NFQES

BRAIN:IT

Certifikačná politika NFQES CA

Verzia: **2.8**

Dátum účinnosti: 21.7.2026

PO-01

Politika

Verejné

Vytvoril:

Ing. Martin Berzák
Bezpečnostný manažér

1.4.2026

Schválil:

Ing. Eduard Baraniak
Konateľ brainit.sk, s. r. o.

1.4.2026

brainit.sk, s. r. o.

Veľká Okružná 2215/66, 010 01 Žilina
IČO: 52577465

www.brainit.sk

História zmien

Verzia	Dátum	Autori	Popis	Dôvod zmien
1.0	1.4.2020	Ing. Martin Berzák	Prvá schválená verzia dokumentu	
2.0	1.12.2020	Ing. Eduard Baraniak	Revidovaná verzia dokumentu podľa RFC3647	
2.1	15.2.2021	Ing. Martin Berzák	Zapracované pripomienky NBÚ	
2.2	15.3.2021	Ing. Martin Berzák	Upravené kapitoly 3.2.2 s 3.2.3	
2.3	15.3.2022	Ing. Martin Berzák Bc. Paula Höhrová	Upravené kapitoly 1.3.3, 1.6, 3.2.2, 3.2.3, 3.3, 4.1.1, 4.1.2, 4.9.1, 4.9.2, 9.1.1, 9.4.1, 9.12.2	Rozšírenie o mandátny certifikát a registračné autority
2.4	1.3.2023	Ing. Martin Berzák	Upravené kapitoly 3.2.2 a 3.2.3	Rozšírenie o možnosť autentifikácie identity FO a PO aj bez potreby KEP
2.5	2.3.2023	Ing. Martin Berzák	Upravené kapitoly 4.1.4, 4.5.1, 6.4.1	Rozšírenie o možnosť autorizácie pomocou mobilnej aplikácie NFQES Qualified Authenticator – softvérový OCRA token
2.5	27.3.2024	Ing. Michal Šterbák, PhD.	Upravená kapitola 6.9	Prijatie predošlých TC a rozšírenie funkcionality dlhodobého uchovávania o možnosť ukladania celých súborov a ich hashu. –
2.6	1.6.2025	Ing. Ľubica Žideková Ing. Michal Šterbák, PhD.	Upravené kapitoly 6.1 , 8.2, 8.3 Doplnená kapitola 7.1.5 o PSD2 certifikáty (QSeal a QWAC) + ostatné položky profilu KC	Dopísanie kapitol 6.1, 8.2,83 Doplnenie ustanovení a profilu certifikátu pre vydávanie QCSeal a QWAC pre PSD2 certifikáty
2.7	1.4.2026	Ing. Martin Berzák Ing. Ľubica Žideková	Revízia dokumentu + rozšírenie CP o nové kvalifikované služby	Rozšírenie CP o RQES Rozšírenie kapitol 3.2.2 a 3.2.3

2.8	21.7.2026	Ing. Ľubica Žideková	Úprava hlavičiek a titulnej strany	Zmena adresy sídla Poskytovateľa

OBSAH

1 Úvod

Certifikačná politika pre certifikáty certifikačných kľúčov certifikačnej autority NFQES (v ďalšom iba „CP“), prezentuje záväzné postupy, metodiku, a zodpovednosti firmy brainit.sk s. r. o., IČO: 52577465 zapísanú v Obchodnom registri Okresného súdu Žilina, oddiel: Sro, vložka č. 72902/L (v ďalšom iba „Poskytovateľ“) pre vydávanie a správu certifikátov certifikačných kľúčov certifikačnej autority (v ďalšom iba „CA“).

CP je záväzným dokumentom, slúžiacim ako štandard postupov, procedúr a zásad, ktoré musia dodržiavať všetky zúčastnené strany.

Webové sídlo poskytovateľa je na adrese https://nfqes.sk

1.1 Prehľad

Štruktúra CP je v súlade s dokumentom RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“. CP je využívaná pre produkty a služby, ktoré poskytuje Poskytovateľ a pre správu certifikátov podľa štandardu X.509 pri implementácii infraštruktúry verejných kľúčov (ďalej „PKI“).

Táto CP sa týka poskytovania nasledovných kvalifikovaných dôveryhodných služieb:

- **Kvalifikovaná dôveryhodná služba vyhotovovania a overenia kvalifikovaných certifikátov pre elektronický podpis, kde súkromný kľúč je uložený v zariadení na vytváranie kvalifikovaného elektronického podpisu / pečate (QSCD)**
  (OID 0.4.0.194112.1.2)
- **Kvalifikovaná dôveryhodná služba vyhotovovania a overenia kvalifikovaných certifikátov pre elektronickú pečať, kde súkromný kľúč je uložený v zariadení na vytváranie kvalifikovaného elektronického podpisu / pečate (QCSD)**
  (OID 0.4.0.194112.1.3)
- **Kvalifikovaná dôveryhodná služba vyhotovovania a overenia kvalifikovaných certifikátov pre autentifikáciu webových sídiel**
  (OID 0.4.0.194112.1.4)
- **Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických podpisov**
- **Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických pečatí**
- **Kvalifikovaná dôveryhodná služba správy zariadení na vyhotovenie kvalifikovaného elektronického podpisu na diaľku (**RQES - Remote Qualified Electronic Signaturel**)**
- **Kvalifikovaná dôveryhodná služba správy zariadení na vyhotovenie kvalifikovanej elektronickej pečate na diaľku (**RQES - Remote Qualified Electronic Seal**)**

Certifikačné autority Poskytovateľa pre poskytovanie kvalifikovaných dôveryhodných služieb:

Certifikačná autorita Poskytovateľa	Sériové číslo certifikátu	Vydavateľ
CA NFQES	01	self-signed

CP sa rovnako týka všetkých certifikátov vydávaných pre potreby Poskytovateľa a to:

- Certifikát certifikačnej autority
- Certifikát na potvrdenie existencie a platnosti certifikátu (OCSP)
- Medziľahlá certifikačná autorita

1.2 Názov a identifikácia dokumentu

Verzia dokumentu: 2.8

Dátum účinnosti: 1.5.2026

CP pre certifikáty certifikačných kľúčov certifikačnej autority NFQES je identifikovaný objektovým identifikátorom OID 1.3.158.52577465.0.0.0.1.3.2, kde jednotlivé zložky OID majú nasledovný význam:

- **1** ISO
- **3** ISO Identified Organization
- **158** Slovakia
- **52577465** jedinečný identifikátor firmy brainit.sk s.r.o. (IČO)
- **0.0.0.1** CA NFQES
- **3** Dokument „Certifikačná politika NFQES CA“
- **2** major verzia dokumentu

1.3 Účastníci PKI

Táto kapitola popisuje totožnosť alebo typy entít, ktoré plnia úlohy účastníkov v rámci PKI.

1.3.1 Certifikačné autority

Certifikačná autorita:

- je subjekt, ktorý poskytuje kvalifikované dôveryhodné služby uvedené v kapitole 1.1,
- je súčasťou hierarchickej PKI štruktúry vo vydaných kvalifikovaných certifikátoch (vydavateľ KC)

Certifikačné autority Poskytovateľa sú:

- Certifikačná autorita CA NFQES (sériové číslo: 01), ktorá vydáva kvalifikované certifikáty používateľom a nie je súčasťou žiadnej hierarchickej PKI štruktúry (Self-signed certifikát).

1.3.2 Registračné autority

Registračná autorita (ďalej len „RA“) je subjekt, ktorý koná v mene Poskytovateľa, pričom vykonáva vybrané činnosti pri poskytovaní dôveryhodných služieb Poskytovateľa v súlade s touto CP v aktuálnom znení.

Poskytovateľ má zriadenú internú RA, ktorá je určená pre všetkých záujemcov, ktorí majú záujem o kvalifikované dôveryhodné služby uvedené v kapitole 1.1. Táto RA nie je samostatný právny subjekt.

1.3.3 Používatelia

Zákazníkom sa rozumie právnická osoba alebo fyzická osoba, ktorej Poskytovateľ poskytuje Dôveryhodné služby na základe dohodnutej Zmluvy a táto osoba za predmetné služby aj platí.

Držiteľom KC sa rozumie osoba uvedená v KC. Držiteľ certifikátu môže byť jedna osoba – Zákazník, alebo aj dve rôzne osoby a to v prípade, že Zákazník je zamestnávateľ, ale Držiteľom certifikátu je zamestnanec. Držiteľom Certifikátu v prípade, že sa jedná o elektronický podpis je podpisovateľ.

Držiteľom KC môže byť:

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

V prípade, že Zákazníkom je fyzická osoba a ako subjekt sú uvedené len jej meno a priezvisko, tak Zákazník a Držiteľ KC sú tá istá fyzická osoba, t. j. V prípade neplnenia si povinností kladených na Zákazníka aj Držiteľa je táto fyzická osoba je priamo zodpovedná.

Keď Zákazník koná v mene jedného alebo viacerých Držiteľov, s ktorými je prepojený (napr. Zákazník je právnická osoba požadujúca vydanie KC pre svojich zamestnancov) tak rozdielne zodpovednosti Zákazníka a Držiteľa sú definované v dokumente Všeobecné podmienky poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov“ (ďalej len „Všeobecné podmienky“) zverejnené na webovom sídle Poskytovateľa.

https://nfqes.com/sk/dokumenty

Podmienky, ktoré musí splniť Držiteľ KC a Zákazník, definuje táto CP.

Vzťah medzi Zákazníkom a Držiteľom môže byť takýto:

Pri žiadaní o KC fyzickej osoby (Držiteľ) je Zákazníkom

- samotná fyzická osoba,
- právnická osoba oprávnená na zastupovanie fyzickej osoby (Držiteľa), alebo
- akýkoľvek subjekt, s ktorým je fyzická osoba (Držiteľ) spojená.

Pri žiadaní o KC pre právnickú osobu je Zákazníkom

- akýkoľvek subjekt, ktorý je podľa príslušného právneho systému oprávnený na zastupovanie právnickej osoby, alebo
- štatutárny orgán právnickej osoby, ktorá žiada za svoje dcérske spoločnosti alebo jednotky, alebo oddelenia.

Pri žiadaní o KC pre zariadenie alebo systém prevádzkovaný fyzickou alebo právnickou osobou je Zákazníkom:

- fyzická alebo právnická osoba prevádzkujúca zariadenie alebo systém,
- štatutárny orgán právnickej osoby, ktorá žiada za svoje dcérske spoločnosti alebo jednotky alebo oddelenia.

1.3.4 Spoliehajúce sa strany

Spoliehajúce sa strany sú fyzické alebo právnické osoby, ktoré sa spoliehajú pri svojom konaní na dôveryhodné služby Poskytovateľa.

1.3.5 Ostatní účastníci

Policy Management Authority

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

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

- výkonu funkcie interného audítora, pričom touto činnosťou poverí samostatného zamestnanca.

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

Poskytovatelia iných služieb

Medzi poskytovateľov iných služieb patria:

- OCSP responder Poskytovateľa, ktorý poskytuje služby overovania platnosti KC.

1.4 Použitie certifikátu

KC vyhotovený pre fyzickú osobu, kde súkromný kľúč sa nachádza v lokálnom QSCD zariadení držiteľa certifikátu, alebo vo vzdialenom QSCD spravovanom poskytovateľom dôveryhodných služieb (identifikátor politiky 1.3.158.36061701.0.0.0.1.2.2 [QCP-n-qscd]), je vyhotovený za účelom podpory kvalifikovaného elektronického podpisu v zmysle článku 3 bod 12 Nariadenia eIDAS.

KC vyhotovený pre právnickú osobu, kde súkromný kľúč sa nachádza v v lokálnom QSCD zariadení držiteľa certifikátu, alebo vo vzdialenom QSCD spravovanom poskytovateľom dôveryhodných služieb (identifikátor politiky 1.3.158.36061701.0.0.0.1.2.2 [QCP-l-qscd]), je vyhotovený za účelom podpory kvalifikovanej elektronickej pečate v zmysle článku 3 bod 27 Nariadenia eIDAS.KC vyhotovený pre autentifikáciu webového sídla (identifikátor politiky 1.3.158.36061701.0.0.0.1.2.2 [QCP-w]) je vyhotovený za účelom podpory autentifikácie webového sídla v zmysle článku 3 bod 38 a článku 45 Nariadenia eIDAS.

1.4.1 Vhodné použitie certifikátu

Žiadne ustanovenia

1.4.2 Zakázané použitie certifikátu

Žiadne ustanovenia

1.5 Správa politiky

1.5.1 Informácie o poskytovateľovi a jeho kontaktné údaje

Názov: brainit.sk, s. r. o.

Sídlo: Veľká Okružná 2215/66, 010 01 Žilina

IČO: 52577465

DIČ: 2121068763

IČ DPH: SK2121068763

Register: Obchodný register okresného súdu Žilina, oddiel Sro, vložka číslo 72902/L

Kontakt:

Mobil: +421 918 022 030

E-mail: info@brainit.sk

Webové sídlo Poskytovateľa: https://nfqes.sk/

Webové sídlo k Dôveryhodným službám: https://zone.nfqes.sk/

Orgán dohľadu:

Kontakt pre žiadosť o zrušenie Certifikátu:

Mobil: +421 918 022 030

E-mail: info@nfqes.sk

1.5.2 Kontaktná osoba

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

Certifikačná autorita CA NFQES:

Adresa: Veľká Okružná 2215/66, 010 01 Žilina

Email: ca@nfqes.sk

Telefón: +421 905 320 821

Webové sídlo: https://nfqes.sk

Nahlasovanie incidentov: infra@nfqes.sk

1.5.3 Osoba, ktorá určuje vhodnosť CPS pre certifikačnú politiku

Osobou, ktorá je zodpovedná za rozhodovanie o súlade postupov Poskytovateľa, ktoré sú uvedené v CPS CA resp. CPS CA s touto politikou je PMA (pozri bod 1.3.5).

1.5.4 Postupy schvaľovania CPS

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

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

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

1.6 Definície a skratky

Certifikát:

- certifikát alebo kvalifikovaný certifikát pre elektronický podpis v zmysle Nariadenia eIDAS;
- certifikát alebo kvalifikovaný certifikát pre elektronickú pečať v zmysle Nariadenia eIDAS;
- certifikát pre autentifikáciu webového sídla v zmysle nariadenia eIDAS;
- mandátny certifikát v zmysle zákona č. 272/2016 Z. z. o dôveryhodných službách
- každý ďalší certifikát, ktorý slúži na šifrovanie, autentifikáciu prípadne iné účely v zmysle Politiky Poskytovateľa, ktorý bol alebo má byť vydaný Poskytovateľom pre Zákazníka.

CRL – zoznam Certifikátov zrušených pred uplynutím ich lehoty platnosti.

Dôveryhodné služby – kvalifikované dôveryhodné služby vyhotovovania a overovania Certifikátov poskytované Poskytovateľom v zmysle Nariadenia eIDAS, Zákona a Politík Poskytovateľa. Dôveryhodné služby môžu byť zložené aj z ďalších pridružených služieb v spojitosti s Certifikátmi.

Ide predovšetkým o:

- overovanie Certifikátov – poskytovanie informácií o platnosti alebo zrušení Certifikátov – CRL, OCSP odpoveď,
- generovanie kľúčových párov,

- a ďalšie...

Držiteľ certifikátu – osoba uvedená v Certifikáte, ktorá je držiteľom súkromného kľúča prislúchajúceho k verejnému kľúču, ku ktorému je vydaný Certifikát.

Nariadenie eIDAS – Nariadenie Európskeho parlamentu a Rady EÚ č. 910/2014 z 23.7.2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

OCSP odpoveď – odpoveď na OCSP požiadavku, ktorá dáva údaj o platnosti Certifikátu k špecifikovanému času.

OCRA token – hardvérový token, ktorý spĺňa štandard RFC6287 – OCRA: OATH Challenge-Response Algorithm

Politika poskytovateľa / Politiky poskytovateľa –

- politika poskytovateľa dôveryhodnej služby vyhotovovania a overovania kvalifikovaných certifikátov, ktorá sa vzťahuje na kvalifikované certifikáty vydávané Poskytovateľom v zmysle Nariadenia eIDAS;
- politika poskytovania dôveryhodnej služby vyhotovovania a overovania kvalifikovaných certifikátov, vzťahujúca sa na ostatné Certifikáty neuvedené v bode vyššie.

Politikmi poskytovateľa sú aj všetky predpisy aj ich aktualizácie, ktoré vydáva Poskytovateľ a sú zverejnené na jeho webovom sídle.

Poskytovateľ – spoločnosť brainit.sk, s. r. o. So sídlom Veľká Okružná 2215/66, Žilina 010 01, IČO: 52577465, zapísaná v obchodnom registri Okresného súdu Žilina, oddiel Sro, vložka číslo 72902/L.

Potvrdenie – potvrdenie o prevzatí Certifikátu, ktorým Držiteľ Certifikátu potvrdzuje okrem iného prevzatie Certifikátov.

Pracovisko – miesto, kde sa vydávajú Certifikáty. Je to miesto prevádzkované Poskytovateľom – jeho sídlo.

Strana spoliehajúca sa na služby – fyzická alebo právnická osoba, ktorá sa pri svojom konaní spolieha na Dôveryhodné služby Poskytovateľa.

Všeobecné podmienky (skrátene VP**)** – tento dokument definuje Všeobecné podmienky poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov, vždy v ich účinnom znení.

Kvalifikované zariadenie – zariadenie na vyhotovenie elektronického podpisu / pečate, ktoré spĺňa požiadavky stanovené v prílohe II Nariadenia eIDAS.

Zmluva – Zmluva o poskytovaní dôveryhodnej služby vydávania certifikátov uzatvorená medzi Poskytovateľom a Zákazníkom, prípadne iná zmluva medzi Poskytovateľom a Zákazníkom, ktorej predmet je poskytovanie Dôveryhodných služieb.

Zmluva s CA – zmluva uzatvorená medzi Poskytovateľom a Držiteľom Certifikátu, upravujúca práva a povinnosti zmluvných strán k používaniu Certifikátu.

Zákazník sa rozumie fyzická osoba alebo právnická osoba, ktorej Poskytovateľ poskytuje Dôveryhodné služby na základe dohodnutej Zmluvy a aj to osoba ktorá tieto služby hradí.

2 Zverejnenie a zodpovednosť za uloženie údajov

2.1 Úložiská

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

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

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

2.2 Zverejnenie informácií o certifikačnej autorite

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

- aktuálne CRL ako aj všetky CRL vydané od začiatku činnosti vyhotovovania KC,
- vlastné certifikáty certifikačných autorít Poskytovateľa, ktoré patria k jej verejným kľúčom, ktorých zodpovedajúci súkromný kľúč je využívaný pri podpisovaní vyhotovovaných KC a CRL.

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

2.3 Čas alebo frekvencia zverejnenia

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

CP a CPS prípadne ich revízie sa musia zverejniť čo najskôr po ich schválení a vydaní.

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

2.4 Kontroly prístupu k úložiskám

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

3 Identifikácia a autentifikácia

3.1 Pomenovania

3.1.1 Druhy mien

Každá CA má byť schopná vytvárať certifikáty, ktoré obsahujú rozlišovacie mená v zmysle X.500 (X.500 Distinguished Name, ďalej ako „rozlišovacie meno“) [10], konkrétne v súlade s X.501 [11] resp. X.520 [12] a aj mená v zmysle RFC5322 Internet Message Format [13].

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

3.1.2 Potreba zmysluplnosti mien

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

Používané mená musia spoľahlivo identifikovať osoby, ktorým sú priradené.

V niektorých prípadoch sa v obsahu KC nepoužívajú znaky s diakritikou a tieto sa nahrádzajú ekvivalentnými znakmi s ASCII tabuľky znakov (napr. á sa nahrádza a; č sa nahrádza c atď.). O takýto prípad môže požiadať zákazník vtedy, keď zariadenie na ktorom sa bude používať KC je špecializovaný HW, ktorý nie je možné nahradiť (príp. Je to pre zákazníka nerentabilné) a nepodporuje znakovú sadu UTF-8.

3.1.3 Anonymita alebo pseudoanonymita predplatiteľov

Poskytovateľ nepodporuje vydanie KC s pseudonymom a Poskytovateľ nesmie vydať KC pre anonymného Držiteľa.

3.1.4 Pravidlá pre tlmočenie rôznych foriem mien

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

3.1.5 Jedinečnosť mien

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

3.1.6 Uznávanie, autentifikácia a úloha ochranných známok

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

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

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

3.2 Počiatočné overenie totožnosti

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

V prípade, že je v rámci Slovenskej republiky vyhlásená mimoriadna situácia v zmysle zákona č. 42/1994 Z. z. o civilnej ochrane obyvateľstva môže PMA rozhodnúť o modifikácii spôsobu vydávania kvalifikovaných certifikátov uložených v QSCD a s tým spojeným generovaním kryptografických kľúčov a overovaním identity jednotlivých subjektov, ktorý sa bude odlišovať od tu uvedených postupov.

Modifikovaný postup, ktorý sa prispôsobí podmienkam mimoriadnej situácie a teda sa nedá bližšie špecifikovať, musí byť spracovaný v písomnej podobe, musí byť schválený PMA, musí byť posúdený orgánom posudzovania zhody a nesmie byť v rozpore s nariadením (EÚ) č. 910/2014 a národnou legislatívou a je ho možné použiť len počas trvania mimoriadnej situácie. Po ukončení mimoriadnej situácie sa musí postupovať v zmysle tu uvedených postupov.

3.2.1 Spôsob preukázania vlastníctva súkromného kľúča

Kľúčový pár, na ktorý sa vyhotovuje KC pre elektronický podpis určený na vyhotovovanie kvalifikovaného elektronického podpisu, resp. KC pre elektronickú pečať určený na vyhotovovanie kvalifikovanej elektronickej pečate musia byť generované priamo v zariadení na vyhotovenie kvalifikovaného elektronického podpisu alebo pečate, ktoré spĺňa požiadavky stanovené v prílohe II Nariadenia eIDAS [3] (ďalej len „QSCD“), bez ohľadu na to či sa jedná o lokálne QSCD držiteľa certifikátu alebo vzdialené QSCD spravované Poskytovateľom.

V prípade vzdialeného QSCD je kvalifikovaný podpis/pečať vytváraná prostredníctvom služby vzdialeného podpisovania, kde súkromný kľúč je uložený v certifikovanom HSM a podpisová operácia je vykonaná po úspešnej silnej autentifikácii Podpisovateľa.

Poskytovateľ zabezpečuje, aby držiteľ mal výlučnú kontrolu nad použitím súkromného kľúča aj v prípade jeho uloženia vo vzdialenom QSCD, a to prostredníctvom mechanizmov autentifikácie a autorizácie.

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

Žiadna zložka Poskytovateľa v nijakom prípade nearchivuje žiadne súkromné kľúče patriace Držiteľovi KC, ktorý vydala. Výnimku tvoria len súkromné kľúče spravované Poskytovateľom pre tretie strany v rámci poskytovania služby spravovania údajov na vyhotovenie elektronického podpisu resp. elektronickej pečate v mene podpisovateľa (vyhotoviteľa)(pozri Príloha č. II Nariadenia eIDAS).

3.2.2 Autentifikácia identity právnickej osoby

Overenie identity právnickej osoby môže byť vykonané v sídle RA a aj na diaľku na ľubovoľnom mieste podpísaním žiadosti o vydanie prostredníctvom certifikátov pre kvalifikovaný elektronický podpis všetkých konateľov, ktoré sú uložené v elektronickom občianskom preukaze s čipom (eID), vydaných v súlade s písmenom a) resp. b) článku 24 Nariadenia eIDAS. Zoznam konateľov je získaný z elektronického výpisu z Obchodného registra použiteľného pre právne úkony, ktorý musí zabezpečiť Zákazník cez portál slovensko.sk (alebo pracovník RA pomocou vyžiadania výpisu ORSR cez portál slovensko.sk). Následne sa všetky podpisy validujú, čím sa overia platnosti podpisov, platnosť a pravosť údajov a platnosť identifikačných dokladov. Pracovník RA následne skontroluje, či sa údaje, ktoré sú uvedené v QES podpisoch a v overenom elektronickom výpise z obchodného registra zhodujú s údajmi, ktoré sú uvedené v aplikácií zone.nfqes.sk a v žiadosti o vydanie certifikátu. Ak sú certifikáty platné, elektronický výpis z obchodného registra platný a údaje v Aplikácií, žiadosti o vydanie certifikátu, vo výpise z obchodného registra a údaje v QES podpise sa zhodujú, považuje sa PO za overenú.

Overenie identity právnickej osoby môže byť vykonané aj v sídle RA alebo aj mimo sídla RA za prítomnosti zodpovedného pracovníka RA (výjazd za zákazníkom) za fyzickej prítomnosti štatutárneho orgánu oprávneného konať za spoločnosť aj pomocou aspoň dvoch platných identifikačných dokladov každého člena štatutárneho orgánu, z toho aspoň jeden doklad každého člena štatutárneho orgánu musí byť úradný doklad s podobizňou tváre tzv. identifikácia tvárou v tvár. V tomto prípade štatutárny orgán prinesie výpis z Obchodného registra použiteľného pre právne úkony nie starší ako 3 mesiace

(prípadne si pracovník RA vyžiada výpis z ORSR cez portál slovensko.sk), štatutárny orgán oprávnený konať za spoločnosť osobne podpíše a vyjadrí súhlas so všeobecnými podmienkami a štatutárny orgán oprávnený konať za spoločnosť podpíše žiadosť o vydanie certifikátu. Pracovník RA posúdi platnosť a pravosť identifikačných dokladov (skontroluje rôzne ochranné prvky dokladov) a uchová si kópie týchto poskytnutých dokladov. V prípade, ak by sa pracovníkovi RA na dokladoch niečo nepozdávalo, musí ich odmietnuť. Následne skontroluje či sa údaje z výpisu z Obchodného registra použiteľného pre právne úkony a údaje, ktoré sú uvedené na identifikačných dokladoch, zhodujú s údajmi, ktoré sú uvedené v aplikácií zone.nfqes.sk a v žiadosti o vydanie certifikátu. Ak sa údaje v Aplikácií a žiadosti o vydanie certifikátu zhodujú s údajmi na identifikačných dokladoch a na výpise z Obchodného registra, považuje sa PO za overenú.

Výpis z obchodného registra obsahuje minimálne nasledovné údaje:

1. obchodné meno, u právnických osôb sídlo, u fyzických osôb bydlisko a miesto podnikania, ak sa líši od bydliska,
2. identifikačné číslo,
3. predmet podnikania (činnosti),
4. právna forma právnickej osoby,
5. meno a bydlisko osoby alebo osôb, ktoré sú štatutárnym orgánom alebo jeho členmi, s uvedením spôsobu, akým konajú v mene právnickej osoby,
6. označenie, sídlo a predmet podnikania (činnosti) odštepného závodu, meno vedúceho a jeho bydlisko,
7. meno prokuristu a jeho bydlisko,
8. rodné číslo spoločníka obchodnej spoločnosti alebo identifikačné číslo, ak je spoločníkom právnická osoba,
9. pri spoločnosti s ručením obmedzeným a akciovej spoločnosti rodné čísla členov dozornej rady,
10. ďalšie skutočnosti, ak to ustanovuje zákon.

Identifikačné doklady člena štatutárneho orgánu musia minimálne obsahovať:

- meno a priezvisko,
- adresu trvalého pobytu,
- rodné číslo alebo dátum narodenia.

V prípade, že sa jedná o nepodnikateľské subjekty ako sú napr. občianske združenie, obec, cirkev, nadácia a podobne, musí takáto právnická osoba preukázať okrem svojej totožnosti aj legálnosť resp. „dôvod“ svojej existencie, s využitím a poukázaním na zákon alebo iný predpis, ktorý o subjekte daného typu pojednáva, zriaďovacou listinou a pod.

Overenie identity štatutárneho orgánu môže byť vykonané aj preukázaním sa platným identifikačným dokladom a záznamom o vykonaní kontroly aktuálnosti údajov voči spoľahlivému zdroju (napr. Register fyzických osôb) 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).

Overenie identity štatutárneho orgánu môže byť vykonané aj na diaľku použitím iných metód identifikácie, ktorými sa zabezpečuje identifikácia osoby s vysokou úrovňou spoľahlivosti, ktorých zhodu potvrdí orgán posudzovania zhody a ktoré spĺňajú referenčné normy na overovanie totožnosti

a atribútov osoby, ktorej sa má vydať kvalifikovaný certifikát alebo kvalifikované elektronické osvedčenie atribútov, ktoré sú uvedené vo VYKONÁVACIOM NARIADENÍ KOMISIE (EÚ) 2025/1566.

3.2.3 Autentifikácia identity fyzickej osoby

Overenie identity fyzickej osoby môže byť vykonané v sídle RA a aj na diaľku na ľubovoľnom mieste, prostredníctvom certifikátu pre kvalifikovaný elektronický podpis uloženého v elektronickom občianskom preukaze s čipom (eID), vydaného v súlade s písmenom a) resp. b) článku 24 Nariadenia eIDAS, ktorým FO podpíše a vyjadrí súhlas so všeobecnými podmienkami a FO podpíše žiadosť o vydanie certifikátu. V oboch prípadoch (aj v sídle RA, aj na diaľku) sa tento kvalifikovaný podpis validuje, čím sa overí platnosť podpisu, platnosť a pravosť údajov a platnosť identifikačných dokladov. Pracovník RA následne skontroluje, či sa údaje, ktoré sú uvedené v QES podpise, zhodujú s údajmi, ktoré sú uvedené v aplikácií zone.nfqes.sk a v žiadosti o vydanie certifikátu. Ak je certifikát platný a údaje v Aplikácií, žiadosti o vydanie certifikátu a údaje v QES podpise sa zhodujú, považuje sa FO za overenú.

Overenie identity fyzickej osoby môže byť vykonané aj v sídle RA alebo aj mimo sídla RA za prítomnosti zodpovedného pracovníka RA (výjazd za zákazníkom) za fyzickej prítomnosti osoby, aj pomocou aspoň dvoch platných identifikačných dokladov, z toho aspoň jeden musí byť úradný doklad s podobizňou tváre tzv. identifikácia tvárou v tvár. V tomto prípade FO osobne podpíše a vyjadrí súhlas so všeobecnými podmienkami a FO podpíše žiadosť o vydanie certifikátu. Pracovník RA posúdi platnosť a pravosť identifikačných dokladov (skontroluje rôzne ochranné prvky dokladov) a uchová si kópie týchto poskytnutých dokladov. V prípade, ak by sa pracovníkovi RA na dokladoch niečo nepozdávalo, musí ich odmietnuť. Následne skontroluje, či sa údaje, ktoré sú uvedené na identifikačných dokladoch, zhodujú s údajmi, ktoré sú uvedené v aplikácií zone.nfqes.sk a v žiadosti o vydanie certifikátu. Ak sa údaje v Aplikácií a žiadosti o vydanie certifikátu zhodujú s údajmi na identifikačných dokladoch, považuje sa FO za overenú.

Identifikačné doklady fyzickej osoby musia minimálne obsahovať:

- meno a priezvisko,
- adresu trvalého pobytu,
- rodné číslo alebo dátum narodenia.

Ak fyzická osoba zastupuje inú fyzickú osobu, musí navyše preukázať, že bola splnomocnená splnomocňujúcou fyzickou osobou konať v danej veci v jej mene, a to prostredníctvom úradne overenou plnou mocou.

V prípade mandátneho certifikátu v zmysle §8 zákona č. 272/2016 Z. z., ktorý sa týka konania za inú osobu alebo orgán verejnej moci, musí Zákazník predložiť oprávnenie na konanie v mene zastupovanej osoby vo forme:

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

V prípade mandátneho certifikátu v zmysle §8 zákona č. 272/2016 Z. z., ktorý sa týka vykonávania činnosti alebo vykonávania funkcie, musí Zákazník hodnoverným spôsobom preukázať, že je orgánom verejnej moci, že vykonáva činnosť alebo funkciu podľa požiadaviek zákona č. 272/2016 Z. z. a v zmysle

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

Overenie identity fyzickej osoby môže byť vykonané aj preukázaním sa platným identifikačným dokladom a záznamom o vykonaní kontroly aktuálnosti údajov voči spoľahlivému zdroju (napr. Register fyzických osôb) 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).

Overenie identity fyzickej osoby môže byť vykonané aj na diaľku použitím iných metód identifikácie, ktorými sa zabezpečuje identifikácia osoby s vysokou úrovňou spoľahlivosti, ktorých zhodu potvrdí orgán posudzovania zhody a ktoré spĺňajú referenčné normy na overovanie totožnosti a atribútov osoby, ktorej sa má vydať kvalifikovaný certifikát alebo kvalifikované elektronické osvedčenie atribútov, ktoré sú uvedené vo VYKONÁVACIOM NARIADENÍ KOMISIE (EÚ) 2025/1566.

3.2.4 Autentizácia identity zariadenia alebo systému

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

Z uvedeného dôvodu musí byť KC webového sídla formálne priradený fyzickej osobe konajúcej v mene právnickej osoby (organizácie), ktorá má preukázateľnú kontrolu nad webovým sídlom, na ktoré je KC vyhotovený. Uplatňujú sa všetky podmienky z kapitol 3.2.2 a 3.2.3 a zároveň ďalšie podmienky, ktoré sú uvedené v tejto kapitole.

Táto fyzická osoba je povinná poskytnúť Poskytovateľovi tieto informácie:

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

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

Metódy na vykonanie tejto kontroly údajov a autentizácie zahrňujú:

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

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

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

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

- Zaslaním náhodne vygenerovanej hodnoty prostredníctvom emailu na emailovú adresu identifikovanú ako oprávnený kontakt pre danú doménu v registri oprávneného registrátora pre danú doménu (napr. pre doménu .sk je to whois.sk-nic.sk). Náhodne vygenerovaná

hodnota musí byť zaslaná spolu s potvrdením oprávnenosti žiadosti o vydanie TLS/SSL certifikátu v spätne zaslanej emailovej správe z emailovej adresy, na ktorú bola zaslaná. Náhodná hodnota musí byť jedinečná pre každú odoslanú emailovú správu. Ak týmto spôsobom prebehne úspešná validácia oprávnenosti použitia FQDN, tak Poskytovateľ môže vydať aj iné TLS/SSL certifikáty, ktoré končia rovnakým FQDN. Túto metódu je možné použiť aj na validáciu žiadosti o vydanie „wildcard" KC pre autentifikáciu webového sídla.

- Telefonicky, zavolaním na číslo identifikované ako oprávnený kontakt pre danú doménu v registri oprávneného registrátora pre danú doménu (napr. pre doménu .sk je to whois.sk-nic.sk) a overením oprávnenosti žiadosti o vydanie TLS/SSL certifikátu zo strany Zákazníka.

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

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

Kontrola údajov na dokladoch

Elektronický dokument podpísaný kvalifikovaných elektronickým podpisom/pečaťou:

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

3.2.5 Neoverené informácie o žiadateľovi

Všetky položky v kvalifikovanom certifikáte musia byť overené.

3.2.6 Validácia autority

Pozri bod 3.2.3

3.2.7 Kritériá interoperability

Poskytovateľ neuplatňuje žiadne kritériá interoperability.

3.3 Identifikácia a autentifikácia pre požiadavky na opätovné zadanie kľúča

Vydanie následného KC znamená zmenu páru kľúčov KC – vytvorí sa nový KC, ktorý bude mať zhodné rozlišovacie meno ako pôvodný, ale nový KC bude mať odlišný verejný kľúč (zodpovedajúci novému, odlišnému súkromnému kľúču), odlišné sériové číslo (Serial Number) a môže mať zmenenú dĺžku platnosti.

Zákazník žiadajúci o následný KC sa musí podrobiť požiadavkám kladeným na prvotnú registráciu (hlavne autentizácii jeho identity).

Vydanie následného mandátneho certifikátu resp. na diaľku bez osobnej prítomnosti držiteľa alebo ním splnomocnenej osoby nie je možné.

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

3.4 Identifikácia a autentifikácia pre žiadosť o odvolanie

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

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

4 Prevádzkové požiadavky na životný cyklus certifikátu

4.1 Žiadosť o vydanie certifikátu

4.1.1 Kto môže podať žiadosť o certifikát

Poskytovateľa môže požiadať o vydanie:

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

4.1.2 Proces registrácie a zodpovednosti

Zákazník musí vykonať nasledovné kroky ako prípravu na návštevu Poskytovateľa:

- oboznámiť sa so Všeobecnými podmienkami poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov brainit.sk, s.r.o. (ďalej len „Všeobecné podmienky“) a Informáciou o spracúvaní osobných údajov, ktoré musia byť v čitateľnej podobe dostupné prostredníctvo trvalého komunikačného kanálu (pozri zone.nfqes.sk),
- oboznámiť sa s týmto postupom, prípadne s princípmi a návodmi na získanie KC,
- pripraviť si hodnoty jednotlivých položiek žiadosti o KC tak, aby tieto hodnoty boli v súlade s touto CP,
- pripraviť si zvolené doklady totožnosti resp. iné potrebné doklady,
- v prípade mandátneho certifikátu pripraviť si oprávnenie na konanie v mene zastupovanej osoby (prehlásenie, poverenie resp. notárom overenú plnú moc resp. dokumenty preukazujúce jeho funkciu alebo vykonávanú činnosť alebo, že je orgánom verejnej moci), podľa zoznamu oprávnení zverejnenom na webovom sídle NBÚ.
- V prípade registrácie pomocou RA dohodnúť si termín návštevy.

Postup pred vydaním KC

Pred vydaním KC zamestnanec zastupujúci Poskytovateľa musí:

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

4.1.3 Generovanie žiadosti

V prípade KC pre autentifikáciu webového sídla pracovník Poskytovateľa musí skontrolovať doručenú žiadosť o KC vo formáte PKCS#10 a to pred overením totožnosti Zákazníka. Kontroluje sa obsah položiek žiadosti a povinnosť ich vyplnenia.

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

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

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

4.1.4 Zaslanie žiadosti o certifikát

V prípade, že KC je vyhotovovaný na QSCD zariadenie, tak žiadosť musí pracovník RA postúpiť na spracovanie priamo do QSCD zariadenia prostredníctvom aplikácie zone.nfqes.sk. Celá aplikácia zone.nfqes.sk je pracovníkovi RA sprístupnená až po autorizácií pomocou mena, hesla a jemu priradenému OCRA tokenu alebo aktivovanej aplikácie NFQES Qualified Authenticator – softvérový OCRA token, pričom potvrdzovanie žiadosti a následné spracovanie požiadavky v QSCD zariadení je tak isto potvrdzované vynútenou autorizáciou pracovníkom RA. Po spracovaní žiadosti v aplikácií zone.nfqes.sk sú následne všetky oprávnenia presunuté na osobu, pre ktorú sa KC vydáva, pričom sú dodržané všetky ustanovenia kapitoly 6.4.

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

4.2 Spracovanie žiadosti o certifikát

4.2.1 Vykonávanie identifikačných a autentifikačných funkcií

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

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

Kontrola vyplnenia údajov (osobné údaje a údaje v žiadosti o KC) bude zároveň vykonaná aj samotnou aplikáciou používanou pracovníkom RA (zone.nfqes.sk), ktorá neumožní pokračovať vo vyhotovovaní KC v prípade nevyplnenej položky, ktorá je povinná resp. v prípade nesprávne vyplnenej položky.

4.2.2 Schválenie alebo zamietnutie žiadostí o certifikát

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

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

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

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

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

Poskytovateľ musí vhodným spôsobom informovať Držiteľa o vydaní KC.

4.2.3 Čas na vybavenie žiadostí o certifikát

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

4.3 Vydanie certifikátu

4.3.1 Akcie CA počas vydávania certifikátu

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

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

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

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

Po vydaní KC na QSCD musí Poskytovateľ zabezpečiť jeho výhradnú kontrolu nad jeho súkromným kľúčom.

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

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

4.3.2 Oznámenie CA žiadateľovi o vydaní certifikátu

Poskytovateľ musí vhodným spôsobom informovať Držiteľa o vydaní KC.

4.4 Prevzatie certifikátu

4.4.1 Správanie, ktoré predstavuje prijatie certifikátu

Poskytovateľ musí bezpečným spôsobom odovzdať vydaný certifikát jeho Držiteľovi.

4.4.2 Zverejnenie certifikátu.

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

4.4.3 Oznámenie o vydaní certifikátu CA ostatným subjektom

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

4.5 Používanie verejných kľúčov a certifikátov

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

4.5.1 Používanie súkromného kľúča a certifikátu účastníka

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

- pri žiadaní o vydanie certifikátu poskytnúť Poskytovateľovi pravdivé, presné a úplné informácie v zmysle tejto CP,
- používať kľúčový pár v súlade s obmedzeniami, ktoré sú uvedené vo Všeobecných podmienkach,
- neustále chrániť svoje súkromné kľúče v súlade s touto CP, Všeobecnými podmienkami, tak aby boli výhradne pod jeho kontrolou,
- používať súkromný kľúč až po obdržaní KC k verejnému kľúču, s ktorým tvorí pár.,
- pri KC, ktorý ešte neexspiroval bezodkladne upovedomiť Poskytovateľa v prípade podozrenia, že:
    - jeho súkromný kľúč bol stratený, odcudzený alebo kompromitovaný,
    - stratil kontrolu nad súkromným kľúčom kompromitáciou jeho prihlasovacích údajov (heslo alebo OCRA token alebo mobilný telefón s aktívnou aplikáciou NFQES Qualified Authenticator – softvérový OCRA token),
    - nepresnostiach alebo zmenách v obsahu certifikátu,
    - bezodkladne požiadať o zrušenie KC v prípade, že akýkoľvek údaj uvedený v subjekte KC sa stal neplatným,
- zdržať sa používania súkromného kľúča a KC, ktorého doba platnosti už uplynula, ktorý bol zrušený alebo kompromitovaný (vrátane prípadu, že došlo ku kompromitácii samotného Poskytovateľa a Držiteľ/Zákazník má o tom vedomosť),
- dodržiavať všetky termíny, podmienky a obmedzenia uložené na využívanie svojho súkromného kľúča a KC ako napr. ukončiť používanie súkromného kľúča po exspirácii alebo zrušení KC verejného kľúča,
- používať poskytnuté KC len na príslušné účely,
- okamžite ukončiť používanie súkromného kľúča po jeho kompromitácii,

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

4.5.2 Využitie verejného kľúča a certifikátu spoliehajúcej sa strany

Spoliehajúce sa strany sú povinné:

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

4.6 Obnovenie certifikátu

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

4.7 Vydanie následného certifikátu

Pod pojmom následný certifikát sa myslí vydanie nového KC rovnakého druhu a s rovnakým obsahom pre existujúceho Držiteľa, ktorého osobné údaje sú zavedené v systéme Poskytovateľa.

4.7.1 Podmienky vydania následného certifikátu

Žiadne ustanovenia.

4.7.2 Kto môže požiadať o vydanie následného certifikátu

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

4.7.3 Spracovanie požiadaviek o vydanie následného certifikátu

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

4.7.4 Oznámenie o vydaní následného certifikátu

Poskytovateľ musí vhodným spôsobom informovať Držiteľa o vydaní následného KC.

4.7.5 Správanie, ktoré predstavuje prijatie následného certifikátu

Pozri odstavec 4.4

4.7.6 Zverejnenie následného certifikátu

Pozri odstavec 4.4.2.

4.7.7 Oznámenie o vydaní následného certifikátu ostatným subjektom

Žiadne ustanovenia

4.8 Úprava certifikátu

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

4.9 Zrušenie certifikátu

4.9.1 Podmienky zrušenia certifikátu

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

- o zrušenie certifikátu požiada Držiteľ KC,
- zistí, že pri vydaní KC neboli splnené požiadavky Nariadenie eIDAS resp. zákona č. 272/2016 Z. z.,
- zrušenie KC nariadi Poskytovateľovi svojím rozhodnutím súd,
- zistí, že KC bol vydaný na základe nepravdivých údajov,
- dozvie sa, že Držiteľ KC zomrel, ak ide o fyzickú osobu resp. zanikol ak ide o právnickú osobu,
- zistí, že došlo ku kompromitácii súkromného kľúča patriaceho k danému KC, napr. ak prístup k súkromnému kľúču patriacemu k verejnému kľúču uvedenému v KC pozná iná osoba, než Držiteľ uvedený v KC,
- Držiteľ porušil svoje povinnosti stanovené touto CP a/alebo Všeobecnými podmienkami,
- dozvie sa, že údaje uvedené v certifikáte sa stali neaktuálnymi,
- dozvie sa, že sa Držiteľ stal nesvojprávnym na základe rozhodnutia súdu,
- došlo ku kompromitácii súkromného kľúča Poskytovateľa.

V prípade mandátneho certifikátu o zrušenie požiada:

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

4.9.2 Kto môže požiadať o zrušenie certifikátu

Držiteľ KC (alebo ním poverená fyzická alebo právnická osoba) môže kedykoľvek požiadať spôsobom stanoveným v tejto CP o zrušenie svojho vlastného KC, pričom v žiadosti o zrušenie nemusí uviesť dôvod.

O zrušenie certifikátu môže tiež požiadať:

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

4.9.3 Postup pri žiadosti o zrušenie certifikátu

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

Aby sa predišlo svojvoľnému zrušeniu KC neautorizovanou stranou je dôležitá autentizácia požiadavky na zrušenie KC.

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

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

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

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

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

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

Poskytovateľ musí po zrušení KC informovať Držiteľa KC o jeho zrušení.

4.9.4 Čas na podanie žiadosti o zrušenie KC

V prípade hrozby kompromitácie súkromného kľúča musí oprávnená osoba (pozri bod 4.9.2) podať čo najskôr žiadosť o zrušenie KC. Osobne je možné žiadať o zrušenie len počas pracovnej doby určenej internou RA, ktorej pracovná doba je zverejnená na webovom sídle Poskytovateľa (pozri bod 1). Pri elektronickej žiadosti je túto možné zaslať na internú RA kedykoľvek.

4.9.5 Čas, v rámci ktorého musí CA spracovať žiadosť o zrušenie

Poskytovateľ musí:

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

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

4.9.6 Požiadavka na kontrolu zrušenia pre spoliehajúce sa strany

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

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

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

4.9.7 Frekvencia vydávania CRL

Požiadavky na frekvenciu vydávania zoznamu zrušených certifikátov (CRL) sú nasledovné:

Vydavateľ CRL	**Frekvencia vydávania**	**nextUpdate thisUpdate interval**
CA NFQES	12 hodín	24 hodín

4.9.8 Maximálna latencia pre CRL

Poskytovateľ musí zabezpečiť, aby čas od vydania CRL do jeho publikovania v úložisku nepresiahol 120 sekúnd.

4.9.9 Dostupnosť OCSP služby

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

4.9.10 Požiadavky na kontrolu OCSP

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

4.9.11 Iné formy dostupnosti informácií o zrušení certifikátu

Overenie aktuálneho stavu certifikátu je možné vykonať manuálne prostredníctvom:

- Zoznamov aktuálnych CRL, ako aj archívu všetkých vydaných CRL pre jednotlivé certifikačné autority Poskytovateľa, ktoré sú k dispozícii na adrese:
    - https://zone.nfqes.sk/crl/
- Poskytovateľ musí zabezpečiť odpoveď na telefonický alebo emailom zaslaný dopyt týkajúci sa stavu konkrétneho certifikátu.

4.9.12 Špeciálne požiadavky na zmenu kľúčov po ich kompromitácií

Žiadne ustanovenia.

4.9.13 Okolnosti, pri ktorých dochádza k pozastaveniu platnosti KC

V zmysle § 7 ods. 2 zákona o dôveryhodných službách 272/2016 Z. z. kvalifikovaný poskytovateľ dôveryhodných služieb, ktorému kvalifikovaný štatút udelil úrad, nesmie dočasne pozastaviť kvalifikovaný certifikát pre elektronický podpis alebo kvalifikovaný certifikát pre elektronickú pečať.

4.9.14 Kto môže požiadať o pozastavenie KC

Žiadne ustanovenia.

4.10 Služby súvisiace so stavom certifikátu

4.10.1 Prevádzkové požiadavky

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

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

4.10.2 Dostupnosť služby

Dostupnosť služieb je v režime 24/7 v úrovni SLA 99%.

4.11 Koniec poskytovania služieb

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

5 Fyzické, personálne a prevádzkové bezpečnostné opatrenia

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

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

Poskytovateľ musí:

- niesť plnú zodpovednosť za súlad svojej činnosti s postupmi definovanými vo svojej bezpečnostnej politike,
- mať zoznam všetkých svojich aktív s vyznačením ich klasifikácie v zmysle vykonaného posúdenia rizika.

Bezpečnostná politika Poskytovateľa a súhrn aktív týkajúci sa bezpečnosti musia byť preskúmavané v pravidelných intervaloch.

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

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

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

5.1 Fyzická bezpečnosť

5.1.1 Priestory

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

5.1.2 Fyzický prístup

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

5.1.3 Napájanie 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 pred vodou

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

5.1.5 Prevencia a ochrana proti požiaru

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

5.1.6 Úložisko médií

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

5.1.7 Likvidácia odpadu

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

5.1.8 Zálohovanie mimo hlavnú lokalitu

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

5.2 Procedurálne bezpečnostné opatrenia

5.2.1 Dôveryhodné role

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

Zároveň musia byť definované zodpovednosti jednotlivých rolí.

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

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

5.2.2 Počet osôb požadovaných pre úlohu

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

5.2.3 Identifikácia a autentifikácia pre každú rolu

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

5.2.4 Role vyžadujúce rozdelenie zodpovednosti

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

5.3 Personálne bezpečnostné opatrenia

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

5.3.1 Požiadavky na kvalifikáciu, skúsenosti a previerky

Zamestnanci v dôveryhodných rolách musia spĺňať kvalifikačné požiadavky, požiadavky na odbornú prax a mali by mať bezpečnostné previerky stanovenej úrovne.

Osoby v manažérskych funkciách musia:

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

5.3.2 Požiadavky previerky

Je odporúčané, aby zamestnanec, ktorý má byť zaradený do dôveryhodnej roly Poskytovateľa mal bezpečnostnú previerku stanovenej úrovne resp. je v procese žiadania o takýto typ previerky. Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami Poskytovateľa.

5.3.3 Požiadavky na školenie

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

5.3.4 Frekvencia obnovy školení

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

5.3.5 Frekvencia rotácie rolí

Žiadne ustanovenia.

5.3.6 Sankcie za neoprávnené konanie

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

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

5.3.7 Požiadavky na externých dodávateľov

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

5.3.8 Dokumentácia poskytnutá zamestnancom

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

5.4 Postupy získavania auditných záznamov

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

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

5.4.1 Typy zaznamenaných udalostí

Poskytovateľ musí zaznamenávať a vyhodnocovať nasledovné dôležité udalosti:

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

5.4.2 Frekvencia spracovania auditných záznamov

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

5.4.3 Lehota uchovania protokolu auditu

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

5.4.4 Ochrana protokolu auditu

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

5.4.5 Postupy zálohovania protokolu auditu

Žiadne ustanovenia.

5.4.6 Systém zhromažďovania auditov (interný vs. externý)

Žiadne ustanovenia.

5.4.7 Oznámenie subjektu iniciujúceho auditu

Žiadne ustanovenia.

5.4.8 Posúdenie zraniteľnosti

Pozri bod 5.4.2.

5.5 Archív záznamov

5.5.1 Typy archivovaných záznamov

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

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

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

5.5.2 Lehota uchovania pre archív

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

5.5.3 Ochrana archívu

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

5.5.4 Postupy zálohovania archívu

Žiadne ustanovenia.

5.5.5 Požiadavky na časovú pečiatku záznamov

Žiadne ustanovenia.

5.5.6 Archivačný systém

Žiadne ustanovenia.

5.5.7 Postupy na získanie a overenie archívnych informácií

Žiadne ustanovenia.

5.6 Zmena kľúča

Celý proces musí prebehnúť bez negatívneho vplyvu na úroveň zabezpečenia.

K zmene kľúčov Poskytovateľa môže dôjsť z nasledovných dôvodov:

- Blíži sa čas skončenia platnosti aktuálne používaných kľúčov Poskytovateľa. Toto je normálny stav – 14 dní pred uplynutím platnosti doteraz používaného páru kľúčov Poskytovateľa sa musí na webovom sídle Poskytovateľa zverejniť oznam o blížiacej sa zmene kľúčov Poskytovateľa. Po tom, čo sa vygeneruje nový kľúčový pár a vyhotoví sa nový certifikát pre Poskytovateľa, tento sa musí zverejniť na webovom sídle Poskytovateľa.
- Je nutné vymeniť aktuálne používané kľúče Poskytovateľa z dôvodu ich kompromitácie. Toto je výnimočný, havarijný stav – Poskytovateľ musí bezodkladne oznámiť orgánu dohľadu (najneskôr do 24 hodín), všetkým Držiteľom vydaných KC a verejnosti, že došlo ku kompromitácii kľúčov Poskytovateľa. Bezodkladne tiež musí zrušiť kompromitovaný certifikát,

ako aj všetky platné KC podpísané kompromitovaným kľúčom. Poskytovateľa musí upozorniť prostredníctvom svojho webového sídla Držiteľov KC, ktoré boli podpísané zrušeným certifikátom Poskytovateľa ako aj Spoliehajúcim sa stranám, že zrušený certifikát Poskytovateľa sa má odstrániť z každej aplikácie, ktorú používajú Spoliehajúce sa strany a má byť nahradený novým certifikátom Poskytovateľa.

5.7 Obnova po kompromitácií a katastrofe

5.7.1 Postupy pri riešení kompromitácie a katastrof

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

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

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

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

5.7.2 Výpočtové prostriedky, softvér alebo dáta sú poškodené

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

5.7.3 Postupy kompromitácie súkromného kľúča

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

5.7.4 Zachovanie kontinuity činnosti po katastrofe

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

5.8 Ukončenie činnosti CA alebo RA

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

Ešte pred ukončením poskytovania služieb Poskytovateľ musí:

- vhodným spôsobom, minimálne 6 mesiacov vopred, oznámiť plánované ukončenie svojej činnosti orgánu dohľadu, Držiteľom všetkých ňou vydaných platných KC, stranám spoliehajúcim sa na KC a verejnosti,
- ukončiť všetky prípadné mandátne zmluvy, splnomocnenia a pod., na základe ktorých mohli iné osoby konať v mene Poskytovateľa (napr. poskytovať služby RA),
- pred ukončením činnosti zrušiť všetky platné KC, ak nezabezpečí kontinuitu v poskytovaní jeho služieb,

- pokúsiť sa uzavrieť zmluvu s iným kvalifikovaným poskytovateľom dôveryhodných služieb, ktorý by zabezpečil kontinuitu v poskytovaní jeho kvalifikovaných dôveryhodných služieb,
- sústrediť a archivovať všetky dokumenty Poskytovateľa,
- vykonať kontrolu dodržania 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“),
- vyradiť z používania všetky súkromné kľúče, vrátane ich kópií takým spôsobom, že nebude možné ich žiadnym spôsobom obnoviť.

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

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

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

6 Technické bezpečnostné opatrenia

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

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

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

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

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

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

6.1 Generovanie a inštalácia dvojice kľúčov

6.1.1 Generovanie párov kľúčov

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

6.1.1.1 Generovanie kľúčového páru CA

Pri generovaní kľúčového páru CA sa bude postupovať nasledovne:

i. CA pripraví skript na generovanie kľúčov, ktorý sa bude striktne dodržiavať.
ii. Kľúčový pár je generovaný vo fyzicky zabezpečených oblastiach.
iii. Na generovanie kľúčových párov sú používané kryptografické moduly, ktoré spĺňajú príslušné technické požiadavky – HSM modul minimálne FIPS 140-2.
iv. Pri generovaní kľúčového páru sú prítomné kvalifikované osoby zodpovedné za správne vyhodnotenie výsledkov generovania kľúčového páru.
v. Kvalifikovaný zamestnanec vyhotoví záznam o správnom postupe pri generovaní kľúčového páru a o dodržaní bezpečnostných zásad na zabezpečenie dôvernosti a integrity vygenerovaného kľúčového páru.
vi. Záznamy z generovania párových kľúčov musia byť zaznamenávané vo forme auditných logov.

6.1.2 Doručenie súkromného kľúča predplatiteľovi

Neuplatňuje sa.

6.1.3 Doručenie verejného kľúča vydavateľovi certifikátu

Neuplatňuje sa

6.1.4 Doručenie verejného kľúča CA spoliehajúcim sa stranám

Neuplatňuje sa

6.1.5 Veľkosti kľúčov

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

6.1.6 Generovanie verejných parametrov a kontrola kvality

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

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

6.1.7 Účely použitia kľúča (podľa poľa použitia kľúča X.509 v3)

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

6.2 Ochrana súkromného kľúča a návrh kryptografického modulu

6.2.1 Štandardy a kontroly kryptografického modulu

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

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

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

6.2.2 Súkromný kľúč (n z m), ovládanie viacerých osôb

Pri operáciách správy súkromných kľúčov Poskytovateľa (napr. zálohovanie, generovanie, zničenie) musí byť vždy prítomný príslušný počet oprávnených osôb na princípe „K“ z „N“ určených oprávnených osôb (4 z 8)

6.2.3 Uloženie súkromného kľúča

Všetky súkromné kľúče využívané pri poskytovaní kvalifikovaných dôveryhodných služieb Poskytovateľa, tak ako to je uvedené v kapitole 1.1 Prehľad musia byť bezpečne ukladané, t.j. uložené v chránenom stave.

6.2.4 Záloha súkromného kľúča

Súkromné kľúče Poskytovateľa sú generované a uchovávané vo vnútri hardvérových kryptografických modulov. V prípade potreby ich prenosu pre proces zálohovania a obnovy, musia byť súkromné kľúče prenášané vždy v zašifrovanej podobe. Prenášanie súkromných kľúčov a ich obnova

v inom hardvérovom kryptografickom module môže byť vykonaná len oprávnenými zamestnancami v zmysle pravidiel uvedených v bode 6.2.2.

6.2.5 Archív súkromného kľúča

Žiadne ustanovenia.

6.2.6 Prenos súkromného kľúča do alebo z kryptografického modulu

Pozri 6.2.4

6.2.7 Uloženie súkromného kľúča na kryptografickom module

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

6.2.8 Spôsob aktivácie súkromného kľúča

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

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

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

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

6.2.9 Spôsob deaktivácie súkromného kľúča

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

6.2.10 Spôsob zničenia súkromného kľúča

Poskytovateľ musí technickými a organizačnými opatreniami zabezpečiť, že súkromné kľúče vydávajúcich CA Poskytovateľa nebude možné po ukončení jeho životného cyklu ďalej používať. O ukončení životného cyklu súkromného kľúča CA a prijatých technických a organizačných opatreniach musí byť vykonaný záznam podpísaný všetkými prítomnými aktérmi. Zničenie súkromného kľúča môže prebehnúť na vyslovenú žiadosť Podpisovateľa, pri výpadku relácii alebo pri zistení možnej kompromitácie súkromného kľúča.

6.2.11 Hodnotenie kryptografického modulu

Pozri bod 6.2.1.

6.3 Ostatné aspekty správy párov kľúčov

6.3.1 Archív verejných kľúčov

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

6.3.2 Prevádzkové obdobia certifikátu a obdobia používania dvojice kľúčov

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

Typ certifikátu	**Platnosť (maximálne)**

Vydávajúca CA	30 rokov
KC pre koncového používateľa	1 rok

6.4 Aktivačné údaje

6.4.1 Generovanie a inštalácia aktivačných údajov

Aktivačné údaje Držiteľov KC (heslo a OCRA token alebo aktivovaná aplikácia NFQES Qualified Authenticator – softvérový OCRA token), ktoré sa viažu ku konkrétnemu Držiteľovi musia byť odovzdané pri osobnom stretnutí počas vyhotovovania KC. Držiteľ musí byť poučený o spôsobe a potrebe ich zmeny a o rizikách pokiaľ uvedené zmeny nevykoná. Aktivačné údaje môžu byť v podobe S/N tokenu, PIN, hesla alebo hesla rozdeleného na viacero častí na princípe k/n a pod.

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

6.4.2 Aktivácia ochrany údajov

Za ochranu súkromných prístupových údajov a PIN kódov ku hardvérovému tokenu Držiteľov sú zodpovední výhradne samotní Držitelia.

Pri vyhotovovaní KC pre webové sídlo musia byť Držitelia upozornení so strany Poskytovateľa o potrebe chrániť súkromný kľúč silným heslom na autentifikáciu webového sídla , tak aby nemohlo dôjsť k jeho zneužitiu a to počas celej doby jeho používania.

Kľúčový pár určený pre vydavateľa KC:

- musí byť generovaný v bezpečnostnom module, ktorý spĺňa minimálne požiadavky štandardu FIPS 140-2 level 2,
- akákoľvek manipulácia so súkromným kľúčom môže byť umožnená len za princípu viacnásobnej kontroly, pričom minimálny počet potrebných oprávnených osôb musí byť štyri (4).

6.4.3 Ostatné aspekty aktivačných údajov

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

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

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

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

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

6.5 Počítačové bezpečnostné kontroly

6.5.1 Špecifické technické požiadavky na počítačovú bezpečnosť

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

Poskytovateľ vyhotovujúci KC sa môže riadiť pri poskytovaní svojich služieb požiadavkami na bezpečnosť informácií, ktoré sú kladené na dôveryhodného poskytovateľa služieb a sú definované

v štandarde ETSI EN 319 411-2 „ Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

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

6.5.2 Hodnotenie počítačovej bezpečnosti

Žiadne ustanovenia.

6.6 Opatrenia v životnom cykle

6.6.1 Kontroly vývoja systému

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

6.6.2 Kontroly riadenia bezpečnosti

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

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

6.6.3 Bezpečnostné opatrenia životného cyklu

Žiadne ustanovenia.

6.7 Ovládacie prvky zabezpečenia siete

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

6.8 Časová pečiatka

Poskytovateľ bude nakupovať časové pečiatky od externých subjektov, ktoré majú štatút kvalifikovaného poskytovateľa dôveryhodných služieb a poskytujú kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovanej elektronickej časovej pečiatky v zmysle ustanovení nariadenia (EU) č. 910/2014 (eIDAS). Tieto časové pečiatky sa budú používať v Aplikácií, v časti PODPISOVANIE, pri podpisovaní dokumentov KC. Ak má Zákazník/Držiteľ záujem, môže si objednať aj kvalifikovanú dôveryhodnú službu uchovávania kvalifikovaných elektronických podpisov/pečatí, kde sa po podpísaní dokumentu, tento podpis/pečať uchová u Poskytovateľa spolu s vypočítaným hashom dokumentu s internou časovou pečiatkou (ISO 14533-4 – TStOCSP), pričom sa v pravidelných intervaloch, ešte počas platnosti predchádzajúcej časovej pečiatky preprečiatkováva, aby sa predĺžila dôveryhodnosť kvalifikovaného elektronického podpisu a pečate aj na obdobie po uplynutí ich technologickej platnosti.

6.9 Služba uchovávania kvalifikovaných elektronických podpisov/pečatí

Proces uchovávania podpisov a pečatí bude spĺňať požiadavky podľa dokumentu ETSI TS 119 511 V1.1.1 (2019-06) s využitím služby uchovávania s dočasným úložiskom s internou časovou pečiatkou (podľa ISO 14533-4 – TStOCSP).

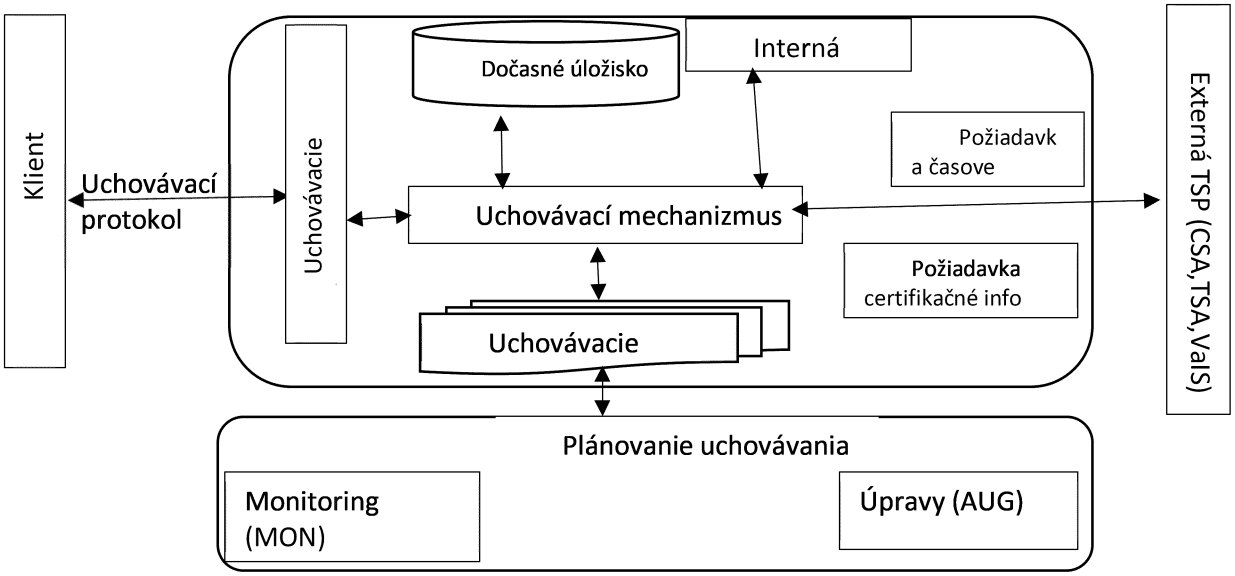
Služba uchovávania kvalifikovaných elektronických podpisov/pečatí s dočasným úložiskom bude uchovávať jeden alebo viacero vypočítaných hash hodnôt zo súborov prijatých od Zákazníka. Služba môže na podnet od Zákazníka zároveň okrem vypočítaných hash hodnôt uchovávať aj všetky súbory prijaté od Zákazníka.

Služba uchovávania bude sprístupňovať pre Zákazníka dôkazy a prijaté súbory, ak Zákazník o takúto službu požiadal, počas časového obdobia, o ktoré Zákazník požiada a s ktorým Poskytovateľ súhlasí. Po tom, ako služba uchovávania vyprodukuje dôkazy, Zákazníkovi sú tieto dôkazy dostupné na vyžiadanie cez aplikáciu počas časového obdobia uchovávania dôkazov. Po vzájomnej dohode medzi Zákazníkom a Poskytovateľom môže byť toto časové obdobie predĺžené.

Ukladacia služba môže kontaktovať externých poskytovateľov dôveryhodných služieb pre potreby získania informácií potrebných k vytvoreniu ukladaných dôkazov. Takýmito môžu byť externé certifikačné autority (CA), externé autority časovej pečiatky (TSA), externé služby vytvorenia podpisu alebo pečate (SigS) alebo validačné služby (VaIS).

Služba uchovávania bude využívať internú alebo externú autoritu časovej pečiatky pre tvorbu uchovávaných dôkazov.

Služba uchovávania bude monitorovať kryptografické algoritmy použité vo vnútri jej aktívnych profilov a zmení skupinu použitých algoritmov, ak to bude potrebné (napríklad v prípade, ak sa nájde zraniteľnosť). Uchovávané dôkazy budú vytvorené podľa aktívnych profilov a upravené v prípade potreby.



7 Certifikát, CRL a procesy OCSP

7.1 Profil certifikátu

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

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

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

7.1.1 Čísla verzií

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

7.1.2 Parametre certifikátu

Verzia (Version)	V3 (hodnota 0x2)
Serial number (Sériové číslo)	Jedinečné číslo pridelené Poskytovateľom > 0
Issuer Signature Algorithm (Podpisový algoritmus vydávateľa)	sha256WithRSAEncryption (1 2 840 113549 1 1 11)
Issuer (Vydávateľ)	Jedinečné X.500 rozlišovacie meno Poskytovateľa
Valid from (Platný od)	Začiatok platnosti certifikátu (UTC čas)
Valid to (Platný do)	Koniec platnosti certifikátu (UTC čas)
Subject ()	Obsah jednotlivých položiek pre jednotlivé typy KC pozri časť 7.1.5.1; 7.1.5.2; 7.1.5.3; 7.1.5.4
Public key (verejný kľúč)	Verejný kľúč, na ktorý je vyhotovený certifikát (min veľkosť 3072 bit)
Extensions (Rozšírenia)	Zoznam rozšírení v KC pozri Tabuľka č. 5

7.1.3 Rozšírenie certifikátu

Názov rozšírenia	ASN.1 názov a OID / Popis	Prítomnosť	Kritickosť
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Určuje (http:// … p7c, certifikát alebo aj ldap://...) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.	Áno	Nie
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	Áno	Nie

authorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} Identifikátor verejného kľúča certifikačnej autority CA, ktorá vydala tento certifikát.	Áno	Nie
certificatePolicies	{id-ce-certificatePolicies} {2.5.29.32} Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný.	Áno	Nie
crlDistributionPoints	{id-ce-CRLDistributionPoints} {2.5.29.31} Určuje, akým spôsobom a odkiaľ je možné získať CRL.	Áno	Nie
QCstatements	{id-pe-qcStatements} {1.3.6.1.5.5.7.1.3} Špecifické prehlásenie týkajúce sa EU kvalifikovaného certifikátu: esi4-qcStatement-1 esi4-qcStatement-2 esi4-qcStatement-4 esi4-qcStatement-5 esi4-qcStatement-6	Áno	Nie
BasicConstraints	{id-ce-basicConstraints} {2.5.29.19} Identifikuje typ certifikátu (end entity, CA).	Áno	Áno
keyUsage	{id-ce-keyUsage} {2.5.29.15} Definuje účel použitia súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno	Áno
extKeyUsage	{id-ce-extkeyUsage} 2.5.29.37 Definuje rozšírené použitie súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno v KC pre autentifikáciu webového sídla	Nie
SubjectAltNames	{id-ce-subjectAltName} {2.5.29.17} Toto rozšírenie obsahuje jedno alebo viac alternatívnych mien, s použitím ľubovoľného z celej rady foriem mien pre subjekt, ktorý je viazaný CA k verejnému kľúča.	Áno v KC pre autentifikáciu webového sídla	Nie

7.1.4 Identifikátory objektov algoritmu

Algoritmus podpisu vyhotovovaných KC (Signature Algorithm)

sha256RSA OID: 1.2.840.113549.1.1.11

7.1.5 Formy mien

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

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

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

V certifikáte vydávajúcej CA sa vždy musí uvádzať identifikátor Poskytovateľa v tvare „CA NFQES".

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

Dĺžky kľúčov a platnosť KC: Verejný kľúč

- RSA, dĺžka minimálne 3092 bitov
- EC, dĺžka minimálne 256 bitov

7.1.5.1 Profil KC pre elektronický podpis

Atribút	Skratka	Popis	Vzor	Poznámka
commonName OID (2.5.4.3)	CN	Meno a priezvisko	*[Meno Priezvisko]*	POVINNÝ
givenName OID (2.5.4.42)	G	Meno, resp. všetky údaje v CN okrem priezviska	*[Meno]*	POVINNÝ
Surname OID (2.5.4.4)	SN	Priezvisko, resp. všetky údaje v CN okrem Mena	*[Priezvisko]*	POVINNÝ
serialNumber OID (2.5.4.5)		Identifikátor FO	*[PNOSK-identifikátor]* *[PASSK-identifikátor]* *[IDCSK-identifikátor]*	POVINNÝ
Title OID (2.5.4.12)	T	Pracovná pozícia alebo funkcia	Manažér	NEPOVINNÝ
organizationName OID (2.5.4.10)	O	Názov organizácie podľa registra	*[brainit.sk, s. r. o.]*	POVINNÝ

serialNumber OID (2.5.4.5) organizationIdentifier OID (2.5.4.97)		Identifikátor PO	*[NTRSK-identifikátor]* *[VATSK-identifikátor]*	POVINNÝ
organizationUnitName OID (2.5.4.11)	OU	Názov oddelenia v organizácii	*[CA]*	NEPOVINNÝ
localityName OID (2.5.4.7)	L	Názov mesta alebo obce, resp. trvalé bydlisko Držiteľa KC	*[Žilina]*	POVINNÝ
stateOfProvinceName OID (2.5.4.8)	ST	Názov územného celku trvalého bydliska Držiteľa KC	*[Žilinský]*	NEPOVINNÝ
countryName OID (2.5.4.6)	C	Skratka štátu	*[SK]*	POVINNÝ
streetName OID ()	STREET	Adresa trvalého bydliska Držiteľa KC	*[Veľký Diel 3323]*	POVINNÝ

7.1.5.2 Profil KC pre elektronickú pečať

Atribút	Skratka	Popis	Vzor	Poznámka
commonName OID (2.5.4.3)	CN	Názov organizácie, resp. PO	*[brainit.sk, s. r. o.]*	POVINNÝ
organizationName OID (2.5.4.10)	O	Názov organizácie podľa registra	*[brainit.sk, s. r. o.]*	POVINNÝ
serialNumber OID (2.5.4.5) organizationIdentifier OID (2.5.4.97)		Identifikátor PO	*[NTRSK-identifikátor]* *[VATSK-identifikátor]*	POVINNÝ
organizationUnitName OID (2.5.4.11)	OU	Názov oddelenia v organizácii	*[Štatutárny orgán]*	NEPOVINNÝ
localityName OID (2.5.4.7)	L	Názov mesta alebo obce, resp. trvalé bydlisko Držiteľa KC	*[Žilina]*	POVINNÝ
stateOfProvinceName OID (2.5.4.8)	ST	Názov územného celku trvalého bydliska Držiteľa KC	*[Žilinský]*	NEPOVINNÝ
countryName OID (2.5.4.6)	C	Skratka štátu	*[SK]*	POVINNÝ

street OID (2.5.4.9)	STREET	Adresa organizácie podľa registra	*[Veľký Diel 3323]*	POVINNÝ

7.1.5.3 Profil KC pre elektronickú pečať pre PSD2

KC pre elektronickú pečať (PSD2) tzv. QSeal pre PSD2 je KC, ktorý vydáva kvalifikovaný poskytovateľ dôveryhodných služieb a KC je v súlade s požiadavkami stanovenými v Nariadení eIDAS (č. 910/2014 (EU)) v prílohe III a požiadavkami ETSI TS 119 495.

Atribút	Skratka	Popis	Vzor	Poznámka
commonName OID (2.5.4.3)	CN	Názov organizácie, resp. PO	*[brainit.sk, s. r. o.]*	POVINNÝ
organizationName OID (2.5.4.10)	O	Názov organizácie (PO) podľa registra	*[brainit.sk, s. r. o.]*	POVINNÝ
organizationIdentifier OID (2.5.4.97)		Autorizačné číslo PSD2	*[PSDSK-NBS-identifikátor]*	POVINNÝ
organizationUnitName OID (2.5.4.11)	OU	Názov oddelenia v organizácii	*[Štatutárny orgán]*	NEPOVINNÝ
localityName OID (2.5.4.7)	L	Názov mesta alebo obce, resp. trvalé bydlisko Držiteľa KC (PO)	*[Žilina]*	POVINNÝ
stateOfProvinceName OID (2.5.4.8)	ST	Názov územného celku trvalého bydliska Držiteľa KC	*[Žilinský]*	NEPOVINNÝ
countryName OID (2.5.4.6)	C	Skratka štátu	*[SK]*	POVINNÝ
street OID (2.5.4.9)	STREET	Ulica a číslo organizácie (PO) podľa registra	*[Veľký Diel 3323]*	POVINNÝ
postalCode OID (2.5.4.17)	STREET	Adresa organizácie podľa registra	*[Veľký Diel 3323]*	POVINNÝ

7.1.5.4 Profil KC pre autentifikáciu webového sídla

Atribút	Skratka	Popis	Vzor	Poznámka
commonName OID (2.5.4.3)	CN	Úplný názov domény (FQDN) na	*[www.brainit.sk]*	POVINNÝ

		ktoré sa KC vydáva		
organizationName OID (2.5.4.10)	O	Názov organizácie (PO) podľa registra	*[brainit.sk, s. r. o.]*	POVINNÝ
serialNumber OID (2.5.4.5) organizationIdentifier OID (2.5.4.97)		Identifikačné číslo PO	*[NTRSK-identifikátor]* *[VATSK-identifikátor]*	POVINNÝ
organizationUnitName OID (2.5.4.11)	OU	Názov oddelenia v organizácii	*[Štatutárny orgán]*	NEPOVINNÝ
localityName OID (2.5.4.7)	L	Názov mesta alebo obce, resp. trvalé bydlisko Držiteľa KC (PO)	*[Žilina]*	POVINNÝ
stateOfProvinceName OID (2.5.4.8)	ST	Názov územného celku trvalého bydliska Držiteľa KC	*[Žilinský]*	NEPOVINNÝ
countryName OID (2.5.4.6)	C	Skratka štátu	*[SK]*	POVINNÝ
jurisdictionOfIncorporationCountryName OID (1.3.6.1.4.1.311.60.2.1.3)		Dvojznaková skratka štátu kde je PO registrovaná	*[SK]*	POVINNÝ
businessCategory OID (2.5.4.15)		Kategória v ktorej PO podniká	*[Biznis entita]*	POVINNÝ

7.1.5.5 Profil KC pre autentifikáciu webového sídla pre PSD2

KC pre autentifikáciu webového sídla (PSD2) tzv. QWAC pre PSD2 je KC, ktorý vydáva kvalifikovaný poskytovateľ dôveryhodných služieb a KC je v súlade s požiadavkami stanovenými v Nariadení eIDAS (č. 910/2014 (EU)) v prílohe IV a požiadavkami ETSI TS 119 495.

Rovnaké ako kapitole 7.1.5.4.

7.1.5.6 Profil KC pre Mandátny certifikát

Atribút	Skratka	Popis	Vzor	Poznámka
commonName OID (2.5.4.3)	CN	Meno a priezvisko mandatára a oprávnenie zo zoznamu oprávnení	*[Mandatár, Meno Priezvisko, Oprávnenie XYZ]*	POVINNÝ
givenName OID (2.5.4.42)	G	Meno v CN okrem priezviska	*[Meno]*	POVINNÝ
Surname OID (2.5.4.4)	SN	Priezvisko uvedené v CN okrem mena	*[Priezvisko]*	POVINNÝ
serialNumber OID (2.5.4.5)		Identifikátor Mandatára	*[IDCSK-identifikátor]*	POVINNÝ
Title OID (2.5.4.12)	T	Pracovná pozícia alebo funkcia	*[Riaditeľ]*	NEPOVINNÝ
organizationName OID (2.5.4.10)	O	Identifikačné údaje mandanta ak je zastupovanou osobou PO alebo OVM	*[MANDANT, brainit.sk, s. r. o.]*	POVINNÝ
serialNumber OID (2.5.4.5) organizationIdentifier OID (2.5.4.97)		Identifikátor PO alebo OVM	*[MANDANT, NTRSK-identifikátor]*	POVINNÝ
organizationUnitName OID (2.5.4.11)	OU	Názov oddelenia PO	*[CA]*	NEPOVINNÝ
givenName OID (2.5.4.42)	G	Meno mandanta pokiaľ zastupovanou osobou je FO	*[Meno]*	POVINNÝ v prípade, že zastupovanou osobou je FO
Surname OID (2.5.4.4)	SN	Priezvisko mandanta pokiaľ zatupovanou osobou je FO	*[Priezvisko]*	POVINNÝ v prípade, že zastupovanou osobou je FO
serialNumber		Identifikátor FO mandanta ak je	*[MANDANT IDCSK-identifikátor]*	POVINNÝ v prípade, že

		zastupovanou osobou FO		zastupovanou osobou je FO
localityName OID (2.5.4.7)	L	Mesto trvalého bydliska zastupovanej osoby v prípade mandanta. V prípade mandanta PO, mesto sídla podľa registra.	*[Žilina]*	POVINNÝ v prípade, že zastupovanou osobou je FO alebo PO prípadne OVM.
stateOrProvinceName OID (2.5.4.8)	ST	Názov územného celku trvalého bydliska držiteľa.	*[Žilinský]*	NEPOVINNÝ
countryName	C	Skratka štátu	*SK*	POVINNÝ

7.1.6 Obmedzenia týkajúce sa mien

Žiadne ustanovenia.

7.1.7 Identifikátor certifikačnej politiky

Pozri kapitolu 1.2

7.1.8 Použitie rozšírení na obmedzenie politiky

Toto rozšírenie nie je používané.

7.1.9 Syntax a sémantika politiky

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

Každý SSL certifikát naviac musí obsahovať identifikátor v podobe OID (2.23.140.1.2.2), že certifikát je vyhotovovaný ako SSL certifikát, kde bola overená organizácia (právnická osoba resp. fyzická osoba), ktorá má pod kontrolou presne stanovené meno domény (FQDN) v ňom uvedené.

7.1.10 Predĺženie

Žiadne ustanovenia.

7.2 Profil CRL

7.2.1 Čísla verzií

CRL vydávané Poskytovateľom musia byť CRL verzie 2.

CRL musia byť vydávané tou istou CA Poskytovateľa ako certifikát.

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

7.2.2 CRL a rozšírenia vstupu CRL

Rozšírenia vydávaného CRL

Názov rozšírenia	**Vyžadované**	**Kritickosť**
Authority Key Identifier (OID: 2.5.29.35)	ÁNO	NIE

CRL Number (OID: 2.5.29.20)	ÁNO	NIE
Issuing Distribution Point (OID: 2.5.29.28)	ÁNO	ÁNO
id-ce-expiredCertsOnCRL (OID: 2.5.29.60)	ÁNO	NIE

7.3 Profil OCSP

7.3.1 Čísla verzií

V prípade, že Poskytovateľ vydáva OCSP odpovede, tieto musia byť v zmysle RFC 6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“. Ak budú OCSP odpovede pre jednotlivé certifikačné autority Poskytovateľa, ktoré vydávajú KC, vydávané samostatnými OCSP respondermi, ich podpisové certifikáty musia byť podpísané zodpovedajúcimi CA Poskytovateľa a musia obsahovať rozšírenie na použitie kľúča OCSP Signing (1.3.6.1.5.5.7.3.9).

7.3.2 Rozšírenia OCSP

Rozšírenia v OCSP odpovedi

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

8 Audit súladu a ďalšie hodnotenia

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

8.1 Frekvencia alebo okolnosti posudzovania

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

8.2 Totožnosť / kvalifikácie posudzovateľa

Orgán posudzovania zhody a nim poverené osoby na výkon auditu musí spĺňať požiadavky ETSI EN 319 403 „Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers“ minimálne vo verzii 2.2.2 v súlade s certifikačnou schémou NBÚ, ktorá upravuje požiadavky tejto EN.

Kontrolu posudzovania zhody vykonáva kvalifikovaný audítor. Kvalifikovaný audítor môže byť fyzickou osobou alebo právnickou osobou, ktorá:

1. Je nestranná a nezávislá od predmetu auditu.
2. Je nestranná aj vo vzťahu k poskytovateľovi.
3. By nemala mať žiadny pracovnoprávny ani iný pracovný pomer s poskytovateľom.
4. Je akreditovaná na výkon činnosti auditu.

5. Zamestnáva na výkon auditu odborníkov na preskúmanie bezpečnosti technológií na vytváranie a správu verejného kľúča.
6. Je viazaná zákonmi, nariadeniami vlády a profesijným etickým kódexom.

8.3 Vzťah hodnotiteľa k hodnotenému subjektu

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

8.4 Témy, ktorých sa hodnotenie týka

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

Poskytovateľ sa na pravidelnej báze podrobuje posudzovaniu zhody orgánom dohľadu, táto činnosť sa vykonáva na vzhľadom na vybrané bezpečnostné normy a zákony, ako sú:

- STN EN ISO/IEC 27 001
- STN EN ISO/IEC 22 301
- STN EN ISO/IEC 20 000-1
- STN EN ISO 9001
- Nariadenie Európskeho parlamentu č. 910/2014 o elektronickej identifikácií a dôveryhodných službách pre elektronické transakcie na vnútornom trhu – nariadenie eIDAS.
- Zákon č. 272/2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov – zákon o dôveryhodných službách.
- Zákon č. 69/2018 o kybernetickej bezpečnosti a zmene a doplnení niektorých zákonov.

A na vzhľadom na kvalifikované služby poskytované CA ako sú:

- Kvalifikovaný elektronický podpis
- Kvalifikovaná elektronická pečať
- Kvalifikované webové sídlo
- Kvalifikovaná časová pečiatka
- Kvalifikované uchovávanie kvalifikovaného elektronického podpisu
- Kvalifikované uchovávanie kvalifikovanej elektronickej pečate
- **Kvalifikovaná dôveryhodná služba správy zariadení na vyhotovenie kvalifikovaného elektronického podpisu na diaľku**
- **Kvalifikovaná dôveryhodná služba správy zariadení na vyhotovenie kvalifikovanej elektronickej pečate na diaľku**

8.5 Opatrenia prijaté v dôsledku nedostatku

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

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

8.6 Oznámenie výsledkov

Orgán posudzovania zhody musí výsledky auditu predložiť v písomnej forme auditovanému subjektu, ktorý na ich základe musí vykonať a prijať potrebné nápravné opatrenia. Vykonanie opatrení na nápravu musí byť dané na vedomie orgánu posudzovania zhody.

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

8.7 Interný audit

Poskytovateľ vykonáva na pravidelnej báze (minimálne 1x ročne) interný audit na kontrolu zabezpečenia dostupnosti, dôvernosti a integrity informácií a procesov súvisiacich s obchodnými činnosťami Poskytovateľa. Interný audit vykonáva kvalifikovaná zodpovedná osoba vymenovaná do roly Interného audítora. Interný audit je vykonávaný podľa vopred pripraveného plánu interného auditu, ktorý je schválený vedením organizácie Poskytovateľa.

9 Ostatné obchodné a právne veci

9.1 Poplatky

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

Poplatky za kvalifikované dôveryhodné služby poskytované Poskytovateľom uhrádza Zákazník.

9.1.1 Poplatky za vydanie alebo predĺženie platnosti certifikátu

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

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

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

9.1.2 Poplatky za prístup k certifikátu

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

9.1.3 Poplatky za odvolanie alebo prístup k informáciám o stave

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

9.1.4 Poplatky za ďalšie služby

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

9.1.5 Pravidlá vrátenia peňazí

Poskytovateľ môže vrátiť platbu za poskytnuté služby Zákazníkovi v odôvodnených prípadoch, na základe odôvodnenej žiadosti Zákazníka a svojho individuálneho posúdenia.

9.2 Finančná zodpovednosť

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

9.2.1 Poistné krytie

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

9.2.2 Ostatné aktíva

Žiadne ustanovenia.

9.2.3 Poistenie alebo záruka pre koncové subjekty

Žiadne ustanovenia.

9.3 Dôvernosť obchodných informácií

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

9.3.1 Rozsah dôverných informácií

Dôvernými informáciami podliehajúcimi zodpovedajúcej ochrane sú:

- interná infraštruktúra (napr. dokumenty, postupy, súbory, skripty, heslá, pass frázy a pod.) slúžiaca na prevádzku Poskytovateľa, vrátane jej RA, súkromné kľúče Poskytovateľa používané na podpisovanie vyhotovovaných KC,
- súkromné kľúče OCSP respondera, používané na podpisovanie odpovedí na požiadavky na potvrdenie existencie a platnosti KC,
- osobné údaje Držiteľov certifikátov podliehajúce ochrane v zmysle Predpisov o ochrane osobných údajov,

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

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

9.3.2 Informácie, ktoré nespadajú do rozsahu dôverných informácií

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

- sú v dobe ich prijatia druhou stranou verejne dostupnými alebo sa takými stanú následne bez toho, aby druhá strana porušila povinnosti podľa tejto politiky, alebo

- boli druhej strane známe ich sprístupnením v súvislosti s poskytovanými dôveryhodnými službami, alebo
- boli druhou stranou preukázateľne získané od tretej osoby, ktorá je preukázateľne oprávnená šíriť takéto informácie, alebo
- boli druhou stranou nezávisle vyvinuté bez toho, aby došlo k neoprávnenej manipulácii s dôvernými informáciami alebo
- sú všeobecne známe aj napriek ich označeniu druhou stranou ako dôverné.

9.3.3 Zodpovednosť za ochranu dôverných informácií

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

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

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

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

9.4 Ochrana osobných údajov

9.4.1 Plán ochrany osobných údajov

Poskytovateľ musí pri spracovaní osobných údajov dodržiavať požiadavky Predpisov o ochrane osobných údajov.

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

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

Na účel informovania Držiteľa/Zákazníka o spracúvaní osobných údajov vykonávaných Poskytovateľom pri poskytovaní dôveryhodných služieb slúži Informácia o spracúvaní osobných údajov, ktorá je:

a) vždy dostupná v elektronickej forme na webovom sídle Poskytovateľa;

b) odosielaná v elektronickej forme na emailovú adresu Zákazníka/Držiteľa pred začatím poskytovania dôveryhodných služieb a

c) dostupná v papierovej alebo elektronickej forme u Poskytovateľa a jednotlivých RA.

9.4.2 Informácie považované za súkromné

Poskytovateľ považuje za súkromné akékoľvek osobné údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť nepriamo alebo priamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík

alebo znakov, ktoré tvoria jej fyzickú, psychickú, ekonomickú, fyziologickú, mentálnu, kultúrnu alebo sociálnu identitu.

9.4.3 Informácie, ktoré sa nepovažujú za súkromné

Poskytovateľ môže v súlade s Predpismi na ochranu osobných údajov definovať typy informácií, ktoré spracováva pri poskytovaní kvalifikovaných dôveryhodných služieb a nie sú považované za osobné údaje.

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

9.4.4 Zodpovednosť za ochranu súkromných informácií

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

9.4.5 Oznámenie a súhlas s použitím súkromných informácií

Poskytovateľ je povinný pri plnení informačnej povinnosti voči dotknutým osobám a pri získavaní ich súhlasu so spracovaním osobných údajov postupovať v súlade s Predpismi na ochranu osobných údajov.

9.5 Práva duševného vlastníctva.

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

9.6 Vyhlásenia a záruky

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

9.6.1 Vyhlásenia a záruky CA

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

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

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

- dodržiavanie svojich povinností v zmysle tejto CP, vydaných CPS ako aj ďalších publikovaných postupov a politík, vrátane politiky informačnej bezpečnosti,
- plnenie svojich povinností v zmysle Nariadenia eIDAS a platnej legislatívy SR,
- okamžité informovanie dotknutých subjektov v prípade kompromitácie svojich súkromných kľúčov v súlade s touto CP,
- zavedenie bezpečnostných mechanizmov, vrátane mechanizmov pri generovaní a ochrane súkromného kľúča, týkajúcich sa ochrany svojej PKI infraštruktúry,
- dostupnosť tlačenej resp. elektronickej verzie tejto CP a ďalších publikovaných politík online,
- skutočnosť, že Držiteľ sa stáva resp. je vlastníkom súkromného kľúča v čase vyhotovovania kvalifikovaného certifikátu v zmysle tejto CP,

- správnosť informácii nachádzajúcich sa vo vyhotovených kvalifikovaných certifikátoch podľa najlepšieho vedomia Poskytovateľa a súlad vydaných kvalifikovaných certifikátov s požiadavkami Nariadenia eIDAS,
- dodržiavanie Predpisov na ochranu osobných údajov pri zaobchádzaní s osobnými údajmi Držiteľov.

9.6.2 Vyhlásenie a záruky RA

Interná registračná autorita poskytujúca kvalifikované dôveryhodné služby Poskytovateľa deklaruje rovnaké vyhlásenia a záruky ako CA (pozri kapitolu 9.6.1)

9.6.3 Vyhlásenia a záruky účastníkov

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

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

9.6.4 Vyhlásenia a záruky spoliehajúcich sa strán

Pozri kapitolu 10 dokumentu Všeobecné podmienky poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov brainit.sk, s.r.o., ktorého aktuálna verzia je dostupná na webovom sídle Poskytovateľa (https://zone.nfqes.sk/).

9.6.5 Vyhlásenia a záruky ostatných účastníkov

Žiadne ustanovenia.

9.7 Zrieknutie sa záruk

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

9.8 Obmedzenia zodpovednosti

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

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

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

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

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

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

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

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

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

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

i) pôsobenia vyššej moci;

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

Od okamihu, kedy zariadenie, na ktorom je uložený súkromný kľúč, ku ktorému patrí KC, nadobudne Držiteľ, Poskytovateľ nezodpovedá:

a) za ochranu zariadenia, v ktorom je uchovaný KC a súkromný kľúč, resp. za ochranu prístupových kódov potrebných na jeho použitie;

b) za to, že sa neoprávnená osoba zmocnila zariadenia alebo súkromného kľúča;

c) za škody spôsobené použitím súkromného kľúča alebo KC, ak Držiteľ/Zákazník nekoná v súlade so svojimi povinnosťami, najmä ak sa súkromného kľúča zmocní neautorizovaná osoba a Držiteľ/Zákazník nepožiada Poskytovateľa o zrušenie KC alebo ak Poskytovateľovi neoznámi zmeny v údajoch.

9.9 Odškodnenie

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

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

9.10 Trvanie a ukončenie

9.10.1 Termín

Tato verzia CP platí odo dňa nadobudnutia jej platnosti t. j. 1.12.2020 až do jej nahradenia novou verziou. Podrobnosti o histórii zmien tejto CP sú uvedené na začiatku dokumentu v časti „História zmien".

9.10.2 Ukončenie

Platnosť tejto verzie CP skončí dňom publikovania novej verzie s vyšším číslom ako je 3.0, prípadne ukončením činnosti poskytovania kvalifikovaných dôveryhodných služieb Poskytovateľom v čase jej platnosti. Všetky revízie CP a CPS ktoré sú uvedené v histórii zmien pre daný dokument musia byť k dispozícii Držiteľom/Zákazníkom resp. Spoliehajúcim sa stranám.

9.10.3 Účinok ukončenia a prežitia

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

9.11 Individuálne oznámenia a komunikácia s účastníkmi

Komunikácia Poskytovateľa s internou RA musí prebiehať oficiálne prostredníctvom autorizovanej emailovej komunikácie medzi poverenou osobou Poskytovateľa a poverenou osobou RA.

9.12 Zmeny a doplnenia

9.12.1 Postup pri zmene a doplnení

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

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

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

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

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

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

9.12.2 Mechanizmus a obdobie oznamovania

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

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

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

9.12.3 Okolnosti, za ktorých sa musí OID zmeniť

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

9.13 Ustanovenia o riešení sporov

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

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

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

9.14 Rozhodné právo

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

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

9.15 Dodržiavanie platných právnych predpisov

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

9.16 Rôzne ustanovenia

Žiadne ustanovenia.

10 Odkazy

- 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 (EÚ) č. 910/2014 a Korigendum
- Nariadenie Európskeho Parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
- Zákon č. 272/2016 Z. z o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (ďalej len zákon o dôveryhodných službách)
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov
- Informácia o spracúvaní osobných údajov (verzia 1.0)
- Všeobecné podmienky poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov brainit.sk, s.r.o. účinné od 1.12.2020 (verzia 1.1)
- SD Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu
- 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
- 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
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC3647)
- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC5280)
- X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (RFC6960)
- OCRA: OATH Challenge-Response Algorithm (RFC6287)
- ETSI TS 119 431-1 V1.3.1 (2024-12) Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev