Pravidlá na výkon certifikačných činností pre NFQES CA - Externá Registračná Autorita

Verzia: **1.0**

Dátum účinnosti: 1.4.2022

PO-09

Politika

Verejné

Vytvoril:

Ing. Martin Berzák
Bezpečnostný manažér

1.4.2024

Schválil:

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

1.4.2022

brainit.sk, s. r. o.

Veľký Diel 3323, 010 08 Žilina
IČO: 52577465

www.brainit.sk

História zmien

Verzia	Dátum	Autori	Popis	Dôvod zmien
1.0	1.4.2022	Ing. Martin Berzák Ing. Michal Šterbák	Prvá schválená verzia dokumentu	

OBSAH

Definície a skratky

Definície

Na účel tohto dokumentu sú použité nasledujúce termíny a definície:

Zmluvný partner – je právnická osoba (PO) alebo fyzická osoba (FO) s ktorou má spoločnosť brainit.sk, s. r. o. uzatvorenú písomnú zmluvu o vydaní a používaní certifikátu a služieb NFQES CA.

Registračná autorita* alebo *RA – je subjekt, ktorý v súlade s Certifikačnou politikou NFQES CA (CP NFQES CA) a/alebo politikou jej podradenej certifikačnej autority (CA) NFQES ACA (CP NFQES ACA) v aktuálnom a platnom znení, ako registračná autorita (RA) v mene NFQES CA vykonáva vybrané certifikačné činnosti pri poskytovaní dôveryhodných služieb NFQES CA, prípadne NFQES ACA a sprostredkúva služby NFQES CA/NFQES ACA Držiteľom certifikátov a žiadateľom o vydanie Certifikátu.

Certifikát – sa pre účely tohto dokumentu rozumie každý certifikát, ktorý je vydávaný pre poskytovanú dôveryhodnú službu certifikačnou autoritou NFQES CA/NFQES ACA (v zmysle nariadenia 910/2014 eIDAS). Certifikát je vydaný prostredníctvom RA v mene NFQES CA/NFQES ACA používateľom elektronického portálu https://www.zone.nfqes.com

Držiteľ Certifikátu – je osoba uvedená v Certifikáte ako držiteľ súkromného kľúča prislúchajúceho k verejnému kľúču, ku ktorému je vydaný Certifikát.

Žiadateľ Certifikátu – je osoba, ktorá žiada o vydanie certifikátu a na základe identifikačných dokladov sa overuje totožnosť danej osoby. Žiadateľ a držiteľ certifikátu sú spravidla rovnaká osoba.

Skratky

Pre účely tohto dokumentu sú použité nasledujúce skratky:

PO - Právnická osoba

FO - Fyzická osoba

CP - Certifikačný poriadok (Certificate Policy)

CA - Certifikačná autorita (Certification Authority)

OID - Identifikátor objektu (Object Identifier)

PKI - Infraštruktúra verejných kľúčov (Public Key Infrastructure)

PMA - Autorita pre správu CP (Policy Management Authority)

CPS - Pravidlá na výkon certifikačných činností (Certificate Practice Statement)

RA - Registračná autorita (Registration Authority)

EFTA - Európska zóna voľného obchodu (European Free Trade Association) – členovia Island, Lichtenštajnsko, Nórsko a Švajčiarsko

CRL - Zoznam zrušených certifikátov (Certification Revocation List)

HSM - Hardware Security Modul

NBÚ - Národný bezpečnostný úrad

CMA - Autorita pre správu certifikátov (Certificate Management Authority)

IČO - Identifikačné číslo organizácie

SC - Systémový certifikát

1 Úvod

Tento dokument definuje pravidlá na výkon certifikačných činností (ďalej len „Pravidlá“ alebo „CPS“) pre registračnú autoritu (ďalej len „RA“) NFQES CA. Pravidlá vychádzajú z CP NFQES CA (OID=1.3.158.52577465.0.0.0.1.3.2), ktoré sa uplatňujú pri implementovaní infraštruktúry verejných kľúčov (ďalej len „PKI“) pozostávajúcej z produktov a služieb, ktoré poskytujú a spravujú certifikáty podľa štandardu X.509 pre kryptografiu verejných kľúčov.

Certifikáty vydávané pre koncových používateľov jednoznačne identifikujú entitu, ktorej je certifikát vydávaný a túto entitu zväzujú s príslušným párom kľúčov. Pokiaľ v dokumente nie je vyslovene uvedené, že sa to týka certifikátu koreňovej CA, resp. podradenej CA, tak slovo certifikát znamená certifikát koncovej entity.

Základný rámec pre poskytovanie kvalifikovaných dôveryhodných služieb tvoria:

- Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)
- 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 (ďalej môže byť uvádzané aj ako „nariadenie eIDAS“)
- Vyhláška Národného bezpečnostného úradu (NBÚ) č. 62/2014 Z. z., ktorou sa mení a dopĺňa vyhláška NBÚ č. 133/2009 Z. z. o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností
- RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008
- ETSI TS 102 042 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates
- Zákon č. 18/2018 o ochrane osobných údajov v znení neskorších predpisov

1.1 Prehľad

Tento dokument predstavuje pravidlá na výkon certifikačných činností na základe ktorých je spoločnosťou brainit.sk, s. r. o., (ďalej len „Poskytovateľ“), zriadená a prevádzkovaná NFQES CA a popisuje činnosť externej RA.

Pravidlá boli vytvorené v súlade s vyhláškou NBÚ č. 62/2014 Z. z. a na základe materiálov Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework (RFC3647) a Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (RFC5280).

Tieto pravidlá definujú vytváranie a správu certifikátov s verejnými kľúčmi podľa štandardu X.509 pre ich vhodné použitie.

1.2 Názov a identifikácia dokumentu

Verzia dokumentu: 1.0

Dátum účinnosti: 1.4.2022

Popis použitého identifikátora objektu (OID):

- **1** ISO
- **3** ISO Identified Organization
- **158** Slovakia
- **52577465** jedinečný identifikátor firmy brainit.sk s.r.o. (IČO)
- **0.0.0.1** NFQES CA
- **9** Dokument „Pravidlá na výkon certifikačných činností pre NFQES CA - Externá Registračná Autorita“
- **1** major verzia dokumentu

Tieto pravidlá sa týkajú všetkých certifikátov pomocou ktorých Poskytovateľ poskytuje nasledovné kvalifikované dôveryhodné služby:

- 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)
- 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)
- Kvalifikovaná dôveryhodná služba vyhotovovania a overenia kvalifikovaných certifikátov pre autentifikáciu webových sídiel
- Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických podpisov
- Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických pečatí
- Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných elektronických časových pečiatok

CA Poskytovateľa pre poskytovanie kvalifikovaných dôveryhodných služieb:

Certifikačná autorita Poskytovateľa	Sériové číslo certifikátu	Vydavateľ
NFQES CA	01	self-signed
NFQES ACA	4a2a267827944e5 323683482e7d5a7 2205491ac1	NFQES CA

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

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

1.3 Účastníci PKI

Táto kapitola popisuje totožnosť entít, ktoré plnia úlohy v rámci poskytovania dôveryhodných služieb vyhotovovania a overovania KC (ďalej len „KC služby“). Účastníkmi v PKI sú entity uvedené tejto časti.

1.3.1 Certifikačná autorita

Je subjekt, ktorý poskytuje kvalifikované dôveryhodné služby uvedené v kapitole 1.2.

CA je súčasťou hierarchickej PKI štruktúry vo vydaných kvalifikovaných certifikátoch (vydavateľ KC).

Certifikačné autority Poskytovateľa sú:

- Certifikačná autorita NFQES CA (sériové číslo: 01), ktorá vydáva kvalifikované certifikáty používateľom a nie je súčasťou žiadnej hierarchickej PKI štruktúry (Self-signed certifikát).
- Certifikačná autorita (intermediate CA) NFQES ACA (sériové číslo: 4a2a267827944e5323683482e7d5a72205491ac1), ktorá vydáva pokročilé certifikáty používateľom a je súčasťou hierarchickej PKI štruktúry (vydavateľ).

CA je entita autorizovaná PMA na vytváranie, podpisovanie a vydávanie certifikátov s verejným kľúčom pre koreňové CA NFQES a certifikáty koncových používateľov.

CA je zodpovedná za všetky aspekty vydávania a správy vyššie uvedených certifikátov, vrátane kontroly nad procesom registrácie, procesom identifikácie a autentizácie, procesom vytvárania certifikátov, publikácie certifikátov a rušením certifikátov. CA zaručuje, že všetky aspekty jej služieb a operácií a infraštruktúry zviazanej s certifikátmi vydanými podľa týchto pravidiel sa vykonávajú v súlade s ich požiadavkami a ustanoveniami.

1.3.2 Registračná autorita

RA je subjekt, ktorý koná na základe zmluvy o RA v mene Poskytovateľa, pričom vykonáva vybrané činnosti a sprostredkúva ich poskytovanie Zákazníkom/Žiadateľom/Držiteľom v súlade s CP NFQES CA, CP NFQES ACA a týmito pravidlami v aktuálnom znení.

RA musí vykonávať svoje aktivity v súlade so schválenou verziou CP NFQES CA, CP NFQES ACA a týmito pravidlami v aktuálnom znení.

Zložkou CA NFQES, o ktorej detailne pojednávajú tieto pravidlá sú:

- **Komerčná RA** – ktorá je určená na sprostredkovanie vybraných kvalifikovaných dôveryhodných služieb Poskytovateľa širokej verejnosti a je prevádzkovaná treťou stranou, na základe písomnej zmluvy o RA s Poskytovateľom. Táto RA je samostatný právny subjekt.
- **Firemná RA** – ktorá je určená na sprostredkovanie vybraných kvalifikovaných dôveryhodných služieb výhradne pre vlastné potreby konkrétnej PO resp. pre potreby ňou prevádzkovaných systémov vyžadujúcich použitie KC a je prevádzkovaná, na základe písomnej zmluvy o RA s Poskytovateľom, danou konkrétnou PO. Takáto RA je samostatný právny subjekt.

Pokiaľ sú vytvárané RA na základe písomnej zmluvy o RA s obchodným partnerom a tento bude prevádzkovať vlastné RA, pre takýto typ budú vydávané samostatné pravidlá danej RA, ktorú musia spĺňať minimálne požiadavky definované Poskytovateľom v CP NFQES CA A CP NFQES ACA v aktuálnej verzii.

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

1.3.3 Koncoví používatelia

Žiadatelia o certifikát NFQES CA a držitelia certifikátov NFQES CA

Žiadateľom o certifikát sa rozumie FO alebo PO, ktorá je oprávnená žiadať o certifikát v mene entity, ktorej meno sa môže objaviť ako subjekt v certifikáte.

Entitou, ktorej meno sa môže objaviť ako subjekt v certifikáte, môže byť:

- fyzická osoba,
- právnická osoba,
- komponent alebo systém.

Žiadateľ o certifikát sa prevzatím certifikátu stáva Držiteľom daného certifikátu. Podmienky, ktoré musí žiadateľ o certifikát NFQES CA splniť, definuje dokument CP NFQES CA, prípadne CP NFQES ACA.

Držiteľom certifikátu sa rozumie FO alebo PO, ktorá sa zaviaže, že bude používať zodpovedajúci súkromný kľúč a certifikát v súlade s CP NFQES CA, prípadne CP NFQES ACA a týmito pravidlami.

Zákazníkom sa rozumie PO alebo FO, ktorej Poskytovateľ poskytuje dôveryhodné služby na základe dohodnutej Zmluvy o poskytovanie dôveryhodných služieb 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:

- FO,
- FO identifikovaná v spojení s PO,
- PO, ktorou môže byť organizácia alebo jej jednotka resp. oddelenie,
- zariadenie alebo systém prevádzkovaný FO alebo PO alebo prevádzkovaný v mene FO, resp. PO.

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

Ak Zákazník koná v mene jedného alebo viacerých Držiteľov, s ktorými je prepojený (napr. Zákazník je PO 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.sk/dokumenty/

Podmienky, ktoré musí splniť Držiteľ KC a Zákazník, definujú tieto pravidlá.

Vzťah medzi Zákazníkom a Držiteľom môže byť takýto:

1. Pri žiadaní o KC FO (Držiteľ) je Zákazníkom
   - samotná FO,
   - PO oprávnená na zastupovanie FO (Držiteľom), alebo
   - akýkoľvek subjekt, s ktorým je s FO (Držiteľom) spojená.
2. Pri žiadaní o KC pre PO je Zákazníkom
   - akýkoľvek subjekt, ktorý je podľa príslušného právneho systému oprávnený na zastupovanie PO, alebo
   - štatutárny orgán PO, ktorý žiada za svoje dcérske spoločnosti alebo jednotky, alebo oddelenia.
3. Pri žiadaní o KC pre zariadenie alebo systém prevádzkovaný FO alebo PO je Zákazníkom:
   - FO alebo PO prevádzkujúca zariadenie alebo systém,
   - štatutárny orgán PO, ktorý žiada za svoje dcérske spoločnosti alebo jednotky alebo oddelenia.

1.3.4 Spoliehajúce sa strany

Spoliehajúcou sa stranou je FO alebo PO, ktorá sa pri svojom konaní spolieha na dôveryhodné služby Poskytovateľa.

Stranou spoliehajúcou sa na certifikát je subjekt, ktorý tým, že používa cudzí certifikát na overenie integrity elektronicky podpísanej správy, alebo na ustanovenie bezpečnej komunikácie s Držiteľom certifikátu, sa spolieha na platnosť väzby Držiteľa certifikátu s daným verejným kľúčom. Strana spoliehajúca sa na certifikát by mala použiť informáciu z certifikátu na určenie vhodnosti certifikátu na dané použitie.

Synonymom pojmu strana spoliehajúca sa na certifikát je pojem používateľ certifikátu. Tento koná na základe dôvery v daný certifikát a/alebo na základe elektronického podpisu overeného daným certifikátom.

1.3.5 Iní účastníci

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

- dohľadu nad vytváraním a aktualizáciou CP a CPS, vrátane vyhodnocovania zmien a plánov na implementovanie prijatých zmien,
- revízie výsledkov auditov, aby sa určilo, či Poskytovateľ zodpovedne dodržiava ustanovenia vydaných CP a CPS,
- usmerňovania a riadenia činnosti Poskytovateľa ako aj RA,
- výkladu ustanovení vydaných CP a 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 po je jschválení vedením organizácie vo všetkých záležitostiach a aspektoch týkajúcich sa Poskytovateľa a jeho činnosti.

1.4 Použitie certifikátov

- **KC vyhotovený pre fyzickú osobu**, kde súkromný kľúč sa nachádza v 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 QSCD, je vyhotovený za účelom podpory kvalifikovanej elektronickej pečate v zmysle článku 3 bod 27 Nariadenia eIDAS.
- **KC vyhotovený pre autentifikáciu webového sídla**, je vyhotovený za účelom podpory autentifikácie webového sídla v zmysle článku 3 bod 38 a článku 45 Nariadenia eIDAS.
- **KC vyhotovený pre FO alebo PO**, kde súkromný kľúč sa nachádza na HSM zariadení (podľa možností aj vzdialenom HSM) za účelom podpory kvalifikovaného elektronického podpisu/pečate

1.4.1 Vhodné použitie certifikátov

Certifikáty vyhotovované v zmysle CP NFQES CA, CP NFQES ACA a týchto CPS sú vydávané na účely identifikácie Držiteľa dvojice kľúčového páru a certifikátu v rámci PKI štruktúry.

Kryptografický pár kľúčov (súkromný a verejný) a certifikát vydávaný Poskytovateľom môžu byť vo všeobecnosti použité bežným spôsobom, výhradne v súlade s ich účelovým určením, a to v závislosti od konkrétneho certifikátu najmä pre potreby:

Poskytovateľ v zmysle CP NFQES CA A CP NFQES ACA a týchto pravidiel vydáva koncovým klientom nasledujúce typy certifikátov:

- certifikáty pre FO určené najmä pre potreby zabezpečenia elektronickej pošty alebo podpisovanie elektronických dokumentov,
- certifikáty pre PO určené na vyhotovovanie elektronickej pečate,
- mandátne certifikáty pre elektronický podpis vydaný FO,
- TLS certifikáty určené pre potreby zabezpečenia autentifikácie webového sídla.

1.4.2 Zakázané použitie certifikátov

Žiadne ustanovenia.

1.5 Kontaktné údaje

Zriaďovateľ, prevádzkovateľ a majiteľ CA NFQES

Spoločnosť: brainit.sk, s. r. o.

Adresa sídla: Veľký Diel 3323, 010 08 Žilina

IČO: 52577465

DIČ: 2121068763

IČ DPH: SK2121068763

Mobil: +421 918 022 030

E-mail: info@brainit.sk

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

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

Externá registračná autorita

Uvedené ustanovenia platia pre všetky RA, pokiaľ dodatočnou zmluvou nie je dohodnuté inak.

1.6 Správa politiky

1.6.1 Organizácia zodpovedná za správu politiky

Názov: brainit.sk, s. r. o.

Sídlo: Veľký Diel 3323, 010 08 Žilina

IČO: 52577465

DIČ: 2121068763

IČ DPH: SK2121068763

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

1.6.2 Kontakt

Mobil: +421 918 022 030

E-mail: info@brainit.sk

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

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

1.6.3 Orgán dohľadu

Kontakt pre žiadosť o zrušenie Certifikátu:

Mobil: +421 918 022 030

E-mail: info@nfqes.sk

2 Všeobecné ustanovenia

2.1 Povinnosti

2.1.1 Povinnosti RA

RA zriadené spoločnosťou brainit.sk vykonávajúce činnosti v mene NFQES CA zabezpečujú funkciu podateľne pre NFQES CA – konkrétne najmä zhromažďovanie a overovanie informácií od zákazníkov – Žiadateľov o certifikát, ktoré majú byť uvedené v certifikátoch. Na RA sa realizuje priamy kontakt medzi zákazníkmi a CA NFQES.

RA prijíma žiadosti o certifikáty, preveruje a identifikuje totožnosť Žiadateľov o certifikáty, odovzdáva vydané certifikáty ich Držiteľom alebo nimi splnomocneným subjektom, sprostredkuje odovzdanie certifikátov a zoznam zrušených certifikátov (CRL) zákazníkom, prijíma a vybavuje ich reklamácie a sťažnosti, vyberá od zákazníkov stanovené poplatky za služby CA. Pri svojej činnosti sa RA riadi týmto pravidlami.

RA zodpovedá za to, že ňou zbierané informácie RA overila a teda že tieto informácie sú v danom čase pravdivé.

Pracovníci RA sú povinní najmä:

- riadiť sa ustanoveniami CP NFQES CA, CP NFQES ACA, pridruženými politikami a týmito pravidlami, ako aj pokynmi PMA,
- uchovávať v utajení súkromný kľúč RA – kompromitáciu súkromného kľúča, stratu svojej čipovej karty prípadne zabudnutie hesla na prístup k svojmu súkromnému kľúču bezodkladne hlásiť na NFQES CA,
- uchovávať korešpondenciu pracoviska RA realizovanú v písomnej alebo elektronickej forme a podľa pokynov odosielať písomné dokumenty CA na archiváciu,
- viesť záznamy o činnosti pracoviska RA v knihe záznamov,
- do knihy záznamov zaznamenávať všetky ostatné udalosti na RA, hlavne udalosti týkajúce sa súkromného kľúča RA (jeho kompromitácia, prijatie alebo strata čipovej karty, zabudnutie hesla na prístup k súkromnému kľúču), bezpečnosti pracoviska RA, prijatie (a spôsob vybavenia) podnetu, pripomienky alebo žiadosti o výklad CP a CPS,
- emailovú komunikáciu medzi RA a CA vykonávať výlučne podpísanými dokumentmi, a prípadne aj s využitím šifrovania dokumentov pomocou hesla,
- vykonávať registráciu zákazníkov – Žiadateľov o certifikát, v rámci nej overovať ich identitu, hodnoty položiek rozlišovacieho mena nachádzajúce sa v žiadosti o certifikát, formát žiadostí o certifikát, zhromažďovať dokumenty použité v procese registrácie, ktoré nevyhovujú ustanoveniam tohto dokumentu, odmietnuť,
- prijaté žiadosti o certifikát postúpiť na vybavenie tým, že ich vloží spolu s potrebnými údajmi do informačného systému (IS) NFQES CA, prípadne osobne doručí na miesto výkonu Poskytovateľa,
- niesť zodpovednosť za to, že ňou zbierané informácie overila, a teda že tieto informácie sú v danom čase pravdivé,

- prijímať, protokolovať a postupovať na vybavenie podnety, pripomienky alebo žiadosti o výklad CP a CPS a ak ich riešenie na základe tohto dokumentu alebo iných pokynov záväzných pre RA nie je jasné, postúpiť ich na vybavenie NFQES CA,
- prijímať žiadosti o zrušenie certifikátu – oprávnené postúpiť na vybavenie, ostatné odmietnuť,
- vyberať od zákazníkov stanovené poplatky za poskytované služby NFQES CA.

RA je oprávnená z naliehavých technických alebo prevádzkových dôvodov pozastaviť svoju činnosť na nevyhnutne potrebnú dobu. Túto skutočnosť je povinná bezodkladne hlásiť na NFQES CA.

RA, ktorá vykonáva registračné funkcie popísané v týchto pravidlách, musí vyhovovať ustanoveniam CP NFQES CA, CP NFQES ACA a ustanoveniam tohto dokumentu a konať podľa týchto ustanovení. Ak sa zistí, že RA nekoná v súlade s týmito povinnosťami, uplatnia sa na ňu príslušné opatrenia vrátane pozastavenia jej činnosti ako RA.

2.1.2 Povinnosti držiteľa certifikátu

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 týchto CPS, CP NFQES CA, prípadne CP NFQES ACA,
- používať KC v súlade s obmedzeniami, ktoré sú uvedené vo Všeobecných podmienkach,
- chrániť svoje súkromné kľúče v súlade s týmito pravidlami, Všeobecnými podmienkami, CP NFQES CA, prípadne CP NFQES ACA,
- používať súkromný kľúč až po obdržaní KC k verejnému kľúču s ktorým tvorí pár (v prípade QSCD zariadení),
- 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),
    - 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,
- používať poskytnuté KC len na príslušné účely,
- okamžite ukončiť používanie súkromného kľúča po jeho kompromitácii,

Povinnosti Držiteľa KC sa týkajú aj FO alebo PO, ktorá prevzala certifikáty pre ňou spravované komponenty, systémy alebo webové sídla.

2.1.3 Povinnosti spoliehajúcich sa strán

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 v CRL 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 KC,
- 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.

2.2 Právne záruky

Poskytovateľ prostredníctvom týchto pravidiel, CP NFQES CA prípadne CP NFQES ACA a zmluvy o poskytovaní služby, ako aj zmluvy o vydaní certifikátu vyjadruje právne predpoklady používania vydaných KC ich Držiteľmi a spoliehajúcimi sa stranami.

2.2.1 Vyhlásenia a záruky poskytovateľa – NFQES CA

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

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

Poskytovateľ v rozsahu stanovenom v jednotlivých častiach CP NFQES CA, prípadne CP NFQES ACA resp. vydaných CPS deklaruje:

- dodržiavanie svojich povinností v zmysle týchto pravidiel, ako aj ďalších publikovaných postupov a politík, vrátane CP NFQES CA a CP NFQES ACA a ich pridružených CPS,
- plnenie svojich povinností v zmysle Nariadenia eIDAS a platnej legislatívy SR,
- okamžité informovanie dotknutých subjektov v prípade kompromitácie svojich súkromných kľúčov v súlade s CP NFQES CA a CP NFQES ACA a týchto pravidiel,
- zavedenie bezpečnostných mechanizmov, vrátane mechanizmov pri generovaní a ochrane súkromného kľúča, týkajúcich sa ochrany svojej PKI štruktúry,
- dostupnosť tlačenej resp. elektronickej verzie týchto pravidiel a ďalších publikovaných politík online,
- skutočnosť, že Držiteľ sa stáva resp. je vlastníkom súkromného kľúča v čase vyhotovovania KC v zmysle CP NFQES CA, CP NFQES ACA a týchto pravidiel,
- správnosť informácii nachádzajúcich sa vo vyhotovených KC podľa najlepšieho vedomia Poskytovateľa a súlad vydaných KC s požiadavkami Nariadenia eIDAS,
- dodržiavanie predpisov na ochranu osobných údajov pri zaobchádzaní s osobnými údajmi Držiteľov.

2.2.2 Vyhlásenie a záruky RA

Všetky externé RA Poskytovateľa musia poskytovať dôveryhodné služby na základe zmluvného vzťahu s Poskytovateľom a v súlade s CP NFQES CA, CP NFQES ACA a týmito pravidlami. Ďalej pozri ustanovenia v časti 2.2.

2.2.3 Vyhlásenia a záruky účastníkov

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

- poskytnutie presných a správnych informácií v komunikácii s Poskytovateľom,
- oboznámenie sa a súhlas so všetkými podmienkami danými v CP NFQES CA, prípadne CP NFQES ACA, príslušnými CPS k CP a s týmito pravidlami, ktoré sú dostupné v úložisku Poskytovateľa (pozri časť 1),
- používanie vydaných KC len na vhodné účely v súlade s CP NFQES CA, prípadne CP NFQES ACA, príslušnými CPS k CP a s týmito pravidlami,
- 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.

2.2.4 Vyhlásenie a záruky spoliehajúcich sa strán

Vyhlásenia a záruky spoliehajúcich sa strán sú súčasťou Všeobecných podmienok poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov Poskytovateľa, ktoré sú dostupné na webovom sídle Poskytovateľa.

2.2.5 Vyhlásenia a záruky ostatných účastníkov

Žiadne ustanovenia.

2.3 Finančná zodpovednosť

2.3.1 Poistné krytie

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

2.3.2 Ostatné aktíva

Žiadne ustanovenia.

2.3.3 Poistenie alebo záruka pre koncové subjekty

Žiadne ustanovenia.

2.4 Rozhodcovské konanie a riešenie sporov

2.4.1 Ustanovenia o riešení sporov

Držiteľ/Zákazník má právo zaslať Poskytovateľovi sťažnosť, podnet alebo reklamáciu na poskytnutú 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.

RA má oprávnenie prijímať a vybavovať jednoduché sťažnosti, reklamácie a dopyty žiadateľov alebo Držiteľov certifikátu, pokiaľ nie je dôvod na ich postúpenie k NFQES CA.

Súdy SR 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 PO zapísaná v zozname subjektov alternatívneho riešenia spotrebiteľských sporov vedenom Ministerstvom hospodárstva SR. Držiteľ/Zákazník má právo voľby, na ktorý z uvedených subjektov alternatívneho riešenia spotrebiteľských sporov sa obráti. Pred pristúpením k súdnemu alebo mimosúdnemu riešeniu sporu sú zmluvné strany povinné pokúsiť sa najskôr vyriešiť tento spor vzájomnou dohodou.

2.4.2 Rozhodné právo

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

Práva a povinnosti zmluvných strán výslovne neupravené v zmluve uzatvorenou medzi Poskytovateľom a Zákazníkom, Všeobecnými podmienkami a týmito pravidlami 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 SR.

2.5 Poplatky

Povinnosťou Poskytovateľa je vhodným spôsobom (prostredníctvom webového sídla) zverejniť platný cenník svojich dôveryhodných služieb resp. informáciu za akých zmluvných podmienok je možné získať dôveryhodné služby.

2.6 Zverejňovanie informácií a úložisko

2.6.1 Zverejňovanie informácií o CA

Úložiská musia byť umiestnené tak, aby boli prístupné Držiteľom KC a Spoliehajúcim sa stranám a v súlade s celkovými bezpečnostnými požiadavkami uvedené v CP NFQES CA prípadne CP NFQES ACA.

Webové sídlo zastáva funkciu úložiska Poskytovateľa. Presná URL adresa je uvedená v časti 1.5 tohto dokumentu. Webové sídlo Poskytovateľa je prostredníctvom internetu verejne prístupné Držiteľom KC, Spoliehajúcim sa stranám a verejnosti vôbec.

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

Poskytovateľ zverejňuje, v on-line režime prostredníctvom svojho webového sídla, informácie ktoré sú prístupné Zákazníkom, Držiteľom KC a Spoliehajúcim sa stranám minimálne v rozsahu:

- aktuálne CRL ako aj všetky CRL vydané od začiatku činnosti vyhotovovania KC,

- vlastné certifikáty CA Poskytovateľa, ktoré patria k jej verejným kľúčom, ktorých zodpovedajúci súkromný kľúč je využívaný pri podpisovaní vyhotovovaných KC a CRL.

Poskytovateľ zverejňuje v on-line režime prostredníctvom svojho webového sídla tieto pravidlá, ako aj ďalšie dokumenty súvisiace s poskytovaním dôveryhodných služieb v zmysle tohto dokumentu.

Poskytovateľ nezverejňuje informácie o vydaných certifikátoch, ktoré sú vydávané pre interné potreby zmluvných partnerov a s partnerom je zmluvne dohodnuté ich nezverejňovanie.

2.6.2 Frekvencia zverejňovania informácií

Zoznam zrušených certifikátov (CRL) musí byť publikovaný nasledovne:

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

Informácie o zrušenom KC musia byť dostupné na webovom sídle Poskytovateľa, 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.

Certifikát sa publikuje ihneď po jeho vydaní a okamžite je možné jeho prevzatie Držiteľom certifikátu. Informácie o vydanom certifikáte možno nájsť na webovom sídle Poskytovateľa, ktoré slúži ako repozitár certifikačnej autority CA NFQES.

2.6.3 Kontroly prístupu

Poskytovateľ chráni každú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozšírenie. Poskytovateľ vynakladá maximálne úsilie na to, aby zaistil dôvernosť, integritu a dostupnosť dát vyplývajúcich z poskytovaných dôveryhodných služieb. Taktiež vykonáva 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.

2.6.4 Úložiská

Pozri časti 2.6.1 a 2.6.3.

2.7 Audit zhody

2.7.1 Frekvencia auditu zhody pre danú entitu

Poskytovateľ sa podrobuje auditu zhody aspoň každých 24 mesiacov v súlade s požiadavkami ním poskytovaných dôveryhodných služieb.

2.7.2 Identita audítora a kvalifikačné požiadavky

Orgán posudzovania zhody a nim poverené osoby na výkon auditu musí byť kompetentný v oblasti auditov zhody, 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 ETSI normy a musí byť dôkladne oboznámený s CP NFQES CA, CP NFQES ACA, príslušnými CPS a týmto dokumentom.

2.7.3 Témy pokrývané auditom zhody

Účelom auditu je potvrdiť, že Poskytovateľ má vyhovujúci systém práce RA, ktorý garantuje kvalitu služieb, ktoré NFQES CA poskytuje a ktorý garantuje, že RA koná v súlade so všetkými požiadavkami týchto pravidiel. Predmetom auditu zhody sú všetky aspekty prevádzky NFQES CA vzťahujúce sa k týmto pravidlám.

2.7.4 Akcie vykonané na odstránenie nedostatkov

Keď audítor zistí rozpor medzi prevádzkou externej RA a platnými požiadavkami alebo ustanoveniami CP, vydaných CPS a týmto dokumentom, musia sa uskutočniť nasledujúce akcie:

- audítor identifikuje a zaznamená rozpor,
    - Audítor presne identifikuje a zdokumentuje, v čom spočíva rozpor medzi aktuálnou prevádzkou externej RA a požiadavkami CP, CPS alebo ustanoveniami tohto dokumentu.
- audítor musí upovedomiť o rozpore všetky zainteresované subjekty,
    - Audítor nahlási rozpor príslušným zodpovedným osobám, čo môžu byť manažéri alebo vedúci pracovníci externej RA, ktorí sú zodpovední za zabezpečenie súladu s CP, CPS a týmto dokumentom, rovnako ako aj zodpovedné osoby NFQES CA.
- NFQES CA navrhne PMA,
    - PMA musí určiť vhodné opatrenie na nápravu vrátane očakávaného času potrebného na jeho realizáciu (môže byť realizovateľné v spolupráci s audítorom).
- monitorovanie implementácie nápravných opatrení
    - určená osoba (zodpovedná osoba za externú RA, ako aj osoba za NFQES CA) sleduje, či externá RA vykonala navrhnuté nápravné opatrenia v primeranej lehote a či došlo k odstráneniu rozporu.
- zaznamenanie postupu a výsledkov
    - Všetky kroky, opatrenia a výsledky sú zaznamenané v správe alebo dokumentácii, ktorá obsahuje, akým spôsobom bol rozpor riešený, a či bola zaistená plná zhoda s požiadavkami.
- opakovaný audit
    - Ak rozpor nebol adekvátne vyriešený alebo ak je potrebné overiť trvalé dodržiavanie požiadaviek, môže byť naplánovaný opakovaný audit alebo kontrola zameraná na posúdenie, či boli všetky nedostatky odstránené.

2.7.5 Zaobchádzanie s výsledkami auditu

Orgán posudzovania zhody musí výsledky auditu predložiť v písomnej alebo elektronickej forme auditovanému subjektu (NFQES CA alebo externej RA), ktorý na ich základe musí vykonať a prijať potrebné nápravné opatrenia.

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

Vykonanie opatrení na nápravu je dané na vedomie príslušnej autorite. Na potvrdenie vykonania a účinnosti opatrení na nápravu sa môže požadovať špeciálny audit zhody alebo čiastkový audit zhody zameraný na daný aspekt činnosti auditovaného subjektu.

2.8 Utajenie

2.8.1 Typy chránených informácií

Všetky informácie podliehajúce zodpovedajúcej ochrane sú uvedené v CP NFQES CA, CP NFQES ACA a súkromné kľúče patriace zložkám NFQES CA a externej RA.

Dôvernými informáciami podliehajúcimi zodpovedajúcej ochrane sú:

- interná infraštruktúra (napr. dokumenty, politiky, smernice, pracovné 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 „Interné“ alebo „Dôverné“. Dôvernými informáciami môžu byť najmä, avšak nie výlučne, dáta, špecifikácie, analýzy, komerčné informácie, know-how, dokumentácie, postupy, procesy, informácie týkajúce sa na klientov alebo obchodných partnerov alebo iné informácie z IS Poskytovateľa, resp. jeho Zákazníkov v akejkoľvek podobe.

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

2.8.2 Okolnosti uvoľnenia dôverných informácií

NFQES CA ani žiadna externá RA nezverejňuje žiadne informácie týkajúce sa Žiadateľa o certifikát alebo Držiteľa certifikátu žiadnej tretej strane (ak to nie je vo Všeobecných podmienkach alebo Pravidlách o spracovaní osobných údajov definované inak), ak dané informácie nie sú považované za verejné, alebo ak to nie je požadované zákonom alebo príkazom kompetentného štátneho orgánu, ako je polícia, súd, prokuratúra resp. je to predmetom zmluvy medzi Poskytovateľom a jej partnerom.

Každá požiadavka na uvoľnenie informácií, ktoré nie sú považované za verejné, je autentizovaná a riadne zadokumentovaná.

Poskytovateľ zaobchádza s osobnými údajmi zákazníka v súlade s platnými zákonmi SR a neposkytuje ich žiadnej tretej strane s výnimkou subjektov, ktoré majú právo kontrolovať činnosť Poskytovateľa a s výnimkou, ktoré sú definované vo Všeobecných podmienkach a Pravidlách pre spracovanie osobných údajov.

2.9 Práva vyplývajúce z intelektuálneho vlastníctva

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

3 Identifikácia a autentifikácia

3.1 Prvotná registrácia

3.1.1 Typy mien

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

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 (FO, PO, OVM, 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 Jedinečnosť mien

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

3.1.4 Procedúra riešenia sporov pri kolízii mien

Interpretácia jednotlivých foriem mien v KC vyhotovovaných Poskytovateľom musí byť v súlade s profilmi KC, ktoré sú popísané v CP NFQES CA v časti 7, prípadne CP NFQES ACA.

3.1.5 Rozpoznanie, autentifikácia a rola obchodných značiek

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

V KC môžu byť použité len tie obchodné značky, ktorých vlastníctvo alebo prenájom Zákazník/Držiteľ 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.

3.1.6 Preukazovanie vlastníctva súkromného kľúča

Kľúčový pár, na ktorý sa vyhotovuje KC pre elektronický podpis určený na vyhotovovanie kvalifikovaného elektronického podpisu, resp. KC pre elektronickú pečať určený na vyhotovovanie kvalifikovanej elektronickej pečate musia byť generované priamo v zariadení na vyhotovenie kvalifikovaného elektronického podpisu alebo pečate, ktoré spĺňa požiadavky stanovené v prílohe II Nariadenia eIDAS (ďalej len „QSCD“). V prípade vzdialených certifikátov musia byť tieto KC vygenerované priamo na bezpečnom hardvérovom zariadení HSM.

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.

3.1.7 Autentizácia identity právnickej osoby (organizácie)

Žiadateľ o certifikát konajúci v mene PO musí predložiť názov PO, iný identifikačný údaj, ak taký existuje (spravidla je to napr. IČO), adresu a dôkaz existencie danej PO výpisom z obchodného registra nie starším ako 3 mesiace.

RA overuje tieto údaje a okrem identity oprávnenej osoby používateľa (žiadajúcej osoby) overuje, že daná osoba má právo jednať v mene danej PO vo veci príslušného certifikátu. Detailné ustanovenia pre predkladanie identifikačných dokladov sú definované v CP/CPS NFQES CA prípadne CP/CPS NFQES ACA.

Overenie identity PO je vykonávané v sídle externej RA alebo aj mimo sídla RA za prítomnosti zodpovedného pracovníka externej 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 (existuje možnosť overenia existencie PO aj pracovníkom RA, a to cez portál slovensko.sk a vyžiadaním výpisu z obchodného registra priamo pracovníkom RA), 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 externej 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 externej 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 IS Poskytovateľa a v žiadosti o vydanie certifikátu. Ak sa údaje v IS a žiadosti o vydanie certifikátu zhodujú s údajmi na identifikačných dokladoch a na výpise z Obchodného registra, považuje sa PO za overenú.

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 PO 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.

3.1.8 Autentizácia identity fyzickej osoby

FO môže byť plnoletý občan SR alebo cudzí štátny príslušník.

Overenie identity FO je vykonávané v sídle externej RA alebo aj mimo sídla RA za prítomnosti zodpovedného pracovníka externej 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 externej 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 IS Poskytovateľa a v žiadosti o vydanie certifikátu. Ak sa údaje v IS a žiadosti o vydanie certifikátu zhodujú s údajmi na identifikačných dokladoch, považuje sa FO za overenú.

Identifikačné doklady FO musia minimálne obsahovať:

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

Ak FO zastupuje inú FO, musí navyše preukázať, že bola splnomocnená splnomocňujúcou FO konať v danej veci v jej mene, a to prostredníctvom úradne overenej plnej moci.

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

- dokladu preukazujúceho, že daná osoba je štatutárnym orgánom danej PO alebo OVM,
- poverenia, ak je daná FO zamestnancom PO, v mene ktorej koná a je s ňou v pracovnoprávnom vzťahu alebo obdobnom pracovnom vzťahu,
- notárom overenej plnej moci, ak daná FO 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 OVM, 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.

3.1.9 Autentizácia identity zariadenia, systému alebo webového sídla

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 FO konajúcej v mene PO (organizácie), ktorá má preukázateľnú kontrolu nad webovým sídlom, na ktoré je KC vyhotovený. Uplatňujú sa všetky podmienky z častí 3.1.7 a 3.1.8 tohto dokumentu a zároveň ďalšie podmienky, ktoré sú uvedené v tejto časti.

Táto FO 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 FO.

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 FO v súlade s požiadavkami z časti 3.1.8,
- alebo overenie identity PO, ktorej patrí daný komponent/systém, v súlade s požiadavkami z časti 3.1.7,
- overenie oprávnenosti použitia údajov, ktoré majú byť uvedené v jednotlivých položkách KC, s dôrazom na obsah položky *commonName (CN)*.

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 PO, obchodnú značku, obchodné meno, adresu, lokalitu, alebo iný text poukazujúci na určiteľnú FO alebo PO, 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.)

3.1.10 Autentizácia identity u zmluvných partnerov

Autentizácia identity FO resp. komponentu u zmluvných partnerov Poskytovateľa (obchodní partneri), sa vykonáva v spolupráci so zodpovednými osobami tejto spoločnosti.

Niektoré postupy sú v tomto prípade zjednodušené a nemusia sa vykonávať napr. overovanie vlastníctva domény, overovanie kontroly e-mail konta a podobne.

3.1.11 Predkladané doklady

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

Ak má pracovník RA pochybnosti o totožnosti potenciálneho zákazníka (napr. zjavný nesúlad medzi fotografiou v predloženom osobnom doklade a vzhľadom zákazníka, rozpor medzi dvomi predloženými dokladmi a podobne), môže odmietnuť jeho registráciu.

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

Na žiadosť potencionálneho zákazníka alebo RA sa prípadné sporné prípady pri preukazovaní totožnosti riešia postupom podľa časti 2.4.

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

Fyzická osoba

FO predkladá dva doklady identifikujúce jej totožnosť.

Primárnym dokladom je u:

- občana SR - platný občiansky preukaz resp. cestovný pas
- cudzieho štátneho príslušníka – preukaz totožnosti, t. j. identifikačná karta, povolenie na pobyt na území SR, resp. cestovný pas alebo cudzinecká kartička.

Sekundárnym dokladom môže byť:

- cestovný pas
- vodičský preukaz
- preukaz poistenca zdravotného poistenia
- rodný list

- osobný preukaz vojaka z povolania alebo vojenská knižka
- povolenie na prechodný pobyt (resp. trvalý pobyt) v prípade cudzinca
- zbrojný preukaz vydaný príslušným policajným útvarom
- služobný preukaz
- iné...

Požaduje sa pritom, aby aspoň jeden z predkladaných dokladov bol dokladom, ktorého súčasťou je fotografia danej osoby (fotka s podobizňou tváre).

V prípade žiadosti o vydanie certifikátu pre potreby zmluvného partnera alebo žiadosti o jeho zrušenie postačuje, aby daná FO preukázala svoju totožnosť jedným z nasledovných osobných dokladov – občiansky preukaz resp. cestovný pas. Žiadateľ o certifikát vydávaný pre potreby zmluvného partnera musí splniť aj ďalšie podmienky pre vydanie certifikátu tohto typu, ktoré si stanoví zmluvný partner.

Ak FO zastupuje na RA inú FO, musí sa navyše preukázať úradne overenou (notárom) plnou mocou, z textu ktorej je jednoznačne jasné, že zastupujúca FO bola splnomocnená splnomocňujúcou FO konať v danej veci v jej mene.

Pokiaľ je žiadateľom o certifikát zákonný zástupca (spravidla rodič), musí navyše predložiť rodný list dieťaťa, osvojiteľ musí navyše predložiť rozhodnutie zo súdu alebo výpis z matriky. Postačujúcim dokladom je aj občiansky preukaz, v ktorom je dieťa zapísané.

Fyzická osoba – zamestnanec

Pokiaľ je žiadateľom o certifikát FO, ktorá má v žiadosti uvedený aj názov organizácie, predkladá doklady podľa predošlej kapitoly (*Fyzická osoba*). Zároveň musí predložiť súhlas s vydaním certifikátu od zamestnávateľa, napríklad predložením splnomocnenia na daný úkon. Pokiaľ je žiadateľom zamestnanec zmluvného partnera táto požiadavka je nahradená súhlasom na vydanie zo strany zmluvne stanovenej kontaktnej osoby.

Právnická osoba

V tomto prípade žiadateľ o certifikát predkladá doklady uvedené v kapitole *Právnická osoba*. Súčasne musí predložiť doklady podľa časti 3.1.7.

Pokiaľ za PO konajú viaceré osoby spoločne, je potrebné predložiť úradne overenú (notárom) plnú moc, z textu ktorej je jednoznačne jasné, že zastupujúca FO bola splnomocnená splnomocňujúcimi FO konať v danej veci v ich mene.

Zariadenia alebo systém

Viď ustanovenia v časti 3.1.9 tohto dokumentu.

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

Ak má pracovník RA pochybnosti o totožnosti potenciálneho zákazníka (napr. zjavný nesúlad medzi fotografiou v predloženom osobnom doklade a vzhľadom zákazníka, rozpor medzi dvomi predloženými dokladmi a podobne), môže odmietnuť jeho registráciu.

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

Na žiadosť potenciálneho zákazníka alebo RA sa prípadné sporné prípady pri preukazovaní totožnosti riešia postupom podľa časti 2.4 tohto dokumentu.

Pri predkladaní dokladov sa vyžaduje, aby na pobočke RA boli predložené originály týchto dokladov slúžiace k nahliadnutiu alebo úradne overené kópie originálov, okrem osobných dokladov identifikujúcich totožnosť žiadateľa resp. splnomocnenej osoby. Pre potreby archivácie týchto dokladov pre NFQES CA, je vhodné predložiť kópie týchto dokladov, ktoré už však nemusia byť úradne overené. Preloženie výpisu z obchodného registra resp. živnostenského registra získaného z Internetu, zo strany žiadateľa, nie je postačujúce, nakoľko tento má len informatívny charakter a nie je použiteľný na právne úkony.

3.1.12 Kontrola údajov na predložených dokladoch

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

Osobné doklady FO:

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

Výpisy z obchodného registra:

- či výpis nie je starší ako 3 mesiace
- či obsahujú FO (stačí jedna FO, ak na výpise nie je uvedené inak), ktoré predložili daný výpis, právo konať (podpisovať) za danú PO (t.j. či sú jej štatutárnymi zástupcami)
- či je výpis úradne overený (notárom alebo matrikou), ak sa nejedná o originál alebo nie je poskytnutý z portálu slovensko.sk

Plné moci:

- či je plná moc úradne overená (notárom alebo matrikou)
- či sa údaje, uvedené v plnej moci, ktoré definujú zastupujúcu FO resp. PO, zhodujú s údajmi uvedenými na osobných dokladoch zastupujúcej FO resp. s údajmi uvedenými na výpise z obchodného registra zastupujúcej PO

- rozsah plnej moci - t.j. či plná moc oprávňuje splnomocnenú FO alebo PO k požadovanému úkonu na RA v mene splnomocňujúcej FO alebo PO
- či plná moc nie je časovo obmedzená alebo ak obsahuje inú podmienku, či je táto splnená

Čestné prehlásenia:

- oprávnenie na podpis – či osoba podpisujúca prehlásenie je oprávnená zastupovať PO. Oprávnenosť sa kontroluje podľa výpisu z ORSR resp. iného registra právnických osôb. Pokiaľ podpisujúca osoba nie je zapísaná v tomto výpise, musí predložiť iný doklad, na základe ktorého môže konať za spoločnosť (spravidla notárom overená plná moc)

Druh predložených dokladov (napr. občiansky preukaz, cestovný pas) a príslušné údaje z nich zaznamená pracovník RA elektronicky do IS Poskytovateľa.

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

Pracovník RA musí akceptovať aj dokumenty predkladané žiadateľom v elektronickej podobe podpísané platným KEP (výpis z ORSR, plná moc, prehlásenie, poverenie atď.)

3.1.13 Prvotná registrácia RA

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

3.2 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 IS Poskytovateľa.

Podmienky vydania následného certifikátu sú podrobne popísané v CP NFQES CA v časti 4.7, prípadne CP NFQES ACA.

RA vykoná vydanie certifikátu bez osobnej návštevy Držiteľa len v prípade osobného certifikátu resp. systémového certifikátu pre PO po splnení podmienok uvedených v časti 3.2 aktuálneho CP NFQES CA, prípadne CP NFQES ACA.

3.3 Vydanie následného certifikátu po zrušení starého

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

3.4 Žiadosť o zrušenie certifikátu

Žiadosť o zrušenie certifikátu musí byť autentizovaná, pozri časť 4.4 tohto dokumentu. Žiadosť o zrušenie certifikátu môže byť autentizovaná použitím súkromného kľúča patriaceho k certifikátu bez ohľadu na to, či daný súkromný kľúč bol alebo nebol kompromitovaný.

4 Prevádzkové požiadavky

4.1 Žiadanie o certifikát

Keď žiadateľ o certifikát požiada o certifikát, žiadateľ a RA musia vykonať nasledovné kroky:

- RA musí overiť a zaznamenať identitu žiadateľa (podľa ustanovení v časti 3.1), ako aj overiť všetky ostatné údaje, ktoré sú v certifikáte, za použitia nezávislých zdrojov a alternatívnych komunikačných kanálov,
- žiadateľ musí preukázať, že verejný kľúč tvorí kľúčový pár so súkromným kľúčom vlastneným žiadateľom o certifikát (podľa ustanovení v časti 3.1.6),
- žiadateľ musí poskytnúť dostatočné podklady na overenie ľubovoľných identifikačných údajov, ktoré majú byť obsahom certifikátu.

Všetka komunikácia medzi jednotlivými zložkami CA týkajúca sa žiadosti o certifikát a procesu vydania certifikátu má byť autentizovaná a chránená pred modifikáciou pomocou mechanizmov primeraných požiadavkám dát, ktoré sa majú chrániť použitím predtým vydaných certifikátov.

4.1.1 Kto môže požiadať o certifikát

Poskytovateľa môže požiadať o vydanie:

- KC pre elektronický podpis
  - FO resp. FO 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 legislatívy SR má oprávnenia konať v mene danej PO
- KC pre autentifikáciu webového sídla
  - FO alebo PO prevádzkujúca zariadenie resp. systém
- mandátny certifikát
  - FO oprávnená zo zákona alebo na základe zákona konať za inú osobu alebo OVM alebo v ich mene resp. alebo FO, 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 FO spojená napr. jej zamestnávateľ, nezisková organizácia, ktorej je členom a podobne.

4.1.2 Postup pre získanie certifikátu

Zákazník musí vykonať nasledovné kroky ako prípravu pred návštevou Poskytovateľa, prípadne RA Poskytovateľa:

- oboznámiť sa so Všeobecnými podmienkami Poskytovateľa a Pravidlami ochrany pri spracúvaní osobných údajov, ktoré sú dostupné na webovom sídle Poskytovateľa,
- oboznámiť sa s príslušnými CP Poskytovateľa (CP NFQES CA, CP NFQES ACA) a týmto dokumentom, prípadne s princípmi a návodmi na získanie KC,

- pripraviť si hodnoty jednotlivých položiek v žiadosti o KC tak, aby tieto hodnoty boli v súlade s týmto dokumentom a príslušnými CP Poskytovateľa,
- 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 OVM), podľa zoznamu oprávnení zverejnenom na webovom sídle NBÚ,
- v prípade fyzickej registrácie pomocou externej RA alebo priamo na CA, dohodnúť si termín návštevy osobného stretnutia.

Postup pred vydaním KC:

Pred vydaním KC zamestnanec zastupujúci Poskytovateľa, prípadne RA musí:

- informovať prítomnú FO o Všeobecných podmienkach a Podmienkach spracovania osobných údajov
- overiť totožnosť Držiteľa/Zákazníka prípadne osoby, ktorá ho zastupuje podľa predložených dokladov a zaznamenať všetky povinné osobné údaje do IS Poskytovateľa,
- vytvoriť fotokópie predložených dokladov totožnosti,
- overiť všetky ďalšie predložené doklady podľa stanovených postupov.

4.2 Vydanie certifikátu

Poskytovateľ nevytvorí KC, kým sa k spokojnosti NFQES CA nedokončia všetky verifikácie a prípadné zmeny, ak sú potrebné. Poskytovateľ nezodpovedá za prípadné dodatočné náklady Žiadateľa o certifikát, ktoré vzniknú v priebehu registrácie, napr. kvôli potrebe opakovanej návštevy externej RA napr. v dôsledku neúplných alebo chýbajúcich dokladov alebo iných nedostatkov.

Hoci Žiadateľ pripravuje väčšinu dátových položiek KC, na externej RA zostáva zodpovednosť overiť, že informácie sú správne. Za preverenie údajov Žiadateľa zodpovedá externá RA.

Poskytovateľ má právo nevytvoriť KC, hoci žiadateľ o KC úspešne prešiel procesom registrácie na RA, ak sa dodatočne zistí závažná skutočnosť, ktorá bráni vydaniu KC (napr. chyba vo formáte žiadosti o certifikát).

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

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

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

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.

4.2.1 Doručenie súkromného kľúča držiteľovi certifikátu

Platia ustanovenia definované v CP NFQES CA, CP NFQES ACA.

4.2.2 Doručenie verejného kľúča CA používateľom

CMA a strany spoliehajúce sa na certifikáty musia konať v súčinnosti, aby sa zaručilo autentizované doručenie certifikátu CA NFQES.

Prijateľné metódy na doručenie certifikátu NFQES CA, prípadne NFQES ACA a jeho autentizovanie sú:

- nahranie certifikátu z IS NFQES CA,
- osobné prevzatie certifikátu na externej RA alebo priamo na CA,
- sprístupnenie používania vzdialeného certifikátu v IS Poskytovateľa v prípade vzdialeného certifikátu.

4.3 Prevzatie certifikátu

Certifikáty sa vytvárajú a vydávajú automatizovane a priebežne, Žiadateľ bude spravidla môcť prevziať vydaný certifikát v priebehu tej istej návštevy externej RA, kedy podal žiadosť o daný certifikát. Bezprostredne po vydaní certifikátu bude môcť žiadateľ o certifikát prevziať svoj certifikát.

Žiadateľ o certifikát sa pri preberaní svojho certifikátu môže dať zastupovať na externej RA inou FO alebo PO za rovnakých podmienok ako pri podávaní žiadosti o certifikát (pozri časti 3.1.7 alebo 3.1.8 tohto dokumentu). Prevzatie certifikátu sa štandardne uskutoční na tej istej RA, kde bola podaná žiadosť o daný certifikát.

Oznam o vydaní certifikátu bude zaslaný na emailovú adresu uvedenú v certifikáte, prípadne telefonicky alebo notifikáciou v IS Poskytovateľa a odovzdaný Držiteľovi certifikátu alebo subjektu, ktorý ho zastupuje, spolu s certifikátom NFQES CA.

4.4 Suspendovanie certifikátu a zrušenie certifikátu

4.4.1 Zrušenie certifikátu

Okolnosti zrušenia certifikátu

Certifikát sa musí zrušiť, keď sa väzba medzi subjektom a jeho verejným kľúčom definovaným v certifikáte už nepovažuje za platnú. Príklady okolností, ktoré rušia túto väzbu, sú:

- Držiteľ certifikátu alebo iná oprávnená strana požiada o zrušenie certifikátu,
- je podozrenie, že bol kompromitovaný súkromný kľúč (zodpovedajúci verejnému kľúču v certifikáte), alebo certifikát bol iným spôsobom zneužitý
- ukázalo sa, že Držiteľ certifikátu nedodržuje svoje povinnosti Držiteľa certifikátu, ktoré ho zmluvne viažu,
- identifikačné informácie alebo pričlenené prvky ľubovoľných mien v certifikáte sa stanú neplatnými,

- je podozrenie, že certifikát nebol vydaný v súlade s platnými CP Poskytovateľa a týmito pravidlami resp. zodpovedajúcimi CPS pre RA a CA,
- zistilo sa, že niektorá z informácií uvedených v certifikáte je chybná alebo nesprávna,
- Poskytovateľ ukončí z akéhokoľvek dôvodu svoju činnosť a zmluvne nezaisti u inej CA, aby poskytovala informácie o zrušených certifikátoch v mene Poskytovateľa,
- skončili okolnosti, ktoré vyžadovali vydanie certifikátu (testovanie, overovanie aplikácií atď.),
- došlo ku strate súkromného kľúča,
- technické parametre alebo formát certifikátu by mohli viesť k neakceptovateľnému riziku z pohľadu dodávateľov softvéru alebo spoliehajúcich sa strán (zmena kryptografických algoritmov na podpisovanie, dĺžka kryptografických kľúčov atď.),
- smrť Držiteľa certifikátu,
- došlo ku kompromitácii súkromného kľúča Poskytovateľa,
- právoplatný rozsudok alebo predbežné opatrenie súdu.

Vždy, keď sa CA dozvie o niektorej z vyššie uvedených okolností, daný certifikát sa zruší a vloží sa do CRL. Zrušené certifikáty sa vyskytujú vo všetkých nových vydaniach CRL, minimálne dovtedy, kým dané certifikáty nestratia platnosť.

Subjekty ktoré môžu požiadať o zrušenie certifikátu

Držiteľ certifikátu (alebo ním poverená FO alebo PO) môže kedykoľvek požiadať spôsobom stanoveným týmto dokumentom a Všeobecnými podmienkami o zrušenie svojho vlastného certifikátu a to aj bez udania dôvodu žiadosti o zrušenie certifikátu.

RA dá NFQES CA návrh na zrušenie certifikátu daného Držiteľa, ak sa dozvie, že nastala niektorá z okolností uvedených vyššie.

Ak bol certifikát vydaný na zamestnanca zmluvného partnera, v príslušnej zmluve je možné dohodnúť, kto okrem Držiteľa certifikátu má právo požiadať o jeho zrušenie, akým spôsobom a za akých okolností.

O zrušenie certifikátu môže tiež požiadať:

- CMA - daný zamestnanec je povinný zdokumentovať túto skutočnosť vrátane dôvodu svojho konania,
- subjekt (FO alebo PO) na základe dedičského konania (k dokumentom o zrušení certifikátu musí Poskytovateľ priložiť kópiu dokladov, z ktorých vyplýva právo daného subjektu žiadať o zrušenie certifikátu),
- súd prostredníctvom svojho rozsudku alebo predbežného opatrenia (k dokumentom o zrušení certifikátu musí Poskytovateľ priložiť kópiu príslušného súdneho rozhodnutia),
- súdom poverená osoba (k dokumentom o zrušení certifikátu musí Poskytovateľ priložiť kópiu príslušného súdneho rozhodnutia).
- OVM 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.

V prípade certifikátu RA môže o zrušenie certifikátu okrem jeho Držiteľa (danej RA) požiadať tiež PMA, ak sa zistí závažná okolnosť (pozri časť *Okolnosti zrušenia certifikátu*) na zrušenie daného certifikátu.

Postup pri žiadosti o zrušenie certifikátu

Žiadosť o zrušenie certifikátu je možné podať elektronicky s využitím IS Poskytovateľa alebo priamo na CA. Zrušenie certifikátu sa musí autentizovať pomocou 2FA v IS Poskytovateľa, v prípade osobnej návštevy na CA/RA sa predložia identifikačné doklady (OP, pas, iné...). RA musí po zrušení certifikátu informovať Držiteľa o jeho zrušení.

Žiadosť o zrušenie certifikátu je možné aj podaním oprávnenej osoby osobne na RA prípadne priamo na CA prostredníctvom rovnakého procesu autentizácie, aký je požadovaný pri prvotnej registrácii Držiteľa/Zákazníka.

Aby sa predišlo svojvoľnému zrušeniu certifikátu neautorizovanou stranou je dôležitá autentizácia požiadavky na zrušenie certifikátu. Držiteľa/Zákazníka môže na RA vo veci zrušenia certifikátu zastupovať poverená/splnomocnená osoba. Zastupujúca osoba sa musí preukázať úradne overeným splnomocnením resp. poverením, v texte ktorého je jednoznačne vyjadrená vôľa Držiteľa/Zákazníka certifikát zrušiť.

RA môže odmietnuť žiadosť o zrušenie certifikátu, ak Držiteľ/Zákazník nesplní podmienky autentizácie svojej identity. Pracovník RA musí preveriť platnosť certifikátu, ktorý sa má zrušiť. RA poskytne v prípade potreby Žiadateľovi o zrušenie pomoc pri zistení čísla (serial number) predmetného certifikátu, aby bolo možné jednoznačne identifikovať certifikát, 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 certifikátu a úspešnom overení identity Držiteľa/Zákazníka sa musí certifikát čo najskôr zrušiť.

Čas na zrušenie certifikátu

CA musí:

- zrušiť certifikát najneskôr do 24 hodín od overenia skutočností, že predmetná žiadosť o zrušenie certifikátu je oprávnená,
- zverejňovať aktuálny CRL a všetky predchádzajúce zoznamy zrušených certifikátov, tak aby boli prístupné Zákazníkom/Držiteľom a všetkým spoliehajúcim sa stranám,
- informovať Zákazníka/Držiteľa certifikátu o zrušení jeho certifikátu, zaslaním e-mailu na e-mailovú adresu, ktorú poskytol Držiteľ v priebehu registrácie na RA, pričom musí uviesť aj informáciu o dôvode zrušenia daného certifikátu,
- 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.

4.4.2 Suspendovanie certifikátu

Poskytovateľ nepodporuje dočasné pozastavenie platnosti *(suspendovanie)* certifikátu.

4.4.3 Zoznam zrušených certifikátov

Frekvencia vydávania CRL

Informácie o zrušenom KC musia byť dostupné na webovom sídle Poskytovateľa, 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.

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

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

Požiadavky na overovanie CRL

Ak dočasne nie je možné získať informácie o zrušených certifikátoch, potom strana spoliehajúca sa na certifikáty musí buď odmietnuť použitie certifikátu alebo urobiť kvalifikované rozhodnutie, ktorým akceptuje riziko, zodpovednosť a dôsledky použitia certifikátu, ktorého autenticita nemôže byť zaručená podľa štandardov tohto dokumentu. Takéto použitie certifikátu môže byť príležitostne nevyhnutné, aby sa vyhovelo urgentným operačným požiadavkám.

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

4.4.4 Overenie aktuálneho stavu certifikátu

Overenie aktuálneho stavu certifikátu sa robí prostredníctvom aktuálneho CRL publikovaného Poskytovateľom.

Overenie aktuálneho stavu certifikátu je možné vykonať manuálne prostredníctvom:

- Zoznamov aktuálnych CRL, ako aj archívu všetkých vydaných CRL pre jednotlivé CA Poskytovateľa, ktoré sú k dispozícii na adrese: https://ocsp.nfqes.com/crl/
- Poskytovateľ musí zabezpečiť odpoveď na telefonický alebo emailom zaslaný alebo pomocou helpdesku Poskytovateľa prijatý dopyt týkajúci sa stavu konkrétneho certifikátu
- Pomocou požiadavky na príslušný OCSP responder, ktorého URI adresy OSCP responderov jednotlivých vydávajúcich CA Poskytovateľa sú obsiahnuté v rozšírení certifikátu (zaslaná žiadosť je v súlade s požiadavkami RFC 6960)

4.4.5 Iné použiteľné spôsoby oznamovania o zrušení certifikátu

RA odpovie na dopyt týkajúci sa stavu konkrétneho certifikátu, ak bol tento dopyt vykonaný telefonicky alebo emailom alebo pomocou helpdesku Poskytovateľa, v prípade, že externá RA má prístup k helpdesku (v prípade, že externá RA nemá prístup k helpdesku, odpovedá iba na telefonické a e-mailom zaslané dopyty).

4.5 Audit bezpečnosti

4.5.1 Typy zaznamenávaných udalostí

Zaznamenávajú sa všetky udalosti na RA a tiež interakcie Žiadateľov o certifikát a Držiteľov certifikátov s RA. Záznamy môžu byť buď v elektronickej alebo v písomnej forme.

Prezeranie záznamov sa umožní jednotlivým zložkám CMA v rozsahu týkajúcom sa nimi vykonávaných činností, v celom rozsahu PMA a osobám vykonávajúcim audit zhody. Záznamy sa pravidelne archivujú po dobu viď kapitola 4.6.

Každé pracovisko RA musí viesť záznamy o činnosti daného pracoviska RA prostredníctvom záznamov v písomnej alebo elektronickej forme.

Vytvárané záznamy predstavujú prijatie žiadosti o zrušenie certifikátu a odovzdanie certifikátu. Okrem týchto sa zaznamenávajú všetky ostatné udalosti na RA - hlavne udalosti týkajúce sa overenia identity žiadateľa, súkromného kľúča RA (jeho kompromitácia, prijatie alebo strata čipovej karty, zabudnutie hesla), bezpečnosti pracoviska RA, prijatie (a spôsob vybavenia) podnetu, pripomienky alebo žiadosti o výklad CP a CPS, odmietnuté žiadosti o certifikát, došlé požiadavky, sťažnosti a pod. a ich vybavenie, požiadavky na zaslanie CRL a certifikátu Poskytovateľa. Zaznamenáva sa tiež vykonanie kontroly alebo audity na danej RA.

RA môže vykonať ľubovoľný zápis týkajúci sa Poskytovateľa, ktorý považuje za potrebný alebo užitočný. Pracovisko RA uchováva všetku e-mailovú korešpondenciu týkajúcu sa Poskytovateľa s inými zložkami aj externým prostredím (zákazníci, záujemca o služby a podobne). Pracovisko RA uchováva tiež všetku svoju písomnú korešpondenciu týkajúcu sa Poskytovateľa.

4.6 Archívne záznamy

Archivácia záznamov sa vykonáva v pravidelných intervaloch, aby sa zabezpečilo dlhodobé uloženie záznamov v zmysle bezpečnostných požiadaviek. Prezeranie archivovaných záznamov je umožnené v celom rozsahu PMA a osobám vykonávajúcim audit zhody. Modifikovanie alebo odstraňovanie archivovaných informácií nie je prípustné.

Poskytovateľ musí uchovávať všetky záznamy o vydaných KC ako aj samotné KC v zmysle požiadaviek aktuálne platnej legislatívy SR. Poskytovateľ musí uchovávať originály (alebo aspoň kópie) žiadosti o vydanie certifikátov spolu s príslušnými dokumentami potvrdzujúcimi totožnosť Držiteľa v papierovej resp. elektronickej podobe po dobu najmenej 10 rokov.

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, fotokópia identifikačných dokladov a pod.).

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

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

4.7 Zmena kľúča

Celý proces zmeny kľúča 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 (NBÚ) (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. Poskytovateľ musí upozorniť prostredníctvom svojho webového sídla alebo e-mailom alebo telefonicky všetkých 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.

4.8 Havarijný plán pre mimoriadne udalosti

V prípade kompromitácie kľúča koreňovej CA Poskytovateľa resp. podriadených CA sa tieto zrušia. Informácia o ich zrušení sa musí publikovať okamžite najrýchlejším možným spôsobom.

Poskytovateľ upozorní všetkých Držiteľov certifikátov, ktoré boli podpísané zrušeným certifikátom Poskytovateľa ako aj strany spoliehajúce sa na dané certifikáty, že zrušený certifikát Poskytovateľa sa má odstrániť z každej aplikácie, ktorú používajú strany spoliehajúce sa na certifikáty a má byť nahradený novým certifikátom Poskytovateľa. Tento sa musí distribuovať spoľahlivým spôsobom.

V prípade havárie, pri ktorej je vybavenie Poskytovateľa poškodené a neschopné prevádzky, ale nie je zničený jej podpisový kľúč, je potrebné obnoviť funkčnosť CA, podľa možnosti čo najrýchlejšie, pričom treba dať prioritu schopnosti rušiť certifikáty a zverejňovať aktuálne CRL. V prípade havárie, pri ktorej je inštalácia CA fyzicky poškodená a jej podpisový kľúč je v dôsledku toho zničený, certifikát Poskytovateľa sa zruší. Potom sa kompletne zopakuje inštalácia CA s obnovením vybavenia CA, vygenerovaním nových kľúčov Poskytovateľa,

vytvorením nového certifikátu CA a nových certifikátov RA. Nakoniec sa nanovo vydajú všetky používateľské certifikáty za použitia nového certifikátu Poskytovateľa. Náklady na vytvorenie nových certifikátov subjektom, ktoré boli dotknuté vytvorením nového certifikátu, nesie v takomto prípade Poskytovateľ.

Strany spoliehajúce sa na certifikáty môžu na vlastné riziko urobiť rozhodnutie pokračovať v používaní certifikátov podpísaných použitím zničeného súkromného kľúča, aby sa splnili ich urgentné operačné požiadavky. V prípade straty alebo poškodenia čipovej karty, na ktorej je uložený certifikát externej RA alebo v prípade zabudnutia hesla na prístup ku súkromnému kľúču uloženému na danej čipovej karte alebo v prípade nefunkčnosti čítačky čipových kariet je externá RA povinná na nevyhnutnú mieru obmedziť alebo pozastaviť výkon svojej činnosti a udalosť okamžite oznámiť PMA. V prípade vzdialeného certifikátu RA platia rovnaké povinnosti ako sú spomenuté vyššie v texte.

Fungovanie externej RA sa obnoví tak, že sa certifikát RA zruší a vytvorí sa nový certifikát RA. O tomto sa urýchlene oboznámia všetky zložky Poskytovateľa a zabezpečí im doručenie nového certifikátu danej RA vhodným spôsobom.

Detailný popis fyzických bezpečnostných opatrení je uverejnený v aktuálne platných CP Poskytovateľa, a to CP NFQES CA a CP NFQES ACA.

4.9 Ukončenie činnosti CA alebo RA

Pri ukončení činnosti Poskytovateľa alebo RA z iných dôvodov ako sú udalosti spôsobené vyššou mocou (napr. prírodná katastrofa, vojnový stav, rozhodnutie štátnej moci a pod.) sa postupuje v súlade s ustanoveniami v časti 4.8.

Poskytovateľ vhodným spôsobom sprístupní informácie o ukončení svojej činnosti Držiteľom všetkých ňou vydaných platných certifikátov a stranám spoliehajúcim sa na certifikáty.

Vhodným spôsobom sa rozumie odoslanie informácie pomocou:

- hromadného e-mailu cez IS Poskytovateľa,
- notifikácie Držiteľov certifikátov v IS Poskytovateľa,
- telefonického rozhovoru s Držiteľmi certifikátov,
- distribúcie tejto informácie cez webové sídlo Poskytovateľa.

Po ukončení svojej činnosti Poskytovateľ nevydá žiaden certifikát a zabezpečí preukázateľné zničenie podpisových dát (súkromného kľúča). Ak je dôvodom ukončenia činnosti Poskytovateľa nejaký dôvod bez vzťahu k bezpečnosti, potom ani certifikát CA, ktorá končí činnosť, ani certifikáty podpísané touto CA nemusia byť zrušené.

Pred ukončením svojej činnosti RA poskytne archivované dáta zložke Poskytovateľa podľa pokynu PMA.

Ešte pred ukončením poskytovania služieb Poskytovateľ musí:

- vhodným spôsobom (viď. vyššie definovaný vhodný spôsob), minimálne 6 mesiacov vopred, oznámiť plánované ukončenie svojej činnosti orgánu dohľadu (NBÚ), 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,
- vyradiť z používania všetky súkromné kľúče, vrátane ich kópií takým spôsobom, že nebude možné ich žiadnym spôsobom obnoviť.

5 Fyzické, procedurálne a personálne bezpečnostné opatrenia

Bezpečnosť Poskytovateľa ako aj externej RA 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. Bezpečnostné opatrenia musia byť k dispozícii všetkým pracovníkom, ktorých sa týkajú.

Poskytovateľ a externá RA 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 externej RA a súhrn aktív týkajúci sa bezpečnosti musia byť preskúmavané v pravidelných intervaloch.

Bezpečnostná politika Poskytovateľa a externej RA a súhrn aktív týkajúci sa bezpečnosti musia byť preskúmavané v prípade významných zmien na zaistenie ich kontinuity, vhodnosti, dostatočnosti a účinnosti.

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

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

5.1 Fyzické bezpečnostné opatrenia

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

Detailný popis fyzických bezpečnostných opatrení je uverený v aktuálne platných CP NFQES CA, pripadne CP NFQES ACA.

5.2 Procedurálne bezpečnostné opatrenia

Osoby vybrané na zastávanie zodpovedných roly RA musia byť zodpovedné a dôveryhodné. Funkcie vykonávané touto rolou patria k funkciám, ktoré formujú v personálnej rovine základ dôvery v celú NFQES CA a NFQES ACA.

Každá RA, ktorá funguje podľa tohto dokumentu, je predmetom jeho ustanovení. Zodpovednosťou RA je v prvom rade:

- overovanie identity prostredníctvom osobného kontaktu alebo prostredníctvom zastupujúceho subjektu,
- zaznamenávanie informácií od Žiadateľov o certifikát a overovanie ich správnosti,
- bezpečná komunikácia s Poskytovateľom,
- distribuovanie SSL certifikátov prijatých od Poskytovateľa,

- komunikácia so Žiadateľmi o certifikát a Držiteľmi certifikátov a dokumentovanie tejto komunikácie.

Osoba spravujúca daný komponent zastáva rolu Žiadateľa o certifikát a Držiteľa certifikátu v prípade hardvérových alebo softvérových komponentov (t.j. neživých systémov), pre ktoré sa vydáva certifikát. Osoba spravujúca daný komponent koná v súčinnosti s CMA pri registrovaní komponentov (routre, firewally atď.) v súlade s časťou 3.1.9 a zodpovedá za plnenie povinností Držiteľov certifikátov ako sú definované v tomto dokumente.

Detailný popis procedurálnych bezpečnostných opatrení je uverejnený v aktuálne platných CP NFQES CA, prípadne CP NFQES ACA.

5.3 Personálne bezpečnostné opatrenia

Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami subjektu – zriaďovateľa. Personál pre ľubovoľnú rolu sa musí vyberať na základe spoľahlivosti, lojality a dôveryhodnosti. Všetky osoby zastávajúce zodpovedné roli RA musia byť náležite poučené a zaškolené. Témy majú obsahovať fungovanie softvéru a hardvéru používaného externou RA ako aj CA, prevádzkové a bezpečnostné procedúry, ustanovenia tohto dokumentu ako aj CP NFQES CA, prípadne CP NFQES ACA.

Detailný popis personálnych bezpečnostných opatrení je uverejnený v aktuálne platných CP NFQES CA, prípadne CP NFQES ACA.

6 Technické bezpečnostné opatrenia

6.1 Generovanie páru kľúčov a inštalácia

6.1.1 Generovanie kľúčového páru

Tieto pravidlá nevylučujú žiadny zdroj kľúčov, ktoré boli vygenerované v súlade s ustanoveniami týchto pravidiel a lokálnymi bezpečnostnými požiadavkami. Predpokladá sa, že súkromný kľúč bude vygenerovaný subjektom, ktorý sa stane jeho vlastníkom: napr. žiadateľom o certifikát alebo RA a na zariadení (napr. počítač, čipová karta alebo iný token, HSM modul a pod.), ktoré je počas generovania kľúča pod bezprostrednou kontrolou subjektu, ktorý sa stane vlastníkom generovaného kľúča, prípadne na zariadeniach Poskytovateľa (vzdialený certifikát).

Súkromný kľúč sa nesmie dostať von z bezpečnostného (HSM) modulu, v ktorom bol vygenerovaný, s výnimkou, že je zašifrovaný kvôli jeho lokálnemu prenosu alebo spracovaniu alebo úschove.

Dôležitým bezpečnostným aspektom, ktorý podstatným spôsobom obmedzuje možnosť zneužitia privátneho kľúča patriaceho externej RA, je to, že daný pár kľúčov externej RA bude generovaný a uložený na čipovej karte, prípadne v zariadeniach Poskytovateľa (vzdialený certifikát). Proces generovania páru kľúčov na čipovú kartu sa iniciuje prostredníctvom pripojenia sa na web Poskytovateľa vhodným prehliadačom, otvorenia stránky, cez ktorú sa generuje žiadosť o osobný certifikát (https://zone.nfqes.com) a príslušnej voľby typu kľúča. V prípade vzdialeného certifikátu si RA vygeneruje CSR, ktoré odošle na podpis Poskytovateľovi, ktorý prijaté CSR podpíše privátnym kľúčom a vygeneruje certifikát pre RA. Generovanie kľúčov je vykonávané v bezpečnom zariadení na uchovávanie kryptografických kľúčov, ktoré spĺňa legislatívne požiadavky dané na takýto typ zariadenia (HSM).

6.1.2 Doručenie súkromného kľúča držiteľovi certifikátu

Žiadne ustanovenia.

6.1.3 Dĺžka kľúčov

Algoritmy a dĺžky kľúčového páru uplatňované v certifikátoch majú definované minimálne dĺžky kľúčov pre všetky typy entít a všetky používané algoritmy.

Algoritmy a dĺžky kľúčov uplatňované v certifikátoch NFQES CA:

Algoritmus podpisu: *sha256RSA*

Verejný kľúč: RSA 3072 bitov alebo RSA 4096 bitov

Algoritmy a dĺžky kľúčov uplatňované v certifikáte koreňovej NFQES CA:

Algoritmus podpisu: *sha256RSA*

Verejný kľúč: RSA 4096 bitov

Algoritmy a dĺžky kľúčov uplatňované v certifikáte podriadených NFQES CA:

Algoritmus podpisu: *sha256RSA*

Verejný kľúč: RSA 4096 bitov

6.2 Ochrana súkromného kľúča

Držiteľ certifikátu musí zabezpečiť, aby sa jeho súkromný kľúč nikdy nedostal v nezašifrovanej forme mimo bezpečnostný modul, kde je uložený. Základným princípom je, že nikto nemá mať prístup k súkromnému kľúču okrem jeho Držiteľa. Poskytovateľ využíva na ochranu súkromných kľúčov svojich vydávajúcich CA hardvérové kryptografické moduly.

Držiteľom kľúčov je dovolené zálohovať ich vlastné páry kľúčov. Počas zálohovania a prenosu musia byť kľúče zašifrované. Držiteľ kľúča zodpovedá za garanciu, že všetky kópie súkromných kľúčov sú chránené, vrátane ochrany všetkých pracovných staníc, na ktorých sa nachádza ľubovoľný z jeho súkromných kľúčov. V prípade vzdialených certifikátov a kľúčových párov, Držiteľ nemôže zálohovať svoje kľúčové páry.

Pass-frázy, PINy, biometrické dáta alebo iné mechanizmy ekvivalentnej autentizačnej robustnosti sa musia použiť na ochranu prístupu k použitiu súkromného kľúča. Kryptografické moduly, ktoré sa aktivovali, nesmú byť ponechané bez dozoru alebo inak otvorené pre neautorizovaný prístup. Hardvérové kryptografické moduly sa musia vyňať a uschovať, keď sa nepoužívajú.

Ak sa aktivačné dáta zapíšu, majú byť zabezpečené na úrovni ochrany dát, na ochranu ktorých sa používa daný kryptografický modul a nemali by byť uložené spolu s ním. Aktivačné dáta pre súkromné kľúče patriace k certifikátom potvrdzujúcim individuálnu identitu nemajú byť nikdy využívané spoločne viacerými osobami. Aktivačné dáta pre súkromné kľúče patriace k certifikátom potvrdzujúcim identitu organizácie resp. jej organizačnej zložky majú byť známe len tým osobám, ktoré sú v organizácii autorizované na použitie daných súkromných kľúčov.

Súkromný kľúč RA uložený na čipovej karte sa nikdy nedostane mimo čipovú kartu, na ktorej bol vygenerovaný, dokonca sa ani nedá zálohovať. Prístup k súkromnému kľúču uloženému na karte je navyše chránený pomocou hesla (pass phrase).

Čipová karta ako odpojiteľný prvok vybavenia RA nesmie byť ponechaná bez dozoru v čítačke kariet, ale vždy, keď sa nepoužíva, sa musí inaktivovať vybraním z čítačky. Čipovú kartu musí osoba, ktorá ju používa, uložiť čo najbezpečnejšie, podľa možnosti v uzamykateľnom zariadení (bezpečnostná skriňa, trezor a pod.). Aktivačné dáta patriace k čipovej karte (t. j. heslo na prístup k súkromnému kľúču uloženému na karte) v žiadnom prípade nesmú byť zaznamenané a uložené spolu s čipovou kartou, aby sa predišlo zneužitiu súkromného kľúča uloženého na karte v prípade straty alebo krádeže karty.

V prípade vzdialených certifikátov sú 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 sú prevádzkované v zabezpečených priestoroch s režimovým prístupom.

6.3 Správa páru kľúčov

Všetky certifikáty, ktoré vydá Poskytovateľ, budú archivované ďalších 10 rokov po ukončení ich platnosti resp. ukončení činnosti Poskytovateľa.

7 Profily certifikátov a zoznam zrušených certifikátov

Profily certifikátov a CRL sú stanovené centrálne – zákazník ani žiadna externá RA nemôžu meniť štruktúru certifikátov.

7.1 Profily certifikátov

Profily vydávaných certifikátov sú uvedené v aktuálne platných CP NFQES CA, prípadne CP NFQES ACA.

7.2 Profily zoznamov zrušených certifikátov

Profily zrušených certifikátov sú uvedené v aktuálne platných CP NFQES CA, prípadne CP NFQES ACA.

CRL vydávané Poskytovateľom sú CRL verzie 2. Vydávané CRL musia byť v súlade s RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and CRL Profile“.

8 Administrácia špecifikácií

8.1 Procedúry na zmenu špecifikácie

PMA Poskytovateľa môže posúdiť a prípadne revidovať tento dokument.

Chyby, požiadavky na aktualizáciu, alebo navrhované zmeny tohto dokumentu sa majú oznámiť RA. Takáto komunikácia musí obsahovať popis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu vykonala. Všetky zmeny motivované PMA musia byť dané na vedomie subjektom, ktorých sa týkajú (viď časť 8.2 tohto dokumentu) v priebehu jedného mesiaca.

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

8.2 Publikačná a oznamovacia politika

PMA publikuje verejne informácie, ktoré sú obsahom tohto dokumentu. V prípade schválenia novej verzie pravidiel pre RA (aj externú RA) sú tieto publikované najneskoršie pred dňom účinnosti prostredníctvom repozitára (pozri časť 2.6 tohto dokumentu), tak aby bola dostupná všetkým spoliehajúcim sa stranám v čase nadobudnutia účinnosti. Schválená verzia pravidiel pre RA je zaslaná v elektronickej forme všetkým externým RA v dostatočne dlhom čase pred nadobudnutím ich účinnosti, tak aby sa mohli tieto pripraviť na ich implementáciu alebo publikovaná na webovom sídle Poskytovateľa. Za zaslanie informácie o zmenách v tomto dokumente je zodpovedný pracovník NFQES CA.

8.3 Procedúry zverejňovania

Tento dokument bude plne k dispozícii pre PMA, Poskytovateľa, externé RA a audítora vykonávajúceho audit Poskytovateľa resp. externej RA. Pre verejnosť sa bude dokument zverejňovať prostredníctvom webovej stránky Poskytovateľa a prípadne aj iným vhodným spôsobom.

8.4 Úľavy

PMA má právo rozhodnúť, či je odchýlka v praxi CMA prijateľná podľa tohto dokumentu, alebo či má CA navrhnúť zmenu tohto dokumentu. PMA môže povoliť úľavu od niektorej požiadavky tohto dokumentu, aby sa vyhovelo urgentným, nepredvídateľným prevádzkovým požiadavkám. Keď sa povolí úľava, má sa to zverejniť pomocou webového sídla Poskytovateľa, aby sa o úľave dozvedeli strany spoliehajúce sa na certifikáty a má sa, buď iniciovať zmena do tohto dokumentu, alebo sa má pre platnosť danej úľavy stanoviť konkrétny časový limit. Každá úľava musí byť zaznamenaná.