Certifikačná politika NFQES ACA – AdES

Verzia: **1.1**

Dátum účinnosti: 1.1.2024

PO-09

Politika

Verejné

Vytvoril:
Ing. Martin Berzák
Bezpečnostný manažér
23.11.2023

Schválil:
Ing. Eduard Baraniak
Konateľ brainit.sk, s. r. o.
23.11.2023

brainit.sk, s. r. o.

Veľký Diel 3323, 010 08 Žilina
IČO: 52577465

www.brainit.sk

Obsah

1. ÚVOD

Certifikačná politika NFQES ACA - AdES v aktuálnej verzii je certifikačnou politikou pre zdokonalený (*známy aj ako pokročilý*) elektronický podpis/pečať, certifikačnej autority NFQES (ďalej iba „CP“) je dokument popisujúci všeobecné pravidlá, predpisy, záväzné postupy, metodiku a zodpovednosti uplatňované spoločnosťou brainit.sk s. r. o., IČO: 52577465, zapísanou v Obchodnom registri Okresného súdu Žilina, oddiel: Sro, vložka č. 72902/L (v ďalšom iba "Poskytovateľ" alebo „brainit.sk“) pri vytváraní a správe zdokonalených certifikátov pre pokročilé elektronické podpisy/pečate, druhy certifikačných služieb uplatniteľných na tieto certifikáty, ako aj rozsah ich použitia pre danú certifikačnú autoritu (ďalej iba „CA“).

Pri vydávaní zdokonaleného certifikátu (ZdC) pre pokročilý elektronický podpis/pečať od spoločnosti brainit.sk s. r. o. sú zavedené postupy na zabezpečenie vysokej úrovne spoľahlivosti a bezpečnosti overených informácií identifikujúcich zákazníkov bližšie definovaných v bode 1.3.3 (ďalej ako „Zákazník“). Sú zavedené postupy na zabezpečenie spoľahlivosti a bezpečnosti pri vydávaní, zverejňovaní a správe (obnovenie, ukončenie, zneplatnenie) zdokonalených certifikátov, podpisov, ukladaní súkromného kľúča a jeho používaní v aplikáciách.

Táto CP je dôležitý dokument obzvlášť pre zákazníkov (podpisovateľov) a spoliehajúce sa strany (bližšie definované v bode 1.3.4) z hľadiska uskutočniteľnosti týchto služieb.

Vzťahy medzi brainit.sk, s. r. o. a zákazníkom sa riadia na základe uzatvorenej zmluvy medzi nimi, ktorá sa uzatvára na zdokonalené certifikačné služby, prípadne akceptáciou na diaľku pri použití SaaS platformy NFQES dostupnej na adrese https://zone.nfqes.com. Ceny certifikátov a služieb pre vydávanie a správu zdokonalených certifikátov sú uvedené v cenníku dostupnom na webovom sídle klientskej zóny NFQES.

CP je záväzným dokumentom, slúžiacim ako štandard postupov, procedúr a zásad, ktoré musia dodržiavať všetky zúčastnené strany pri poskytovaní dôveryhodných služieb Poskytovateľom.

Webové sídlo Poskytovateľa je na adrese https://nfqes.com

1.1 Definície a skratky

1.1.1 Definície

Certifikácia – Poskytovateľovi certifikačných služieb môže byť udelený štatút „zdokonalený“ na určité obdobie v súlade s nariadením (EÚ) č. 910/2014 po úspešnom audite zhody vykonávanom akreditovanými audítormi.

Certifikát:

- zdokonalený certifikát pre poskytovanie pokročilého elektronického podpisu
- každý ďalší certifikát, ktorý slúži na šifrovanie, autentifikáciu prípadne iné účely v zmysle tejto CP a CPS Poskytovateľa, ktorý bol alebo má byť vydaný Poskytovateľom pre Zákazníka.

CRL - zoznam Certifikátov zrušených pred uplynutím ich lehoty platnosti.

Validačné údaje – údaje, ktoré sa používajú na overenie elektronického podpisu/pečate.

Validácia – proces overovania a potvrdzovania, že elektronický podpis alebo pečať je platný/á.

Osobné identifikačné údaje – súbor údajov, ktoré umožňujú zistiť totožnosť fyzickej alebo právnickej osoby, alebo fyzickej osoby zastupujúcu právnickú osobu.

Údaje na vytvorenie elektronického podpisu – jedinečné údaje, ktoré podpisovateľ používa na vytvorenie elektronického podpisu.

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

Ide predovšetkým o:

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

Pokročilý elektronický podpis – je podpis, ktorý je vytvorený aplikáciou/systémom na vyhotovenie pokročilého elektronického podpisu a ktorý je založený na zdokonalenom certifikáte pre elektronické podpisy.

Pokročilá elektronická pečať – je pečať, ktorá je vytvorená aplikáciou/systémom na vyhotovenie pokročilej elektronickej pečate a ktorá je založená na zdokonalenom certifikáte pre elektronickú pečať.

Koordinovaný svetový čas (UTC) – čas, do ktorého sa počíta čas v rôznych časových pásmach. Ako základ používa International Atomic Time (TAI).

CPS – Vyhlásenie o politike pre prax pri poskytovaní zdokonalených certifikačných služieb je dokument obsahujúci pravidlá vydávania, pozastavenia, zrušenia a zneplatnenia certifikátov, ako aj podmienky udelenia prístupu k certifikátom.

Súkromný kľúč – reťazec symbolov, ktorý sa používa v algoritme na konverziu informácií z čitateľnej do šifrovanej formy alebo naopak.

Verejný kľúč – jeden z kľúčových párov používaných pri asymetrickej kryptografii, ktorý je prístupný a možno ho použiť na overenie elektronického podpisu/pečate.

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

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

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

OCRA token – hardvérový token, ktorý spĺňa štandard RFC 6287 - OCRA: OATH Challenge-Response Algorithm

Politika poskytovateľa / Politiky poskytovateľa -

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

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

Poskytovateľ - spoločnosť brainit.sk, s. r. o. so sídlom Veľký diel 3323, Žilina 010 08, IČO: 52577465, zapísaná v obchodnom registri Okresného súdu Žilina, oddiel Sro, vložka číslo 72902/L.

Prevádzkovateľ RA – subjekt, ktorý prevádzkuje registračnú autoritu Poskytovateľa

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

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

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

Všeobecné podmienky alebo skrátene VP - dokument „Všeobecné podmienky“, vždy v ich účinnom znení dostupnom na webovom sídle Poskytovateľa.

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

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

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

1.1.2 Skratky

QCP-l – Politika kvalifikovaného certifikátu vydaná právnickej osobe, keď je súkromný kľúč pridruženého certifikátu generovaný v zabezpečenom prostredí.

QCP-n – Kvalifikovaná certifikačná politika vydaná fyzickej osobe, keď je súkromný kľúč pridruženého certifikátu vygenerovaný v zabezpečenom prostredí.

NCP+ - Vylepšená normalizovaná certifikačná politika, ktorá zahŕňa ďalšie požiadavky na zdokonalené certifikáty v súlade s nariadením (EÚ) č. 910/2014.

CN - bežné meno (Common Name)

CPS – vyhlásenie o certifikačnej politike/praxi (Certification Practice Statement)

HSM – hardvérový bezpečnostný modul (Hardware Security Module)

LDAP – protokol pre jednoduchý prístup do registra (Lightweight Directory Access Protocol)

PKI – infraštruktúra verejného kľúča (Public Key Infrastructure)

PO – právnická osoba

RA – registračná autorita (Registration authority)

SHA – hash algoritmus pre extrahovanie hash identifikátora (Secure Hash Algorithm)

SSL – bezpečný kanál na prenos dát (Secure Socket Layer)

SMIME – bezpečný e-mailový protokol cez internet (Secure Multipurpose Internet Mail Extensions)

ZdC – Zdokonalený certifikát

IETF – Internet Engineering Task Force

RFC – Request for comments

1.2 Prehľad

Dokument CP sa vzťahuje na zdokonalené certifikáty vydané Poskytovateľom podľa nariadenia Európskeho parlamentu a Rady EÚ č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/ES. CP je v súlade s platnou legislatívou Slovenskej republiky. Dokument je štruktúrovaný v súlade s rámcom definovaným v RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“. CP je využívaná pre produkty a služby, ktoré poskytuje Poskytovateľ a pre správu certifikátov podľa štandardu X.509 pri implementácii infraštruktúry verejných kľúčov (ďalej „PKI“).

Vydávanie zdokonalených certifikátov (ďalej ako „ZdC“) pre pokročilé elektronické podpisy/pečate je spojené s:

- **Vydaním zdokonaleného certifikátu fyzickej osobe (Podpisovateľ) – Zdokonalený certifikát pre pokročilý elektronický podpis**
- **Vydaním zdokonaleného certifikátu právnickej osobe (Tvorca pečate) – Zdokonalený certifikát pre pokročilú elektronickú pečať**

Certifikačné autority Poskytovateľa pre poskytovanie zdokonalených dôveryhodných služieb:

Certifikačná autorita Poskytovateľa	Sériové číslo certifikátu	Vydavateľ
ACA NFQES	4a2a267827944e5323683482e7d5a72205491ac1	CA NFQES

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

- Certifikát ACA NFQES
- Certifikát na potvrdenie existencie a platnosti certifikátu (OCSP)

1.3 Názov a identifikácia dokumentu

Verzia dokumentu: 1.1

Dátum účinnosti: 1.1.2024

Dokument CP pre pokročilý elektronický podpis/pečať certifikačnej autority NFQES je identifikovaný objektovým identifikátorom, ktorý môžu spoliehajúce sa strany použiť na určenie ich použiteľnosti pre aplikáciu, ako je opísané v odporúčaní IETF RFC 3647, oddiel 3.3. CP je definovaná OID 1.3.158.52577465.0.0.0.2.1.1, kde jednotlivé zložky OID majú nasledovný význam:

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

Poskytovateľ zaisťuje, že nezmení identifikátor objektu tohto dokumentu, ako aj identifikátory objektov politík, postupov a iných odporúčacích dokumentov. Ak existuje rozšírenie alebo aktualizácia v politike, ktorá neovplyvní predtým vydané certifikáty, Poskytovateľ aktualizuje nový identifikátor objektu, ktorý pokrýva nové certifikáty alebo rozšírené/aktualizované certifikáty. Poskytovateľ sa riadi interným postupom riadenia OID.

História zmien:

Verzia	Dátum	Popis revízie
1.0	1.3.2023	Prvá schválená verzia dokumentu
1.1	23.11.2023	Upravená a schválená verzia dokumentu

1.4 Účastníci Infraštruktúry

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

Poskytovateľ ako poskytovateľ zdokonalených certifikačných služieb poskytuje služby generovania a správy (pozastavenie, obnovenie a ukončenie) zdokonalených certifikátov prostredníctvom autentifikačného orgánu „NFQES ACA“ a služby pre identifikáciu a autentifikáciu Zákazníkov prostredníctvom registračnej autority.

Ďalšími účastníkmi infraštruktúry Poskytovateľa sú Zákazníci a spoliehajúce sa strany.

1.4.1 Certifikačné autority

Certifikačná autorita:

- je subjekt, ktorý poskytuje zdokonalené certifikáty pre pokročilé elektronické podpisy/pečate, ktoré sú spravované podľa tejto CP
- je súčasťou hierarchickej PKI štruktúry vo vydaných zdokonalených certifikátoch (vydavateľ ZdC)

Certifikačné autority Poskytovateľa sú:

- Certifikačná autorita ACA NFQES (sériové číslo: 4a2a267827944e5323683482e7d5a72205491ac1), ktorá vydáva zdokonalené certifikáty používateľom a je súčasťou hierarchickej PKI štruktúry CA NFQES.

1.4.2 Registračné autority

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

Poskytovateľ má zriadenú internú RA, ktorá je určená pre všetkých Zákazníkov, ktorí majú záujem o zdokonalené certifikáty pre pokročilé elektronické podpisy/pečate. Táto RA nie je samostatný právny subjekt.

RA vykonáva nasledovné činnosti:

- Prijíma žiadosti o zdokonalené certifikáty, schvaľuje alebo zamieta tieto žiadosti v súlade s internými pravidlami schvaľovania
- Overuje totožnosť osôb žiadajúcich o certifikáty
- Overí, že vydaný certifikát je odovzdaný Zákazníkovi
- Ukončuje zdokonalené certifikáty na základe pravidiel ukončenia platnosti

1.4.3 Používatelia

Každá fyzická alebo právnická osoba, ktorá má s Poskytovateľom uzatvorenú písomnú zmluvu, je Zákazníkom zdokonalenej certifikačnej služby poskytovanej Poskytovateľom, pričom Zákazník za predmetné služby aj platí.

Držiteľom ZdC sa rozumie osoba uvedená v ZdC. Držiteľ certifikátu môže byť jedna osoba - Zákazník, alebo aj dve rôzne osoby, a to napríklad v prípade, že Zákazník je zamestnávateľ, ale Držiteľom certifikátu je zamestnanec.

Držiteľom ZdC môže byť:

- fyzická osoba (podpisujúca osoba), ktorá vytvára pokročilý elektronický podpis
- fyzická osoba (podpisovateľ), ktorá je splnomocneným zástupcom právnickej osoby a vyhotovuje pokročilý elektronický podpis
- fyzická osoba identifikovaná v spojení s právnickou osobou
- právnická osoba, ktorou môže byť organizácia alebo jej jednotka resp. oddelenie

- právnická osoba, ktorá vytvára pokročilú elektronickú pečať

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

Keď Zákazník koná v mene jedného alebo viacerých Držiteľov, s ktorými je prepojený (napr. Zákazník je právnická osoba požadujúca vydanie ZdC pre svojich zamestnancov) tak rozdielne zodpovednosti Zákazníka a Držiteľa sú definované v dokumente „Všeobecné podmienky“ v aktuálnej verzii (ďalej len „Všeobecné podmienky“) zverejnené na webovom sídle Poskytovateľa:

https://nfqes.com/dokumenty/

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

Vzťah medzi Zákazníkom a Držiteľom môže byť takýto:

Pri žiadaní o ZdC fyzickej osoby (Držiteľ) je Zákazníkom

- samotná fyzická osoba,

Pri žiadaní o ZdC pre právnickú osobu je Zákazníkom

- štatutárny orgán právnickej osoby, ktorá žiada za svoje dcérske spoločnosti alebo jednotky alebo oddelenia.

1.4.4 Spoliehajúce sa strany

Spoliehajúce sa strany sú fyzické alebo právnické osoby, ktoré akceptujú ZdC vydaný Poskytovateľom a pri svojom konaní sa spoliehajú na postupy pre dôveryhodné služby Poskytovateľa.

1.4.5 Ostatní účastníci

Poskytovateľ si vyhradzuje právo v prípade potreby uzavrieť zmluvy s externými osobami na poskytovanie určitých certifikačných služieb.

Policy Management Authority

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

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

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

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

Poskytovatelia iných služieb

Medzi poskytovateľov iných služieb patria:

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

1.5 Použitie certifikátu

ZdC vyhotovený pre fyzickú osobu je vyhotovený za účelom podpory zdokonaleného elektronického podpisu v zmysle článku 3 bod 11 Nariadenia eIDAS.

ZdC vyhotovený pre právnickú osobu je vyhotovený za účelom podpory zdokonalenej elektronickej pečate v zmysle článku 3 bod 26 Nariadenia eIDAS.

1.5.1 Vhodné použitie certifikátu

Zdokonalený certifikát fyzickej/právnickej osoby alebo splnomocneného zástupcu právnickej osoby uvedenej v certifikáte ako podpisovateľ môže byť použitý na vytvorenie pokročilého elektronického podpisu/pečate v elektronických dokumentoch a prílohách/transakciách, ktoré si vyžadujú vysokú úroveň informačnej bezpečnosti.

1.5.2 Zakázané použitie certifikátu

Zdokonalené certifikáty Poskytovateľa nie je možné používať spôsobom, ktorý nie je v súlade s ich uvedeným účelom a rozsahom/zásadami. Zdokonalené certifikáty vydané v súlade s touto politikou sa nesmú používať na nezákonné účely.

1.6 Správa politiky

Poskytovateľ je zodpovedný za riadenie týchto zásad.

Každá verzia zásad je v platnosti až do schválenia a zverejnenia novej verzie. Každá nová verzia je vyvinutá zamestnancami Poskytovateľa a je zverejnená po schválení CEO Poskytovateľa. Zákazníci sú povinný dodržiavať iba platnú verziu zásad v čase využívania služieb Poskytovateľa.

1.6.1 Informácie o Poskytovateľovi a jeho kontaktné údaje

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
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/

Kontakt pre žiadosť o zrušenie Certifikátu:
Mobil: +421 918 022 030
E-mail: info@nfqes.sk

1.6.2 Kontaktná osoba

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

Certifikačná autorita NFQES ACA:

Adresa: Veľký Diel 3323, 010 08 Žilina

Email: ca@nfqes.sk

Telefón: +421 905 320 821

Webové sídlo: https://nfqes.com

Nahlasovanie incidentov: infra@nfqes.sk

1.6.3 Osoba, ktorá určuje vhodnosť CPS pre certifikačnú politiku

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

CP a CPS pokrývajú rovnaký súbor tém, ktoré slúžia používateľom a spoliehajúcim sa stranám, za účelom poskytnutia bezpečnej a spoľahlivej aplikácie ZdC pre pokročilý elektronický podpis/pečať vydávané Poskytovateľom.

Hlavným rozdielom medzi oboma dokumentmi je zameranie ich ustanovení a ich zamýšľaný účel. CP skúma požiadavky na implementáciu potrebných štandardov a infraštruktúry. CP okrem toho identifikuje účastníkov činností certifikačných služieb. CPS na druhej strane popisuje ako CA a iní účastníci infraštruktúry uplatňujú postupy a kontroly na splnenie požiadaviek CP. Inými slovami, účelom oboch dokumentov je zabezpečiť jednotné pravidlá a postupy, ako si účastníci infraštruktúry Poskytovateľa plnia svoje povinnosti a zodpovednosti.

1.6.4 Postupy schvaľovania CPS

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

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

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

Každá verzia CP a CPS je v platnosti do účinnosti novej verzie schválenej a uverejnenej na webovom sídle Poskytovateľa. Uverejnenie schválenej novej schválenej verzie je vždy, aspoň 30 dní pred jej účinnosťou, ak sa nejedná o mimoriadnu okolnosť. Za mimoriadnu okolnosť je považovaná taká okolnosť, ktorá neznesie odklad.

2. ZVEREJNENIE A ZODPOVEDNOSŤ ZA ULOŽENIE ÚDAJOV

2.1 Úložiská

Úložisko, v ktorom sa nachádzajú aktuálne a predchádzajúce verzie elektronických dokumentov a sú umiestnené tak, aby boli prístupné Držiteľom ZdC a Spoliehajúcim sa stranám a v súlade s celkovými bezpečnostnými požiadavkami.

Poskytovateľ spravuje a kontroluje webové sídlo spoločnosti, ktoré zastáva funkciu úložiska Poskytovateľa. Presná URL adresa je uvedená v kapitole 1. Na webovom sídle Poskytovateľa sú zverejnené všetky aktuálne verzie elektronických dokumentov a poskytuje zainteresovaným stranám bezpečný a nepretržitý prístup k týmto dokumentom. Webové sídlo Poskytovateľa je prostredníctvom internetu verejne prístupné Držiteľom ZdC, Spoliehajúcim sa stranám a verejnosti vôbec.

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

2.2 Zverejnenie informácií o certifikačnej autorite

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

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

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

2.3 Čas a frekvencia zverejnenia

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

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

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

2.4 Kontroly prístupu k úložiskám

Poskytovateľ musí chrániť každú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozšírenie. Poskytovateľ musí vynaložiť maximálne úsilie na to, aby zaistil dôvernosť, integritu a dostupnosť dát vyplývajúcich z poskytovaných dôveryhodných služieb. Taktiež musí vykonať logické a

bezpečnostné opatrenia, aby zabránil neautorizovanému prístupu k úložisku osobám, ktoré by mohli akýmkoľvek spôsobom poškodiť, zmeniť, pridať resp. vymazať údaje uložené v úložisku.

Spoločnosť brainit.sk ponúka prístup k informáciám uloženým na úložisku, ktoré poskytujú prístup založený na HTTP/HTTPS a OSCP.

3. Identifikácia, autentifikácia a overovanie názvov

Táto kapitola predstavuje všeobecné pravidlá pre autentifikáciu používateľov, ktoré Poskytovateľ uplatňuje pri vydávaní ZdC. Pravidlá sú založené na určitých typoch informácií, ktoré sú zahrnuté v certifikátoch. Presné postupy kontrol a zadávania mien sú popísané v dokumente CPS tejto CP.

3.1 Názvy, Mená, Pomenovania

Požiadavky na názvy/mená pre certifikát sú definované v odporúčaniach ITU-T X.509 alebo IETF RFC 5280 a ETSI EN 319 412. Názvy môžu byť v súlade so službou Domain Name System (DNS) opísanou v RFC 2247. RA overuje a zabezpečuje, že mená v žiadosti o vydanie certifikátu sú v súlade s normou X.509.

Pole „Predmet“ na certifikáte obsahuje meno Podpisovateľa (Autora. Meno a ďalšie rozlišovacie znaky Podpisovateľa v zodpovedajúcich poliach pre každý typ certifikátu sú v súlade s DN (Distinguished Name), ktoré je tvorené podľa štandardu X.500 a X.520.

Podrobná špecifikácia certifikátov vydaných Poskytovateľom je uvedená v ďalších častiach tohto dokumentu, ako aj dokumentu CPS tejto CP.

3.1.1 Druhy mien

Každá CA má byť schopná vytvárať certifikáty, ktoré obsahujú rozlišovacie mená v zmysle X.500 (X.500 Distinguished Name, ďalej ako „rozlišovacie meno“), konkrétne v súlade s X.501 resp. X.520 a aj mená v zmysle RFC 5322 Internet Message Format.

Požiadavky na názvy vydaných certifikátov sú uvedené v odporúčaní ITU-T X.509 alebo IETF RFC 5280 a ETSI EN 319 412. Názvy môžu byť v súlade so službou DNS (Domain Name System) opísanou v RFC 2247. Tento spôsob umožňuje predplatiteľom použiť dva typy mien: DN a DNS.

3.1.2 Potreba zmysluplnosti mien

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

Používané mená musia spoľahlivo identifikovať osoby, ktorým sú priradené. V niektorých prípadoch sa v obsahu ZdC 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 ZdC je špecializovaný HW, ktorý nie je možné nahradiť (príp. je to pre zákazníka nerentabilné) a nepodporuje znakovú sadu UTF-8.

3.1.3 Anonymita alebo pseudoanonymita predplatiteľov

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

3.1.4 Pravidlá pre tlmočenie rôznych foriem mien

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

3.1.5 Jedinečnosť mien

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

3.1.6 Uznávanie, autentifikácia a úloha ochranných známok

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

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

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

3.2 Počiatočné overenie totožnosti

Počiatočná registrácia Zákazníka sa uskutoční pri prvom odoslaní žiadosti o registráciu Poskytovateľovi.

Registrácia zahŕňa postupy, ktoré umožňujú zhromažďovanie údajov o jeho identite a rovnako aj o jeho identifikácii pred vydaním certifikátu. Toto overenie údajov vyžaduje vzdialenú prítomnosť pred zamestnancom Poskytovateľa alebo jeho RA, notárom alebo inou oprávnenou osobou potvrdzujúcou jeho/jej totožnosť, prípadne je overenie údajov sprostredkované pomocou externej RA. Tento postup môže byť vykonaný na diaľku a ak je to možné, automatizovane, pomocou systému vzdialenej identifikácie, ktorý spĺňa požiadavky nariadenia (EÚ) č. 910/2014.

Zákazník je povinný predložiť/dodať všetky potrebné údaje na jednoznačnú identifikáciu a overenie svojej totožnosti:

- Meno a Priezvisko uvedené v doklade totožnosti
- Doklad totožnosti – občiansky preukaz, medzinárodný pas alebo iný doklad totožnosti
- Národné identifikačné číslo, *ak neexistuje, tak dátum narodenia*
- Kontaktné údaje – mobilný telefón, e-mail a adresa

Po úspešnom overení totožnosti Zákazníka, oprávnený Prevádzkovateľ v RA:

- Ponúka všeobecné podmienky o zdokonalených certifikačných službách podpísané v mene Poskytovateľa a uchováva všetky dokumenty priložené k zmluve
- Potvrdí žiadosť o vydanie certifikátu a zašle elektronickú žiadosť o vydanie certifikátu
- Zaznamenáva vydaný certifikát na bezpečné zariadenie na vytváranie podpisov a odošle ho Zákazníkovi alebo oprávnenej osobe

V prípade, že Zákazník využije možnosť vzdialenej identifikácie, požiada o poskytnutie služby na diaľku predložením osobných údajov ako aj mobilné číslo a e-mail. V takomto prípade dochádza k uzatvoreniu zmluvy medzi Zákazníkom a Poskytovateľom a vydaniu zdokonaleného certifikátu pre pokročilý elektronický podpis a okamžitému podpísaniu zmluvy s Poskytovateľom. Registračný profil je udržiavaný pre každú osobu v systémoch Poskytovateľa.

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

V prípade, že je v rámci Slovenskej republiky vyhlásená mimoriadna situácia v zmysle zákona č. 42/1994 Z. z. o civilnej ochrane obyvateľstva v znení neskorších predpisov môže PMA rozhodnúť o modifikácii spôsobu vydávania zdokonalených certifikátov a s tým spojeným generovaním kryptografických kľúčov a overovaním identity jednotlivých subjektov, ktorý sa bude odlišovať od tu uvedených postupov. Modifikovaný postup, ktorý sa prispôsobí podmienkam mimoriadnej situácie a teda sa nedá bližšie špecifikovať, musí byť spracovaný v písomnej podobe, musí byť schválený PMA, musí byť posúdený orgánom posudzovania zhody a nesmie byť v rozpore s nariadením (EÚ) č. 910/2014 a národnou legislatívou a je ho možné použiť len počas trvania mimoriadnej situácie. Po ukončení mimoriadnej situácie sa musí postupovať v zmysle tu uvedených postupov.

3.2.1 Spôsob preukázania vlastníctva súkromného kľúča

Na vydanie alebo predĺženie certifikátu Poskytovateľom dostane elektronickú žiadosť vo formáte PKCS#10. Špecifikácia tohto formátu žiadosti o certifikát vyžaduje, aby žiadosť podpísal Podpisovateľ, ktorý vlastní súkromný kľúč. Poskytovateľ overuje platnosť elektronického podpisu/pečate sprevádzajúcej žiadosti. Preukázanie platnosti umiestneného elektronického podpisu/pečate je dostatočným dôvodom na predpoklad, že Podpisovateľ podal elektronickú žiadosť a vlastní súkromný kľúč, ktorý je technicky vhodný a zodpovedá verejnému kľúču uvedenému v žiadosti.

V prípade žiadosti o vydanie ZdC elektronického podpisu/pečate na diaľku Poskytovateľ poskytne Podpisovateľovi službu na diaľku vygenerovaním páru kľúčov v šifrovacom module, ktorý spĺňa požiadavky bezpečného zariadenia na vytváranie podpisov.

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

3.2.2 Autentifikácia identity právnickej osoby

Overenie identity právnickej osoby môže byť vykonané v sídle RA alebo na diaľku, podpísaním žiadosti o vydanie ZdC, prostredníctvom zdokonalených certifikátov pre pokročilý elektronický podpis všetkých konateľov, vydaných v súlade s odsekom 1 písmenom a) resp. b) článku 24 Nariadenia eIDAS. Zoznam konateľov je získaný z elektronického výpisu z Obchodného registra použiteľného na právne úkony, ktorý musí zabezpečiť Zákazník cez portál slovensko.sk. Následne sa všetky podpisy validujú, čím sa overia platnosti podpisov, platnosť a pravosť údajov a platnosť identifikačných dokladov.

Právnické osoby (ďalej aj ako „PO“), ktoré nemôžu byť podrobené automatizovanému overeniu, by mali predložiť:

- rozsudok alebo iný dokument osvedčujúci vznik PO,
- ľubovoľný dokument potvrdzujúci ich dobrý stav, ktorý posúdi RA
- jedinečný národný identifikátor.

Pracovník RA následne skontroluje, či sa údaje, ktoré sú uvedené v AdES podpisoch a v overenom elektronickom výpise z obchodného registra, resp. iného zákonom určeného registra, zhodujú s údajmi, ktoré sú uvedené v aplikácií zone.nfqes.com a v žiadosti o vydanie certifikátu.

Ak sú certifikáty platné, elektronický výpis z obchodného registra (resp. iného zákonom určeného registra) platný a údaje v Aplikácií, žiadosti o vydanie certifikátu, vo výpise z obchodného registra (resp. iného zákonom určeného registra) a údaje v AdES podpise sa zhodujú, považuje sa PO za overenú.

Na vydanie zdokonaleného certifikátu pre FO, ktorá je splnomocnená právnickou osobou, sa splnomocnený zástupca dostaví pred RA. Overenie informácií obsiahnutých v predložených dokumentoch vykonáva RA prostredníctvom:

- Potvrdenia „verné originálu“ s vlastnoručným podpisom dotknutej osoby na dokladoch, ktoré vydá pracovník RA, v prípade osobného predloženia dokladov splnomocneného zástupcu a podpísania sa splnomocneného zástupcu pred pracovníkom RA.
- Notárskeho overenia dokumentov, ktoré sú zaslané poštou na RA.
- Podpísania priložených elektronických formátov dokumentov splnomocneným zástupcom, platným zdokonaleným certifikátom pre pokročilý elektronický podpis/pečať.
- Kontrolou a potvrdením pomocou aplikácie poskytovateľa dostupnej na adrese https://zone.nfqes.com.

Overením totožnosti právnickej osoby sa má preukázať, že pri skúmaní žiadosti právnická osoba existuje a že zástupca, ktorý žiada o zdokonalený certifikát, má právomoc požiadať o vydanie zdokonaleného certifikátu v mene právnickej osoby. Zamestnanec RA môže overiť registráciu prostredníctvom všetkých dostupných verejných služieb v súlade so Slovenskou legislatívou.

Overenie identifikácie, resp. identity právnickej osoby môže byť vykonané aj pomocou externého informačného systému v správe externej RA, pokiaľ sú údaje v tomto systéme dostatočne overované v zmysle nariadenia (EÚ) č. 910/2014, Prevádzkovateľ RA bol oboznámený so všetkými postupmi overovania identity a Prevádzkovateľ RA s poskytnutím takejto identity súhlasí.

3.2.3 Autentifikácia identity fyzickej osoby

Identifikáciu a overenie totožnosti, resp. identifikácie fyzickej osoby (Podpisovateľa) vykonáva RA. Overenie identifikácie fyzickej osoby môže byť vykonané v sídle RA alebo na diaľku.

Na identifikáciu a overenie identifikácie fyzickej osoby (ďalej ako „FO“) je potrebné predložiť doklad totožnosti. FO, ktorá žiada o vydanie alebo správu ZdC, vyplní a odošle Poskytovateľovi dokumenty v súlade s politikou Poskytovateľa pre vydávanie a správu ZdC. Osobné údaje môžu zahŕňať číslo mobilného telefónu, e-mailovú adresu, adresu trvalého pobytu, atď.

Overenie identity FO môže byť vykonané prostredníctvom zdokonaleného certifikátu pre pokročilý elektronický podpis, ktorým FO podpíše a vyjadrí súhlas so Všeobecnými podmienkami a FO podpíše žiadosť o vydanie certifikátu podľa CP.

V oboch prípadoch (aj v sídle RA, aj na diaľku) sa tento zdokonalený podpis validuje, čím sa overí platnosť podpisu, platnosť a pravosť údajov a platnosť identifikačných dokladov.

Pracovník RA následne skontroluje, či sa údaje, ktoré sú uvedené v AdES podpise, zhodujú s údajmi, ktoré sú uvedené v aplikácií zone.nfqes.com a v žiadosti o vydanie certifikátu.

Ak je certifikát platný a údaje v Aplikácií, žiadosti o vydanie certifikátu a údaje v AdES podpise sa zhodujú, považuje sa FO za overenú.

Fyzická osoba potvrdzuje pravosť údajov nasledovne:

- Vlastnoručným podpisom na dokumentoch pred pracovníkom RA, pri osobnom predložení dokumentov.
- Notárskym overením dokumentov, ktoré sú zaslané poštou RA.
- Podpísaním priložených elektronických dokumentov platným zdokonaleným certifikátom pre pokročilý elektronický podpis v zmysle nariadenia (EÚ) č. 910/2014.

Poskytovateľ vykonáva overenie pravosti informácií vo vyplnených dokumentoch všetkými zákonom povolenými prostriedkami. Zoznam požadovaných dokumentov pre FO na vydanie a správu zdokonaleného certifikátu je uvedený v týchto politikách.

Overenie identity fyzickej osoby môže byť vykonané aj pomocou externého informačného systému v správe externej RA, pokiaľ sú údaje v tomto systéme dostatočne overované v zmysle nariadenia (EÚ) č. 910/2014, Prevádzkovateľ RA bol oboznámený so všetkými postupmi overovania identity a Prevádzkovateľ RA s poskytnutím takejto identity súhlasí.

3.2.4 Neoverené informácie o žiadateľovi a osobitné atribúty

Všetky položky v zdokonalenom certifikáte musia byť overené. Akékoľvek informácie nad rámec povinného overenia sú neoverené informácie.

Poskytovateľ môže vo vydanom certifikáte uviesť osobitné atribúty spojené s Podpisovateľom, ak je certifikát vydaný na konkrétny účel podľa príslušnej politiky. Tieto informácie podliehajú overeniu RA.

3.2.5 Validácia autority

Po úspešnej identifikácii a overení podmienok na vydanie alebo správu zdokonaleného certifikátu RA, zástupca RA potvrdí údaje CA. CA bezodkladne zverejní vydaný certifikát v registri certifikátov, resp. informácie o údržbe v CRL.

V spoločnosti brainit.sk môže tento certifikát zrušiť iba certifikačná autorita NFQES ACA, ktorá vydala zdokonalený certifikát elektronického podpisu/pečate alebo iný dôveryhodný systém.

Pozri bod 3.2.3

3.2.6 Kritériá interoperability

Zdokonalené certifikáty vydané Poskytovateľom spĺňajú požiadavky nariadenia (EÚ) 910/2014 a sú uznávané v Európskej únii. Vzhľadom na cezhraničnú interoperabilitu formátov zdokonalených elektronických podpisov a pečatí zavedených nariadením (EÚ) č. 910/2014 zdokonalené certifikáty

neprekračujú povinné požiadavky nariadenia (EÚ) č. 910/2014. Na vnútroštátnej úrovni zdokonalené certifikáty zahŕňajú špecifické údaje, ako napríklad občianske identifikačné číslo a ďalšie špecifické údaje na žiadosť používateľa, ale Poskytovateľ zabezpečuje, aby nebránili cezhraničnej interoperabilite a uznávaniu zdokonalených certifikátov a elektronických podpisov/pečatí v Európskom spoločenstve.

3.3 Identifikácia a autentifikácia pre požiadavky na opätovné zadanie kľúča

Poskytovateľ môže obnoviť platne zdokonalený certifikát, ktorý nebol ukončený počas doby platnosti, vygenerovaním nového páru kľúčov („Re-Key“).

Poskytovateľ neposkytuje možnosť obnovy so zachovaným existujúceho páru kľúčov alebo so zachovaním sériového čísla.

Vydanie následného ZdC znamená zmenu páru kľúčov ZdC – vytvorí sa nový ZdC, ktorý bude mať zhodné rozlišovacie meno ako pôvodný, ale nový ZdC bude mať odlišný verejný kľúč (zodpovedajúci novému, odlišnému súkromné kľúču), odlišné sériové číslo (Serial Number) a môže mať zmenenú dĺžku platnosti. Toto obnovenie aktuálneho certifikátu s novým párom kľúčov je možné len v prípade, že nedošlo k žiadnym zmenám v už overených informáciách.

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

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

Poskytovateľ pri obnove ZdC, dodržiava nasledovné lehoty a identifikačné požiadavky:

Obdobie / Period	**Obnova / Renewal**	**Požiadavky / Requirements**
Do 30 dní pred skončením platnosti ZdC, ktorý nebol ukončený a ktorý nemá žiadnu zmenu v údajoch v ňom certifikovaných.	Opätovný kľúč (Re-key)	• Certifikát sa nemení • Požiadavku na obnovenie je možné zadať na diaľku
Do 30 dní po skončení platnosti ZdC, ktorý nebol ukončený a nedošlo k zmene údajov v ňom certifikovaných.	Opätovný kľúč (Re-key)	• Certifikát sa nemení • Žiadosť o obnovenie možno podať na mieste (v RA)
Viac ako 30 dní po skončení platnosti ZdC.	Neobnovuje sa	

V prípade vydávania a obnovy ZdC na diaľku pomocou aplikácie je obnova vždy Re-key. V tomto prípade sa nevykonávajú kontroly totožnosti a identifikácie, ale vykonávajú sa kontroly overenia totožnosti.

3.4 Identifikácia a autentifikácia v prípade ukončenia certifikátu

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

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

V prípade, že Poskytovateľ vypovedá zdokonalený certifikát, premietne to do svojich databáz podľa možnosti čo najskôr od prijatia žiadosti. Zrušenie nadobúda platnosť ihneď po jeho zverejnení.

Poskytovateľ ukončí platnosť certifikátu až po úspešnej identifikácii a overení totožnosti Podpisovateľa a špecifického dôvodu ukončenia.

3.5 Identifikácia a autentifikácia po ukončení zdokonaleného certifikátu

Politika poskytovania zdokonalených certifikačných služieb Poskytovateľa neumožňuje obnovenie zdokonaleného certifikátu po jeho ukončení.

Podpisovateľ ukončeného certifikátu môže požiadať o vydanie nového certifikátu.

Poskytovateľ prostredníctvom RA vykoná prvotnú identifikáciu a overenie totožnosti Podpisovateľa, ak požiada o nový certifikát.

4. PREVÁDZKOVÉ POŽIADAVKY NA ŽIVOTNÝ CYKLUS CERTIFIKÁTU

Poskytovateľ prostredníctvom RA v rámci uzatvorenej zmluvy o poskytovaní zdokonalených certifikačných služieb poskytuje nasledujúce prevádzkové postupy pre zdokonalené certifikačné služby vzťahujúce sa na zdokonalené elektronické podpisy/pečate:

- Registrácia žiadosti o zdokonalený certifikát
- Vybavenie žiadosti o zdokonalený certifikát
- Vydanie zdokonaleného certifikátu
- Odovzdanie vydaného zdokonaleného certifikátu
- Použitie párového kľúča a zdokonaleného certifikátu
- Obnovenie zdokonaleného certifikátu
- Ukončenie platnosti zdokonaleného certifikátu
- Stav zdokonaleného certifikátu

Poskytovateľ prostredníctvom RA umožňuje Podpisovateľovi ukončiť medzi nimi Zmluvu o zdokonalených certifikačných službách. Čas v systémoch spojených s ukončením certifikátov sa synchronizuje s UTC aspoň raz za 24 hodín.

Poskytovateľ poskytuje prevádzkové postupy pre zdokonalené certifikačné služby použiteľné pre zdokonalené certifikáty elektronických podpisov/pečatí popísané vo vyhlásení pre zdokonalené certifikačné služby (CPS) tejto politiky.

4.1 Použitie zdokonaleného certifikátu a páru kľúčov

4.1.1 Používatelia

Používatelia musia používať súkromné kľúče a príslušné zdokonalené certifikáty:

- v súlade s ich zamýšľaným účelom,
- len v rámci doby ich platnosti.

Zodpovednosť za používanie súkromného kľúča nesie podpisovateľ.

4.1.2 Spoliehajúce sa strany

Spoliehajúce sa strany, vrátane prevádzkovateľa v RA, musia používať verejné kľúče a ich príslušné certifikáty:

- v súlade s ich zamýšľaným účelom,
- až po skontrolovaní ich stavu a skontrolovaní elektronického podpisu CA, ktorá certifikát vydala,
- dovtedy, kým sa platnosť kľúča nezruší/neukončí.

4.1.3 Používanie verejných kľúčov a certifikátov

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

4.1.3.1 Používanie súkromného kľúča a certifikátu účastníka

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

- pri žiadaní o vydanie certifikátu poskytnúť Poskytovateľovi pravdivé, presné a úplné informácie v zmysle tejto CP,
- používať kľúčový pár v súlade s obmedzeniami, ktoré sú uvedené vo Všeobecných podmienkach,
- neustále chrániť svoje súkromné kľúče v súlade s touto CP, Všeobecnými podmienkami, tak aby boli výhradne pod jeho kontrolou,
- používať súkromný kľúč až po obdržaní ZdC k verejnému kľúču s ktorým tvorí pár,
- pri ZdC, 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, mobilná aplikácia alebo OCRA token),
    - nepresnostiach alebo zmenách v obsahu certifikátu,
    - bezodkladne požiadať o zrušenie ZdC v prípade, že akýkoľvek údaj uvedený v subjekte ZdC sa stal neplatným,
- zdržať sa používania súkromného kľúča a ZdC, 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 ZdC ako napr. ukončiť používanie súkromného kľúča po exspirácii alebo zrušení ZdC verejného kľúča,
- používať poskytnuté ZdC len na príslušné účely, ktoré sú odporúčané v tejto CP,
- okamžite ukončiť používanie súkromného kľúča po jeho kompromitácii.

4.1.3.2 Využitie verejného kľúča a certifikátu spoliehajúcej sa strany

Spoliehajúce sa strany sú povinné:

- vytvoriť vzťah dôvery k CA, ktorá vydala daný ZdC, verifikovaním certifikačnej cesty v súlade so štandardom X.509 verzie 3 a povinným použitím dôveryhodného zoznamu krajiny, v ktorej má vydavateľ sídlo a je uvedené v položke countryName mena vydavateľa v kvalifikovanom certifikáte,
- uchovávať originálne podpísané údaje, aplikácie potrebné na čítanie a spracovanie týchto údajov a kryptografické aplikácie potrebné na overovanie zdokonalených elektronických podpisov týchto údajov, pokiaľ môže byť potrebné overovať podpis týchto údajov.

4.2 Obnovenie zdokonaleného certifikátu

Poskytovateľ nesmie vydať ZdC na verejný kľúč, na ktorý už bol ním v minulosti ZdC vydaný. Obnovenie ZdC znamená nahradenie platného certifikátu novým certifikátom bez zmeny existujúcich informácií, ktoré certifikát obsahuje, s výnimkou nového sériového čísla a nového obdobia platnosti. Obnovenie sa vykonáva iba v rámci obdobia platnosti aktuálneho certifikátu. Pred obnovením musí existovať zápis žiadosti o obnovenie certifikátu vo vhodnej forme prijatej a schválenej prevádzkovateľom RA. Musí byť overená totožnosť a správnosť na základe predloženej žiadosti.

O obnovu zdokonaleného certifikátu môže požiadať Podpisovateľ alebo oprávnená osoba v rámci lehôt, požiadaviek a podmienok na obnovu.

Zdokonalená obnova certifikátu uchováva informácie Podpisovateľa alebo oprávnenej osoby z aktuálneho certifikátu, kde je v obnovenom certifikáte zmenená doba platnosti a sériové číslo.

Zdokonalené certifikáty, ktoré neboli počas doby platnosti ukončené, je možné obnoviť vygenerovaním nového páru kľúčov (Re-key). Poskytovateľ neudržiava možnosť obnovy so zachovaním existujúceho páru kľúčov alebo so zachovaním sériového čísla.

Obnove zdokonaleného certifikátu predchádza registrácia žiadosti o obnovu na RA alebo online.

Keď platnosť ZdC vyprší a žiadosť o obnovenie je v stanovených lehotách a požiadavkách na identifikáciu obnovenia, Podpisovateľ alebo oprávnená osoba navštívi RA spoločnosti brainit.sk alebo vykoná identifikáciu na diaľku.

Certifikát zdokonaleného elektronického podpisu/pečate môže Podpisovateľ alebo oprávnená osoba opakovane obnoviť. Poskytovateľ neumožňuje použitie páru kľúčov pre elektronický podpis/pečať na dobu dlhšiu ako 3 roky.

RA obnoví ZdC elektronického podpisu/pečate pomocou Re-key za nasledujúcich podmienok:

- certifikát nie je počas doby jeho platnosti vypovedaný,
- Podpisovateľ alebo oprávnená osoba vyhlasuje, že v jeho aktuálnom certifikáte nedošlo k zmene certifikovaných údajov,
- žiadosť o obnovenie zdokonaleného certifikátu sa podáva do 30 dní pred uplynutím doby platnosti certifikátu,
- dôsledne vykonáva identifikáciu a overenie používateľa ako aj dodržuje lehoty uvedené pri obnove.

Vo všetkých prípadoch, keď dôjde k zmene certifikovaných údajov pre Podpisovateľa alebo oprávnenú osobu aktuálneho certifikátu, tento nie je obnoviteľný a brainit.sk vydá nový ZdC.

Žiadosť o obnovenie zdokonaleného certifikátu musí obsahovať minimálne:

- jedinečné meno Podpisovateľa alebo oprávnenej osoby,
- typ/označenie ZdC,
- identifikátor autentizačnej politiky certifikačnej politiky AdES, na základe ktorej je certifikát vydaný.

Niektoré alebo všetky údaje obsiahnuté v žiadosti o obnovenie ZdC môžu byť overené pomocou elektronického podpisu/pečate za podmienky, že účastník má v danom čase platný súkromný kľúč na vytvorenie podpisu/pečate. Poskytovateľ neumožňuje zmenu profilu certifikátov elektronického podpisu/pečate.

4.2.1 Vydanie následného certifikátu

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

4.2.2 Podmienky vydania následného certifikátu

Žiadne ustanovenia.

4.2.3 Kto môže požiadať o vydanie následného certifikátu

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

4.2.4 Spracovanie požiadaviek o vydanie následného certifikátu

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

4.2.5 Oznámenie o vydaní následného certifikátu

Poskytovateľ musí vhodným spôsobom informovať Držiteľa o vydaní následného ZdC.

4.3 Vydanie zdokonaleného certifikátu

Podrobný postup je popísaný v dokumente CPS tejto politiky.

Podanie žiadosti o zdokonalený certifikát je proces, pri ktorom Používateľ podá žiadosť o vydanie zdokonaleného certifikátu RA Poskytovateľa v písomnej alebo elektronickej forme v rámci politiky vydávania príslušného certifikátu. Žiadosť môže podať Podpisovateľ alebo splnomocnený zástupca.

Používateľ zaregistruje žiadosť o vydanie zdokonaleného certifikátu online alebo prostredníctvom operátora na RA Poskytovateľa. V režime online sa požiadavky odosielajú prostredníctvom sieťových protokolov, ako sú HTTP/HTTPS, S/MIME alebo TCP/IP.

4.3.1 Kto môže podať žiadosť o vydanie ZdC

Poskytovateľa môže požiadať o vydanie ZdC:

- **ZdC pre pokročilý elektronický podpis**
    - fyzická osoba resp. fyzická osoba splnomocnená Držiteľom alebo osoba, ktorá koná v jej mene na základe zákona alebo rozhodnutia príslušného orgánu
- **ZdC pre pokročilú elektronickú pečať**
    - akákoľvek entita (Zákazník), ktorá v zmysle platnej národnej legislatívy má oprávnenia konať v mene danej právnickej osoby

4.3.2 Proces registrácie a zodpovednosti

Zákazník musí vykonať nasledovné kroky ako prípravu na návštevu alebo online stretnutie s Poskytovateľom, ak je stretnutie potrebné:

- oboznámiť sa so Všeobecnými podmienkami poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov brainit.sk, s.r.o. (ďalej len „Všeobecné podmienky“) a Informáciou o spracúvaní osobných údajov, ktoré musia byť v čitateľnej podobe dostupné prostredníctvo trvalého komunikačného kanálu (pozri zone.nfqes.com),
- oboznámiť sa s týmto postupom, prípadne s princípmi a návodmi na získanie ZdC,
- pripraviť si hodnoty jednotlivých položiek žiadosti o ZdC tak, aby tieto hodnoty boli v súlade s touto CP,
- pripraviť si zvolené doklady totožnosti resp. iné potrebné doklady,
- V prípade registrácie pomocou RA, dohodnúť si termín návštevy.

4.3.3 Postup pred vydaním ZdC osobne

Pred vydaním ZdC zamestnanec zastupujúci Poskytovateľa musí:

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

4.3.4 Generovanie žiadosti o ZdC

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

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

Žiadosť o registráciu používateľov zdokonalených certifikačných služieb predkladajú na RA fyzické, právnické alebo oprávnené osoby a obsahuje tieto údaje:

- celé meno Podpisovateľa alebo oprávnenej osoby,
- doklad o zastupiteľskej moci Podpisovateľa nad autorom a oprávnenej osoby autora,
- identifikátor UIC (Unique Identification Code),
- poštová adresa osoby (krajina, okres, PSČ, mesto alebo obec, číslo budovy, názov ulice),
- emailová adresa,
- typ požadovaného zdokonaleného certifikátu s prihliadnutím na jeho označenie,
- identifikátor autentizačnej politiky, na základe ktorej je certifikát vydaný,
- prítomnosť súkromného kľúča zodpovedajúceho verejnému kľúču,
- verejný kľúč,
- dodatočné informácie, ktoré sa môžu zahrnúť do certifikátu,
- podpísané zmluvy o zdokonalených certifikačných službách a súhlas s podmienkami zásad a postupov poskytovania zdokonalených certifikačných služieb spoločnosťou brainit.sk.

V závislosti od obsahu certifikátu a jeho typu môžu niektoré z vyššie uvedených údajov chýbať.

Ak je pár kryptografických kľúčov vygenerovaný Podpisovateľom, RA skontroluje podanú žiadosť o elektronickú registráciu a požiadavky na úroveň bezpečnosti zariadenia na vytváranie bezpečného podpisu. Po úspešnej identifikácii, overení totožnosti osoby žiadajúcej o zdokonalený certifikát a po obdržaní potvrdenia RA sa žiadosť o registráciu odošle CA na vydanie certifikátu.

4.3.5 Odoslanie žiadosti o certifikát

Žiadosť môže byť odoslaná technologicky prepojením dvoch systémov, pokiaľ je prepojenie, autorizácia a identifikácia Držiteľov dostatočná a pokiaľ s tým Poskytovateľ súhlasí, prípadne pomocou aplikácie Poskytovateľa.

V prípade použitia aplikácie Poskytovateľa je pracovníkovi RA sprístupnená až po autorizácií pomocou mena, hesla a druhého faktoru, pričom potvrdzovanie žiadosti a následné spracovanie

požiadavky je tak isto potvrdzované vynútenou autorizáciou pracovníkom RA. Po spracovaní žiadosti v aplikácií zone.nfqes.com sú následne všetky oprávnenia presunuté na osobu, pre ktorú sa ZdC vydáva, pričom sú dodržané všetky ustanovenia platné pre aktivačné údaje.

4.3.6 Spracovanie žiadosti o certifikát

4.3.6.1 Spracovanie používateľských certifikátov

Podpísaním zmluvy o certifikačných službách prípadne akceptáciou žiadostí o vydanie ZdC všetci používatelia ZdC akceptujú záväzky a záruky v nej uvedené, ako aj túto politiku. Každý používateľ ZdC prechádza registračným procesom, ktorý zahŕňa nasledujúce kroky:

- podanie žiadosti o zdokonalený certifikát, ktorý obsahuje pravdivé a presné údaje. Žiadosť môže obsahovať dodatočné, neoveriteľné informácie, z ktorých časť je certifikovaná a iná časť uľahčuje kontakt medzi spoločnosťou brainit.sk a Podpisovateľom,
- vygenerovanie kryptografického párového kľúča spoločnosťou brainit.sk alebo ho vykoná používateľ sám,
- elektronický formát žiadosti o vydanie zdokonaleného certifikátu s údajmi, ktoré má certifikát obsahovať, je štruktúra podpísaná súkromným kľúčom vygenerovaného párového kľúča na zariadení na vytvorenie bezpečného podpisu/pečate,
- v prípade potreby predloží RA Podpisovateľovi alebo ním poverenej osobe v chránenej forme informácie/kód na prístup k súkromnému kľúču na zabezpečenom zariadení na vytvorenie podpisu/pečate,
- v prípade diaľkového generovania párového kľúča užívateľom, používateľ poskytne verejný kľúč spoločnosti brainit.sk prostredníctvom RA a preukáže vlastníctvo zodpovedajúceho súkromného kľúča zodpovedajúceho verejnému kľúču,
- na základe schválených žiadostí o vydanie a správu zdokonaleného certifikátu je podpísaná zmluva so spoločnosťou brainit.sk.

4.3.6.2 Certifikáty Registračnej a Certifikačnej Autority

RA poskytujúce zdokonalené služby, ktoré nie sú v organizačnej štruktúre brainit.sk (externá RA), sú povinné pred vykonaním tejto činnosti uzatvoriť príslušnú zmluvu so spoločnosťou brainit.sk. V zmluve by okrem práv a povinností oboch zmluvných strán mala byť uvedená aj totožnosť osôb zúčastnených v RA a ich oprávnenie zastupovať obe zmluvné strany pri plnení zmluvy. Osoby oprávnené vykonávať túto činnosť definujú pred vydaním certifikátov typ a označenie.

Kľúče a certifikáty CA je možné generovať iba počas procesu generovania kľúčov, na ktorom sa podieľajú iba osoby oprávnené spoločnosťou brainit.sk.

4.3.6.3 Vykonávanie identifikačných a autentifikačných funkcií

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

Po vykonaní autentifikácie a identifikácie Držiteľa ZdC a zapísaní požadovaných osobných údajov do systému Poskytovateľa musí pracovník RA vykonať zadanie údajov žiadosti o ZdC a v prípade použitia vopred zaslanej elektronickej žiadosti zabezpečiť správnosť údajov v systéme.

4.3.6.4 Schválenie alebo zamietnutie žiadostí o certifikát

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

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

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

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

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

Poskytovateľ musí vhodným spôsobom informovať Držiteľa o vydaní ZdC.

4.3.6.5 Čas na vybavenie žiadosti o certifikát

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

4.3.7 Akcie CA počas vydávania certifikátu

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

- bola odoslaná oprávnenou RA,
- zodpovedá štandardu PKCS#10.

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

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

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

Poskytovateľ môže na žiadosť Zákazníka vyhotoviť v produkčnom prostredí ZdC 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 ZdC musia byť splnené všetky požiadavky tejto CP týkajúce sa overenia identity Držiteľa ZdC.

4.3.8 Oznámenie CA žiadateľovi o vydaní certifikátu

Poskytovateľ musí vhodným spôsobom informovať Držiteľa o vydaní ZdC.

4.3.9 Prevzatie certifikátu

4.3.9.1 Správanie, ktoré predstavuje prijatie certifikátu

Poskytovateľ musí bezpečným spôsobom odovzdať vydaný certifikát jeho Držiteľovi.

4.3.9.2 Zverejnenie certifikátu

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

4.3.9.3 Oznámenie o vydaní certifikátu CA ostatným subjektom

Žiadne ustanovenia

4.4 Zmena zdokonaleného certifikátu

Zmena ZdC znamená zmenu obsahu údajov v predtým vydanom a publikovanom certifikáte pokročilého elektronického podpisu/pečate. Po zmene ZdC je potrebné vygenerovať nový pár kľúčov.

Pri zmene ZdC sa zaobchádza rovnako ako s vydaním nového ZdC, pričom je nutné dodržať všetky definované postupy vydávania nového ZdC.

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

4.5 Pozastavenie a ukončenie zdokonaleného certifikátu

Podrobný postup je popísaný v dokumente CPS tejto politiky.

4.5.1 Okolnosti ukončenia zdokonaleného certifikátu

Poskytovateľ ukončí ZdC, ktorý vydal, keď sa väzba medzi Podpisovateľom a jeho verejným kľúčom v certifikáte už nepovažuje za platnú. Poskytovateľ je povinný zrušiť ZdC, ktorý spravuje, v týchto prípadoch:

- v prípade, že sa informácie uvedené v certifikáte zmenili a stali sa neaktuálnymi,
- ak existuje podozrenie, že súkromný kľúč spojený s verejným kľúčom obsiahnutým v certifikáte je ohrozený,
- používateľ sa rozhodne ukončiť zmluvu so spoločnosťou brainit.sk,
- dozvie sa, že Držiteľ ZdC zomrel, ak ide o FO resp. ak ide o PO zanikol,
- ukončením zastupiteľskej právomoci Podpisovateľa voči Tvorcovi,
- o zrušenie certifikátu požiada Držiteľ ZdC,
- zistením, že pri vydaní ZdC neboli splnené požiadavky naraidenia eIDAS, resp. zákona č. 272/2016 Z.z,
- zistením, že ZdC bol vydaný na základe nepravdivých údajov,
- zistí, že došlo ku kompromitácii súkromného kľúča patriaceho k danému ZdC, napr. ak prístup k súkromnému kľúču patriacemu k verejnému kľúču uvedenému v ZdC pozná iná osoba, než Držiteľ uvedený v ZdC,
- zrušenie ZdC nariadi Poskytovateľovi svojím rozhodnutím súd,
- Držiteľ porušil svoje povinnosti stanovené touto CP a/alebo Všeobecnými podmienkami,
- dozvie sa, že sa Držiteľ stal nesvojprávnym na základe rozhodnutia súdu,
- došlo ku kompromitácii súkromného kľúča Poskytovateľa,
- v prípade, že CA ukončí svoju činnosť,

- v prípade, že používateľ dlhuje neuhradené poplatky za poskytovanie zdokonalených certifikačných služieb.

4.5.2 Postup ukončenia zdokonaleného certifikátu

Podrobný postup je popísaný v dokumente CPS tejto politiky.

Procesu ukončenia zdokonaleného certifikátu predchádza zaslanie žiadosti o ukončenie certifikátu. Žiadosť o ukončenie platnosti ZdC podáva Podpisovateľ alebo oprávnená osoba na mieste na RA alebo elektronicky na diaľku. V čase ukončenia platnosti ZdC RA informuje užívateľa o tejto skutočnosti (napríklad e-mailom).

Poskytovateľ okamžite ukončí prevádzku platného certifikátu vydaného za každej z vyššie uvedených okolností. Poskytovateľ zruší vydané certifikáty, ak ukončí svoju činnosť bez toho, aby ich previedol na iného poskytovateľa. V takom prípade to oznámi svojim používateľom a ukončí certifikáty s mesačnou výpovednou lehotou. Do jedného mesiaca od oznámenia spoločnosť brainit.sk vráti sumu zaplatenú používateľom vo výške zodpovedajúcej zostávajúcej dobe platnosti zmluvy o zdokonalenej certifikačnej službe. Poskytovateľ môže pozastaviť a ukončiť činnosť CA, ak existujú primerané dôvody na ohrozenie súkromného kľúča CA.

Zánikom certifikátu prevádzkovej CA na vydávanie a udržiavanie ZdC pre pokročilý elektronický podpis/pečať zaniká platnosť všetkých ňou vydaných a platných certifikátov. Tento certifikát môže zrušiť iba funkčná CA, ktorá vydala zdokonalený certifikát pokročilého elektronického podpisu/pečate. Ak k ukončeniu dôjde v dôsledku chyby operátora alebo v dôsledku ohrozenia prevádzkového súkromného kľúča brainit.sk, Poskytovateľ na vlastné náklady vydá ekvivalentný užívateľský certifikát.

Služby riadenia, ukončenia a pozastavenia sú k dispozícii 24 hodín denne, 7 dní v týždni. V prípade zlyhania systému, služieb alebo iných faktorov, ktoré sú mimo kontroly CA, spoločnosť brainit.sk vynaloží maximálne úsilie, aby zabezpečila dostupnosť služby do 3 (troch) hodín.

4.5.2.1 Kto môže požiadať o zrušenie certifikátu

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

O zrušenie certifikátu môže tiež požiadať:

- **Poskytovateľ** – daný zamestnanec je povinný zdokumentovať túto skutočnosť vrátane dôvodu svojho konania,
- **Subjekt** – (fyzická alebo právnická osoba) na základe dedičského konania (k dokumentom o zrušení ZdC musí Poskytovateľ priložiť kópiu dokladov, z ktorých vyplýva právo daného subjektu žiadať o zrušenie ZdC),
- **súd** prostredníctvom svojho rozsudku alebo predbežného opatrenia (k dokumentom o zrušení ZdC musí Poskytovateľ priložiť kópiu príslušného súdneho rozhodnutia),
- **súdom poverená osoba**, napr. poručník subjektu ZdC, ktorý sa má zrušiť (k dokumentom o zrušení ZdC musí Poskytovateľ priložiť kópiu príslušného súdneho rozhodnutia).

4.5.2.2 Postup pri žiadosti o zrušenie certifikátu

O zrušenie ZdC musí požiadať oprávnená osoba osobne u Poskytovateľa alebo technologicky na diaľku. Osoba, požadujúca zrušenie ZdC sa musí u Poskytovateľa podrobiť rovnakému procesu autentizácie, aký je požadovaný pri prvotnej registrácii Držiteľa/Zákazníka (pozri odstavec 3.2), alebo sa musí preukázať dohodnutým heslom na zrušenie ZdC, ktoré Držiteľ/Zákazník môže dostať po vydaní ZdC alebo musí žiadosť prísť z dôveryhodného systému, ktorému Prevádzkovateľ dôveruje.

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

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

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

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

V prípade oprávnenej žiadosti o zrušenie ZdC a úspešnom overení identity Držiteľa/Zákazníka sa musí ZdC čo najskôr zrušiť.

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

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

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

4.5.2.3 Čas na podanie žiadosti o zrušenie ZdC

V prípade hrozby kompromitácie súkromného kľúča musí oprávnená osoba podať čo najskôr žiadosť o zrušenie ZdC. Osobne je možné žiadať o zrušenie len počas doby určenej RA. Pri elektronickej žiadosti je túto možné zaslať na internú RA kedykoľvek.

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

Poskytovateľ musí:

- zrušiť ZdC bezodkladne najneskôr do 24 hodín od overenia skutočností, že predmetná žiadosť o zrušenie certifikátu je oprávnená,

- zverejňovať aktuálny zoznam zrušených ZdC a všetky predchádzajúce zoznamy zrušených certifikátov, tak aby boli prístupné Zákazníkom/Držiteľom a všetkým spoliehajúcim sa stranám,
- informovať Zákazníka/Držiteľa ZdC o zrušení jeho ZdC, zaslaním e-mailu na e-mailovú adresu, ktorú poskytol Držiteľ v priebehu registrácie na RA, pričom musí uviesť aj informáciu o dôvode zrušenia daného ZdC,
- 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.

4.5.2.5 Požiadavka na kontrolu zrušenia pre spoliehajúce sa strany

Spoliehajúca sa strana je povinná pri spoľahnutí sa na ZdC overiť si jeho platnosť prostredníctvom dostupného CRL resp. prostredníctvom služby OCSP.

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

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

4.5.2.6 Frekvencia vydávania CRL

Poskytovateľ, pokiaľ je to možné, okamžite zverejní CRL vždy, keď bude platný certifikát vydaný touto CA zrušený.

Požiadavky na frekvenciu vydávania CRL sú nasledovné:

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

4.5.2.7 Maximálna latencia pre CRL

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

Poskytovateľ musí zabezpečiť aby každý CRL bol zverejnený bezodkladne po jeho vytvorení, najneskôr však do 60 minút (1 hodina) od zaradenia nového certifikátu do CRL.

4.5.2.8 Dostupnosť OCSP služby

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

4.5.2.9 Požiadavky na kontrolu OCSP

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

4.5.2.10 Iné formy dostupnosti informácií o zrušení certifikátu

Overenie aktuálneho stavu certifikátu je možné vykonať manuálne prostredníctvom:

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

4.5.2.11 Špeciálne požiadavky na zmenu kľúčov po ich kompromitácií

V prípade porušenia zabezpečenia privátneho kľúča (jeho zverejnenia) zo strany CA alebo iných subjektov pôsobiacich v rámci Poskytovateľa, bude Poskytovateľ bezodkladne informovať spoliehajúce sa strany.

4.5.2.12 Okolnosti, pri ktorých dochádza k pozastaveniu platnosti ZdC

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

4.5.2.13 Kto môže požiadať o pozastavenie ZdC

Žiadne ustanovenia.

4.6 Služby súvisiace so stavom certifikátu

4.6.1 Prevádzkové požiadavky

Zoznam zrušených certifikátov musí byť dostupný na URL adrese Poskytovateľa a musí byť prístupný prostredníctvom HTTP protokolu na porte 80.

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

4.6.2 Dostupnosť služby

Dostupnosť služieb je v režime 24/7 v úrovni SLA 95%.

4.6.3 Koniec poskytovania služieb

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

5. FYZICKÉ, PERSONÁLNE A PREVÁDZKOVÉ BEZPEČNOSTNÉ OPATRENIA

Táto časť politiky popisuje všeobecné požiadavky týkajúce sa kontroly fyzickej a organizačnej bezpečnosti, ako aj personálnych operácií používaných v spoločnosti brainit.sk. Preveruje bezpečnostné požiadavky a postupy v čase generovania kľúčov, pri identifikácii a overovaní identity zákazníkov, pri vydávaní zdokonalených certifikátov a ich správe, pri audite a archivácií.

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

Opatrenia prijaté s ohľadom na fyzickú bezpečnosť Poskytovateľa sú súčasťou informačného bezpečnostného systému Poskytovateľa, ktorý spĺňa požiadavky ISO/IEC 27001, ISO 9001, ISO 22301.

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

Poskytovateľ musí:

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

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

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

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

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

5.1 Fyzická bezpečnosť

Opatrenia týkajúce sa fyzickej ochrany informačných údajov, technologických systémov, priestorov a súvisiacich podporných systémov sú navrhnuté tak, aby zabránili narušeniu:

- Poskytovateľ kontroluje fyzický prístup k objektom, ktorých bezpečnosť je nevyhnutná pre poskytovanie dôveryhodných služieb a minimalizuje akékoľvek riziká spojené s fyzickou bezpečnosťou. Bezpečnosť systémov na vydávanie a správu certifikátov je v súlade s požiadavkami medzinárodných noriem a odporúčaní,
- Fyzický prístup ku komponentom systému Poskytovateľa, ktorých bezpečnosť je nevyhnutná pre poskytovanie dôveryhodných služieb, je obmedzený len na oprávnené osoby. Kritickosť komponentov sa identifikuje hodnotením rizika. Fyzická integrita je

zabezpečená vzhľadom na zariadenia umiestnené v chránených a izolovaných priestoroch. Zavedená je dvojfaktorová kontrola prístupu a 24/7 fyzická ostraha. Nie je povolený žiadny fyzický prístup ku kritickému zariadeniu na viac ako 30 minút na návštevu. Ku skrini zariadenia nesmú mať prístup viac ako 2 oprávnení technickí pracovníci Poskytovateľa. Akýkoľvek prístup do priestorov s kritickou infraštruktúrou je dokumentovaný a vedený v zápisoch,

- Kontrola sa uplatňuje za účelom predchádzania stratám, škodám alebo ohrozeniu majetku a prerušeniu obchodnej činnosti. Oprávnené osoby z radov zamestnancov Poskytovateľa prísne dodržiavajú interné postupy pre prístup do rôznych zón s obmedzeným fyzickým prístupom,
- Kontrola sa uplatňuje s cieľom zabrániť ohrozeniu údajov alebo krádeži nástrojov na spracovanie informácií. Fyzická bezpečnosť priestorov, v ktorých je umiestnená základná infraštruktúra, je zabezpečená ich masívnou stabilnou konštrukciou so silnými dverami a kľúčovými zámkami,
- Poskytovateľ konfiguruje svoje systémy odstránením alebo deaktiváciou všetkých účtov, aplikácií, služieb, protokolov a portov, ktoré nepoužíva pri svojej činnosti,
- Poskytovateľ poskytuje prístup do chránených oblastí a oblastí s vysokou bezpečnosťou iba dôveryhodným rolám,
- Systém ACA Poskytovateľa sa nachádza v zóne s vysokým stupňom zabezpečenia. Základná CA Poskytovateľa sa nachádza v certifikovanom dátovom centre.

Spoločnosť brainit.sk poskytuje fyzickú ochranu a kontrolu prístupu do priestorov, kde sú v infraštruktúre nainštalované kritické komponenty:

- Kvalifikovaná Root CA - CA Signing Certificate
- Kvalifikovaná prevádzková CA – NFQES ACA,
- Kvalifikovaná OCSP služba na overenie stavu certifikátov vydaných základnou a prevádzkovou autoritou (OSCP service) - CA OCSP Signing Certificate,
- Kvalifikovaná TSA pre certifikáciu času – NFQES TSA,
- Registre a webová stránka poskytovateľa,
- Registračné autority,

Infraštruktúra Poskytovateľa je fyzicky a logicky oddelená a nepoužíva sa na iné aktivity realizované spoločnosťou brainit.sk.

5.1.1 Priestory

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

5.1.2 Fyzický prístup

Fyzická bezpečnosť systémov vydávania certifikátov a riadenia je v súlade s požiadavkami medzinárodných noriem a odporúčaní.

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

5.1.3 Napájanie a klimatizácia

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

5.1.4 Ochrana pred vodou

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

5.1.5 Prevencia a ochrana proti požiaru

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

5.1.6 Úložisko médií

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

5.1.7 Likvidácia odpadu

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

5.1.8 Zálohovanie mimo hlavnú lokalitu

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

5.2 Procedurálne bezpečnostné opatrenia – organizačná kontrola

Všetky bezpečnostné postupy pre vydávanie, správu a používanie ZdC pre pokročilý elektronický podpis/pečať vykonáva dôveryhodný personál Poskytovateľa.

Brainit.sk má dostatočný počet kvalifikovaných zamestnancov, ktorí sú schopní v každom okamihu svojou činnosťou zabezpečiť dodržiavanie platnej legislatívy, interných pravidiel spoločnosti a nariadení.

5.2.1 Dôveryhodné roly

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

Poskytovateľ má podrobné definované rozdelené funkcie a zodpovednosti zamestnancov (*Interné dokumenty Poskytovateľa: popis práce, plán pracovných miest a príslušné interné dokumenty*).

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

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

Prideľovanie funkcií sa vykonáva, aby sa minimalizovalo riziko kompromitácie, úniku dôveryhodných informácií alebo vzniku konfliktu záujmov.

5.2.2 Počet osôb požadovaných pre úlohu

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

5.2.3 Identifikácia a autentifikácia pre každú rolu

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

5.2.4 Role vyžadujúce rozdelenie zodpovednosti

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

5.3 Personálne bezpečnostné opatrenia

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

Personál Poskytovateľa pozostáva z dostatočného počtu vysokokvalifikovaných zamestnancov. Dôveryhodné osoby majú potrebné odborné vzdelanie a skúsenosti na zabezpečenie týchto bezpečnostných požiadaviek a štandardov hodnotenia technickej bezpečnosti. Disponujú znalosťou informačných systémov, kryptografie a PKI, aby mohli riadne vykonávať svoje povinnosti.

5.3.1 Požiadavky na kvalifikáciu, skúsenosti a previerky

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

Osoby v manažérskych funkciách musia:

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

5.3.2 Požiadavky previerky

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

5.3.3 Požiadavky na školenie

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

5.3.4 Frekvencia obnovy školení

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

5.3.5 Frekvencia rotácie rolí

Žiadne ustanovenia.

5.3.6 Sankcie za neoprávnené konanie

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

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

5.3.7 Požiadavky na externých dodávateľov

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

5.3.8 Dokumentácia poskytnutá zamestnancom

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

5.4 Postupy získavania auditných záznamov

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

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

Pre efektívne riadenie a prevádzku Poskytovateľa sa zaznamenávajú všetky udalosti, ktoré majú významný vplyv na bezpečnosť a spoľahlivosť technologického systému, personálu a používateľskú kontrolu a bezpečnostný dopad poskytovaných zdokonalených certifikačných služieb.

Informácie v elektronickom denníku sa generujú automaticky a záznamy zaznamenaných udalostí sú uložené v súboroch na systémovom disku minimálne do času ukončenia nasledovného pravidelného externého auditu.

Poskytovateľ klasifikuje a vedie registre všetkých aktív v súlade s ISO/IEC 27001. Podľa Bezpečnostnej politiky brainit.sk sa vykonáva analýza na posúdenie zraniteľnosti všetkých interných postupov, aplikácií a informačných systémov. Analytické požiadavky môže určiť aj externá inštitúcia oprávnená vykonávať audit Poskytovateľa. Analýza rizík sa vykonáva aspoň raz ročne.

5.4.1 Typy zaznamenaných udalostí

Poskytovateľ musí zaznamenávať a vyhodnocovať nasledovné dôležité udalosti:

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

5.4.2 Frekvencia spracovania auditných záznamov

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

5.4.3 Lehota uchovania protokolu auditu

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

5.4.4 Ochrana protokolu auditu

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

5.4.5 Postupy zálohovania protokolu auditu

Žiadne ustanovenia.

5.4.6 Systém zhromažďovania auditov (interný vs. externý)

Žiadne ustanovenia.

5.4.7 Oznámenie subjektu iniciujúceho auditu

Žiadne ustanovenia.

5.4.8 Posúdenie zraniteľnosti

Pozri bod 5.4.2.

5.5 Archív záznamov

Informácie o významných udalostiach sú pravidelne archivované v elektronickej podobe. Poskytovateľ zálohuje všetky údaje a súbory týkajúce sa: registračných informácií, bezpečnosť systému, všetky žiadosti predložené používateľmi, všetky informácie o používateľovi, všetky kľúče používané certifikačnými autoritami a registračnou autoritou, celú korešpondenciu medzi Poskytovateľom a Používateľmi. Všetky dokumenty a údaje používané v procese overovania totožnosti podliehajú archivácii.

Poskytovateľ uchováva záznam vo formáte umožňujúcom reprodukciu a obnovu.

5.5.1 Typy archivovaných záznamov

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

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

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

5.5.2 Lehota uchovania pre archív

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

5.5.3 Ochrana archívu

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

5.5.4 Postupy zálohovania archívu

Možnosť úplného obnovenia záloh (napr. po zlyhaní systému) je nevyhnutná pre správne fungovanie Poskytovateľa.

Podrobné postupy archivácie, vytvárania kópií a obnovy systému po nehodách sú popísané v internej dokumentácii Poskytovateľa, pričom táto dokumentácia je dostupná len oprávneným pracovníkom.

5.5.5 Požiadavky na časovú pečiatku záznamov

Archívne záznamy sú zabezpečené časovou pečiatkou ich vzniku.

5.5.6 Archivačný systém

Systém zberu archívnych údajov je interným systémom Poskytovateľa. Výnimkou z tohto pravidla sú archívy zhromažďované RA. Archívne informácie (na papieri a na elektronických médiách) sú riadne uložené a podliehajú fyzickej bezpečnosti vysokého stupňa ochrany.

5.5.7 Postupy na získanie a overenie archívnych informácií

Prístup do archívu je možný len pre oprávnené osoby. Údaje sa pravidelne kontrolujú a porovnávajú s pôvodnými údajmi, aby sa overila integrita archivovaných informácií. Na túto činnosť dohliada bezpečnostný správca. Ak sa zistia poškodenia alebo úpravy pôvodných údajov, škody sa čo najrýchlejšie odstránia v súlade s internými postupmi a pravidlami Poskytovateľa.

5.6 Zmena kľúča

Celý proces musí prebehnúť bez negatívneho vplyvu na úroveň zabezpečenia.

K zmene kľúčov Poskytovateľa môže dôjsť z nasledovných dôvodov:

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

Poskytovateľa. Bezodkladne tiež musí zrušiť kompromitovaný certifikát, ako aj všetky platné ZdC podpísané kompromitovaným kľúčom. Poskytovateľ musí upozorniť prostredníctvom svojho webového sídla Držiteľov ZdC, 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.

Poskytovateľ môže zmeniť kľúč zodpovedajúci vydanému certifikátu iba vydaním nového certifikátu alebo obnovením aktuálneho certifikátu.

Súkromný kľúč certifikačnej autority je možné zmeniť v prípade:

- uplynutia platnosti sprievodného certifikátu,
- zavedením nových služieb zo strany Poskytovateľa, ktoré so sebou prinášajú zmeny v charakteristikách súkromného kľúča (napríklad zmeny týkajúce sa bezpečnosti a požiadavka na nové použiteľné kryptografické kombinácie).
- v prípade zmeny súkromného kľúča CA Poskytovateľa sa dodržujú nasledujúce pravidlá:
    - CA, ktorej kľúčom sú užívateľské certifikáty podpísané a ktorej kľúč bude upravený, pozastaví vydávanie certifikátov 60 dní pred okamihom, kedy sa zostávajúca doba platnosti súkromného kľúča rovná dobe platnosti posledného vydaného certifikátu,
    - CA, ktorej súkromný kľúč podpisuje CRL a ktorej súkromný kľúč bude zmenený, pokračuje vo zverejňovaní zoznamov podpísaných starým súkromným kľúčom až do momentu uplynutia platnosti posledného zverejneného certifikátu.

5.7 Obnova po kompromitácií a katastrofe

5.7.1 Postupy pri riešení kompromitácie a katastrof

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

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

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

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

5.7.2 Výpočtové prostriedky, softvér alebo dáta sú poškodené

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

5.7.3 Postupy kompromitácie súkromného kľúča

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

5.7.4 Zachovanie kontinuity činnosti po katastrofe

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

5.8 Ukončenie činnosti CA alebo RA

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

Ešte pred ukončením poskytovania služieb Poskytovateľ musí:

- vhodným spôsobom, ak je to možné minimálne 6 mesiacov vopred, oznámiť plánované ukončenie svojej činnosti orgánu dohľadu, Držiteľom všetkých ňou vydaných platných ZdC, stranám spoliehajúcim sa na ZdC 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 ZdC, ak nezabezpečí kontinuitu v poskytovaní jeho služieb,
- pokúsiť sa uzavrieť zmluvu s iným kvalifikovaným poskytovateľom dôveryhodných služieb, ktorý by zabezpečil kontinuitu v poskytovaní jeho zdokonalených dôveryhodných služieb,
- sústrediť a archivovať všetky dokumenty Poskytovateľa,
- vykonať kontrolu dodržania predpisov o ochrane osobných údajov t. j. Nariadenie Európskeho Parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a zákon č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „Predpisy o ochrane osobných údajov“),
- vyradiť z používania všetky súkromné kľúče, vrátane ich kópií takým spôsobom, že nebude možné ich žiadnym spôsobom obnoviť.

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

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

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

6. TECHNICKÉ BEZPEČNOSTNÉ OPATRENIA

Táto časť popisuje postupy generovania a správy kryptografických kľúčov a súvisiace technické požiadavky. Poskytovateľ používa iba spoľahlivý a bezpečný hardvér a softvér, ktoré sú súčasťou počítačového systému Poskytovateľa. Počítačové systémy, v ktorých fungujú všetky kritické komponenty infraštruktúry sú vybavené a konfigurované nástrojmi na lokálnu ochranu prístupu k softvéru a informačným dátam. Poskytovateľ uplatňuje postupy riadenia informačnej bezpečnosti pre celú infraštruktúru spoločnosti brainit.sk v súlade so všeobecne uznávanými a medzinárodnými postupmi a štandardmi.

S cieľom zabezpečiť spoľahlivú prevádzku a bezpečnosť životného cyklu počítačových systémov Poskytovateľ vykonáva činnosti v súlade s nasledujúcimi požiadavkami:

- Pri vývoji nových systémov, Poskytovateľ vykonáva analýzu bezpečnostných požiadaviek už v štádiu návrhu a špecifikácie a tým garantuje integráciu bezpečnosti do IT systémov.
- Poskytovateľ uplatňuje bezpečnostnú politiku a postup kontroly zmien počas aktualizácií, úprav núdzového a operačného softvéru a zmien v konfigurácii.
- Postupy zahŕňajú zdokumentovanie zmien.
- Poskytovateľ chráni integritu systémov a informácií pred vírusmi, malvérom a neautorizovaným softvérom.
- Poskytovateľ vyvíja a aplikuje postupy pre všetky dôveryhodné a administratívne úlohy, ktoré majú vplyv na poskytovanie služieb.
- Poskytovateľ špecifikuje a uplatňuje postupy na zabezpečenie toho, aby:
    - všetky dostupné ochranné a funkčné aktualizácie softvéru sa aplikujú v primeranom čase po ich sprístupnení,
    - ochranné a funkčné aktualizácie sa neuplatňujú, ak je pravdepodobné, že prinesú ďalšie zraniteľné miesta alebo nestability, ktoré prevažujú nad výhodami ich uplatnenia,
    - je zdokumentované odôvodnenie odmietnutia aplikácie akýchkoľvek ochranných alebo funkčných aktualizácií.

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

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

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

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

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

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

6.1 Generovanie a inštalácia dvojice kľúčov

Páry kryptografických kľúčov pre prevádzkové certifikáty Poskytovateľa sa generujú a inštalujú podľa pokynov a postupov v dokumente CP alebo CPS.

Generovanie vykonávajú oprávnené osoby Poskytovateľa pri dodržaní požiadaviek minimálne duálnej kontroly. Na vytvorenie podpisu sa používa ochranný mechanizmus s bezpečnostným profilom vytvoreným v súlade s technickými špecifikáciami definujúcimi úrovne bezpečnosti.

Poskytovateľ používa svoje súkromné kľúče iba na účely svojej činnosti, a to nasledovne:

- podpisovať vydané prevádzkové certifikáty CA vo svojej infraštruktúre,
- podpisovať vydané a zverejnené CRL,
- podpisovať všetky vydané a zverejnené certifikáty elektronického podpisu/pečate používateľov.

Pár kryptografických kľúčov (súkromný a verejný) certifikátov elektronického podpisu/pečate vydaných v infraštruktúre Poskytovateľa sa generuje takto:

- podpisovateľ, s hardvérom a softvérom pod jeho kontrolou, ale schválený spoločnosťou brainit.sk,
- prevádzkovateľom RA Poskytovateľa s hardvérom a softvérom pod jeho kontrolou, ale schválený spoločnosťou brainit.sk,
- prevádzkovateľom RA Poskytovateľa s hardvérom a softvérom pod kontrolou infraštruktúry Poskytovateľa,
- spoločnosťou brainit.sk, keď sa o vydanie certifikátu žiada na diaľku, prostredníctvom aplikácie Poskytovateľa,

Podpisovateľ sa zaväzuje používať licencovaný softvér na prácu so zariadením na vytváranie elektronického podpisu/pečate.

6.1.1 Generovanie párov kľúčov

Kľúče Podpisovateľa ZdC pre pokročilý elektronický podpis/pečať sa generujú v bezpečnom prostredí, ako sa vyžaduje v nariadení (EÚ) č. 910/2014.

Ovládanie súkromného kľúča je prostredníctvom prístupového kódu. Podpisovateľ používa súkromný kľúč na vytvorenie podpisu/pečate zadaním kódu v zabezpečenom prostredí na vytvorenie zaručeného elektronického podpisu/pečate.

Keď je pár kľúčov vygenerovaný Podpisovateľom, brainit.sk odporúča, aby autor použil schválené prostredie v infraštruktúre Poskytovateľa na vytvorenie pokročilého elektronického podpisu/pečate alebo ekvivalentu, ktorý spĺňa požiadavky nariadenia (EÚ) č. 910/2014 a je kompatibilný s infraštruktúrou Poskytovateľa.

V prípadoch, keď je pár kľúčov vygenerovaný Signatárom alebo Tvorcom, tento nesie plnú zodpovednosť za ochranu súkromného kľúča s cieľom zabrániť jeho prezradeniu, zverejneniu, úprave, strate alebo neoprávnenému použitiu. Podpisovateľ je zodpovedný za opomenutie alebo konanie oprávnených osôb, ktoré sú oprávnené vytvárať, uchovávať alebo uchovávať ich súkromné kľúče.

Podpisovateľ sa zaväzuje používať licencovaný softvér na prácu s prostredím na vytvorenie pokročilého elektronického podpisu/pečate.

Generovanie a inštalácia páru kľúčov Poskytovateľa sa musí vykonávať štandardizovaným spôsobom, ktorý je podrobne popísaný v dokumentácii Poskytovateľa. Spôsob generovania musí zabezpečiť dostatočnú dôveru v postupe generovania. Celý proces spôsobu generovania musí byť zaznamenaný. Generovanie kľúčov musí byť vykonané v bezpečnom zariadení na uchovávanie kryptografických kľúčov, ktoré spĺňa legislatívne požiadavky dané na takýto typ zariadenia.

Spoločnosť brainit.sk generuje páry kryptografických kľúčov v sídle spoločnosti a na operačných certifikačných autoritách pomocou HSM hardvérového bezpečnostného modulu na úrovni minimálne FIPS 140-2 level 2 alebo vyššej.

6.1.1.1 Požiadavky na životné prostredie pri tvorbe pokročilého elektronického podpisu/pečate

Prostredie na vytvorenie pokročilého elektronického podpisu/pečate musí vhodnými technickými a procedurálnymi prostriedkami zabezpečiť aspoň to, aby:

- bola primerane zaručená dôvernosť údajov na vytvorenie elektronického podpisu/pečate,
- údaje na vytvorenie elektronického podpisu/pečate boli prakticky splnené len raz,
- údaje o vytvorení elektronického podpisu/pečate sú dostatočne zabezpečené a nie je možné ich s istotou odvodiť a elektronický podpis je spoľahlivo chránený proti falšovaniu pomocou v súčasnosti dostupnej technológie,
- údaje na vyhotovenie elektronického podpisu/pečate musia byť spoľahlivo chránené oprávneným Podpisovateľom podpisu/pečate proti použitiu inými osobami.

Prostredie na vytváranie pokročilého elektronického podpisu/pečate nesmie meniť údaje, ktoré sa majú podpísať, ani brániť predloženiu takýchto údajov Podpisovateľovi pred podpisom.

Generovanie alebo správa údajov na vytvorenie elektronického podpisu/pečate v mene Podpisovateľa elektronického podpisu/pečate môže vykonávať iba Poskytovateľ.

6.1.1.2 Vzdialené generovanie dvojice kľúčov

Podpisovateľ používa špecializovaný softvér poskytovaný spoločnosťou brainit.sk, ktorý implementuje proces generovania a správy kryptografického páru kľúčov.

Generovanie, používanie a ukladanie súkromného kľúča má vysokú úroveň zabezpečenia, ktorá je zaručená prostredím, kde je vytvorený. Je bezpečne chránený a prístupný iba Podpisovateľovi alebo oprávnenému zástupcovi právneho subjektu.

Podpisovateľ alebo oprávnený zástupca PO vygeneruje elektronickú žiadosť o ZdC vo formáte PKCS# 10 a odošle ju Poskytovateľovi. Podľa odporúčaní RFC 2314 – PKCS# 10 elektronický formulár žiadosti obsahuje DN, verejný kľúč a ďalšie atribúty, z ktorých všetky atribúty sú podpísané súkromným kľúčom.

Ak sa vykoná vzdialené generovanie kľúčového páru na požiadanie, vygeneruje sa v spoľahlivom prostredí Poskytovateľa, ktoré spĺňa požiadavky a nariadenia pre prostredie pokročilého elektronického podpisu.

6.1.2 Doručenie súkromného kľúča predplatiteľovi

Neuplatňuje sa

6.1.3 Doručenie verejného kľúča vydavateľovi certifikátu

Neuplatňuje sa

6.1.4 Doručenie verejného kľúča CA spoliehajúcim sa stranám

Neuplatňuje sa

6.1.5 Veľkosti kľúčov

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

Dĺžka páru kľúčov pre pokročilý elektronický podpis/pečať vygenerovaného Zákazníkom cez infraštruktúru Poskytovateľa je aspoň 3072 bitov, s použiteľnou kombináciou asymetrických a hashovacích algoritmov: sha256-with-RSA. Bez ohľadu na to, kde sa generuje pár kľúčov pre certifikát pre pokročilý elektronický podpis/pečať, kľúč musí mať dĺžku aspoň 2048 bitov pre algoritmy RSA a DSA a 160 bitov pre algoritmy ECDSA.

6.1.6 Parametre verejného kľúča a kontrola kvality

Kvalitu a parametre verejných kľúčov Poskytovateľa musí určiť PMA. Stanovené parametre musia byť dodržiavané počas ceremónie generovania kľúčov. Poskytovateľ musí využívať na generovanie a uchovávanie kľúčov kryptografické hardvérové moduly spĺňajúce požiadavky FIPS 140-2 Level 2, ktoré zabezpečujú náhodné generovanie RSA kľúčov veľkosti minimálne 3072 bitov.

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

Podpisovateľ alebo autorizovaný zástupca právnickej osoby kľúčového páru je zodpovedný za overenie kvality vygenerovaných parametrov súkromného kľúča. Je potrebné overiť schopnosť kľúča šifrovať, dešifrovať a vytvárať elektronické podpisy.

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

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

6.2 Ochrana súkromného kľúča a návrh kryptografického modulu

Každý používateľ si vytvára a ukladá súkromný kľúč pomocou spoľahlivého systému pre svoju bezpečnosť. CA na požiadanie používateľa vygeneruje pár kľúčov a odošle ho, pričom používateľa upozorní na pravidlá jeho uchovávania a ochrany jeho súkromného kľúča.

6.2.1 Štandardy a kontroly kryptografického modulu

Súkromný kľúč Podpisovateľa alebo splnomocneného zástupcu právnickej osoby sa používa len v bezpečnom prostredí na vytvorenie pokročilého elektronického podpisu/pečate, ako sa vyžaduje v nariadení (EÚ) č. 910/2014.

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

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

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

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

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

6.2.3 Uloženie súkromného kľúča

Poskytovateľ žiadnym spôsobom neukladá ani nearchivuje súkromný kľúč používateľa na vytvorenie elektronického podpisu/pečate.

Žiadne ustanovenia.

6.2.4 Záloha súkromného kľúča

Súkromné kľúče Poskytovateľa sú generované a uchovávané vo vnútri hardvérových kryptografických modulov. V prípade potreby ich prenosu pre proces zálohovania a obnovy, musia byť súkromné kľúče prenášané vždy v zašifrovanej podobe. Prenášanie súkromných kľúčov a ich obnova v inom hardvérovom kryptografickom module môže byť vykonaná len oprávnenými zamestnancami v zmysle pravidiel uvedených v bode 6.2.2.

6.2.5 Archív súkromného kľúča

Pozri 6.2.3

6.2.6 Prenos súkromného kľúča do alebo z kryptografického modulu

Pozri 6.2.4

6.2.7 Uloženie súkromného kľúča na kryptografickom module

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

6.2.8 Spôsob aktivácie súkromného kľúča

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

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

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

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

6.2.9 Spôsob deaktivácie súkromného kľúča

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

6.2.10 Spôsob zničenia súkromného kľúča

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

6.2.11 Hodnotenie kryptografického modulu

Pozri bod 6.2.1.

6.3 Ostatné aspekty správy párov kľúčov

6.3.1 Archív verejných kľúčov

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

Verejné kľúče Podpisovateľov alebo oprávnených zástupcov PO sú obsiahnuté v ZdC, ktoré im boli vydané a ktoré sú zverejnené v registri certifikátov na webovom sídle Používateľa.

6.3.2 Prevádzkové obdobia certifikátu a obdobia používania dvojice kľúčov

Doba používania verejných kľúčov je určená hodnotou poľa v certifikáte popisujúcom platnosť verejného kľúča. Platnosť certifikátov a ich príslušných súkromných kľúčov sa môže v prípade ukončenia platnosti certifikátov skrátiť.

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

Typ certifikátu	Platnosť (maximálne)
Vydávajúca CA	30 rokov
Vydávajúca ACA	8 rokov
ZdC pre koncového používateľa	3 roky

6.4 Aktivačné údaje

Pri prítomnosti Používateľa na RA (osobne alebo technologicky pomocou systému) sú aktivačné údaje súkromného kľúča primárne využívané prevádzkovateľom RA. Používatelia používajú autentifikáciu a riadia prístup k svojmu súkromnému kľúču.

V prípadoch keď Podpisovateľ alebo splnomocnený zástupca PO vygeneruje pár zdokonalených kľúčov certifikátu, sám vytvorí a spravuje aktivačné údaje.

6.4.1 Generovanie a inštalácia aktivačných údajov

Aktivačné údaje sa používajú pri prvotnom vydaní certifikátu v prostredí na vytvorenie pokročilého elektronického podpisu/pečate.

Prístupové kódy a odblokovanie prostredia na vytvorenie pokročilého elektronického podpisu/pečate sa poskytujú Podpisovateľovi alebo splnomocnenému zástupcovi PO v opečiatkovanej a nepriehľadnej papierovej obálke alebo v elektronickej forme alternatívnym kanálom.

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

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

6.4.2 Aktivácia ochrany údajov

Za ochranu súkromných prístupových údajov, mobilných aplikácií a PIN kódov ku tokenom Držiteľov sú zodpovední výhradne samotní Držitelia.

Kľúčový pár určený pre vydavateľa ZdC:

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

6.4.3 Ostatné aspekty aktivačných údajov

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

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

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

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

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

6.5 Počítačové bezpečnostné kontroly

Brainit.sk používa iba spoľahlivý a bezpečný hardvér a softvér, ktoré sú súčasťou počítačového systému Poskytovateľa.

Počítačové systémy, ktoré prevádzkujú všetky kritické komponenty infraštruktúry Poskytovateľa, sú vybavené a konfigurované prostriedkami lokálnej ochrany softvéru a prístupu k informáciám.

Poskytovateľ používa postupy na riadenie informačnej bezpečnosti celej svojej infraštruktúry so všeobecne uznávanými medzinárodnými štandardmi.

6.5.1 Špecifické technické požiadavky na počítačovú bezpečnosť

Poskytovateľ musí vykonávať všetky funkcie kvalifikovaného poskytovateľa dôveryhodných služieb za použitia dôveryhodného systému, ktorý spĺňa všetky bezpečnostné požiadavky pre poskytovanie dôveryhodných služieb.

Poskytovateľ vyhotovujúci ZdC sa môže riadiť pri poskytovaní svojich služieb požiadavkami na bezpečnosť informácií, ktoré sú kladené na dôveryhodného poskytovateľa služieb a sú definované v štandarde ETSI EN 319 411-2 " Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

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

6.5.2 Hodnotenie počítačovej bezpečnosti

Žiadne ustanovenia.

6.6 Opatrenia a zabezpečenie v životnom cykle

Všetky zmeny hardvéru sú monitorované a registrované autorizovaným personálom Poskytovateľa. Pri kúpe nového technického vybavenia, je dodávané s potrebnými prevádzkovými postupmi a návodom na použitie. Je zabezpečený dohľad nad funkčnosťou technologického systému a je zabezpečená jeho správna funkcia a v súlade s dodanou výrobnou konfiguráciou.

6.6.2 Kontroly vývoja systému

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

6.6.3 Kontroly riadenia bezpečnosti

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

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

6.6.4 Bezpečnostné opatrenia životného cyklu

Žiadne ustanovenia.

6.7 Ovládacie prvky zabezpečenia siete

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

Poskytovateľ využíva moderné technické prostriedky výmeny a ochrany informácií na zabezpečenie sieťovej bezpečnosti systémov pred vonkajšími zásahmi a hrozbami.

6.8 Časová pečiatka

Poskytovateľ používa vlastné kvalifikované časové pečiatky, ktoré majú štatút kvalifikovaného poskytovateľa dôveryhodných služieb a poskytujú kvalifikovanú dôveryhodnú službu vyhotovovania zdokonalenej elektronickej časovej pečiatky v zmysle ustanovení nariadenia (EU) č. 910/2014 (eIDAS). CERTIFIKÁT, CRL A PROCESY OCSP

6.9 Profil certifikátu

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

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

Profily zdokonalených certifikátov sú v súlade s formátom popísaným v štandarde X.509 verzie 3. Certifikát typu X.509 verzie 3 je súbor údajov, ktorý jednoznačne autentifikuje verejný kľúč pre autora pokročilého elektronického podpisu/pečate.

6.9.1 Čísla verzií

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

6.9.2 Parametre certifikátu

Verzia (Version)	V3 (hodnota 0x2)
Serial number (Sériové číslo)	Jedinečné číslo pridelené Poskytovateľom > 0
Issuer Signature Algorithm (Podpisový algoritmus vydávateľa)	sha256WithRSAEncryption (1 2 840 113549 1 1 11)
Issuer (Vydávateľ)	Jedinečné X.500 rozlišovacie meno Poskytovateľa

Valid from (Platný od)	Začiatok platnosti certifikátu (UTC čas)
Valid to (Platný do)	Koniec platnosti certifikátu (UTC čas)
Subject ()	Obsah jednotlivých položiek pre jednotlivé typy ZdC **C (countryName)** = **Krajina:** dvojznakový kód krajiny podľa ISO 3166 štátnej príslušnosti fyzickej osoby uvedený v poskytnutom doklade totožnosti. **CN (commonName)** = **Celé meno**: Celé meno fyzickej osoby latinkou podľa dokladu totožnosti. **G (givenName)** = **Krstné meno**: Meno fyzickej osoby latinkou podľa dokladu totožnosti. **S (surname)** = **Priezvisko**: Priezvisko fyzickej osoby latinkou podľa dokladu totožnosti. **SERIALNUMBER (serialNumber)** = Národný identifikátor fyzickej osoby podľa ETSI EN 319412-1, bod 5.1.3. Príklad: PNOSK-1234567890 *(rodné číslo)* **dateOfBirth** = Dátum narodenia vyjadrený vo formáte ZULU, napríklad: 19801220120000Z. **placeOfBirth*** = miesto narodenia **gender** = pohlavie fyzickej osoby **stateOrProvinceName*** = aktuálna adresa trvalého pobytu: názov regiónu, štátu alebo provincie **localityName*** = aktuálna adresa trvalého pobytu: názov mesta **streetAdress*** = aktuálna adresa trvalého pobytu: názov ulice, číslo, prípadne poschodie **telephoneNumber*** = číslo mobilného telefónu **emailAddress*** = emailová adresa **Title*** = Povolanie/pozícia/profesia **O** (organizationName)** = Meno právnickej osoby: celé meno/názov podľa osvedčenia o registrácii právnickej osoby, s ktorou je fyzická osoba spojená **organizationIdentifier** = identifikátor právnickej osoby podľa ETSI EN 319 412-2, bod 5.1.4. Príkald: NTRSK-123456789 (IČO)
Public key (verejný kľúč)	Verejný kľúč, na ktorý je vyhotovený certifikát (RSA, min. veľkosť 3072 bit)
Extensions (Rozšírenia)	Zoznam rozšírení v ZdC pozri Tabuľka č. 5

* - Polia označené hviezdičkou (*) nemusia byť v certifikáte uvedené

** - Polia označené dvomi hviezničkami(**) - atribúty právnickej osoby organizationName a organizationIdentifier sa vypĺňajú len v prípade, ak je fyzická osoba zástupcom právnickej osoby. Ak

nie sú vyplnené žiadne atribúty pre organizationName a organizationIdentifier, atribút identifikujúci prepojenie na právnickú osobu (id-etsi-qcs-SemanticId-Legal) bude nevyplnený.

6.9.3 Rozšírenie certifikátu

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

	Definuje účel použitia súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.		
extKeyUsage	{id-ce-extkeyUsage} 2.5.29.37 Definuje rozšírené použitie súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno v ZdC pre autentifikáciu webového sídla	Nie

6.9.4 Identifikátory objektov algoritmu

Algoritmus podpisu vyhotovovaných ZdC (Signature Algorithm)

sha256RSA OID: 1.2.840.113549.1.1.11

6.9.5 Formy mien

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

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

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

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

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

Dĺžky kľúčov a platnosť ZdC: Verejný kľúč

- RSA, dĺžka minimálne 3092 bitov
- EC, dĺžka minimálne 160 bitov

6.9.6 Obmedzenia týkajúce sa mien

Žiadne ustanovenia.

6.9.7 Identifikátor certifikačnej politiky

Pozri kapitolu 1.2

6.9.8 Použitie rozšírení na obmedzenie politiky

Toto rozšírenie nie je používané.

6.9.9 Syntax a sémantika politiky

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

6.9.10 Predĺženie

Žiadne ustanovenia.

6.10 Profil CRL

6.10.1 Čísla verzií

CRL vydávané Poskytovateľom musia byť CRL verzie 2.

CRL musia byť vydávané tou istou CA Poskytovateľa ako certifikát.

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

6.10.2 CRL a rozšírenia vstupu CRL

Rozšírenia vydávaného CRL

Názov rozšírenia	Vyžadované	Kritickosť
Authority Key Identifier (OID: 2.5.29.35)	ÁNO	NIE
CRL Number (OID: 2.5.29.20)	ÁNO	NIE
Issuing Distribution Point (OID: 2.5.29.28)	ÁNO	ÁNO
id-ce-expiredCertsOnCRL (OID: 2.5.29.60)	ÁNO	NIE

6.11 Profil OCSP

6.11.1 Čísla verzií

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

6.11.2 Rozšírenia OCSP

Rozšírenia v OCSP odpovedi

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

7. AUDIT SÚLADU A ĎALŠIE HODNOTENIA

Audity vykonávané Poskytovateľom sa týkajú spracovania informačných údajov a riadenia kľúčových postupov. Poskytovateľ vykonáva aspoň jeden interný audit ročne a je kontrolovaný najmenej raz za 24 mesiacov orgánom posudzovania zhody.

Účelom auditu je potvrdiť, že Poskytovateľ ako kvalifikovaný poskytovateľ certifikačných služieb spĺňa požiadavky stanovené v nariadení (EÚ) č. 910/2014, prípadne požiadavky stanovené v nariadení eIDAS.

7.1 Frekvencia alebo okolnosti posudzovania

Poskytovateľ sa musí aspoň každých 24 mesiacov podrobiť auditu ním poskytovaných zdokonalených dôveryhodných služieb orgánom na posudzovanie zhody.

7.2 Totožnosť / kvalifikácie posudzovateľa

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

7.3 Vzťah hodnotiteľa k hodnotenému subjektu

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

7.4 Témy, ktorých sa hodnotenie týka

Účelom auditu je potvrdiť, že Poskytovateľ ako zdokonalený poskytovateľ dôveryhodných služieb a zdokonalené dôveryhodné služby, ktoré poskytuje, spĺňajú požiadavky stanovené v nariadení (EÚ) č. 910/2014, prípadne požiadavky stanovené v nariadení eIDAS.

7.5 Opatrenia prijaté v dôsledku nedostatku

Správy o interných a externých auditoch sa zasielajú Poskytovateľovi. Na základe hodnotení uvedených v správe, PMA stanoví vhodné opatrenia a termíny na nápravu zistených medzier a nezrovnalostí. Zamestnanci Poskytovateľa podniknú konkrétne kroky na ich odstránenie v rámci stanovených lehôt.

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

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

7.6 Oznámenie výsledkov

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

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

8. OSTATNÉ OBCHODNÉ A PRÁVNE VECI

8.1 Poplatky

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

Poplatky za zdokonalené dôveryhodné služby poskytované Poskytovateľom uhrádza Zákazník, ak nie je s Poskytovateľom dohodnuté inak.

8.1.1 Poplatky za vydanie alebo predĺženie platnosti certifikátu

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

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

8.1.2 Poplatky za prístup k certifikátu

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

8.1.3 Poplatky za odvolanie alebo prístup k informáciám o stave

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

8.1.4 Poplatky za ďalšie služby

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

8.1.5 Pravidlá vrátenia peňazí

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

8.2 Finančná zodpovednosť

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

8.2.1 Poistné krytie

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

8.2.2 Ostatné aktíva

Žiadne ustanovenia.

8.2.3 Poistenie alebo záruka pre koncové subjekty

Žiadne ustanovenia.

8.3 Dôvernosť obchodných informácií

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

8.3.1 Rozsah dôverných informácií

Dôvernými informáciami podliehajúcimi zodpovedajúcej ochrane sú:

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

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

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

8.3.2 Informácie, ktoré nespadajú do rozsahu dôverných informácií

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

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

8.3.3 Zodpovednosť za ochranu dôverných informácií

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

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

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

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

8.4 Ochrana osobných údajov

Poskytovateľ prísne dodržiava požiadavky na dôvernosť a nešírenie osobných údajov Zákazníka/Držiteľa alebo splnomocnených zástupcov právnických osôb, s ktorými sa oboznámil ako poskytovateľ zdokonalených certifikačných služieb.

8.4.1 Plán ochrany osobných údajov

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

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

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

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

- vždy dostupná v elektronickej forme na webovom sídle Poskytovateľa,
- odosielaná v elektronickej forme na emailovú adresu Zákazníka/Držiteľa pred začatím poskytovania dôveryhodných služieb a
- dostupná v papierovej forme u Poskytovateľa.

8.4.2 Informácie považované za súkromné

Poskytovateľ považuje za súkromné akékoľvek osobné údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť nepriamo alebo priamo, najmä na

základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, psychickú, ekonomickú, fyziologickú, mentálnu, kultúrnu alebo sociálnu identitu.

8.4.3 Informácie, ktoré sa nepovažujú za súkromné

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

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

8.4.4 Zodpovednosť za ochranu súkromných informácií

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

8.4.5 Oznámenie a súhlas s použitím súkromných informácií

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

8.5 Práva duševného vlastníctva

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

Rôzne údaje zahrnuté v zdokonalených certifikátoch Poskytovateľa alebo zverejnené v registri/úložisku podliehajú právam duševného vlastníctva a iným vlastníckym a nemateriálnym právam.

Pár používateľských kľúčov a príslušný certifikát verejného kľúča vydaný Poskytovateľom, ako aj príslušný tajný materiál, sú vlastníctvom Poskytovateľa bez ohľadu na vlastníctvo fyzického prostredia, v ktorom sú kľúče uložené a chránené.

8.6 Vyhlásenia a záruky

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

8.6.1 Vyhlásenia a záruky CA

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

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

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

- dodržiavanie svojich povinností v zmysle tejto CP, vydaných CPS ako aj ďalších publikovaných postupov a politík, vrátane politiky informačnej bezpečnosti,
- plnenie svojich povinností v zmysle nariadenia (EÚ) 910/2014 a vnútroštátnymi predpismi pri výkone svojej činnosti ako kvalifikovaný poskytovateľ certifikačných služieb,
- plnenie svojich povinností v zmysle Nariadenia eIDAS a platnej legislatívy SR,
- okamžité informovanie dotknutých subjektov v prípade kompromitácie svojich súkromných kľúčov v súlade s touto CP,
- zavedenie bezpečnostných mechanizmov, vrátane mechanizmov pri generovaní a ochrane súkromného kľúča, týkajúcich sa ochrany svojej PKI infraštruktúry,
- dostupnosť tlačenej resp. elektronickej verzie tejto CP a ďalších publikovaných politík online,
- skutočnosť, že Držiteľ sa stáva resp. je vlastníkom súkromného kľúča v čase vyhotovovania zdokonaleného certifikátu v zmysle tejto CP,
- správnosť informácii nachádzajúcich sa vo vyhotovených zdokonalených certifikátoch podľa najlepšieho vedomia Poskytovateľa a súlad vydaných zdokonalených certifikátov s požiadavkami Nariadenia eIDAS,
- dodržiavanie Predpisov na ochranu osobných údajov pri zaobchádzaní s osobnými údajmi Držiteľov,
- vydávanie zdokonalených certifikátov pre elektronický podpis/pečať po overení informácií stanovenými zákonom,
- ukončenie alebo pozastavenie výkonu certifikátov za podmienok popísaných v tejto CP

8.6.2 Vyhlásenie a záruky RA

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

8.6.3 Vyhlásenia a záruky účastníkov

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

- generovanie kľúčového páru verejný kľúč/súkromný kľúč v prípade, že si kľúče k žiadosti na vydanie ZdC generuje vo vlastnej réžii,
- poskytnutie presných a správnych informácií v komunikácii s Poskytovateľom,
- oboznámenie sa a súhlas so všetkými podmienkami danými v tejto CP a s ňou spojenými politikami, ktoré sú dostupné v úložisku Poskytovateľa a na jeho webovom sídle (pozri kapitola 1),
- používanie vydaných ZdC len na právne účely a účely autorizácie v súlade s touto CP,
- ukončenie používania ZdC, 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 ZdC vydanom Poskytovateľom.

8.6.4 Vyhlásenia a záruky spoliehajúcich sa strán

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

8.6.5 Vyhlásenia a záruky ostatných účastníkov

Žiadne ustanovenia.

8.7 Zrieknutie sa záruk

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

8.8 Obmedzenia zodpovednosti

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

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

- porušenia povinností Držiteľom/Zákazníkom certifikátu alebo Spoliehajúcou sa stranou uvedených v všeobecne záväzných právnych predpisoch, príslušnej zmluve, Všeobecných podmienkach alebo v politikách Poskytovateľa, vrátane povinnosti vynaložiť primeranú starostlivosť pri používaní certifikátov a pri spoliehaní sa na certifikát;
- neposkytnutia potrebnej súčinnosti zo strany Držiteľa/Zákazníka certifikátu;
- technickými vlastnosťami, nekompatibilitou, konfiguráciou, nevhodnosťou alebo inými vadami nimi použitých softvérových alebo hardvérových prostriedkov;
- používania, resp. spoliehania sa na certifikát, ktorého platnosť uplynula alebo ktorý bol zrušený;
- použitia certifikátu Držiteľom/Zákazníkom certifikátu v rozpore so zmluvou, Všeobecnými podmienkami alebo politikami Poskytovateľa;
- že certifikát bol použitý v rozpore s jeho určením, účelom alebo obmedzeniami uvedenými v certifikáte, v týchto Všeobecných podmienkach resp. v politikách Poskytovateľa;
- nedoručenia alebo omeškania požiadaviek na overenie statusu certifikátu Poskytovateľovi, z dôvodov, ktoré nie sú na strane Poskytovateľa (najmä prípady nedostupnosti alebo preťaženosti siete internet alebo vady zariadenia alebo technického vybavenia používaného overovateľom);
- neposkytnutia niektorej z dôveryhodných služieb alebo jej nedostupnosti v priebehu plánovanej údržby alebo reorganizácie oznámenej na webovom sídle Poskytovateľa;
- pôsobenia vyššej moci;

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

Od okamihu, kedy prístup ku súkromnému kľúču, ku ktorému patrí ZdC, nadobudne Držiteľ, Poskytovateľ nezodpovedá:

- za ochranu zariadenia, v ktorom je uchovaný ZdC a súkromný kľúč, resp. za ochranu prístupových kódov potrebných na jeho použitie;
- za to, že sa neoprávnená osoba zmocnila zariadenia alebo súkromného kľúča;
- za škody spôsobené použitím súkromného kľúča alebo ZdC, ak Držiteľ/Zákazník nekoná v súlade so svojimi povinnosťami, najmä ak sa súkromného kľúča zmocní neautorizovaná osoba a Držiteľ/Zákazník nepožiada Poskytovateľa o zrušenie ZdC alebo ak Poskytovateľovi neoznámi zmeny v údajoch.

Zodpovednosť Zákazníka/Držiteľa alebo splnomocneného zástupcu právnickej osoby vyplýva z výkonu jeho povinností. Podmienky zodpovednosti sa riadia zmluvou s Poskytovateľom. Zákazník/Držiteľ alebo splnomocnený zástupca právnickej osoby je zodpovedný voči Poskytovateľovi a spoliehajúcim sa stranám, ak:

- pri vytváraní páru súkromný-verejný kľúč použil algoritmus a prostredie na vytvorenie pokročilého elektronického podpisu/pečate, ktorý nespĺňa požiadavky nariadenia (EÚ) č. 910/2014
- nespĺňa bezpečnostné požiadavky stanovené Poskytovateľom
- nepožiada Poskytovateľa o pozastavenie alebo ukončenie platnosti ZdC po tom, čo sa dozvie, že súkromný kľúč bol zneužitý alebo ohrozený nesprávnym použitím
- urobil pre Poskytovateľa nepravdivé vyhlásenia týkajúce sa obsahu alebo vydania ZdC

Za obsah príloh a dôsledky ich použitia zodpovedá Zákazník/Držiteľ alebo zástupca právnickej osoby.

8.9 Odškodnenie

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

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

8.10 Trvanie a ukončenie

8.10.1 Termín

Táto verzia CP platí odo dňa nadobudnutia jej platnosti t. j. 1.1.2024 až do jej nahradenia novou verziou. Podrobnosti o histórii zmien tejto CP sú uvedené na začiatku dokumentu v časti „História zmien“.

8.10.2 Ukončenie

Platnosť tejto verzie CP skončí dňom publikovania novej verzie s vyšším číslom ako je 1.1, prípadne ukončením činnosti poskytovania zdokonalených dôveryhodných služieb Poskytovateľom v čase jej platnosti. Všetky revízie CP a CPS ktoré sú uvedené v histórii zmien pre daný dokument musia byť k dispozícii Držiteľom/Zákazníkom resp. Spoliehajúcim sa stranám.

8.10.3 Účinok ukončenia a prežitia

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

8.11 Individuálne oznámenia a komunikácia s účastníkmi

Komunikácia Poskytovateľa s internou RA musí prebiehať oficiálne prostredníctvom autorizovanej emailovej komunikácie medzi poverenou osobou Poskytovateľa a poverenou osobou RA, ak nie je v zmluve inak.

8.12 Zmeny a doplnenia

8.12.1 Postup pri zmene a doplnení

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

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

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

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

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

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

8.12.2 Mechanizmus a obdobie oznamovania

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

Interní zamestnanci musia byť rovnako informovaní o novej verzii tejto CP.

8.12.3 Okolnosti, za ktorých sa musí OID zmeniť

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

8.13 Ustanovenia o riešení sporov

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

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

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

8.14 Rozhodné právo

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

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

8.15 Dodržiavanie platných právnych predpisov

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

8.16 Rôzne ustanovenia

Žiadne ustanovenia.

9. Odkazy

- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES, Nariadenie (EÚ) č. 910/2014 a Korigendum
- Nariadenie Európskeho Parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
- Zákon č. 272/2016 Z. z o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (ďalej len zákon o dôveryhodných službách)
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov
- Informácia o spracúvaní osobných údajov (verzia 1.1)
- Všeobecné podmienky (verzia 1.4)
- SD Schéma dohľadu zdokonalených dôveryhodných služieb definovaná orgánom dohľadu
- ETSI EN 319 411-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC3647)
- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC5280)
- X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (RFC6960)
- OCRA: OATH Challenge-Response Algorithm (RFC6287)