

Žiadne ustanovenia

4.8.6 Zverejňovanie modifikovaného certifikátu zo strany Poskytovateľa

Žiadne ustanovenia.

4.8.7 Oznámenie o vydaní modifikovaného certifikátu iným subjektom

Žiadne ustanovenia.

4.9 Zrušenie a suspendovanie certifikátu

4.9.1 Podmienky zrušenia certifikátu

Pozri časť 4.9.1 aktuálnej verzie CP CA Disig.

4.9.1.1 Zrušenie certifikátu Zákazníka/Držiteľa

Pozri časť 4.9.1.1 aktuálnej verzie CP CA Disig.

4.9.2 Kto môže žiadať o zrušenie certifikátu

Pozri časť 4.9.2 aktuálnej verzie CP CA Disig.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 31/53

4.9.3 Postup žiadosti o zrušenie certifikátu

Osoba požadujúca zrušenie certifikátu sa buď musí na RA podrobiť rovnakému procesu autentizácie, aký je požadovaný pri prvotnej registrácii žiadateľa o certifikát alebo musí hodnoverným spôsobom preukázať, že je oprávnenou osobou, ktorá môže žiadať o zrušenie daného certifikátu.

Ak sa držiteľ certifikátu nechá na RA zastupovať vo veci zrušenia certifikátu, zastupujúci subjekt sa musí preukázať overenou plnou mocou (notárom alebo matrikou), z textu ktorej je jednoznačne zrejmé vôľa držiteľa certifikátu zrušiť svoj certifikát. Zastupujúci subjekt je povinný nechať na RA doklad potvrdzujúci jeho plnú moc alebo jeho kópiu (nemusí byť overená). Pracovník RA prevezme a uschová tento doklad, v prípade neoverenej kópie túto porovná s originálom a napíše na ňu text „Potvrdzujem zhodu s originálom“ a doplní dátum a svoj podpis.

Pracovník RA posúdi oprávnenosť žiadosti o zrušenie certifikátu a v prípade, že je zrejmé, že žiadateľ o zrušenie nie je oprávnenou osobou, RA môže danú žiadosť o zrušenie odmietnuť.

Pracovník RA odmietne žiadosť, ak žiadateľ nesplní podmienky autentizácie svojej identity (pozri časti 3.2.2 resp. 3.2.3).

Kontakty pre nahlasovania a postup nahlasovania incidentov v prípade možnej kompromitácie súkromného kľúča, zneužitia certifikátu alebo iného druhu podvodu, neoprávneného vydania alebo inej záležitosti týkajúcej sa vydaného Certifikátu sú uvedené v kapitole 1.5.2.

V prípade požiadavky na zrušenie certifikátu z niektorého z dôvodov uvedených v časti 4.9.1.1 aktuálneho CP CA Disig (keyCompromise (RFC 5280 CRLReason #1), privilegeWithdrawn (RFC 5280 CRLReason #9), cessationOfOperation (RFC 5280 CRLReason #5), affiliationChanged (RFC 5280 CRLReason #3) alebo superseded (RFC 5280 CRLReason #4) musí RA požadovať zaslanie písomnej požiadavky v zmysle časti 4.9.3 aktuálneho CP CA Disig.

4.9.4 Čas na podanie žiadosti o zrušenie certifikátu

Žiadne ustanovenia.

4.9.5 Čas na spracovanie žiadosti o zrušenie certifikátu

Pozri časť 4.9.5 aktuálnej verzie CP CA Disig.

Po prijatí žiadosti o zrušenie certifikátu, ktorú Pracovník RA považuje za oprávnenú (t. j. ktorá vyhovuje príslušným ustanoveniam týchto pravidiel), Pracovník RA vloží prijatú žiadosť o zrušenie certifikátu prostredníctvom aplikácie RA Client do informačného systému Poskytovateľa, aby sa daný certifikát mohol automatizovane zrušiť. Zrušenie je vykonané najneskoršie do 24 hodín od overenia oprávnenosti žiadosti o zrušenie.

Po zrušení certifikátu je zo systému Poskytovateľa automaticky zaslaná držiteľovi e-mailová notifikáciu o zrušení jeho certifikátu aj s informáciou o dôvodoch jeho zrušenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 32/53

4.9.6 Overovanie platnosti zo strany spoliehajúcej sa strany

Žiadne ustanovenia.

4.9.7 Frekvencia vydávania CRL

Žiadne ustanovenia.

4.9.8 Doba publikovania CRL

Žiadne ustanovenia.

4.9.9 Dostupnosť služby OCSP

Žiadne ustanovenia.

4.9.10 Požiadavky na OCSP overovanie

Žiadne ustanovenia.

4.9.11 Iné formy dostupnosti informácií o zrušení certifikátu

Žiadne ustanovenia

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.

4.9.15 Postup pre pozastavenie platnosti certifikátu

Žiadne ustanovenia.

4.9.16 Limity pre obdobie pozastavenia

Žiadne ustanovenia.

4.10 Služby súvisiace so stavom certifikátu

4.10.1 Prevádzkové charakteristiky

Aktuálne CRL je dostupné na webovom sídle Poskytovateľa (pozri časť 1) a je prístupné prostredníctvom HTTP protokolu na porte 80.

Služba OCSP je dostupná na URL adrese uvedenej vo vydanom certifikáte.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 33/53

4.10.2 Dostupnosť služieb

Distribučné body, na ktorých sú publikované CRL sú k dispozícii v režime 24x7.

Služba OCSP je dostupná v režime 24x7.

Nahlasovanie problémov s certifikátom je k dispozícii 24x7 na adrese podpora@disig.sk.

4.10.3 Doplnkové funkcie

Žiadne ustanovenia.

4.11 Ukončenie poskytovanie služieb

Žiadne ustanovenia.

4.12 Uchovávanie a obnova kľúčov

4.12.1 Politika a postupy uchovávania a obnovy kľúčov

Žiadne ustanovenia.

4.12.2 Politika a postupy ochrany „session key“

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 34/53

5. Fyzické, procedurálne a personálne bezpečnostné opatrenia

5.1 Opatrenie týkajúce sa fyzickej bezpečnosti

5.1.1 Priestory

Základná infraštruktúra Poskytovateľa je umiestnená 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 pozostáva len z vybavenia vyhradeného na poskytovanie dôveryhodných služieb a neslúži 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 sú zabezpečené tak, že priestory sú chránené bezpečnostným alarmom a vstup do nich je umožnený len osobám, ktoré vlastnia bezpečnostný token a sú uvedené na zozname oprávnených osôb na vstup do chránených priestorov Poskytovateľa. Vybavenie Poskytovateľa je neprestajne chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom.

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, sú umiestnené tak, že ohrozeniu vodou s akýchkoľvek zdrojov je málo pravdepodobné.

5.1.5 Ochrana pred ohňom

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

5.1.6 Úložisko médií

Médiá sú 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 sú uložené v lokalite oddelenej od vybavenia CMA.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 35/53

5.1.7 Nakladanie s odpadom

S odpadom vznikajúcim v súvislosti s prevádzkou Poskytovateľa je nakladané tak, že v žiadnom prípade nemôže dôjsť k znečisteniu životného prostredia.

5.1.8 Zálohovanie off-site

Pre prípad nenávratného poškodenia priestorov hlavnej lokality, v ktorých je umiestnená infraštruktúra Poskytovateľa má tento k dispozícii kópiu všetkých najdôležitejších aktív v záložnej lokalite, ktorá je geograficky vzdialená od hlavnej lokality.

5.2 Procedurálne bezpečnostné opatrenia

Pri výbere osôb na zastávanie roly Pracovník RA sa kladie dôraz, aby boli zodpovedné a dôveryhodné, lebo táto rola si vyžaduje dôveryhodnosť. Funkcie vykonávané touto rolou patria k funkciám, ktoré formujú v personálnej rovine základ dôvery v Poskytovateľa.

Každá RA, ktorá pracuje v súlade s týmito CPS, je povinná dodržiavať ich ustanovenia. Zodpovednosťou Pracovníka RA je v prvom rade:

- overovanie identity buď prostredníctvom osobného kontaktu alebo prostredníctvom zastupujúceho subjektu,
- zaznamenávanie informácií od žiadateľov o certifikát a overovanie ich správnosti,
- bezpečná komunikácia s Poskytovateľom,
- komunikácia so Zákazníkom/Držiteľom a dokumentovanie tejto komunikácie.

5.2.1 Dôveryhodné role

V rámci CA sú definované dôveryhodné role zodpovedné za jednotlivé aspekty poskytovaných dôveryhodných služieb a rovnako sú definované zodpovednosti jednotlivých rolí.

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

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

5.2.2 Počet osôb v jednotlivých rolách

Pre každú úlohu je identifikovaný počet jednotlivcov, ktorí sú určení na ich vykonávanie (pravidlo K z N).

5.2.3 Identifikácia a autentizácia pre každú rolu

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

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 36/53

5.2.4 Role vyžadujúce oddelenie zodpovednosti

Každá rola má stanovené kritériá, ktoré zohľadňujú potrebu oddelenie funkcií z hľadiska samotnej roly t. j. sú uvedené roly, ktoré nemôžu byť vykonané rovnakými jednotlivcami.

5.3 Personálne bezpečnostné opatrenia

Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami právnickej osoby, ktorá má zmluvu s Poskytovateľom o poskytovaní jeho služieb prostredníctvom svojej registračnej autority.

Personál pre rolu Pracovník RA sa vyberá na základe spoľahlivosti, lojality a dôveryhodnosti.

Všetky osoby zastávajúce rolu Pracovníka RA sú náležite poučené a zaškolené v rozsahu potrebnom na výkon činnosti Pracovníka RA a vždy majú k dispozícii aktuálne verzie dokumentov Poskytovateľa určených na výkon činnosti Pracovníka RA, ktoré sú dostupné na webovom sídle <https://razona.disig.sk>.

Prístup Pracovníka RA k IS Poskytovateľa prostredníctvom aplikácie RA Client, ktoré RA využíva pri svojej činnosti, je chránený pred neautorizovaným prístupom tým, že RA používa na autentizáciu vlastný certifikát RA, prostredníctvom ktorého sa identifikuje a autorizuje.

Dôležitým bezpečnostným opatrením, ktoré podstatným spôsobom obmedzuje možnosť zneužitia elektronickej identity Pracovníka RA (certifikátu RA a najmä k nemu patriaceho súkromného kľúča), je to, že daný pár kľúčov RA je uložený na čipovej karte. Prístup k súkromnému kľúču uloženému na karte je chránený heslom.

Na ochranu vybavenia RA sa použijú aj ďalšie bezpečnostné mechanizmy primerané úrovni hrozby v prostredí vybavenia RA.

5.3.1 Požiadavky na kvalifikáciu, skúsenosti a previerky

Pracovníci v roly registračnej autority spĺňajú kvalifikačné požiadavky požadované pre túto rolu.

5.3.2 Požiadavky na previerky

U roly Pracovník RA sa nepožaduje bezpečnostná previerka.

5.3.3 Požiadavky na školenia

Každý pracovník RA musí prejsť, pred tým ako začne vykonávať svoju funkciu, povinným školením, ktoré vykonávajú poverení pracovníci Poskytovateľa. Tieto školenia sú povinné pre všetky typy RA (pozri časť 1.3.2 CP CA Disig).

5.3.4 Požiadavky na frekvenciu obnovy školení

Obnova školenia pracovníkov RA sa vykonáva na základe rozhodnutia PMA v tých prípadoch, kedy dochádza k významným zmenám, či už v legislatíve alebo

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 37/53

v softvérovom vybavení RA.

5.3.5 Rotácia rolí

Žiadne ustanovenia.

5.3.6 Postihy za neoprávnenú činnosť

Zlyhanie akéhokoľvek pracovníka RA, ktorého výsledok je stav, ktorý nie je v súlade s ustanoveniami tejto CP resp. prijatých CPS, či už sa to týka nedbanlivosti alebo zlého úmyslu, bude predmetom zodpovedajúcich administratívnych a disciplinárnych konaní zo strany Poskytovateľa na základe interných predpisov resp. existujúcich zmlúv s externými RA

5.3.7 Požiadavky na externých dodávateľov

Žiadne ustanovenia.

5.3.8 Dokumentácia dodávané pre personál

Pracovníci RA majú k dispozícii dokumenty potrebné pre výkon funkcie, na ktorú sa sú priradení, vrátane kópie tejto CP resp. CPS a všetky technické a prevádzkovej dokumentácie potrebné k zachovaniu integrity operácií Poskytovateľa. Táto dokumentácia je pre nich dostupná na portáli razona.disig.sk.

5.4 Postupu získavania auditných záznamov

5.4.1 Typy zaznamenávaných udalostí

Všetky udalosti týkajúce sa vykonaných operácií v aplikácii RA Client sú zaznamenávané priamo aplikáciou. Rovnako, všetky informácie zasielané z aplikácie RA Client sú zaznamenávané na serverovej strane u Poskytovateľa služby.

Udalosti týkajúce sa životného cyklu certifikátov pre koncových používateľov v rozsahu:

- žiadosť o vydanie certifikátu,
- schválenie žiadosti o vydanie,
- vydanie certifikátu,
- rušenie certifikátu,

sú zaznamenávané v databáze SWACA.

5.4.2 Frekvencia spracovávania auditných záznamov

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 38/53

5.4.3 Uchovávanie logov

Pozri časť 5.4.3 CP CA Disig.

5.4.4 Ochrana auditných záznamov

Všetky záznamy sú na RA uchovávané a chránené tak, aby nedošlo k ich znehodnoteniu.

5.4.5 Postupy zálohovania auditných logov

Žiadne ustanovenia.

5.4.6 Systém zálohovania logov

Poskytovateľ má vybudovaný systém na zálohovania logov.

5.4.7 Notifikácia subjektu iniciujúceho log záznam

Žiadne ustanovenia.

5.4.8 Posudzovanie zraniteľností

Žiadne ustanovenia.

5.5 Uchovávanie záznamov

5.5.1 Typy archivovaných záznamov

RA uchováva všetky záznamy o vydaných certifikátoch po dobu, ktorá je stanovená v príslušnej zmluve o RA a tieto odovzdáva Poskytovateľovi v intervaloch stanovených v zmluve o RA.

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

5.5.2 Doba uchovávania záznamov

Poskytovateľ uchováva záznamy v súlade s požiadavkou v bode 5.5.2 CP CA Disig.

5.5.3 Ochrana archívnych záznamov

Žiadne ustanovenia.

5.5.4 Zálohovanie archívnych záznamov

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 39/53

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 pracovníka RA

Pracovník RA môže používať svoje prístupové kľúče iba na prístup k IS Poskytovateľa prostredníctvom aplikácie RA Client, podpisovanie operácií v aplikácii RA Client a prístup k portálu razona.disig.sk.

Prístupové kľúče Pracovníka RA sú pravidelne obmieňané v intervale cca 1 rok.

5.7 Obnova po kompromitácia alebo havárii

5.7.1 Postupy riešenia incidentov a kompromitácie

V prípade, že dôjde ku kompromitácii kľúča pracovníka RA napr. stratou kľúča, prezradením prístupových hesiel ap., musí byť tento incident zo strany Pracovníka RA okamžite nahlásený Poskytovateľ, aby mohli byť prijaté príslušné opatrenia na minimalizáciu možnosti zneužitia prístupových práv k IS Poskytovateľa.

5.7.2 Poškodenie hardvéru, softvéru alebo údajov

Žiadne ustanovenia.

5.7.3 Postupy pri kompromitácii kľúča CA

V prípade kompromitácie súkromného kľúča Pracovníka RA musí Poskytovateľ okamžite zrušiť príslušný certifikát a zrušiť jeho autorizáciu vo svojom IS.

5.7.4 Zachovanie kontinuity činnosti po havárii

Žiadne ustanovenia.

5.8 Ukončenie činnosti RA

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 40/53

6. Technické bezpečnostné opatrenia

6.1 Generovanie a inštalácia páru kľúčov

6.1.1 Generovanie a inštalácia páru pre jednotlivé subjekty

6.1.1.1 Vydavateľ certifikátov

Žiadne ustanovenia.

6.1.1.2 Registračné authority

Generovanie prístupových kľúčov a vydávanie autentifikačných certifikátov pre Pracovníkov RA vykonávajú poverení pracovníci Poskytovateľa. Všetky prístupové kľúče sú uložené na kvalifikovanom zariadení pre elektronický podpis, kde prístup ku kľúčom je chránený prístupovým heslom, ktoré si volí Pracovník RA. Takto je zabezpečená dvojfaktorová autentifikácia pri vydávaní certifikátu prostredníctvom IS Poskytovateľa.

6.1.1.3 Koncoví používatelia

Žiadne ustanovenia.

6.1.2 Doručenie súkromného kľúča držiteľovi certifikátu

Pozri časť 6.1.2 aktuálnej verzie CP CA Disig.

Všetky kvalifikované zariadenia pracovníkov RA sú buď odovzdávané osobne v sídle Poskytovateľa alebo sú zasielané doporučenou poštou do vlastných rúk Pracovníka RA. Pri zasielaní doporučenou poštou je inicializácia prístupových práv pre Pracovníkov RA v IS Poskytovateľa vykonaná až po potvrdení doručenia kvalifikovaného zariadenia zo strany Pracovníka RA.

6.1.3 Doručenie verejného kľúča vydavateľovi certifikátu

Verejný kľúč je pri vydávaní certifikátu doručený certifikačnej autorite bezpečne prostredníctvom aplikácie RA Client v on-line režime počas procesu vydávania certifikátu. Komunikácia medzi aplikáciou RA Client a vydávajúcou CA je autorizovaná podpísaním všetkých zasielaných údajov pracovníkom RA, kde oprávnenie na vydanie daným pracovníkom RA je kontrolované na strane CA v automatickom režime.

6.1.4 Doručenie verejného kľúča CA spoliehajúcim sa stranám

Žiadne ustanovenia.

6.1.5 Dĺžky kľúčov

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 41/53

6.1.6 Parametre a kvalita verejného kľúča

Pozri časť 6.1.5 týchto CPS a rovnako aj časť 7 aktuálnej verzie CP CA Disig.

6.1.7 Použitie kľúčov

Kľúče vydané pracovníkom RA je možné využívať len na prístup k IS Poskytovateľa prostredníctvom aplikácie RA Client a tiež na podpisovanie zasielaných údajov v procese vydávania certifikátu v aplikácii RA Client. Tiež môžu byť použité na prístup k portálu razona.disig.sk, kde sú dostupné všetky potrebné informácie pre Pracovníkov RA.

6.2 Ochrana súkromného kľúča a technické opatrenia pre kryptografický modul

6.2.1 Štandardy a opatrenia pre kryptografický modul

Žiadne ustanovenia.

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

Žiadne ustanovenia.

6.2.3 „Key escrow“ súkromného kľúča

Žiadne ustanovenia.

6.2.4 Zálohovanie súkromného kľúča

Žiadne ustanovenia..

6.2.5 Archivácia súkromného kľúča

Žiadne ustanovenia

6.2.6 Prenos súkromných kľúčov z a do HSM modulu

Žiadne ustanovenia.

6.2.7 Uchovávanie súkromných kľúčov v HSM module

Žiadne ustanovenia.

6.2.8 Spôsob aktivácie súkromných kľúčov

Žiadne ustanovenia.

6.2.9 Spôsob deaktivácie súkromného kľúča

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 42/53

6.2.10 Spôsob zničenia súkromného kľúča

Žiadne ustanovenia.

6.2.11 Charakteristika HSM modulu

Žiadne ustanovenia.

6.3 Ďalšie aspekty manažmentu kľúčového páru

6.3.1 Archivácia verejných kľúčov

Žiadne ustanovenia.

6.3.2 Dĺžka platnosti certifikátov a použiteľnosť kľúčového páru

Platnosť Poskytovateľom vydávaných certifikátov pre Pracovníkov RA nesmie prekročiť nasledovné:

Typ certifikátu	Platnosť (maximálne)
Certifikát Pracovníka RA	maximálne 365 dní

6.4 Aktivačné údaje

6.4.1 Vytváranie a inštalácia aktivačných údajov

Aktivačné údaje k súkromnému kľúču pracovníka RA si volí sám Pracovník RA sám ihneď po prebratí kvalifikovaného zariadenia ešte pred jeho prvým použitím na prístup k IS Poskytovateľa prostredníctvom aplikácie RA Client.

6.4.2 Ochrana aktivačných údajov

Za ochranu súkromných kľúčov Pracovníka RA je zodpovedný výhradne samotný Pracovník RA.

Pri vydávaní certifikátu je každý Pracovník RA upozornený so strany zodpovednej osoby Poskytovateľa o potrebe chrániť súkromný kľúč silným heslom, aby nemohlo dôjsť k jeho zneužitiu, počas celej doby jeho používania.

6.4.3 Ostatné aspekty aktivačných údajov

Žiadne ustanovenia.

6.5 Riadenie bezpečnosti počítačov

6.5.1 Špecifické požiadavky na bezpečnosť počítačov

Pozri časť 6.5.1 aktuálnej verzie CP CA Disig..

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 43/53

6.5.2 Hodnotenie bezpečnosti informácií

Žiadne ustanovenia.

6.6 Opatrenia v životnom cykle

6.6.1 Opatrenia pri vývoji systémov

Žiadne ustanovenia.

6.6.2 Opatrenia na riadenie bezpečnosti

Žiadne ustanovenia.

6.6.3 Bezpečnostné opatrenia v životnom cykle

Žiadne ustanovenia.

6.7 Sieťové bezpečnostné opatrenia

Žiadne ustanovenia.

6.8 Využívanie časovej pečiatky

Žiadne ustanovenie

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 44/53

7. Profily certifikátov a zoznamov zrušených certifikátov

Profily certifikátov a zoznamov zrušených certifikátov sú stanovené centrálné - pracovníci RA nemôžu meniť štruktúru certifikátov.

7.1 Profily certifikátov

7.1.1 Verzia

Pozri časť 7.1.1 CP CA Disig.

7.1.2 Obsah a rozšírenia certifikátu

Pozri časť 7.1.2 CP CA Disig.

7.1.3 Identifikátory použitých algoritmov

Pozri časť 7.1.3 CP CA Disig.

7.1.4 Kódovanie názvov

Žiadne ustanovenia.

7.1.5 Obmedzenia týkajúce sa mien

Žiadne ustanovenia.

7.1.6 Identifikátor pravidiel CPS

Pozri časť 1.2.

7.1.7 Použitie rozšírení na obmedzenie politiky

Žiadne ustanovenia.

7.1.8 Syntax a sémantika politiky

Žiadne ustanovenia

7.1.9 Sémantika spracovania kritických certifikačných politik

Žiadne ustanovenia.

7.1.10 Ostatné ustanovenia

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 45/53

7.2 Profily zoznamov zrušených certifikátov

7.2.1 Verzia

Pozri časť 7.2 aktuálnej verzie CP CA Disig.

7.2.2 Použité rozšírenia (CRL extensions) v CRL vydávanom Poskytovateľom

Žiadne ustanovenia

7.3 Profil OCSP

7.3.1 Verzia

Žiadne ustanovenia.

7.3.2 OCSP rozšírenia

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 46/53

8. Audit zhody

Pozri časť 8 aktuálnej verzie CP CA Disig.

Na základe rozhodnutia externej organizácie, ktorá vykonáva posúdenie zhody poskytovaných dôveryhodných služieb Poskytovateľa, sa musí každá externá RA podrobiť auditu poskytovaných služieb a poskytnúť maximálnu súčinnosť, pokiaľ bude o umožnenie auditu požiadaná. Prípadné odmietnutie bude mať za následok ukončenie zmluvy a spolupráce s predmetnou RA.

8.1 Frekvencia auditu zhody pre danú entitu

Pozri časť 8.1 aktuálnej verzie CP CA Disig.

8.2 Identita audítora a kvalifikačné požiadavky na neho

Pozri časť 8.2 aktuálnej verzie CP CA Disig.

8.3 Vzťah audítora k auditovanému subjektu

Žiadne ustanovenia.

8.4 Témy pokryté audiom

Pozri časť 8.4 aktuálnej verzie CP CA Disig.

8.5 Akcie vykonané na odstránenie nedostatkov

Pozri časť 8.5 aktuálnej verzie CP CA Disig.

8.6 Zaobchádzanie s výsledkami auditu

Pozri časť 8.2 aktuálnej verzie CP CA Disig.

8.7 Interný audit

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 47/53

9. Iné obchodné a právne záležitosti

9.1 Poplatky

Cenník dôveryhodných služieb resp. informáciu, za akých zmluvných podmienok je možné tieto služby objednať je zverejnený na webovom sídle Poskytovateľa: <https://eidas.disig.sk/sk/poskytovatel/cenniky/>.

9.1.1 Poplatky za vydanie certifikátu

Pozri časť 9.1.1. aktuálnej verzie CP CA Disig.

9.1.2 Poplatok za prístup k certifikátu

Žiadne ustanovenia.

9.1.3 Poplatky za služby vydávania CRL a OCSP

Tieto služby sú poskytované bezodplatne.

9.1.4 Poplatky za ostatné služby

Žiadne ustanovenia.

9.1.5 Vrátenie platby

Žiadne ustanovenia.

9.2 Finančná zodpovednosť

Poskytovateľ má dostatočné zdroje na výkon ním poskytovaných dôveryhodných služieb.

9.2.1 Poistenie

Poskytovateľ je poistený v súvislosti s možnými škodami, ktoré môžu byť spôsobené Zákazníkom/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 Zákazníkov

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 48/53

9.3 Dôvernosť

9.3.1 Typy informácií, ktoré sa majú chrániť

Pozri časť 9.3.1 aktuálnej verzie CP CA Disig.

9.3.2 Nechránené informácie

Pozri časť 9.3.2 aktuálnej verzie CP CA Disig.

9.3.3 Zodpovednosť za ochranu dôverných informácií

Externé RA sú zodpovedné za ich ochranu dôverných informácií v zmysle zmluvy, ktorú majú uzavretú s Poskytovateľom.

9.4 Ochrana osobných údajov

9.4.1 Politika ochrany osobných údajov

Pozri časť 9.4.1 aktuálnej verzie CP CA Disig.

Poskytovateľ spracováva osobné údaje Zákazníkov/Držiteľov certifikátov, resp. nimi splnomocnených osôb v súlade s požiadavkami predpisov o ochrane osobných údajov t. j. Nariadenie Európskeho Parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a zákon č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „Predpisy o ochrane osobných údajov“) [10].

9.4.2 Informácie považované za osobné údaje

Poskytovateľ má definovaný rozsah osobných údajov, ktorý spracováva pri poskytovaní dôveryhodných služieb.

9.4.3 Informácie, ktoré nie sú považované za osobné údaje

Žiadne ustanovenia.

9.4.4 Zodpovednosť za ochranu osobných údajov

Externé RA sú zodpovedné za ochranu osobných údajov Zákazníkov/Držiteľov certifikátov a musia ich chrániť pred prezradením a musia sa zdržať ich poskytnutia tretej strane.

9.4.5 Súhlas so spracovaním osobných údajov

Poskytovateľ si plní informačnú povinnosť voči dotknutým osobám v súlade s požiadavkami predpisov o ochrane osobných údajov [10].

9.4.6 Zverejnenie na základe súdneho alebo správneho procesu

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 49/53

9.4.7 Ďalšie okolnosti zverejňovania informácií

Žiadne ustanovenia.

9.5 Práva duševného vlastníctva

Táto CPS a s ňou súvisiace dokumenty predstavujú významné know-how Poskytovateľa a sú chránené jeho autorskými právami.

9.6 Vyhlásenie a záruky

Pozri časť 9.6, aktuálnej verzie CP CA Disig.

9.6.1 Vyhlásenia a záruky Poskytovateľa

Pozri časť 9.6.1 aktuálnej verzie CP CA Disig.

9.6.2 Vyhlásenia a záruky RA

Všetky externé registračné authority Poskytovateľa poskytujú dôveryhodné služby na základe zmluvného vzťahu s poskytovateľom a v súlade s týmito CPS.

Ďalej pozri ustanovenia v časti 9.6.

9.6.3 Vyhlásenie a záruky Držiteľa

Žiadne ustanovenia.

9.6.4 Vyhlásenia a záruky spoliehajúcej sa strany

Žiadne ustanovenia.

9.6.5 Vyhlásenia a záruky iných strán

Žiadne ustanovenia.

9.7 Odmietnutie poskytnutia záruky

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

9.8 Obmedzenie zodpovednosti

Pozri časť 9.6.1 aktuálnej verzie CP CA Disig.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 50/53

9.9 Náhrada škody

Pre tieto CPS platí v plnom rozsahu časť 9.9 aktuálnej verzie CP CA Disig.

9.10 Doba platnosti, ukončenie platnosti

9.10.1 Doba platnosti

Tato verzia CPS platí odo dňa nadobudnutia jej platnosti t. j. 10. 1. 2025 až do jej nahradenia novou verziou. Podrobnosti o histórii zmien tejto CP sú uvedené v časti 1.2.1 „História zmien“.

9.10.2 Ukončenie platnosti

Platnosť tejto verzie CPS skončí dňom publikovania novej verzie s vyšším číslom ako je 6.3, prípadne ukončením činnosti poskytovania dôveryhodných služieb Poskytovateľom v čase ich platnosti.

9.10.3 Dôsledky ukončenia platnosti

V prípade, že tento dokument nebude nahradený novou verziou a v čase jeho platnosti dôjde k ukončeniu poskytovania dôveryhodných služieb zo strany Poskytovateľa, musia byť dodržané všetky ustanovenia týchto CPS týkajúce sa Poskytovateľa, ktoré je povinný dodržať po ukončení svojej činnosti (pozri časť 9).

9.11 Jednotlivé oznámenia a komunikácia s účastníkmi

Žiadne ustanovenia.

9.12 Zmeny

9.12.1 Postup vykonávania zmien

Aktualizácia CPS sa vykonáva na základe ich preskúmania, ktoré je vykonané minimálne 1x ročne od schválenia aktuálnej platnej verzie. Preskúmanie vykonáva poverený pracovník Poskytovateľa, ktorý na základe výsledkov preskúmania pripravuje písomný návrh na prípadné navrhované zmeny.

Schválenie navrhovaných zmien vykonáva poverený člen PMA v zmysle požiadaviek daných V časti 9.12.1 aktuálnej verzie CP CA Disig.

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

Všetky schválené zmeny CPS sú dávané na vedomie subjektom, ktorých sa týkajú, v lehote jedného týždňa pred nadobudnutím ich účinnosti, a to prostredníctvom kanálov publikačnej a oznamovacej politiky.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 51/53

Každá zmenená verzia týchto CPS 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 týchto CPS.

9.12.2 Postup a periodicita oznamovania zmien

Poskytovateľ publikuje informácie týkajúce sa aktuálnej verzie CPS prostredníctvom svojho webového sídla (pozri časť 1).

Poverený zástupca Poskytovateľa informuje všetky zmluvne viazané RA Poskytovateľa o schválení novej verzie CPS, zaslaním jeho verzie elektronickou poštou.

9.12.3 Okolnosti zmeny OID

Všetky pravidlá majú stanovený svoj OID Poskytovateľom. OID týchto CPS je uvedený v časti 1.2 a pre každú novú verziu CPS zostáva nezmenený.

9.13 Riešenie sporov

Pozri časť 9.13 aktuálnej verzie CP CA Disig.

9.14 Rozhodné právo

Pozri časť 9.14 aktuálnej verzie CP CA Disig.

9.15 Súlad s platnými právnymi predpismi

Pozri časť 9.13 aktuálnej verzie CP CA Disig.

9.16 Rôzne ustanovenia

9.16.1 Rámcová dohoda

Žiadne ustanovenia.

9.16.2 Postúpenie práv

Žiadne ustanovenia.

9.16.3 Salvatárska klauzula

Pokiaľ akékoľvek ustanovenie týchto CPS je alebo sa stane neplatným alebo nevymáhateľným, nespôsobí to neplatnosť alebo nevymáhateľnosť celých CPS, ak je úplne oddeliteľným od ostatných ustanovení týchto CPS. Poskytovateľ bezodkladne nahradí neplatné alebo nevymáhateľné ustanovenie CPS novým platným a vymáhateľným ustanovením, ktorého predmet bude v najvyššej možnej

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 52/53

miere zodpovedať predmetu pôvodného ustanovenia a zároveň bude zachovaný účel týchto CPS a obsah jednotlivých ustanovení týchto CPS.

9.16.4 Uplatnenie práv

Pozri časť 9.16.4 aktuálnej verzie CP CA Disig.

9.16.5 Vyššia moc

Pozri časť 9.16.5 aktuálnej verzie CP CA Disig.

9.17 Iné ustanovenia

Žiadne ustanovenia.

Súbor	cps_ra_cadisig	Verzia	6.3	
Typ	Pravidlá (OID: 1.3.158.35975946.0.0.0.1.3)	Dátum platnosti	10. 1. 2025	Strana 53/53