ARDACO
DATA & COMMUNICATION SECURITY

Pravidla na výkon certifikačných činností (CPS) Ardaco

ver. 1.5.7

História zmien

Verzia	Dátum vydania	Schválil	Poznámka
1.0	19.2.2021	Richard Margala	Prvá verzia dokumentu.
1.1	14.5.2021	Richard Margala	Doplnený profil mandátneho certifikátu
1.2	28.7.2021	Richard Margala	Úprava textov pre kvalifikované certifikáty, ktorých súkromné kľúče nie sú generované na QSCD.
1.3	28.7.2021	Richard Margala	Doplnenie bezpečnostnej rady ako zodpovednej osoby, popis paragrafu, § 6 ods. 2 zákona č. 272/2016, možnosť použitia elektronického podpisu Upresnená doba archivácie záznamov. Doplnené možnosti podpisovania zmluvnej dokumentácie. Doplnené monitorovanie platnosti certifikácie zariadení.
1.4.	28.7.2021	Richard Margala	Doplnený profil časovej pečiatky Doplnený profil vydávajúcej CA a OCSP respondera a aktualizované profily certifikátov. Aktualizovaná hierarchia CA.
1.5	1.9.2021	Richard Margala	Zapracovanie nedostatkov v správe o posúdení zhody Ardaco
1.5.1	16.12.2021	Richard Margala	Oprava chýb v terminológii (kapitola 6.1 Skratky)
1.5.2	3.3.2022	Richard Margala	Doplnenie aplikovania aj na nasledovné služby • Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov • Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických pečatí
1.5.3	12.4.2023	Richard Margala	Doplnenie požiadaviek na RA
1.5.4	30.5.2023	Richard Margala	Zapracovanie pripomienok z výkonu auditu a zmena okresného súdu Upresnenie profilu certifikátu (nsComment).
1.5.5	8.12.2023	Richard Margala	Doplnený zoznam spresňujúcich znakov pre uvádzanie dokladov v položke serialNumber.
1.5.6	8.12. 2023	Richard Margala	Zmena pojmu „Okresný súd Bratislava III“ na „Mestský súd Bratislava III“
1.5.7	26.1.2024	Richard Margala	Opravené formátovanie odstavca v 3.6.2 Overenie identity fyzickej osoby

1 Úvod

Tento dokument definuje pravidlá na výkon certifikačných činností Ardaco, a.s, so sídlom. Polianky 5, 841 01 Bratislava, zapísanej v Obchodnom registri Mestského súdu Bratislava III, v oddiely Sa, vložka číslo 2903/B (ďalej aj ,,Ardaco" alebo ,,Poskytovateľ")

Základný rámec pre poskytovanie kvalifikovaných dôveryhodných služieb tvoria:

- 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 (nariadenie eIDAS)
- Zákon č. 272/2016 Z.z. z 20. septembra 2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)
- Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu - NBÚ SR

1.1 Prehľad

Pravidlá na výkon certifikačných činností (CPS) Ardaco (Certificate Practice Statement, ďalej aj ,,CPS") spoločnosti Ardaco, a.s., slúžia účastníkom PKI ako podklad pre posúdenie dôveryhodnosti certifikátu.

Tieto CPS podporuje CA pre:

- Kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis
- Kvalifikovanú dôveryhodnú služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať
- Kvalifikovaná dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok
- Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov
- Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických pečatí

Plnenie CP KCA NBÚ pri vydávaní a overovaní kvalifikovaných certifikátov je podľa 5.2.1 SD čl. 17 ods. 5, čl. 24, 28, 38 a 45 nariadenia (EÚ) č. 910/2014 postup plnenia požiadaviek národnej legislatívy je uvedený najmä v kapitole 10 v certifikačnej politike koreňovej certifikačnej autority NBÚ (CP KCA NBÚ) OID (1.3.158.36061701.0.0.0.1.2.2), ktorá profiluje ETSI EN 319 411-2 V2.1.1 (2016-02) [8] certifikačné politiky pre vydávanie kvalifikovaných certifikátov.

Pre poskytovanie Kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok sa ďalej uplatňujú podmienky uvedené v dokumente ,,Certifikačná politika kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok".

1.2 Názov dokumentu a jednoznačná identifikácia

Názov dokumentu (jednoznačná identifikácia)	Pravidlá na výkon certifikačných činností (CPS) Ardaco ver. 1.5.4
OID	Neudeľuje sa

1.3 Kontaktné údaje

Adresa sídla spoločnosti	Ardaco, a.s.

	Polianky 5 841 01 Bratislava Slovenská republika
Internetová adresa	https://tsp.ardaco.com
E-mail:	info@ardaco.com
E-mail pre nahlasovanie incidentov:	incidents@ardaco.com

1.4 Skratky

CA	Certifikačná autorita
CP	Certifikačná politika
CPS	Pravidlá pre výkon certifikačných činností
CRL	Zoznam zneplatnených certifikátov (Certification Revocation List)
ČP	Časová pečiatka
KC	Kvalifikovaný certifikát
PKI	Infraštruktúra verejných kľúčov (Public Key Infrastructure)
RA	Registračná autorita
QSCD	Zariadenia na vyhotovenie kvalifikovaného elektronického podpisu (Qualified Signature Creation Device)
TSP	Poskytovateľ dôveryhodných služieb (Trusted Services Provider)

1.5 Účastníci PKI

1.5.1 Certifikačná autorita (CA)

Poskytovateľ – subjekt zodpovedný za poskytovanie dôveryhodných služieb podľa tejto certifikačnej politiky. Poskytovateľ môže vykonávaním časti služieb poveriť iný subjekt (napr. registračnú autoritu), avšak nesie zodpovednosť za dodržanie požiadaviek a opatrení, ktoré sú predmetom tejto politiky.

Hierarchia certifikačnej autority a autority časovej pečiatky je tvorená koreňovou certifikačnou autoritou, ktorá je zároveň vydávajúcou certifikačnou autoritou pre kvalifikované certifikáty a pečate. Vydávajúca certifikačná autorita zároveň vydáva certifikát pre kvalifikovanú službu časovej pečiatky a certifikát na potvrdenie existencie a platnosti certifikátu (OCSP).

Základné informácie o vydávajúcej CA:

Sériové číslo:	7ff729b79fdb1cb1bda611af098ecc33d9b18ecf
Algoritmus podpisu:	sha256RSA
DN vydavateľa	C = SK O = Ardaco a.s. 2.5.4.97 = NTRSK-35829036 CN = Ardaco QSCA
DN držiteľa	C = SK O = Ardaco a.s. 2.5.4.97 = NTRSK-35829036 CN = Ardaco QSCA
Číslo záznamu v dôveryhodnom zozname	TLISK-133

1.5.2 Registračná autorita (RA)

Služby poskytované registračnou autoritou sú zabezpečované priamo Poskytovateľom alebo externým zmluvným partnerom.

Služby registračnej autority typicky zhŕňajú:

a) príjem žiadosti o certifikát
b) overenie identity žiadateľa a ďalších náležitostí, ak sú pre požadovaný typ certifikátu potrebné
c) odovzdanie certifikátu Držiteľovi
d) príjem žiadostí o zneplatnenie

RA môže svoje činnosti delegovať na iného zmluvného partnera, ale daný zmluvný partner musí spĺňať rovnaké požiadavky ako samotná RA. RA je povinná informovať Poskytovateľa o aký subjekt sa jedná, preukázať zmluvnú dokumentáciu a taktiež informovať o každej zmene na úrovni zmluvného vzťahu spolupráce medzi RA a zmluvným partnerom.

RA na základe zmluvný podmienok môže:

1. prevádzkovať časť technického riešenia pre autentifikáciu používateľov na vlastných systémoch, pričom aj v takomto prípade, musí byť zaručený súlad s bezpečnostnou politikou prevádzkovateľa,
2. využívať vlastné vnútorné procesy a postupy (napr. definícia a výkon disciplinárneho procesu, či riadenie ľudských zdrojov), ale aj v takomto prípade, musí byť zaručený súlad s bezpečnostnou politikou prevádzkovateľa a jej procesmi ako aj komunikácia o zmenách v prepojených procesoch a postupoch,
3. menovať zamestnancov do dôveryhodných rolí určených na výkon RA činností, pričom musí zabezpečiť plnenia definované v kapitole 5.6 Personálne opatrenia.

1.5.3 Zákazník a držiteľ

Zákazník je fyzická alebo právnická osoba, ktorej Poskytovateľ poskytuje Dôveryhodné služby na základe Zmluvy.

Držiteľ je osoba uvedená v kvalifikovanom certifikáte ako držiteľ súkromného kľúča patriacemu k verejnému kľúču, ktorý je uvedený v danom certifikáte.

Zákazník a Držiteľ môžu byť dve rôzne entity. Zákazník môže byť napr. organizácia, ktorá využíva služby Poskytovateľa na zabezpečenie certifikátov pre fyzické osoby - Držiteľov, ktoré sú s touto organizáciou v určitom vzťahu (zamestnanci, konatelia a pod). Povinnosti Držiteľa a Zákazníka sú uvedené v Zmluve o vydaní a používaní kvalifikovaného certifikátu.

1.5.4 Spoliehajúce sa strany

Spoliehajúcimi stranami sú subjekty spoliehajúce sa pri svojej činnosti na výstupy poskytovania Dôveryhodných služieb podľa tejto CPS.

1.5.5 Bezpečnostná rada

Bezpečnostná rada (ďalej len ,,Rada") prijíma dôležité opatrenia v oblasti bezpečnosti. Súčasťou Rady sú minimálne nasledovné role

- Security Officer
- Information Security Officer
- System Auditor

Bezpečnostná rada sa stretáva aspoň raz za 6 mesiacov aby vyhodnotila bezpečnostnú situáciu a vykonala potrebné zmeny v bezpečnostných praktikách.

Bezpečnostná rada má konečnú právomoc a zodpovednosť za špecifikáciu a schválenie certifikačných politík, samotnej CPS ako aj za zabezpečenie procesu preskúmania daných certifikačných politík z dôvodu ich neustálej aktuálnosti.

Členov Rady menuje a menoval prevádzkový riaditeľ.

1.5.6 Iní účastníci

Participácia ďalších účastníkov je vymedzená platnými právnymi predpismi (orgán dohľadu, orgány činné v trestnom konaní, a pod).

Dodávateľ cloud služieb disponuje vlastnou optickou sieťou a poskytuje technologický priestor pre klientské zariadenia v 3 dátových centrách a je držiteľom certifikát ISO27001:2014 na poskytovanie služieb v oblasti telekomunikácií, informačných technológii a služieb dátových centier.

1.6 Použitie certifikátov

Kvalifikované certifikáty je možné používať iba v súlade s platnými právnymi predpismi. Kvalifikovaný certifikát podľa tejto CPS môže byť vydaný pre:

- fyzickú osobu za účelom podpory zdokonaleného elektronického podpisu podľa čl. 26 a 27 Nariadenia eIDAS [QCP-n]
- pre právnickú osobu za účelom podpory zdokonalenej elektronickej pečate podľa čl. 36 a 37 Nariadenia eIDAS [QCP-l]
- fyzickú osobu, kde súkromný kľúč sa nachádza na zariadení na vyhotovenie kvalifikovaného elektronického podpisu/pečate, za účelom podpory kvalifikovaného elektronického podpisu podľa čl. 3 bod 12 Nariadenia eIDAS [QCP-n-qscd]
- právnickú osobu, kde súkromný kľúč sa nachádza na zariadení na vyhotovenie kvalifikovaného elektronického podpisu/pečate, za účelom podpory kvalifikovanej elektronickej pečate podľa čl. 3 bod 27 Nariadenia eIDAS [QCP-l-qscd]

2 Zverejňovanie informácií a úložiská

Certifikáty musia byť umiestnené tak aby boli prístupné Držiteľom, Zákazníkom a spoliehajúcim sa stranám. Funkciou úložiska certifikátov plní webové sídlo Poskytovateľa podľa kap. 1.3. Webové sídlo je verejne dostupné. Prístup k informáciám o certifikátoch certifikačných autorít Poskytovateľa je verejne dostupný bez obmedzení. Poskytovateľ nezverejňuje na svojom sídle koncové certifikáty Držiteľov, pokiaľ na to nezíska priamy súhlas Držiteľa alebo subjektu, pre ktorý sa certifikát vydáva, pričom sú uplatnené nasledovné pravidlá.

a) Po vygenerovaní bude certifikát k dispozícii Držiteľovi alebo subjektu, pre ktorý sa certifikát vydáva.
b) Certifikáty sú k dispozícii na vyhľadanie iba v tých prípadoch, pre ktoré bol získaný súhlas subjektu. Ak je subjektom zariadenie alebo systém, je potrebné namiesto subjektu získať súhlas fyzickej alebo právnickej osoby zodpovednej za prevádzku zariadenia alebo systému.
c) Poskytovateľ sprístupní spoliehajúcim sa stranám podmienky týkajúce sa použitia certifikátu (viď odsek 6.9.4).
d) Uplatniteľné podmienky musia byť pre daný certifikát ľahko identifikovateľné.

CP, CPS je schvaľovaná a upravovaná v súlade s definovaným procesom „GL-450-Control of Documents“ vrátane zodpovedností za udržiavanie CP, CPS ako aj ich aktualizáciu.

Všetky zmeny CP ako aj CPS či zmluvných podmienok musia byť a budú publikované aj na webovom sídle (viď položka „Internetová adresa“ v kapitole 1.3 Kontaktné údaje)

3 Identifikácia a autentifikácia

3.1 Typy mien

Poskytovateľ musí vytvárať certifikáty s rozlišovacími menami v súlade s platnými technickými normami, menovite odporúčaním ITU-T X.509 [10] a IETF RFC 5280 [9] a príslušnej časti ETSI EN 319 412 [8]

3.2 Zmysluplnosť mien

Používané mená majú spoľahlivo identifikovať osoby, ktorým sú certifikáty vydané a musia byť ľahko zrozumiteľné. Forma mien je založená na tvare, ktorý je bežne používaný na identifikáciu osoby (skutočné meno a priezvisko fyzickej osoby, názov právnickej osoby uvedený v príslušnom registri, názov orgánu verejnej moci).

3.3 Anonymita a používanie pseudonymov

Poskytovateľ neumožňuje vydanie certifikátu pre anonymnú osobu.

Poskytovateľ umožňuje vydanie certifikátu, v ktorom je miesto bežne používaného mena uvedený iný názov. V takomto prípade v názve uvedie aj text "PSEUDONYM". Mandátny certifikát podľa § 8 ods. 5 zákona č. 272/2013 Z. z nesmie obsahovať pseudonym.

Poskytovateľ si vyhradzuje právo zamietnuť názov, ktorý je hanlivý, narúša všeobecnú mravnosť, alebo môže spoliehajúcu sa stranu uviesť do omylu tým, že vzbudzuje mylnú a klamlivú predstavu o tom, kto je jeho skutočným držiteľom.

3.4 Jedinečnosť mien

Poskytovateľ garantuje jedinečnosť mien (pole *Subject*) pre všetky vydané certifikáty.

3.5 Uznávanie, overovanie a význam obchodných značiek

V certifikáte môžu byť použité len tie obchodné značky, ktorých vlastníctvo alebo prenájom žiadateľ o certifikát uspokojivo doložil.

Poskytovateľ si vyhradzuje právo obchodnú značku v certifikáte neuviesť. Poskytovateľ nenesie zodpovednosť za zneužitie obchodnej značky.

3.6 Úvodné overenie identity

3.6.1 Preukazovanie vlastníctva súkromného kľúča

Ak kľúčový pár nie je generovaný Poskytovateľom, vlastníctvo súkromného kľúča, ktorý zodpovedá verejnému kľúču sa preukazuje žiadosťou vo formáte PKCS#10. PKCS#10 žiadosť je podpísaná súkromným kľúčom, čím preukazuje, že je súkromný kľúč v držbe Žiadateľa.

Ak má kvalifikovaný certifikát obsahovať atribút, že kľúč je umiestnený na QSCD, kľúčový pár, na ktorý sa vyhotovuje kvalifikovaný certifikát musí byť generovaný priamo na kvalifikovanom zariadení na vyhotovenie kvalifikovaného elektronického podpisu (QSCD), ktoré spĺňa požiadavky Nariadenia eIDAS. Poskytovateľ je povinný túto skutočnosť overiť.

3.6.2 Overenie identity fyzickej osoby

Poskytovateľ musí overiť identitu fyzickej osoby a akýchkoľvek špecifických atribútov, ktoré sú uvádzané v certifikáte.

Overenie identity je možné jedným z nasledovných spôsobov:

a) preukázaním sa primárnym a sekundárnym dokladom
b) podpisom kľúčom, ktorý patrí kvalifikovanému certifikátu, pričom tento pôvodný kvalifikovaný certifikát
   - bol vydaný Poskytovateľom, čím nie je dotknutá povinnosť Poskytovateľa overiť aktuálnosť údajov, alebo
   - ide o kvalifikovaný certifikát vydaný na elektronický občiansky preukaz s čipom podľa § 4 Zákona č 395/2019 Z. z. o občianskych preukazoch a o zmene a doplnení niektorých zákonov a Poskytovateľ overí živosť osoby
c) preukázaním sa primárnym dokladom a záznamom o vykonaní kontroly aktuálnosti údajov voči spoľahlivému zdroju (napr. Register fyzických osôb, Registr obyvatel) a to najmä v prípade, že je registračnou autoritou banka, pričom bola osoba identifikovaná v zmysle AML predpisov
   - v SR: zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov
   - v ČR: zákon č. 253/2008 Sb. zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
   - v iných štátoch vnútroštátny predpis adresujúci problematiku AML za dodržania podmienky preukázania sa primárnym dokladom a kontroly aktuálnosti údajov

Primárnym dokladom je:

a) pre občanov Slovenskej republiky je občiansky preukaz alebo cestovný pas
b) občanov iných členských štátov EÚ osobný doklad používaný na preukazovanie totožnosti na území daného členského štátu alebo cestovný pas
c) pre iných cudzincov cestovný pas

Sekundárnym dokladom je:

a) občiansky preukaz
b) cestovný pas
c) vodičský preukaz
d) zbrojný preukaz
e) služobný preukaz

Za jednoznačné identifikačné údaje sa považuje nasledovná kombinácia:

a) meno a priezvisko osoby (súčasné ako aj pri narodení)

b) rodné číslo, ak ho má osoba pridelené (ide o jedinečný identifikátor vytvorený odosielajúcim členským štátom v súlade s technickými špecifikáciami na účely)
c) dátum narodenia, ako ho osoba pridelené nemá
d) miesto narodenia
e) súčasná adresa

Poskytovateľ musí vytvoriť záznam o overení identity, ktorý obsahuje každú z nasledovných položiek:
a) jednoznačné identifikačné údaje overovanej osoby podľa predošlého odstavca
b) identifikáciu prostriedkov použitých na identifikáciu osoby, ak bol použitý
   - doklad - jeho číslo, vydavateľ a dátum platnosti (ak je vyznačený)
   - kvalifikovaný certifikát - common name, sériové číslo a vydavateľ
   - transakcia - číslo transakcie, číslo účtu odosielateľa a prijímateľa
c) identifikáciu osoby, ktorá identifikáciu vykonala
d) dátum identifikácie

3.6.3 Overenie oprávnenia konať

Overenie oprávnenia konať je potrebné pre vydanie mandátneho certifikátu podľa § 8 zákona č. 272/2016 Z. z.

Pri žiadosti o mandátny certifikát musí Žiadateľ preukázať preukazuje oprávnenie budúceho Držiteľa:
a) konať za, alebo v mene mandanta (fyzická osoba alebo právnická osoba),
b) vykonávať činnosť podľa osobitného predpisu, alebo
c) vykonávať funkciu podľa osobitného predpisu.

Oprávnenie sa preukazuje podľa zoznamu dokladov, ktoré sú pre dané oprávnenie uvedené v zozname oprávnení podľa § 9 zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov.

Doklad slúžiaci na overenie oprávnenia konať musí byť originál alebo úradne overená kópia.

Poskytovateľ môže na preukázanie oprávnenia konať akceptovať aj hromadný zoznam oprávnených osôb a ich oprávnení. Zoznam musí byť autorizovaný štatutárnym orgánom organizácie, ktorá o vydanie mandátneho certifikátu žiada, alebo inou oprávnenou osobou.

Hromadný zoznam musí obsahovať
a) meno a priezvisko osoby, ktorej má byť mandátny certifikát vydaný,
b) typ a číslo identifikačného dokladu
c) číslo oprávnenia

Poskytovateľ musí vytvoriť záznam o overení identity, ktorý obsahuje každú z nasledovných položiek:
a) identifikáciu prostriedkov použitých preukázanie oprávnenia konať (číslo dokladu ak existuje, vydavateľ, dátum platnosti)
b) identifikáciu osoby, ktorá identifikáciu vykonala
c) dátum identifikácie

3.6.4 Overenie identity právnickej osoby

Poskytovateľ musí overiť identitu právnickej osoby a akýchkoľvek špecifických atribútov, ktoré sú uvádzané v certifikáte buď:

a) fyzickou prítomnosťou oprávneného zástupcu alebo
b) metódami, ktoré poskytujú rovnaký stupeň záruk ako fyzická prítomnosť oprávneného zástupcu

Na overenie identity právnickej slúži výpis z registra, v ktorom je daná právnická osoba evidovaná (napr. Obchodný register, Živnostenský register, Register neziskových organizácií a pod).

Doklad slúžiaci na overenie oprávnenia konať musí byť originál alebo úradne overená kópia.

Minimálny súbor údajov pre právnické osoby

a) Minimálny súbor údajov pre právnické osoby musí obsahovať všetky tieto povinné atribúty:
    a. súčasný úradný názov (názvy),
    b. jedinečný identifikátor vytvorený odosielajúcim členským štátom v súlade s technickými špecifikáciami na účely cezhraničnej identifikácie a pokiaľ možno následne nemenený.
b) Minimálny súbor údajov pre právnické osoby musí obsahovať jeden alebo viacero týchto povinných atribútov:
    a. súčasná adresa,
    b. registračné číslo DPH,
    c. daňové registračné číslo,
    d. identifikátor (identifikačný znak) uvedený v článku 3 ods. 1 smernice Európskeho parlamentu a Rady 2009/101/ES (1),
    e. identifikátor právneho subjektu (LEI) uvedený vo vykonávacom nariadení Komisie (EÚ) č. 1247/2012 (2),
    f. číslo registrácie a identifikácie hospodárskych subjektov (EORI) uvedené vo vykonávacom nariadení Komisie (EÚ) č. 1352/2013 (3),

Poskytovateľ musí vytvoriť záznam o overení identity, ktorý obsahuje každú z nasledovných položiek:

a) identifikáciu prostriedkov použitých preukázanie oprávnenia konať (číslo dokladu ak existuje, vydavateľ, dátum platnosti)
b) identifikáciu osoby, ktorá identifikáciu vykonala
c) dátum identifikácie

3.7 Identifikácia a autentifikácia pre žiadosti opakované vydanie kľúča

Pri opakovanom vydaní kľúča (následný certifikát) Zákazník preukazuje vlastníctvo kľúča, identitu a oprávnenia spôsobom uvedeným v sekcii 3.6 Úvodné overenie identity. Na podpis žiadosti môže použiť pôvodný kvalifikovaný certifikát platný v čase jeho žiadosti.

Ak sa ktorákoľvek z podmienok poskytovania Služby zmenila, budú zmeny oznámené účastníkovi a odsúhlasené v súlade s ustanoveniami kap. 4.4.

3.8 Identifikácia a autentifikácia pre žiadosti o zrušenie platnosti certifikátu

Oprávnenými osobami pre zaslanie žiadosti o zrušenie platnosti certifikátu sú

a) Držiteľ certifikátu

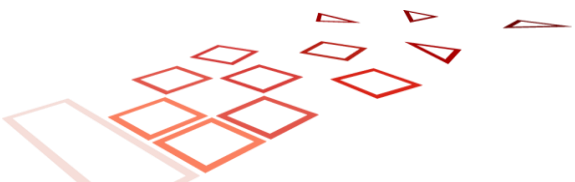
b) osoba, v mene ktorej Držiteľ koná (typicky zánik oprávnenia)
c) štátne orgány, ktoré na to majú zo zákona oprávnenie

Žiadosť o zrušenie platnosti certifikátu je možné predložiť v listinnej alebo elektronickej forme. Žiadosť musí byť autentizovaná, pričom oprávnený subjekt ju môže autentizovať :

a) osobne, po identifikácii spôsobom podľa sekcie 3.6
b) vzdialene s uvedením autentizačného hesla určeného na tento účel
c) vzdialene, podpisom žiadosti o zrušenie certifikátu kľúčom, ktorý má byť zrušený

Poskytovateľ si vyhradzuje právo zrušiť po dohode s oprávneným subjektom certifikát aj iným spôsobom, na ktorom sa dohodnú, a ktorý jednoznačne preukazuje vôľu oprávneného subjektu. Platnosť certifikátu môže byť zrušená aj Poskytovateľom, oprávnená rola je uvedená v prevádzkovej smernici.

Podrobné informácie o oprávnených osobách, procese zrušenia platnosti sú uvedené v sekcii 4.9.



4 Požiadavky na životný cyklus certifikátu

4.1 Žiadosť o certifikát

4.1.1 Kto môže požiadať o vydanie certifikátu

Osoby, ktoré sú oprávnené Poskytovateľa žiadať o vydanie certifikátu sú:

a) **kvalifikovaný certifikát** - fyzická osoba pre seba alebo osoba ňou splnomocnená
b) **kvalifikovaný mandátny certifikát –** fyzická osoba po preukázaní splnenia požiadaviek v zmysle §8 ods. 3 zákona 272/2016 Z. z alebo subjekt, s ktorým je táto fyzická osoba spojená v zmysle daného odseku. .
c) **kvalifikovaný certifikát pre pečať** – osoba oprávnená konať v mene právnickej osoby, alebo osoba ňou splnomocnená pre túto organizáciu

V prípade, že o vydanie certifikátu žiada splnomocnená osoba, musí sa preukázať úradne overeným splnomocnením, ktoré preukazuje oprávnenosť splnomocnenca vykonať daný úkon v mene splnomocniteľa.

4.1.2 Registračný proces a zodpovednosti

Registračný proces je vykonávaný pred prvotným vydávaním certifikátu. Proces je iniciovaný Žiadateľom .

Registračný proces je možné vykonať:

a) na mieste, osobnou návštevou CA alebo RA
b) vzdialene, pričom technické prostriedky musia poskytovať rovnakú úroveň záruk overenia identity ako pri osobnej návšteve

Žiadateľ je povinný najmä:

a) poskytovať pravdivé a úplné informácie potrebné pre vydanie certifikátu
b) pripraviť si a predložiť doklady potrebné pre overenie identity a vydanie certifikátu
c) oboznámiť sa a odsúhlasiť Zmluvu o vydaní a používaní kvalifikovaného certifikátu a Súhlas so spracovaním osobných údajov
d) zvoliť si vhodné heslo pre zneplatnenie certifikátu (min. požiadavky sú uvedené v dokumentácii pre vydanie certifikátu)

Poskytovateľ je povinný najmä:

a) venovať primeranú pozornosť vykonávaniu všetkých aktivít, ktoré súvisia s poskytovaním kvalifikovaných služieb
b) informovať Žiadateľa o zmluvných podmienkach
c) overiť údaje uvedené v predložených dokladoch v primeranom rozsahu
d) ak kľúčový pár nie je generovaný Poskytovateľom, overiť, či subjekt vlastní alebo ovláda súkromný kľúč spojený s verejným kľúčom, ktorý bol predložený na vydanie certifikátu
e) ak má certifikát obsahovať atribút, že kľúč je umiestnený na QSCD, overiť túto skutočnosť

Žiadateľ má umožnené požadovanú dokumentáciu podpisovať:

1. zdokonaleným alebo kvalifikovaným podpisom pomocou na to určených nástrojov resp.
2. zaslaním podpísanej dokumentácie v papierovej forme.

Spoločnosť sa riadi ako aj má definovaný interný proces, definujúci podrobnosti pre realizáciu riešenia pre podpisovanie kvalifikovaným elektronickým podpisom na diaľku v rámci výkonu kvalifikovaných dôveryhodných služieb Ardaco, a.s. podľa VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu. Daný popis riešenia je garantovaný certifikačnou politikou pre kvalifikovaný certifikát.

4.2 Spracovanie žiadosti o certifikát

Po vykonaní identifikácie a autentifikácie (3.6 Úvodné overenie identity, 3.7 Identifikácia a autentifikácia pre žiadosti opakované vydanie kľúča musí byť žiadosť odoslaná Poskytovateľovi. Registračné údaje musia byť prenášané zabezpečeným kanálom. V prípade externej RA musia byť údaje prijaté iba od známych RA, ktorých identita bola overená.

4.3 Vydanie certifikátu

Poskytovateľ vydáva certifikáty bezpečným spôsobom tak, aby bola zabezpečená ich autenticita. Ak kľúčový pár generuje Poskytovateľ, musí zabezpečiť dôvernosť údajov v priebehu celého procesu. Poskytovateľ pomocou programového vybavenia kontroluje splnenie štandardu pre formát žiadosti (PKCS#10).

Počas celej existencie CA nesmie byť rovnaké rozlišujúce meno (distinguished name) v certifikáte použité pre dve rôzne entity.

4.4 Prevzatie certifikátu

4.4.1 Spôsob prevzatia

Podrobné podmienky toho, čo je považované za prevzatie certifikátu ustanovujú zmluvné podmienky.

4.4.2 Zverejnenie certifikátu

Certifikát je zverejnený v zmysle kap. 2. Aplikujú sa obmedzenia pre zverejňovanie osobných údajov.

4.4.3 Oznámenie o vydaní certifikátu iným stranám

Na základe § 6 ods. 2 zákona č. 272/2016 Z. z. Poskytovateľ odosiela vydané certifikáty Národnému bezpečnostnému úradu.

Kvalifikovaný poskytovateľ dôveryhodných služieb, ktorému úrad udelil kvalifikovaný štatút, zasiela úradu

a) vydané kvalifikované certifikáty pre kvalifikovaný elektronický podpis a pre kvalifikovanú elektronickú pečať do 30 dní od vydania kvalifikovaného certifikátu,
b) po zrušení certifikátov podľa písmena a) potvrdenie o dátume a čase ich zrušenia do 30 dní od ich zrušenia,
c) informáciu o ukončení používania údajov na vyhotovenie elektronického podpisu alebo elektronickej pečate kvalifikovanej dôveryhodnej služby, ktoré zodpovedajú údajom na validáciu elektronického podpisu alebo elektronickej pečate z certifikátov uvedených pre túto službu v dôveryhodnom zozname do 30 dní od ukončenia

používania týchto údajov; to neplatí, ak dátum a čas konca platnosti posledného certifikátu uvedeného pre túto službu v dôveryhodnom zozname je zhodný s dátumom a časom ukončenia používania údajov na vyhotovenie elektronického podpisu alebo elektronickej pečate.

4.5 Použitie kľúčového páru a certifikátu

4.5.1 Používanie súkromného kľúča a certifikátu Držiteľom

Držiteľ je povinný najmä

a) používať súkromný kľúč a certifikát iba na účel, na ktorý bol určený
b) dodržiavať všetky ustanovenia tohto CPS, Zmluvy o poskytovaní Služby a legislatívy pre dôveryhodné služby, ktoré sa vzťahujú k povinnostiam Držiteľa
c) zabrániť neoprávnenému použitiu súkromného kľúča
d) bezodkladne informovať Poskytovateľa o skutočnostiach, ktoré vedú k zneplatneniu certifikátu, predovšetkým stratu, podozrenie s neoprávneného použitia súkromného kľúča alebo kompromitáciu prístupových údajov
e) pri kompromitácii súkromného kľúča okamžite ukončiť jeho používanie

4.5.2 Používanie verejného kľúča a certifikátu Spoliehajúcou sa stranou

Spoliehajúce sa strany sú povinné:

a) používať certifikát iba na účel, na ktorý bol určený
b) overiť stav certifikátu pomocou aktuálnych informácií o stave zrušenia, ako sú zverejňované spoliehajúcim sa stranám
c) dodržiavať všetky ustanovenia tejto CPS a legislatívy pre dôveryhodné služby, ktoré sa vzťahujú k povinnostiam Spoliehajúcej sa strany

4.6 Obnova certifikátu

Poskytovateľ neposkytuje službu obnovy certifikátu. Pod obnovou certifikátu sa chápe vydanie následného certifikátu k ešte platnému certifikátu, bez toho, aby bol zmenený verejný kľúč alebo informácie uvedené v certifikáte. Poskytovateľ nesmie vydať certifikát na verejný kľúč, na ktorý už bol v minulosti certifikát vydaný.

4.7 Vydanie následného certifikátu

Pod vydaním následného certifikátu chápe vydanie nového certifikátu rovnakého typu a s rovnakým obsahom pre registrovaného Držiteľa.

4.7.1 Podmienky vydania následného certifikátu

Žiadne ustanovenia.

4.7.2 Kto môže žiadať o vydanie následného certifikátu

O vydanie následného certifikátu môže žiadať existujúci Zákazník a/alebo Držiteľ, ktorý musí splniť požiadavky na identifikáciu a autentifikáciu podľa 3.6.

4.7.3 Postup žiadania o vydanie následného certifikátu

Postup žiadania je identický s žiadaním o vydanie prvotného certifikátu, kap. 4.1. Poskytovateľ musí oznámiť Zákazníkovi a Držiteľovi akúkoľvek zmenu podmienok poskytovania služby a dať mu ich na odsúhlasenie.

4.7.4 Oznámenie o vydaní následného certifikátu

Poskytovateľ musí vhodným spôsobom informovať Držiteľa o vydaní následného certifikátu.

4.7.5 Prevzatie následného certifikátu

Aplikuje sa postup podľa kap. 4.4.1.

4.7.6 Zverejňovanie následného certifikátu

Aplikuje sa postup podľa kap. 4.4.2

4.7.7 Oznámenie o vydaní následného certifikátu iným stranám

Aplikuje sa postup podľa 4.4.3

4.8 Modifikácia certifikátu

Poskytovateľ nepodporuje službu modifikácie certifikátu (vydanie certifikátu s upraveným obsahom bez zmeny kľúčového páru).

4.9 Zrušenie a pozastavenie certifikátu

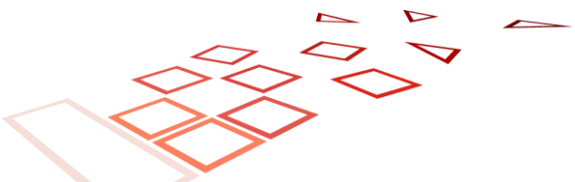
4.9.1 Podmienky zrušenia certifikátu

Poskytovateľ zruší Certifikát najmä na základe nasledujúcich okolností:

a) o zrušenie certifikátu požiada oprávnená osoba podľa 4.9.2
b) Poskytovateľ zistí, že došlo ku kompromitácii, resp. existuje dôvodné podozrenie, že došlo ku kompromitácii súkromného kľúča patriaceho k danému certifikátu
c) Poskytovateľ zistí, že pri vydaní certifikátu neboli splnené požiadavky platnej legislatívy najmä Nariadenia eIDAS alebo zákona č. 272/2016 Z.z.
d) Poskytovateľ zistí, že certifikát bol vydaný na základe nepravdivých údajov
e) Poskytovateľ sa dozvie podstatnú skutočnosť, ktorá znamená, že certifikát naďalej nemôže plniť svoj účel napr. Držiteľ zomrel, bol vyhlásený za mŕtveho, bol zbavený svojprávnosti, organizácia uvedená v certifikáte zanikla alebo došlo k zmene údajov, ktoré sú uvedené v certifikáte
f) V prípadoch, kedy nastanú skutočnosti uvedené v právnych predpisoch pre dôveryhodné služby alebo príslušných štandardoch a normách (napr. neplatnosť údajov v Certifikáte)

Poskytovateľ si vyhradzuje akceptovať aj iné podmienky pre zrušenie, ktoré však nesmú byť v rozpore s platnou legislatívou.

Platnosť zrušeného certifikátu jeho nesmie byť obnovená za žiadnych okolností.



4.9.2 Kto môže žiadať o zrušenie certifikátu

Žiadosť o zrušenie certifikátu môže podať:

a) Držiteľ
b) iná osoba uvedená v Zmluve o poskytovaní Služieb
c) oprávnené osoby podľa § 8 ods. 4. zákona č. 272/2016 Z.z. v prípade mandátneho certifikátu
d) Poskytovateľ pri dodržaní podmienok 4.9.1
e) ďalšie subjekty v súlade s platnou legislatívou

4.9.3 Postup žiadosti o zrušenie certifikátu

Žiadosť o zrušenie certifikátu je možné podať osobne v prevádzkových hodinách uvedených na webovom sídle Poskytovateľa alebo elektronicky na kontaktných adresách uvedených v kap. 1.3. Formulár pre zrušenie certifikátu Poskytovateľ zverejňuje na svojom webovom sídle.

Žiadosť musí byť autentifikovaná a to buď:

a) identifikáciou a autentifikáciou rovnakým spôsobom, ako pri úvodnom overení identity 3.6
b) identifikáciou a autentifikáciou na to určenými technickými prostriedkami
c) preukázaním sa dohodnutými autentizačnými údajmi pre zrušenie certifikátu, ktoré Zákazník/Držiteľ dostane pri vydaní certifikátu
d) podpisom žiadosti o zrušenie certifikátu kľúčom, ktorý patrí k certifikátu, ktorý má byť zrušený

Žiadosť musí obsahovať jednoznačnú identifikáciu certifikátu, ktorý má byť zrušený. Jednoznačnou identifikáciou je sériové číslo certifikátu, v prípade ak nie je oprávnenej osobe známe, je možné použiť kombináciou iných údajov, ktoré umožňujú jednoznačnú identifikáciu. Dátum a čas zrušenia platnosti certifikátu sú dané spracovaním žiadosti.

Poskytovateľ po vybavení žiadosti informuje Žiadateľa o výsledku vybavenia. V prípade kompromitácie súkromného kľúča alebo hrozby kompromitácie musí byť žiadosť podaná bezodkladne, t.j. okamžite, ako sa Žiadateľ o kompromitácii súkromného kľúča alebo hrozbe kompromitácie dozvedel. Poskytovateľ nezodpovedá za škodu vzniknutú v dôsledku nedodržania lehoty Žiadateľom podľa predchádzajúcej vety. Poskytovateľ nezodpovedá za škodu spôsobenú použitím Certifikátu v období po podaní žiadosti o jeho zrušenie za predpokladu, že dodržal lehoty stanovené v bodoch 4.9.4 a 4.9.5.

4.9.4 Doba na spracovanie žiadosti

Maximálna doba medzi prijatím žiadosti o jeho zneplatnením je 24 hodín. Zrušenie je účinné ihneď po jeho uverejnení.

4.9.5 Latencia pre publikovanie CRL

Poskytovateľ publikuje CRL ihneď po jeho vydaní. Latencia pre publikovanie je daná výhradne latenciou infraštruktúry a je časovo zanedbateľná.

4.9.6 Oznámenie o zrušení certifikátu iným stranám

Na základe § 6 ods. 2 písm. b) zákona č. 272/2016 Z. z. Poskytovateľ odosiela potvrdenie o dátume a čase ich zrušenia do 30 dní od ich zrušenia Národnému bezpečnostnému úradu.

4.10 Služby overovania stavu certifikátu

Overovanie stavu certifikátov vydaných Poskytovateľom je možné na základe CRL alebo OCSP. Zoznamy CRL sa generujú minimálne každých 24 hodín a sú automaticky zverejnené v úložisku (viď kap. 2). Stav certifikátu vydaného Poskytovateľom je možné overiť aj pomocou služby OCSP, táto informácia je vždy obsiahnutá vo vydanom certifikáte. Ak bola adresa služby OCSP zahrnutá v certifikáte, znamená to, že táto služba je k dispozícii pre tento certifikát.

Služby sú dostupné 24 hodí, 7 dní v týždni, pričom Poskytovateľ garantuje integritu a autenticitu poskytovaných informácií. V prípade poruchy systému, alebo iných faktorov, ktoré sú mimo kontroly Poskytovateľa, Poskytovateľ vynaloží maximálne úsilie aby doba nedostupnosti nepresiahla nevyhnutný čas.

Informácie o zrušení certifikátu v CRL a OCSP sú konzistentné a sú udržiavané v CRL alebo OCSP odpovedi minimálne do času exspirácie certifikátu.

4.11 Ukončenie poskytovania služieb

Podmienky ukončenia poskytovania služieb sú uvedené v zmluvných podmienkach.

4.12 Úschova a obnova kľúčov

Poskytovateľ túto službu neposkytuje.

5 Opatrenia fyzickej bezpečnosti, riadenia a prevádzky

5.1 Všeobecné

Uplatňujú sa požiadavky uvedené v ustanovení 5, 6.3 a 7.3 normy ETSI EN 319 401 , ktoré sú definované v samostatnom dokumente Politika pre KC a ČP ako aj certifikačná politika pre KC a ČP.
Taktiež sa uplatňujú požiadavky uvedené v ustanovení 6.4.1 normy ETSI EN 319 411-2 , ktoré sú definované v samostatnom dokumente Politika pre KC ako aj certifikačná politika pre KC a ČP.

5.1.1 Risk Assesment

Poskytovateľ vykoná posúdenie rizika s cieľom identifikovať, analyzovať a vyhodnotiť riziká dôveryhodných služieb s prihliadnutím na obchodné a technické problémy. Následne identifikuje a vyberie vhodné opatrenia na ošetrenie rizika s prihliadnutím na výsledky posúdenia rizika. Opatrenia na ošetrenie rizika zabezpečia, aby úroveň bezpečnosti bola primeraná stupňu rizika.
Rizikový manažment je plne integrovaný v rámci existujúcich procesov riadených podľa normy ISO9001 s integrovanými vybranými a platnými postupmi definovanými normou ISO27005.

5.1.1.1 Posúdenie rizík

Poskytovateľ minimálne počas preskúmania manažmentom posudzuje organizačné riziká pričom uchováva aj zdokumentované informácie. Ďalšia možnosť posudzovania rizika je pravidelne počas projektovej porady ako aj počas porád jednotlivých oddelení organizácie. Následne riziká sú ošetrované priebežne podľa výskytu a vlastníka .

Projektové riziká sú zaznamenávané v rámci dokumentu „Risk assessment“. IT riziká (do danej skupiny patria aj bezpečnostné riziká) sú evidované na procesnom portály , aby bolo zabezpečené riešenie na úrovni manažmentu. Takto odsúhlasené kroky sú následne evidované v internom systéme alebo vytvorením samostatného interného projektu.

Kompletný proces postup je definovaný v samostatnom dokumente s názvom „Risk Manažment“.

5.2 Bezpečnostná politika (Information security policy)

Organizácia má definovanú politiku bezpečnosti informácií ako samostatný dokument, ktorá je schválená vedením organizácie, ktorá stanovuje prístup organizácie k riadeniu jej informačnej bezpečnosti.

Zmeny v politike bezpečnosti informácií sa v prípade potreby oznamuje tretím stranám (predplatiteľom, spoliehajúcim sa stranám, hodnotiacim orgánom, dozorným alebo iným regulačným orgánom).

Politika bezpečnosti informácií je teda zdokumentovaná, implementovaná a udržiavaná vrátane bezpečnosti kontroly a prevádzkové postupy pre zariadenia, systémy a informačné aktíva organizácie poskytujúce dôveryhodné služby. Taktiež je zverejnená a oznámená všetkým zamestnancom, ktorých sa to týka.

Politika bezpečnosti informácií a súpis aktív pre informačnú bezpečnosť je pravidelne preskúmavaná v plánovaných intervaloch alebo ak dôjde k významným zmenám s cieľom zabezpečiť ich nepretržitú vhodnosť a primeranosť a efektívnosť. Všetky zmeny, ktoré majú vplyv na úroveň poskytovanej bezpečnosti, sú schválené.

Konfigurácia systémov je taktiež pravidelne kontrolovaná na zmeny, ktoré porušujú bezpečnostné politiky.

5.3 Správa majetku (Asset management)

5.3.1 Všeobecné požiadavky (General requirements)

Organizácia zabezpečuje primeranú úroveň ochrany svojich aktív vrátane informačných aktív. Taktiež vedie inventarizáciu všetkých informačných aktív a prideľuje klasifikáciu v súlade s hodnotením rizika, ako samostatný dokument.

5.3.2 Správa médií (Media handling)

So všetkými médiami sa zaobchádza bezpečne v súlade s požiadavkami schémy klasifikácie informácií. Médiá obsahujúce citlivé údaje sú bezpečne zneškodnené, ak už nie sú potrebné.

Proces riadenie médií je definovaný ako samostatný dokument.

5.4 Opatrenia fyzickej bezpečnosti

5.4.1 Priestory

Všetky systémy a zariadenia pre prevádzku kvalifikovaných dôveryhodných služieb sú prevádzkované v priestoroch, ktoré sú chránené pred neautorizovaným prístupom. Fyzická ochrana priestorov spočíva v jasne oddelených bezpečnostných perimetroch (fyzické bariéry – steny, mreže), pričom bezpečnostný perimeter nie je zdieľaný s inými organizáciami.

5.4.2 Fyzický prístup

Každý prístup do fyzicky zabezpečených priestorov je predmetom nezávislého dohľadu. Ochrana objektu je riešená strážnou službou a elektronickým zabezpečovacím systémom. Prístup neautorizovaných osôb je možný iba v sprievode autorizovaných osôb. Každý vstup a opustenie priestorov je zaznamenaný. Mechanizmy použité na autorizáciu prístupu sú uvedené v dokumentácii dátového centra.

5.4.3 Napájanie a klimatizácia

Elektrické napájanie je zabezpečené viacerými vetvami s vlastnými transformátormi a záložným zdrojom napájania (UPS, generátor). Chladenie je zabezpečené redundantnými klimatizačnými jednotkami.

5.4.4 Ochrana pred vodou

Priestory sú umiestnené mimo záplavového územia a realizované tak, aby nemohlo dôjsť k ohrozeniu vodou z iných zdrojov.

5.4.5 Ochrana pred ohňom

Priestory sú oddelené od priamych zdrojov tepla a ohňa a sú chránené automatickým protipožiarnym systémom na báze elektricky nevodivého hasiaceho média.

5.4.6 Uchovávanie médií

Médiá v elektronickej a listinnej forme sú uchovávané tak, aby boli chránené pred náhodným alebo úmyselným poškodením a neautorizovaným prístupom (kovová skriňa, trezor). Záložné kópie sú uchovávané v priestoroch, ktoré nie sú fyzicky spojené s prevádzkovými priestormi.

5.4.7 Nakladanie s odpadom

Úložné médiá obsahujúce dôverné informácie musia byť pred vyradením alebo znovu použitím fyzicky zničené, alebo musia byť zničené informácie, ktoré obsahujú (vymazanie a prepis údajov miesto jednoduchého vymazania/formátovania). Postupy sú podrobne upravené internou smernicou.

Nakladanie s odpadom nesmie poškodzovať životné prostredie.

5.5 Procedurálne opatrenia

5.5.1 Dôveryhodné roly

Poskytovateľ zamestnáva zamestnancov, prípadne subkontraktorov, ktorí majú potrebné odborné znalosti, spoľahlivosť, skúsenosti a kvalifikáciu a ktorí prešli školením o pravidlách bezpečnosti a ochrany osobných údajov vhodným pre ponúkané služby a pracovnú funkciu. Pracovníci sú do dôveryhodných rolí formálne menovaní manažmentom spoločnosti. Pre každú rolu sú definované kvalifikačné požiadavky, rozsah zodpovednosti a zlučiteľnosť príslušnej roly s ďalšími rolami . Prevádzkové postupy pre jednotlivé role, vrátane požiadaviek na duálnu kontrolu pri ich vykonávaní, sú definované v internej dokumentácii. Ich výkon je kontrolovaný interným auditom.

Pre prevádzku sú definované nasledovné základné roly:

- **Security Officer:** celková zodpovednosť za návrh, implementáciu, zlepšovanie a monitorovanie bezpečnostných postupov.
- **Information Security Officer:** návrh, implementácia, zlepšovanie a monitorovanie zabezpečenia informácií a riadenie IT rizík.
- **System Administrator**: inštalácia, konfigurácia a údržba TSP dôveryhodných systémov.
- **System Operator:** prevádzka dôveryhodných systémov TSP na dennej báze vrátane zálohovania.
- **System Auditor:** vykonávanie interných auditov, zber a vyhodnocovanie dôkazov o súlade prevádzky TSP s platnou legislatívou CP, CPS a internými politikami a smernicami . Oprávnený prehliadať archívy a auditné záznamy TSP dôveryhodných systémov.
- **RA Operator:** zabezpečuje registráciu a overenie identity Zákazníkov a Držiteľov a informácií uvádzaných v certifikáte, schvaľuje žiadosti o vydanie a zrušenie certifikátu.

5.5.2 Počet osôb vyžadovaných na vykonávanie činností

Zabezpečené v zmysle interných prevádzkových postupov.

5.5.3 Identifikácia a autentifikácia

Pre činnosti zahŕňajúce manipuláciu s TSP zariadeniami vrátane obnovy ich zálohy sa používajú čipové karty, pre registračné činnosti zas bezpečné meno a heslo.

5.5.4 Nezlučiteľnosť rolí

Zabezpečené v zmysle interných prevádzkových postupov.

5.6 Personálne opatrenia

Pracovníci v dôveryhodných roliach sú do nich dosadení formálnym menovaním manažmentom a sú preukázateľne poučení o svojej pracovnej náplni, povinnosti, zodpovednosti a pracovných postupoch.

5.6.1 Požiadavky na kvalifikáciu, skúsenosti a oprávnenia

Kvalifikačné požiadavky pre jednotlivé role sú uvedené v internej prevádzkovej smernici a sú používané pri výberových konaniach.

Personál ako aj schválení subdodávatelia disponujú s potrebnou odbornosťou, spoľahlivosťou, skúsenosťami, kvalifikáciou a vhodnou odbornou prípravou týkajúcou sa predpisov v oblasti bezpečnosti a ochrany osobných údajov a uplatňuje administratívne a riadiace postupy, ktoré zodpovedajú európskym alebo medzinárodným normám.

5.6.2 Postupy preverovania osôb

Pracovníci v dôveryhodných roliach sú preverovaní personálnym oddelením na základe poskytnutých referencií a nesmú byť odsúdení za úmyselný trestný čin.

5.6.3 Požiadavky na školenia personálu

Pracovníci v dôveryhodných roliach sú zaškolení pri menovaní a následne pravidelne preškoľovaní v témach, ktoré sú relevantné pre výkon ich činností (min. 1x ročne). Súčasťou školení sú informácie o nových bezpečnostných hrozbách a praktikách.

5.6.4 Požiadavky preškoľovanie personálu a ich frekvencia

Viď kap. 5.6.3

5.6.5 Frekvencia a postupnosť rotácie rolí

Riadia sa interným organizačným poriadkom Poskytovateľa.

5.6.6 Sankcie za neoprávnené činnosti

Riadia sa interným organizačným poriadkom Poskytovateľa podľa stupňa závažnosti previnenia.

5.6.7 Dokumentácia poskytovaná pracovníkom

Na vykonávanie každej role je pracovníkom preukázateľne poskytnutá dokumentácia v potrebnom rozsahu (viď 5.6). Pracovníci sú povinní používať dokumenty len na určený účel.

5.7 Auditné záznamy

Poskytovateľ zaznamenáva a uchováva po primeranú dobu, aj po ukončení činnosti TSP, všetky príslušné informácie týkajúce sa údajov, ktoré vydal a prijal, najmä na účely poskytovania dôkazov v súdnych konaniach a na účely zabezpečenia kontinuity služby.

5.7.1 Typy zaznamenávaných udalostí

Poskytovateľ zaznamenáva nasledovné typy udalostí.

- Životný cyklus certifikátov držiteľov
  - Žiadosti o vydanie KC, vrátane registračných informácií a výsledky ich preverenia
  - Záznamy o vydaní KC
  - Záznamy o prevzatí KC
  - Žiadosti o zrušenie KC a výsledky ich preverenia
- Životný cyklus kľúča CA
  - akákoľvek manipulácia s kľúčovým párom CA (generovanie, zálohovanie a obnova, zneplatnenie)
- Zariadenia na vyhotovenie kvalifikovaného elektronického podpisu/pečate
  - Záznamy o ich príprave
- Publikovanie
  - Záznamy o zrušených KC
  - Záznamy o vytváraní zoznamov zrušených KC a ich publikovaní
- Bezpečnosť a infraštruktúra
  - Záznamy o zmenách týkajúcich sa bezpečnostnej politiky, spustení a vypnutí systému, zlyhaní systému a zlyhaní hardvéru, aktivitách brány firewallu a smerovača a pokusov o prístup do systému PKI a synchronizácii času.
  - Záznamy o inštaláciách, aktualizáciách a zmenách konfigurácie
  - Záznamy o prevádzkových a bezpečnostných incidentoch a ich riešení

5.7.2 Frekvencia spracovania záznamov

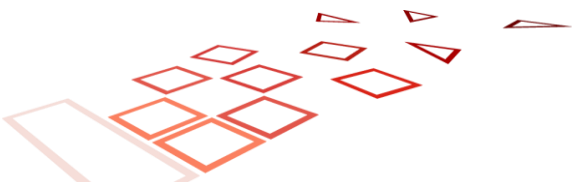
Záznamy sú spracovávané vo frekvencii závislej od ich povahy podľa internej smernice.

5.7.3 Doba uchovávania

Auditné záznamy sú uchovávané v aktívnej podobe min. 1 rok, v prípade záznamov týkajúce sa životného cyklu certifikátov min. 1 rok po ukončení ich platnosti. Následne sú presunuté do archívu s dobou archivácie podľa kap. 5.8.2.

5.7.4 Ochrana auditných záznamov

Elektronické auditné záznamy sú chránené spôsobom, ktorý zaručuje ich integritu a autenticitu (kombinácia HW a SW opatrení, WORM, elektronický podpis) a sú pravidelne zálohované.



Listinné auditné záznamy sú spracovávané a uchovávané tak, aby nedošlo k ich strate, poškodeniu alebo zničeniu.

5.7.5 Postupy zálohovania auditných záznamov

Auditné záznamy sú zálohované v súlade s internou smernicou a platnými právnymi predpismi SR.

5.7.6 Systém zberu auditných záznamov

Zber listinných auditných záznamov prebieha manuálne. Zber elektronických auditných záznamov, ktoré generujú priamo systémy a zariadenia TSP infraštruktúry je automatizovaný, ostatné elektronické auditné záznamy sú zbierané manuálne.

5.7.7 Notifikácia subjektu, ktorý spôsobil udalosť

Neuplatňuje sa.

5.7.8 Posudzovanie zraniteľností

Uplatňujú sa požiadavky uvedené v ustanovení 7.7 písmeno g) bod ii., 7.8 písmeno g), 7.9 písmeno h) a 7.11 normy ETSI EN 319 401 [5] , ktoré sú definované v samostatnom dokumente Politika pre KC ako aj certifikačná politika pre KC a ČP.

5.8 Archivácia záznamov

Záznamy sú uchovávané vo forme, v ktorej vznikli (listinná alebo elektronická), alebo v konvertovanej forme s využitím zaručenej konverzie v zmysle zákona č. 305/2013 Z. z. Záznamy musia byť uchovávané tak, aby nemohlo dôjsť k ich poškodeniu alebo strate.

5.8.1 Typy archivovaných záznamov

Poskytovateľ archivuje záznamy minimálne v nasledovnom rozsahu:

- záznamy podľa 5.7.1
- vydané certifikáty
- zoznamy zrušených certifikátov
- oficiálna korešpondencia
- bezpečnostná dokumentácia
- inštalačné médiá

5.8.2 Doba archivácie

V zmysle § 5 Zákona č. 272/2016 Z.z.je doba archivácie min. 10 rokov.

5.8.3 Ochrana archívu

Archívne záznamy sú chránené pred negatívnymi vplyvmi prostredia ako sú vlhkosť, teplota, v prípade elektronických archivačných médií magnetizmus, ak to ich technológia vyžaduje. Záznamy sú chránené kombináciou prístupových a režimových opatrení.

5.8.4 Postupy zálohovania

Postupy zálohovania archívu sú navrhnuté tak, aby umožňovali plnú obnovu. Podrobnosti sú ustanovené v internej smernici.

5.8.5 Požiadavky na pridávanie časových pečiatok

Neuplatňujú sa.

5.8.6 Zberný systém archívu

Neuplatňuje sa.

5.8.7 Postupy na získanie a overenie archívnych informácií

Neuplatňujú sa.

5.9 Výmena kľúčov

Výmena kľúčov je realizovaná:

- pred exspiráciou platnosti certifikátu CA, minimálne 30 dní, optimálne však 1 rok vopred
- pri kompromitácii alebo dôvodnom podozrení z kompromitácie súkromného kľúča CA

Pri informovaní účastníkov a hlásení bezpečnostných incidentov sa postupuje podľa relevantných ustanovení týchto CPS a interných smerníc.

5.10 Obnova po kompromitácii a havárii

V prípade kompromitácie alebo havárie Poskytovateľ postupuje podľa interného plánu obnovy a riešenia incidentov, ktorý popisuje aj mechanizmy pre informovanie dotknutých strán a orgánu dohľadu .

5.10.1 Postupy pre riešenie incidentov a kompromitácie

Postupy pre riešenie incidentov a kompromitácie sú upravené internými smernicami. Postupy sú min. 1x ročne testované, preskúmavané a aktualizované. Spoločnosť zabezpečí zalogovanie nahláseného incidentu do 48 hodín resp. podľa platných zákonov.

5.10.2 Postupy pri poškodení výpočtových prostriedkov, softvéru a/alebo údajov

Aplikujú sa ustanovenia podľa kap. 5.10.1.

5.10.3 Postupy pri kompromitácii súkromného kľúča

Aplikujú sa ustanovenia podľa kap. 5.10.1.

5.10.4 Biznis kontinuita po havárii

Aplikujú sa ustanovenia podľa kap. 5.10.1.

5.11 Ukončenie činnosti TSP

Uplatňujú sa požiadavky uvedené v ustanovení 7.12 normy ETSI EN 319 401 **Chyba! Nenalezen zdroj odkazů.** , ktoré sú definované v samostatnom dokumente Politika pre KC a ČP ako aj certifikačná politika pre KC a ČP..

Ďalej platia tieto osobitné usmernenia:

a) Pokiaľ ide o požiadavku na odrážku b) iii) kapitoly 7.12 dokumentu Politika pre KC ako aj certifikačná politika pre KC a ČP., toto platí pre informácie o registrácii (pozri články 6.2.2, 6.3.1 a 6.3.4), informácie o stave odvolania (pozri článok 6.3.10) a udalosti archivovať protokoly (pozri články 6.4.5 a 6.4.6) na príslušné časové obdobie, ako je určené účastníkovi a spoliehajúcej sa strane (pozri článok 6.8.10).

b) Pokiaľ ide o požiadavku d) článku 7.12 dokumentu Politika pre KC ako aj certifikačná politika pre KC a ČP. sú zahrnuté aj riešenia stavu odvolania vydaných certifikátov, ktorým neskončila platnosť.

6 Technické bezpečnostné opatrenia

6.1 Generovanie kľúčového páru a inštalácia

6.1.1 Generovanie kľúčového páru CA

Kľúče používané na vydávanie kvalifikovaných certifikátov a podpisovanie CRL a OCSP sú generované na HSM certifikovanom v zmysle nariadenia eIDAS a príslušných technických noriem.

Proces generovania kľúčov prebieha pod duálnou kontrolou pracovníkmi v dôveryhodných roliach za účasti tretej nezávislej osoby, ktorá naň dohliada a priebeh formálne zaznamenáva. Jednotlivé role a zodpovednosti sú popísané v dokumentácii Poskytovateľa.

Súkromný kľúč je generovaný priamo na HSM a v žiadnom okamihu ho neopúšťa v otvorenej forme.

6.1.2 Generovanie kľúčového páru Držiteľa

V prípade, že má mať kvalifikovaný certifikát atribút, že je kľúč umiestnený na QSCD zariadení, musí byť generovaný na QSCD zariadení certifikovanom pre tento účel v zmysle nariadenia eIDAS a príslušných technických noriem bez ohľadu na to, či je generovaný Poskytovateľom, jeho Registračnou autoritou, alebo priamo Držiteľom. Poskytovateľ monitoruje platnosť certifikácie používaných zariadení.

Poskytovateľ ani Registračná autorita neuchováva žiadnu kópiu privátneho kľúča Držiteľa s výnimkou prípadu, keď je kľúč Držiteľa generovaný priamo na zariadení Poskytovateľa za účelom vzdialeného podpisovania. V tomto prípade Poskytovateľ používa technické postupy a prostriedky, ktoré garantujú vysokú mieru výlučnej kontroly Držiteľa nad kľúčom v zmysle príslušných technických noriem [12].

6.1.3 Doručenie súkromného kľúča Držiteľovi

Súkromné kľúče generované Poskytovateľom alebo Registračnou autoritou na zariadení na vyhotovovanie kvalifikovaného podpisu/pečate, ktoré neprevádzkuje Poskytovateľ a autentifikačnú údaje k zariadeniu sú odovzdané Držiteľovi spolu so zariadením osobne alebo dôveryhodným kanálom, ktorý zabezpečuje dôvernosť a integritu.

V prípade kľúčov generovaných na zariadení Poskytovateľa je použitie súkromných kľúčov aktivované Držiteľom vzdialene na základe autentifikačných faktorov systému pre vzdialené podpisovanie. Aktivačné mechanizmy sú definované v internom dokumente.[1]

6.1.4 Doručenie verejného kľúča vydavateľovi certifikátu

Verejný kľuč Držiteľa musí byť doručený vydavateľovi certifikátu (Poskytovateľovi) vo formáte PKCS#10 Certification Request Format. Žiadosť musí byť podpísaná súkromným kľúčom patriacim k verejnému kľúču. Žiadosti musí predchádzať identifikácia a autentifikácia podľa kap. 3 na základe ktorej Poskytovateľ jednoznačne asociuje PKCS#10 žiadosť s overenou identitou.

[1] Popis riešenia remote QSCD v. 1.0, Ardaco, a.s.

6.1.5 Doručenie verejného kľúča spoliehajúcim sa stranám

Verejné kľúče CA poskytovateľa sú publikované prostredníctvom európskeho a národného zoznamu poskytovateľov dôveryhodných služieb (TSL) a na webovej stránke poskytovateľa podľa kap. 1.3 a 2.

Verejné kľúče Držiteľov Poskytovateľ nepublikuje s výnimkou zverejnenia certifikátov s ich výslovným súhlasom vo verejnom úložisku podľa kap. 2.

6.1.6 Dĺžka kľúčov

Pre všetky typy certifikátov a algoritmy musí byť stanovená minimálna dĺžka kľúčov. Dĺžku kľúčov stanovuje PMA v súlade s príslušnými technickými normami (ETSI TS 119 312), odporúčaniami Orgánu dohľadu a na základe bezpečnostných vlastností konkrétnych kryptografických zariadení.

6.1.7 Parametre a kvalita verejného kľúča

Parametre a kvalitu verejných kľúčov stanovuje PMA v súlade s príslušnými technickými normami (ETSI TS 119 312), odporúčaniami Orgánu dohľadu a na základe bezpečnostných vlastností konkrétnych kryptografických zariadení.

Tabuľka 1: Minimálne dĺžky kľúčov (bit):

Subjekt	RSA	ECDSA
Poskytovateľ	4096	-
Koncové entity	2048	256

6.2 Ochrana súkromného kľúča a technické opatrenia pre kryptografický modul

6.2.1 Štandardy pre kryptografické moduly

Poskytovateľ na ochranu súkromných kľúčov CA musí používať hardvérové moduly (HSM) certifikované podľa eIDAS Protection Profile (PP) EN 419 221-5 “Cryptographic Module for Trust Services”. HSM musí byť aktivované min. dvoma osobami v dôveryhodných roliach (duálna kontrola). Súkromné kľúče nie je možné exportovať z HSM v otvorenej forme za žiadnych okolností.

HSM sú chránené pred neoprávnenými zmenami (tamper protection) a je s nimi bezpečne manipulované v priebehu dodávky, uskladnenia a používania. Pri spustení HSM sú automaticky vykonané self-testy na kontrolu správnej funkčnosti HW a SW komponentov.

6.2.2 Opatrenia pre ochranu súkromného kľúča (K z N)

Pri akejkoľvek manipulácii so súkromnými kľúčmi CA je vyžadovaná prítomnosť viacerých osôb. Žiadny jednotlivec nedisponuje kompletnými aktivačnými údajmi, ktoré sú potrebné na prístup k ľubovoľnému súkromnému kľúču CA.

6.2.3 Úschova kľúčov Držiteľov (key escrow)

Poskytovateľ neposkytuje úschovu kľúčov Držiteľov ako samostatnú službu. Kľúče generované na zariadenie Poskytovateľa pre potreby vzdialeného podpisovania sú aktivované výhradne s využitím SAM, ktoré je certifikované pre tento účel.

6.2.4 Zálohovanie súkromných kľúčov

CA kľúče sú generované a uchovávané na zariadení, ktoré spĺňa požiadavky podľa 6.2.1 a ktoré neumožňuje export kľúča v otvorenej forme. V priebehu zálohovania je kľúč exportovaný v zašifrovanej podobe tak, aby bola dosiahnutá rovnaká alebo vyššia miera bezpečnosti ako je miera bezpečnosti pôvodného kľúča. Obnova je technicky možná iba pri dodržaní min. duálnej kontroly.

Kľúče Držiteľov, ktoré spravuje Poskytovateľ pre potreby vzdialeného podpisovania, sú generované na rovnakom type zariadenia s rovnakými zálohovacími mechanizmami, ako je uvedené vyššie.

Kľúče Držiteľov, ktoré nespravuje Poskytovateľ, nie sú Poskytovateľom zálohované a to ani v prípade, že nie sú generované na QSCD zariadení (t.j. sú generované bez príslušného atribútu).

6.2.5 Archivácia súkromných kľúčov

Na účely archivácie slúži postup uvedený v 6.2.4. Archivované kľúče sú na konci úložnej lehoty zničené postupom vyžadujúcim duálnu kontrolu a nikdy nie sú obnovené v produkčnej prevádzke.

6.2.6 Vstup privátnych kľúčov do kryptografického modulu

Kľúče sú generované a uchovávané na zariadeniach, ktoré spĺňajú požiadavky podľa 6.2.1. Pri obnove súkromných kľúčov zo zálohy je vyžadovaná duálna kontrola.

6.2.7 Metódy aktivácie súkromného kľúča

Súkromné kľúče CA Poskytovateľa môžu byť aktivované iba za podmienok kap. 6.2.2 (duálna kontrola). Aktivácia prebieha s použitím smart karty a prístupového hesla. Kľúč je aktivovaný až do deaktivácie.

Súkromné kľúče Držiteľa, ktoré sú v správe Poskytovateľa, sú aktivované prostredníctvom SAM kap. 6.2.3. Aktivácia prebieha pomocou prihlasovacieho hesla/overovacieho kódu Držiteľom. Aktivácia je platná vždy pre jednu podpisovaciu operáciu.

Za aktiváciu súkromných kľúčov Držiteľa, ktoré nie sú v správe Poskytovateľa, zodpovedá výlučne Držiteľ.

6.3 Iné aspekty správy kľúčového páru

CA kľúče Poskytovateľa používané na podpisovanie certifikátov a informácií o ich stave, nesmú byť použité za iným účelom a musia byť používané výlučne vo fyzicky zabezpečených priestoroch.

Použitie CA kľúčov musí byť kompatibilné s hašovacími algoritmami, podpisovými algoritmami a dĺžkou kľúčov v zmysle kap. 6.1.6 a 6.1.7.

Všetky CA súkromné kľúče musia byť na konci ich životného cyklu zničené.

6.4 Aktivačné údaje

Aktivačné údaje ku kľúčom CA Poskytovateľa, musia by byť generované v súlade s kap. 6.2.2.

Aktivačné údaje ku kľúčom generovaným na zariadení určenom pre Držiteľa musia byť generované spôsobom, ktorý zaručuje ich dôvernosť a byť distribuované bezpečným kanálom oddelene od zariadenia (kap. 6.1.3)

6.5 Opatrenia počítačovej bezpečnosti

Opatrenia počítačovej bezpečnosti sa riadia bezpečnostnou politikou schválenou manažmentom, ktorá je prístupná a vhodne komunikovaná všetkým zamestnancom, ktorí zabezpečujú prevádzku kvalifikovaných dôveryhodných služieb. Preskúmanie a prehodnotenie opatrení počítačovej bezpečnosti sú vykonávané na Bezpečnostnej rade.

6.6 Opatrenia bezpečnosti životného cyklu

Uplatňujú sa požiadavky uvedené v ustanovení 7.7 normy ETSI EN 319 401 **Chyba! Nenalezen zdroj odkazů.** , ktoré sú definované v samostatnom dokumente Politika pre KC ako aj certifikačná politika pre KC a ČP.

6.7 Opatrenia sieťovej bezpečnosti

Uplatňujú sa požiadavky uvedené v ustanovení 7.8 normy ETSI EN 319 401 **Chyba! Nenalezen zdroj odkazů.** , ktoré sú definované v samostatnom dokumente Politika pre KC ako aj certifikačná politika pre KC a ČP..

Ďalej platia nasledovné osobitné ustanovenia:

a) organizácia udržiava a chráni všetky systémy CA najmenej v zabezpečenej zóne a implementuje a konfiguruje bezpečnostný postup, ktorý chráni systémy a komunikáciu medzi systémami v zabezpečených zónach a zónach vysokej bezpečnosti.
b) organizácia má nakonfigurované všetky systémy CA odstránením alebo zakázaním všetkých účtov, aplikácií, služieb, protokolov a portov, ktoré sa nepoužívajú v operáciách CA.
c) organizácia udeľuje prístupy do zabezpečených zón a zón vysokej bezpečnosti iba dôveryhodným rolám.
d) Systém CA je vo vysoko bezpečnostnej zóne.

6.8 Používanie časovej pečiatky

Uplatňujú sa požiadavky uvedené v ustanovení normy ETSI EN 319 421 **Chyba! Nenalezen zdroj odkazů.**, ktoré sú definované v samostatnom dokumente Politika pre KC ako aj certifikačná politika pre KC a ČP.

7 Profily certifikátov, CRL a OCSP

Pravidlá obsahu kvalifikovaného certifikátu pre elektronické podpisy:

a) označenie, vo forme vhodnej na automatizované spracovanie, že certifikát sa vydáva ako kvalifikovaný certifikát pre elektronický podpis;
b) súbor údajov jednoznačne reprezentujúcich kvalifikovaného poskytovateľa dôveryhodných služieb, ktorý vydáva kvalifikované certifikáty, zahŕňajúci členský štát, v ktorom je tento poskytovateľ usadený,
    a. v prípade právnickej osoby: názov a prípadné registračné číslo, ako sa uvádza v úradných záznamoch,
    b. v prípade fyzickej osoby: meno osoby;
c) meno podpisovateľa alebo pseudonym s jasnou špecifikáciou, že ide o pseudonym;
d) údaje na validáciu elektronického podpisu, ktoré zodpovedajú údajom na vyhotovenie elektronického podpisu;
e) údaje o začiatku a konci obdobia platnosti certifikátu;
f) identifikačný kód certifikátu, ktorý je jedinečný pre kvalifikovaného poskytovateľa dôveryhodných služieb;
g) zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať vydávajúceho kvalifikovaného poskytovateľa dôveryhodných služieb;
h) lokalitu, na ktorej je certifikát pre zdokonalený elektronický podpis alebo zdokonalenú elektronickú pečať podľa písmena g dostupný bezplatne;
i) lokalitu služieb, ktoré možno využiť na zistenie štatútu platnosti kvalifikovaného certifikátu;
    a. ak sa údaje na vyhotovenie elektronického podpisu súvisiace s údajmi na validáciu elektronického podpisu nachádzajú v zariadení na vyhotovenie kvalifikovaného elektronického podpisu/pečate , vo forme vhodnej na automatizované spracovanie.

Certifikáty vydávané Poskytovateľom musia byť vo formáte X.509 verzia 3 podľa RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [9].

7.1 Profil vydávajúcej certifikačnej autority

7.1.1 Položky vydávajúcej certifikačnej autority

Pole	Hodnota
version	3
serialNumber	Jedinečné sériové číslo pridelené Poskytovateľom
signatureAlgorithm	**sha256withRSAEncryption**
issuer	Zhodné so subject (self-signed certifikát).
validity	
notBefore	Začiatok platnosti certifikátu (UTCTime)
notAfter	Koniec platnosti certifikátu (UTCTime) Max. 30 rokov
subject	Identifikácia CA, ktorá je asociovaná s verejným kľúčom. Jednotlivé položky sú uvedené v nasledovných kapitolách.
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	Verejný kľúč subjektu
extensions	Rozšírenia. Viď Rozšírenia certifikátu vydávajúcej CA
signature	Pečať CA Poskytovateľa (self-signed)

7.1.2 Rozlišovacie meno vydávajúcej CA

Pole	Povinné	Hodnota
countryName	Áno	Dvojznakový kód štátu.
commonName	Áno	Identifikácia - názov CA pre kvalifikované dôveryhodné služby.
organizationalName	Áno	Oficiálny názov právnickej osoby Poskytovateľa.
organizationIdentifier	Nie	Identifikátor organizácie, ako sa uvádza v príslušnom registri. Viď aj Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu [3].
organizationalUnitName	Nie	Názov organizačnej jednotky
stateOrProviceName	Nie	Územný celok
localityName	Nie	Obec
streetAdress	Nie	Adresa ulice
postalCode	Nie	Poštové smerovacie číslo

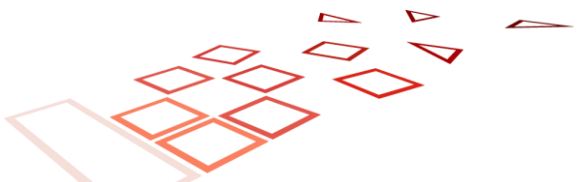
7.1.3 Rozšírenia certifikátu vydávajúcej CA

Rozšírenie	Kritické	Hodnota
basicConstraints	Áno	cA: TRUE pathlen:0
keyUsage	Áno	keyCertSign crlSign
certificatePolicies	Nie	CP, podľa ktorej bol certifikát vydaný (táto CP) Policy 1.3.158.35829036.0.0.0.0
crlDistributionPoints	Nie	Neprítomné
subjectKeyIdentifier	Nie	Identifikátor verejného kľúča Držiteľa tohto certifikátu.
authorityKeyIdentifier	Nie	Identifikátor verejného kľúča certifikačnej autority, ktorá vydala tento certifikát.

7.2 Profil certifikátu TSA

7.2.1 Položky certifikátu TSA

Pole	Hodnota
version	3
serialNumber	Jedinečné sériové číslo pridelené Poskytovateľom
signatureAlgorithm	sha256withRSAEncryption
issuer	Vydavateľ certifikátu (CA)
validity	
notBefore	Začiatok platnosti certifikátu (UTCTime)
notAfter	Koniec platnosti certifikátu (UTCTime)
subject	Viď rozlišovacie meno.
subjectPublicKeyInfo	



algorithm	rsaEncryption
subjectPublicKey	Verejný kľúč subjektu
extensions	Viď Rozšírenia certifikátu TSA
signature	Pečať CA Poskytovateľa

7.2.2 Rozlišovacie meno certifikátu TSA

Pole	Povinné	Hodnota
countryName	Áno	Dvojznakový kód štátu.
commonName	Áno	Identifikácia vydávajúcej jednotky.
organizationalName	Áno	Oficiálny názov právnickej osoby Poskytovateľa.
organizationIdentifier	Nie	Identifikátor organizácie, ako sa uvádza v príslušnom registri. Viď aj Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu [3].

7.3 Profil certifikátu na potvrdenie existencie a platnosti certifikátu (OCSP)

7.3.1 Položky certifikátu OCSP respondera

Pole	Hodnota
version	3
serialNumber	Jedinečné sériové číslo pridelené Poskytovateľom
signatureAlgorithm	sha256withRSAEncryption
issuer	Vydavateľ certifikátu (CA)
validity	
notBefore	Začiatok platnosti certifikátu (UTCTime)
notAfter	Koniec platnosti certifikátu (UTCTime)
subject	Viď rozlišovacie meno.
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	Verejný kľúč subjektu
extensions	Viď Rozšírenia certifikátu OCSP Respondera
signature	Pečať CA Poskytovateľa

7.3.2 Rozlišovacie meno certifikátu OCSP respondera

Pole	Povinné	Hodnota
countryName	Áno	Dvojznakový kód štátu.
commonName	Áno	Identifikácia OCSP respondera.
organizationalName	Áno	Oficiálny názov právnickej osoby Poskytovateľa.
organizationIdentifier	Nie	Identifikátor organizácie, ako sa uvádza v príslušnom registri. Viď aj Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu [3].

7.3.3 Rozšírenia certifikátu certifikátu OCSP respondera

Rozšírenie	Kritické	Hodnota
basicConstraints	Áno	cA: FALSE
keyUsage	Áno	digitalSignature nonRepudiation
extendedKeyUsage	Áno	id-kp-OCSPSigning
certificatePolicies	Nie	Policy 1.3.158.35829036.0.0.0.0 CPS: https://www.qsign.sk/tsp/ardaco_cp_qtsp_qc.pdf
crlDistributionPoints	Nie	https://tsp.ardaco.com/status/crl
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	Nie	
subjectKeyIdentifier	Nie	Generované
authorityKeyIdentifier	Nie	Identifikátor verejného kľúča certifikačnej autority, ktorá vydala tento certifikát.

7.4 Profil kvalifikovaného certifikátu

7.4.1 Položky kvalifikovaného certifikátu

Pole	Hodnota
version	3
serialNumber	Jedinečné sériové čislo pridelené Poskytovateľom
signatureAlgorithm	Minimálne sha256withRSAEncryption pre RSA alebo Minimálne ecdsa-with-SHA256 pre ECDSA
issuer	Vydavateľ certifikátu (CA)
validity	
notBefore	Začiatok platnosti certifikátu (UTCTime)
notAfter	Koniec platnosti certifikátu (UTCTime)
subject	Identifikácia entity, ktorá je asociovaná s verejným kľúčom. Položky pre kvalifikovaný certifikát pre podpis a pečať sú uvádzané v nasledovných kapitolách.
subjectPublicKeyInfo	
algorithm	rsaEncryption alebo id-ecPublicKey
subjectPublicKey	Verejný kľúč subjektu
extensions	Rozšírenia. Viď Rozšírenia kvalifikovaného certifikátu
signature	Pečať CA Poskytovateľa.

7.4.2 Rozlišovacie meno kvalifikovaného certifikátu pre podpis

Pole	Povinné	Hodnota
countryName	Áno	Dvojznakový kód štátu.
givenName	Áno	Mená osoby okrem priezviska.
surname	Áno	Priezvisko

pseudonym	Ak ide o certifikát obsahujúci pseudonym	Pseudonym
serialNumber	Nie	Odkaz na identitu fyzickej osoby vo formáte podľa dokumentu Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu [3]. Existujúci zoznam spresňujúcich znakov v Schéme dohľadu rozširuje Poskytovateľ nasledovne: - **Slovenská republika:** preberá konvenciu Slovenskej národnej certifikačnej autority (SNCA) podľa Zoznamu spresňujúcich znakov SNCA, ktorý je zverejnený na webovom sídle SNCA - **Česká republika:** preberá konvenciu podľa informácií a odporúčaní Digitální a informační agentury, Dokument upřesňující problematiku zápisu údajů o čísle dokladu do kvalifikovaného certifikátu, menovite:[2] o IR - Povolení k pobytu/Pobytová karta/Karta trvalého pobytu s biometrickými údaji (forma: plastiková karta s čipem) o IX - Forma: knížečka (označení CIS: PB - povolení k pobytu, PE - průkaz o povolení k trvalému pobytu obč. EU, PO - průkaz o povolení k trv. pobytu - vazba EU, PP - průkaz o povolení k pobytu, PR - průkaz o pobytu rod. př. obč. EU - přech. pobyt)
commonName	Áno	Meno a priezvisko alebo pseudonym. V prípade pseudonymu musí obsahovať reťazec “PSEUDONYM”
organizationalName	Nie	Názov organizácie Držiteľa, ako sa uvádza v príslušnom registri.
organizationIdentifier	Nie	Identifikátor organizácie, ako sa uvádza v príslušnom registri. Viď aj Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu [3].
organizationalUnitName	Nie	Názov organizačnej jednotky
title	Nie	Pozícia alebo funkcia
stateOrProviceName	Nie	Územný celok
localityName	Nie	Obec
streetAdress	Nie	Adresa ulice
postalCode	Nie	Poštové smerovacie číslo

7.4.3 Rozlišovacie meno kvalifikovaného mandátneho certifikátu pre podpis

V zmysle § 8 ods. 1 písm. b) bod 1 zákona č. 272/2016 Z. z. sa identifikačné údaje mandanta podľa § 2 zákona č. 272/2016 Z. z. uvádzajú tak, že každá položka obsahujúca identifikačné údaje mandanta v položke subjektu certifikátu musí začínať reťazcom "MANDANT", aby nedošlo k zámene obsahu položky mandanta a mandatára.

[2] Dokument (v0.1) nebol v čase tvorby CPS verejne dostupný, preto kvôli jednoznačnosti menovite uvádzame konkrétne používavané položky.

Pole	Povinné	Hodnota
countryName	Áno	Dvojznakový kód štátu.
givenName	Áno	Mená osoby okrem priezviska.
Surname	Áno	Priezvisko
pseudonym	Ak ide o certifikát obsahujúci pseudonym	Pseudonym
serialNumber	Áno	Odkaz na identitu fyzickej osoby vo formáte podľa dokumentu Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu [3]. Ďalej identifikačné údaje mandanta začínajúce reťazcom MANDANT Príklad: SERIALNUMBER = IDCSK-HE1234 SERIALNUMBER = NTRSK-3456 SERIALNUMBER = MANDANT NTRSK-78910 Poznámka: Z hľadiska požiadaviek Schémy dohľadu NBÚ v. 1.4 sa identifikačné údaje orgánu verejnej moci alebo osoby, u ktorej mandatár vykonáva činnosť podľa osobitného predpisu alebo vykonáva funkciu podľa osobitného predpisu, podľa § 2 zákona č. 272/2016 Z. z., uvádzajú minimálne v položkách organizationName OID (2.5.4.10) a serialNumber OID (2.5.4.5) alebo organizationIdentifier OID (2.5.4.97) subjektu certifikátu. V rámci tohoto profilu bola zvolená alternatíva serialNumber, preto je v rámci neho povinná, aj keď schéma Dohľadu pripúšťa aj iné riešenie
commonName	Áno	Meno a priezvisko, ďalej sa na uľahčenie neautomatizovanej manipulácie s mandátnym certifikátom, uvádza textový reťazec "OPRÁVNENIE", ďalej medzerou oddeliť číslo oprávnenia xyz a následne medzerou oddeliť textový názov oprávnenia zo zoznamu registrovaných typov oprávnení (splnomocnení). Príklad: Peter Novák OPRÁVNENIE 1042 Advokát
organizationalName	Nie pre údaje mandatára Áno pre údaje mandanta.	Názov organizácie Držiteľa, ako sa uvádza v príslušnom registri. Názov orgánu verejnej moci alebo osoby, u ktorej mandatár vykonáva činnosť podľa osobitného predpisu alebo vykonáva funkciu podľa osobitného predpisu, ako sa uvádza v príslušnom registri. Príklad:

		O = JUDr. Peter Polák O = MANDANT Slovenská advokátska komora
organizationIdentifier	Nie	Identifikátor organizácie, ako sa uvádza v príslušnom registri.
organizationalUnitName	Nie	Názov organizačnej jednotky
title	Nie	Pozícia alebo funkcia
stateOrProviceName	Nie	Územný celok
localityName*	Nie	Obec
streetAdress*	Nie	Adresa ulice
postalCode*	Nie	Poštové smerovacie číslo

* Údaje z primárneho dokladu.

7.4.4 Rozlišovacie meno kvalifikovaného certifikátu pre pečať

Pole	Povinné	Hodnota
countryName	Áno	Dvojznakový kód štátu.
serialNumber	Nie	Odkaz na identitu právnickej osoby vo formáte podľa dokumentu Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu [3].
commonName	Áno	Popisný názov právnickej osoby alebo systému.
organizationalName	Áno	Názov právnickej osoby, ako sa uvádza v príslušnom registri.
organizationIdentifier	Nie	Identifikátor organizácie, ako sa uvádza v príslušnom registri.
organizationalUnitName	Nie	Názov organizačnej jednotky
stateOrProviceName	Nie	Územný celok
localityName	Nie	Obec
streetAdress	Nie	Adresa ulice
postalCode	Nie	Poštové smerovacie číslo

7.4.5 Rozšírenia kvalifikovaného certifikátu

Rozšírenie	Kritické	Hodnota
basicConstraints	Nie	cA: FALSE
keyUsage	Áno	digitalSignature nonRepudiation
extKeyUsage	Nie	emailProtection (1.3.6.1.5.5.7.3.4)
certificatePolicies	Nie	Certifikačná politika NBÚ (1.3.158.36061701.0.0.0.1.2.2). Táto certifikačná politika Jedna z politík QCP-n-qscd, QCP-l-qscd, QCP-l, QCP-n v závislosti od typu subjektu a či je certifikát vydaný na zariadenie na vyhotovenie kvalifikovaného elektronického podpisu/pečate. V prípade madátnych certifikátov naviac: 1.3.158.36061701.1.1.xyz – kde xyz je číslo oprávnenia podľa Zoznamu oprávnení podľa § 9 zákona č. 272/2016 Z. z. Názov (označenie) oprávnenia uviesť v jednej alebo viacerých položkách typu UserNotice v položke explicitText ako utf8String o maximálnej veľkosti 200 znakov minimálne v slovenskom jazyku

subjectAltName	Nie	Alternatívne (nepovinné) meno Držiteľa certifikátu. Môže zahŕňať napr. e-mail prípadne iné položky explicitne vymenované v RFC 5280, alebo lokálne definované položky (t.j. custom OID) ako napr. identifikátor Držiteľa, ktorý používa v rámci určitej agendy v konkrétnom systéme.
crlDistributionPoints	Nie	Adresy pre získanie informácií o stave certifikátov
qcStatement	Nie	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD - pre certifikáty vydané na zariadenie na vyhotovenie kvalifikovaného elektronického podpisu/pečate
subjectKeyIdentifier	Nie	Identifikátor verejného kľúča Držiteľa tohto certifikátu.
authorityKeyIdentifier	Nie	Identifikátor verejného kľúča certifikačnej autority, ktorá vydala tento certifikát.
nsComment	Nie	Nepovinné doplňujúce informácie k certifikátu (voľný text).

7.5 Profil CRL

CRL vydávané Poskytovateľom musia byť vo formáte X.509 verzia 3 podľa RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [9].

Pole	Hodnota
version	Hodnota (0x1)
signatureAlgorithm	sha256withRSAEncryption
issuer	Vydavateľ CRL (CA)
thisUpdate	Dátum a čas vydania CRL (UTC)
nextUpdate	Predpokladaný dátum a čas vydania CRL (UTC)
revokedCertificates	Zoznam zneplatnených certifikátov
userCertificate	Sériové číslo zneplatneného cetifikátu,
revocationDate	Dátum a čas zneplatnenia (UTC)
crlEntryExtensions	Rozšírenia položiek CRL
CRLReason	Dôvod zneplatnenia. Nesmie byť certificateHold.
crlExtensions	Rozšírenia CRL
authorityKeyIdentifier	Identifikátor verejného kľúča certifikačnej autority, ktorá vydala toto CRL.
signature	Elektronická pečať vydavateľa CRL.

7.6 Profil OCSP

Profily OCSP žiadosti a odpovedi sú v súlade s RFC 6960 a RFC 5019. Informácia o štatúte platnosti alebo zrušenia kvalifikovaných certifikátov v OCSP odpovedi musí obsahovať pozitívne prehlásenie o existencii a správnosti údajov.

Štruktúra odpovede:

Pole	Povinné	Hodnota
ResponseStatus	Áno	0 alebo návratový kód chyby
ResponseBytes		
ResponseType	Áno	id-pkix-ocsp-basic

BasicOCSPResponse		
tbsResponseData		
Version	Áno	1
responderID	Áno	Distinguished Name OCSP respondéra
producedAt	Áno	Čas v ktorom OCSP repondér podpísal odpoveď.
Responses		
certID	Áno	Polia CertID v zmysle RFC 6560
certStatus	Áno	Stav certifikátu
revocationTime	Nie	Čas zneplatnenia alebo exspirácie (ako súčasť RevokedInfo v prípade CertStatus revoked)
revocationReason	Nie	Dôvod zneplatnenia (ako súčasť RevokedInfo v prípade CertStatus revoked)
thisUpdate	Áno	Čas, kedy bol stav získaný z databázy
Archive Cutoff	Nie	
Extended Revoked Definition	Nie	NULL Indikuje, či respondér podporuje rozšírenia podľa bodu 2.2 RFC 6960
nextUpdate	Áno	Čas kedy najneskôr bude dostupná najbližšia aktualizácia stavu certifikátu.
singleExtensions	Áno	Rozšírenia
certHash	Áno	hash hodnotu certifikátu, ktorého stav je v položke *certStatus* objektu *SingleResponse*, pre podrobný výklad viď Schému dohľadu NBÚ 5.2.13 písm. d)
Nonce	Nie	Nonce z požiadavky, ak bol uvedený.
signatureAlgorithm	sha256WithRSAEncryption	Algoritmus použitý na podpis odpovede
signature	Áno	Podpis odpovede
certificate	Áno	Certifikát OCSP respondera

7.7 Profil časovej pečiatky

Profil požiadavky a odpovede je v súlade s [ETSI 319 422] a IETF RFC 3161. Hodnoty sú v súlade s definíciou v uvedenom RFC a sú explicitne uvedené iba ak TSA očakáva alebo vracia konkrétnu hodnotu.

7.7.1 Profil požiadavky

Pole	Povinné	Hodnota
version	Áno	v1 (1)
messageImprint	Áno	OID algoritmu pre výpočet odtlačku a otlačok údajov, ktoré majú byť opečiatkované
reqPolicy	Nie	Ak je uvedené, musí byť OID: 1.3.158.35829036.0.0.0.1.0 (Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania

		kvalifikovaných elektronických časových pečiatok)
nonce	Nie	
certReq	Áno	Default False

7.7.2 Profil odpovede

Pole	Povinné	Hodnota
status	Áno	Stav volania
timeStampToken	Nie	
contentType	Áno	id-ct-TSTInfo
content	Áno	
version	Áno	v1 (1)
policy	Áno	Vždy: OID: 1.3.158.35829036.0.0.0.1.0 (Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok)
messageImprint	Áno	Vždy sa zhoduje v rovnakou hodnotou v požiadavke.
serialNumber	Áno	Jedinečné sériové číslo pridelené TSA
genTime	Áno	Čas z TSA
accuracy	Áno	max 1s
ordering	Áno	
nonce	Nie	Uvádza sa v prípade ak bolo Nonce uvedené v požiadavke – rovnaká hodnota.
tsa	Nie	Všeobecný názov TSA
extensions	Nie	Nepoužíva sa

8 Audit súladu a ďalšie hodnotenia

Účelom auditu je potvrdiť, že kvalifikovaný Poskytovateľ dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytuje na základe tejto CPS, spĺňajú požiadavky stanovené nariadením eIDAS. Poskytovateľ musí podstúpiť audit aspoň každých 24 mesiacov, alebo kedykoľvek na žiadosť orgánu dohľadu v súlade s ustanoveniami článku 20, bod 1 a 2 nariadenia eIDAS. Audit vykonáva akreditovaný orgán posudzovania zhody v súlade s platnou legislatívou pre dôveryhodné služby. Poskytovateľ predloží výslednú správu o posúdení zhody orgánu dohľadu v lehote troch pracovných dní od jej doručenia.

Za odstránenie prípadných nedostatkov je zodpovedný bezpečnostný manažér. V prípade nedostatkov, ktoré by zásadným spôsobom znemožňovali poskytovanie konkrétnej služby, Poskytovateľ preruší jej poskytovanie až do ich odstránenia.

9 Iné obchodné a právne záležitosti

9.1 Poplatky

Poplatky za poskytované služby sú uvedené v aktuálnom cenníku, ktorý je uvedený na webovom sídle Poskytovateľa podľa kap. 1.3, prípadne sa riadia inou dohodou zmluvných strán.

9.2 Finančná zodpovednosť

Poskytovateľ v súvislosti s rizikom zodpovednosti za škodu v súlade s článkom 13 nariadenia eIDAS udržiava postačujúce finančné prostriedky a/alebo uzatvára vhodné poistenie zodpovednosti za škodu v súlade s aplikovateľným právom.

Poskytovateľ má uzavreté a udržiava poistenie podnikateľských rizík v takom rozsahu, aby boli pokryté prípadné finančné škody.

9.3 Dôvernosť obchodných informácií

Dôvernosť obchodných informácií sa riadi platnou legislatívou a zmluvnými vzťahmi medzi Poskytovateľom a jeho partnermi a zákazníkmi.

9.4 Ochrana osobných údajov

Osobné údaje poskytované Poskytovateľovi podliehajú ochrane podľa Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) a zákona č. 18/2018 Z. z. o ochrane osobných údajov.

Poskytovateľ považuje za súkromné všetky informácie súvisiace s poskytovaním dôveryhodných služieb ktoré sú definované Záznamoch o spracovateľských činnostiach, ktorý je vytvorený na základe požiadavky zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov § 37 Záznamy o spracovateľských činnostiach, s výnimkou nasledujúcich:

a) aktuálne informácie určené na zverejnenie (napríklad cenníky, ponuky, kontaktné údaje)
b) certifikačná politika a vyhlásenie o certifikačnej politike
c) osvedčenia týkajúce sa prevádzky dôveryhodných služieb
d) informácie o stave certifikátov
e) infraštruktúrne certifikáty
f) iné informácie, pokiaľ s tým Zákazník/Držiteľ výslovne súhlasí a Poskytovateľ disponuje písomným súhlasom Zákazníka/ Držiteľa

9.5 Práva duševného vlastníctva

Táto CPS a všetky súvisiace dokumenty ako aj obsah webového sídla, postupy Poskytovateľa pri poskytovaní dôveryhodných služieb sú chránené autorskými právami Poskytovateľa.

9.6 Vyhlásenia a záruky

Akékoľvek vyhlásenie, ktoré majú dopad na predplatiteľov ako aj ostatné relevantné strany , či zmeny certifikačnej politiky ako aj politiky informačnej bezpečnosti sú oznámené predplatiteľom, ako aj ostatným relevantným stranám, hodnotiacim orgánom, dozorným alebo iným regulačným orgánom pomocou verejného webového sídla spoločnosti.

9.7 Odmietnutie záruk

Poskytovateľ zodpovedá v zmysle čl. 13 Nariadenia eIDAS výhradne za škodu, ktorú spôsobí úmyselne alebo z nedbanlivosti akejkoľvek fyzickej alebo právnickej osobe tým, že nesplní svoje povinnosti podľa tohto Nariadenia.
Poskytovateľ nezodpovedá za vady poskytnutých služieb v prípade nesprávneho alebo neoprávneného využívania služieb poskytnutých na základe Zmluvy o poskytovaní služieb držiteľom certifikátu, najmä, nie však výlučne za využívanie služieb v rozpore s podmienkami uvedenými v tejto CPS.

Sťažnosti a reklamácie je možné uplatniť emailom na adresy uvedené v bode 1.3 tejto CP alebo doporučenou poštovou zásielkou na adresu sídla Poskytovateľa. Sťažovateľ/ reklamujúci (držiteľ certifikátu, zákazník alebo spoliehajúca sa strana) je v sťažnosti/ reklamácii povinná uviesť minimálne sériové číslo reklamovaného produktu a popis vady. Sťažnosť/ reklamácia bude vybavená Poskytovateľom v lehote 30 dní, pokiaľ sa strany nedohodnú inak.

9.8 Obmedzenie zodpovednosti

V prípade delegovaných úloh môžeme ako CA alebo akákoľvek nami delegovaná tretia strana , zmluvne si medzi sebou rozdeliť zodpovednosť, ako ju aj určiť, avšak ako CA budeme naďalej plne zodpovedný za výkon všetkých strán v súlade s týmito požiadavkami, akoby úlohy neboli delegované. Zodpovednosť externých subjektov je zmluvne zabezpečená a taktiež zaväzuje externé subjekty povinne vykonávať všetky kontroly nami vyžadované.

Taktiež ako poskytovateľ nezodpovedáme za

- nepriame či iné straty alebo škody,
- za škodu (vrátane ušlého zisku),

ktorá vznikli zákazníkovi alebo držiteľovi certifikátu, spoliehajúcej sa strane príp. akýmkoľvek tretím stranám z dôvodu:

1. porušenia povinností zákazníkom alebo držiteľom certifikátu alebo spoliehajúcou sa stranou uvedených v právnych predpisoch, zmluve, v politikách Poskytovateľa, vrátane povinnosti vynaložiť primeranú starostlivosť pri používaní certifikátov a pri spoliehaní sa na ne;
2. neposkytnutia potrebnej súčinnosti zo strany zákazníka a držiteľa certifikátu;
3. technickými vlastnosťami, konfiguráciou, nekompatibilitou, nevhodnosťou alebo inými vadami nimi použitých softvérových alebo hardvérových prostriedkov;
4. používania, resp. spoliehania sa na certifikát, ktorého platnosť uplynula alebo ktorý bol zrušený;
5. použitia certifikátu Zákazníkom/Držiteľom certifikátu v rozpore so zmluvou, politikami Poskytovateľa;
6. použitia certifikátu v rozpore s jeho určením alebo obmedzeniami uvedenými v certifikáte, v politikách Poskytovateľa;
7. omeškania alebo nedoručenia požiadaviek na overenie statusu certifikátu Poskytovateľovi, z dôvodov, ktoré nie sú na strane Poskytovateľa (najmä prípady nedostupnosti alebo preťaženosti siete internetu alebo chybami zariadenia alebo technického vybavenia používaného overovateľom) alebo z dôvodu nedostupnosti v priebehu plánovanej údržby alebo inej organizačnej oznámenej činnosti
8. pôsobenia vyššej moci.

Poskytovateľ nezodpovedá za škody, ktoré vznikli spoliehajúcej sa strane z dôvodu, že pri spoliehaní sa na certifikát a dôveryhodné služby Poskytovateľa, resp. na elektronický podpis alebo pečať vyhotovené na ich základe nepostupovala v zmysle CP ako aj tejto CPS.

9.9 Náhrada škody

Poskytovateľ nezodpovedá za škody spôsobené zákazníkovi, držiteľovi alebo spoliehajúcim sa stranám v prípade, ak bola škoda spôsobená v dôsledku a/ alebo v súvislosti s nesplnením povinností požadovaných právnymi predpismi pre dôveryhodné služby a touto CPS ako aj CP.

Poskytovateľ nezodpovedá za porušenie svojich povinností, ak bolo porušenie týchto povinností spôsobené vyššou mocou. Za vyššiu moc sa považuje najmä vojna, požiar, povodeň, veľké prírodné anomálie, prerušenie dopravy, embargo, vládne opatrenia, pandémie, výbuch, ako aj dôsledok akýchkoľvek iných príčin, na ktoré Poskytovateľ nemá vplyv. Tieto okolnosti sú dôvodom k odkladu plnenia povinností na strane Poskytovateľa po dobu a v rozsahu účinnosti týchto okolností.

9.10 Podmienky a ukončenie

Táto CPS sa vzťahuje na všetky certifikáty vydané v súlade s ňou až do ukončenia ich platnosti.

Z pohľadu ukončenia svojich služieb sa uplatňuje nasledovný postup:

1) informovať o ukončení všetkých účastníkov a iné subjekty, s ktorými máme dohody alebo inú formu nadviazaných vzťahov, medzi ktorými sú spoliehajúce sa strany, TSP a príslušné orgány, napríklad orgány dohľadu. Okrem toho budú tieto informácie sprístupnené ďalším spoliehajúcim sa stranám;
2) ukončiť všetky oprávnenie všetkých subdodávateľov ,ktoré môžu konať v našom mene pri výkone akýchkoľvek funkcií týkajúcich sa procesu vydávania tokenov dôveryhodných služieb.

9.11 Jednotlivé oznámenia a komunikácia s účastníkmi

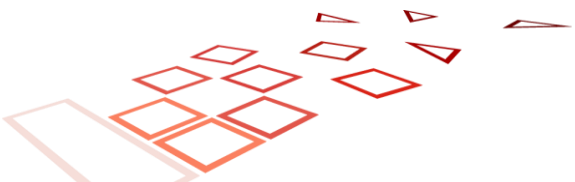
Oznámenia a komunikácia s Poskytovateľom prebiehajú pomocou kontaktných údajov, ktoré sú uvedené v kap. 1.3. Poskytovateľ môže komunikovať s účastníkmi aj inými formami, na základe kontaktných údajov, ktoré Poskytovateľovi poskytnú. Proces riadenia zmien je jednotne definovaný v internom procese Riadenie a schvaľovania zmien.

9.12 Novelizácia

Postup novelizácie tejto CPS je realizovaný interným riadeným procesom podľa internej dokumentácie. V prípade ľubovoľných zmien je vždy zmenená verzia dokumentu. V prípade významných zmien v spôsobe poskytovania Služby musí byť zmenený OID CPS. Ako kvalifikovaný poskytovateľ dôveryhodných služieb taktiež poskytujeme Národnému bezpečnostnému Úradu informácie o zmenách v jeho kvalifikovaných dôveryhodných službách najneskôr do 30 dní pred plánovanou zmenou podľa ním definovaných postupov a pravidiel. Informácie o zmenách sú zverejňované spôsobom podľa kap. 9.11.

9.13 Riešenie sporov

Všetky spory, ktoré vznikli v súvislosti s výkonom dôveryhodnej služby Poskytovateľom budú riešené prioritne zmierovacím konaním medzi stranami sporu. Ak nedôjde k dohode o sporných nárokoch do 30 pracovných dní odo dňa



uplatnenia nároku u druhej zmluvnej strany, ktorákoľvek zo strán je oprávnená podať žalobu na príslušný súd Slovenskej republiky. Súdy Slovenskej republiky sú vždy príslušné aj na prejednanie sporov s cudzím prvkom.

9.14 Rozhodné právo

Vzťahy medzi Poskytovateľom a Zákazníkom/Držiteľom ako aj činnosť spoločnosti Ardaco a.s. sa spravujú právnym poriadkom Slovenskej republiky.

9.15 Súlad s platnými právnymi predpismi

Poskytovateľ poskytuje dôveryhodné služby s platnými právnymi predpismi EU a Slovenskej republiky ako i príslušnými medzinárodnými štandardmi.
Taktiež je zabezpečené dodržiavanie Common Criteria EAL4+ pre HSM

9.16 Rôzne ustanovenia

Poskytované dôveryhodné služby a produkty pre koncových používateľov používané pri poskytovaní týchto služieb sú vždy, keď je to uskutočniteľné, prístupné osobám so zdravotným postihnutím.

10 Referencie

[1] 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 - https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32014R091

[2] Zákon č. 272/2016 Z. z. v znení neskorších predpisov o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)

[3] Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu v1.4 - https://www.nbu.gov.sk/wp-content/uploads/doveryhodne-sluzby/docs/SchemaDohladu.pdf

[4] ISO/IEC 27002:2013 Information Security Management standard, https://www.praxiom.com/iso-27002.htm

[5] ETSI EN 319 401 V2.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI);General Policy Requirements for Trust Service Providers, https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf

[6] ETSI EN 319 411-1 V1.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI);Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements - https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf

[7] ETSI EN 319 411-2 V2.1.1 (2016-02): 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, https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/en_31941102v020101p.pdf

[8] ETSI EN 319 412-1 V1.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures, https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf

[9] RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://tools.ietf.org/html/rfc5280

[10] ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

[11] CA/Browser Forum (V1.3.0): "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", https://cabforum.org/wp-content/uploads/CAB-Forum-BR-1.3.0.pdf

[12] CEN EN 419241-2:2019: Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

[13] Politika Ardaco

[14] Certifikačná politika pre KC a Certifikačná politika pre ČP

[15] Popis riešenia Remote QSCD – interný dokument