



NFQES

Číslo: PO-03	POLITIKA		
Názov: Vyhlásenie o certifikačnej politike NFQES TSA			
Predchádzajúce č.:	Dátum vydania:	Dátum aktuálnej revízie:	Registr. znak a lehota:
	10.12.2021	10.12.2021	
	Dátum účinnosti:	Dátum účinnosti revízie:	
	10.12.2021	10.12.2021	


	Meno a Priezvisko:	Podpis schvaľujúceho:	Dátum:
Vytvoril:	Ing. Martin Berzák Bezpečnostný manažér		10.12.2021
Schválil:	Ing. Eduard Baraniak CEO		10.12.2021

Vyhlásenie o certifikačnej politike NFQES TSA

Verzia: **1.0**


Dátum účinnosti: 10.12.2021

brainit.sk, s. r. o.	Veľký Diel 3323, Žilina 010 08	IČO: 52577465
----------------------	-----------------------------------	---------------


 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	2 z 29

Obsah


1.	ÚVOD	5
1.1	Prehľad.....	5
1.2	Názov a identifikácia dokumentu	5
1.3	Správa politiky	6
1.3.1	Informácie o poskytovateľovi a jeho kontaktné údaje.....	6
1.3.2	Kontaktná osoba	6
1.3.3	Osoba, ktorá určuje vhodnosť CPS pre certifikačnú politiku.....	6
1.3.4	Postupy schvaľovania CPS	7
1.4	Definície a skratky.....	7
1.5	Používatelia a platnosť.....	8
1.6	Zhoda	8
2.	Všeobecné ustanovenia	9
2.1	Služba poskytovania časovej pečiatky	9
2.2	Vydavateľ časovej pečiatky	9
2.3	Používateľ časovej pečiatky.....	9
3.	Povinnosti a zodpovednosť.....	11
3.1	Povinnosti poskytovateľa služby časovej pečiatky	11
3.1.1	Všeobecne	11
3.1.2	Povinnosti poskytovateľa služby časovej pečiatky voči žiadateľovi.....	11
3.2	Povinnosti žiadateľa.....	11
3.3	Povinnosti spoliehajúcich sa strán.....	11
3.4	Zodpovednosť.....	12
4.	Požiadavky na výkon služby časovej pečiatky (TSA)	13
4.1	Prehlásenie o výkone služby a zverejňovaných informáciách.....	13
4.1.1	Prehlásenie o výkone služby.....	13
4.1.2	Zverejňované informácie.....	13
4.2	Manažment životného cyklu kľúčov	14
4.2.1	Generovanie kľúčov	14
4.2.2	Ochrana súkromného kľúča TSA	14
4.2.3	Distribúcia verejného kľúča TSA NFQES	14
4.2.4	Obnovovanie kľúča TSA NFQES.....	14
4.2.5	Ukončenie životnosti kľúčov TSA NFQES.....	15

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	3 z 29

4.2.6	Manažment životného cyklu kryptografického modulu používaného na podpisovanie časových pečiatok	15
4.3	Vytváranie časovej pečiatky	15
4.3.1	Časová pečiatka	15
4.3.2	Vyhotovenie a overenie časovej pečiatky	15
4.3.3	Synchronizácia času s UTC	16
4.4	Manažment a prevádzka TSA NFQES	16
4.4.1	Manažment bezpečnosti	16
4.4.2	Klasifikácia a manažment aktív	16
4.4.3	Personálna bezpečnosť	16
4.4.4	Fyzická a priestorová bezpečnosť	17
4.4.5	Prevádzkový manažment	17
4.4.6	Manažment prístupu k systému	18
4.4.7	Nasadenie a údržba dôveryhodných systémov	18
4.4.8	Kompromitácia služieb TSA NFQES	18
4.4.9	Ukončenie činnosti TSA NFQES	18
4.4.10	Súlad s právnymi požiadavkami	18
4.4.11	Zaznamenávanie údajov týkajúcich sa výkonu služby časovej pečiatky	19
4.5	Organizačné aspekty	19
5.	AUDIT SÚLADU A ĎALŠIE HODNOTENIA	21
5.1	Frekvencia alebo okolnosti posudzovania	21
5.2	Totožnosť / kvalifikácie posudzovateľa	21
5.3	Vzťah hodnotiteľa k hodnotenému subjektu	21
5.4	Témy, ktorých sa hodnotenie týka	21
5.5	Opatrenia prijaté v dôsledku nedostatku	21
5.6	Oznámenie výsledkov	21
6.	OSTATNÉ OBCHODNÉ A PRÁVNE VECI	22
6.1	Poplatky	22
6.1.1	Poplatky za vydanie časovej pečiatky	22
6.1.2	Poplatky za ďalšie služby	22
6.1.3	Pravidlá vrátenia peňazí	22
6.2	Finančná zodpovednosť	22
6.2.1	Poistné krytie	22
6.3	Dôvernoscť obchodných informácií	22

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	4 z 29

6.3.1	Rozsah dôverných informácií.....	22
6.3.2	Informácie, ktoré nespádajú do rozsahu dôverných informácií.....	23
6.3.3	Zodpovednosť za ochranu dôverných informácií	23
6.4	Ochrana osobných údajov.....	24
6.4.1	Plán ochrany osobných údajov	24
6.4.2	Informácie považované za súkromné	24
6.4.3	Informácie, ktoré sa nepovažujú za súkromné.....	24
6.4.4	Zodpovednosť za ochranu súkromných informácií.....	24
6.4.5	Oznámenie a súhlas s použitím súkromných informácií	24
6.5	Práva duševného vlastníctva.....	25
6.6	Vyhlásenia a záruky	25
6.6.1	Vyhlásenia a záruky TSA	25
6.6.2	Vyhlásenia a záruky účastníkov	25
6.6.3	Vyhlásenia a záruky spoliehajúcich sa strán	25
6.6.4	Vyhlásenia a záruky ostatných účastníkov	26
6.7	Zrieknutie sa záruk.....	26
6.8	Obmedzenia zodpovednosti.....	26
6.9	Odškodnenie	26
6.10	Trvanie a ukončenie.....	27
6.10.1	Termín	27
6.10.2	Ukončenie.....	27
6.10.3	Účinok ukončenia a prežitia.....	27
6.11	Zmeny a doplnenia	27
6.11.1	Postup pri zmene a doplnení	27
6.11.2	Mechanizmus a obdobie oznamovania.....	28
6.11.3	Okolnosti, za ktorých sa musí OID zmeniť	28
6.12	Ustanovenia o riešení sporov	28
6.13	Rozhodné právo.....	28
6.14	Dodržiavanie platných právnych predpisov	28
7.	Odkazy	29

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	5 z 29

1. ÚVOD

Vyhlásenie o certifikačnej politike NFQES TSA (v ďalšom iba „CPS“), prezentuje záväzné postupy, metodiku, a zodpovednosti firmy brainit.sk s.r.o., IČO: 52577465 zapísanú v Obchodnom registri Okresného súdu Žilina, oddiel: Sro, vložka č. 72902/L (v ďalšom iba "Poskytovateľ") pre vydávanie časových pečiatok a správu certifikátu TSA certifikačnej autority CA NFQES (v ďalšom iba „CA“).

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

Požiadavky tohto vyhlásenia sú zamerané na výkon kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok, (ďalej len časová pečiatka) použitých na podporu kvalifikovaných elektronických podpisov alebo na ľubovoľnú aplikáciu vyžadujúcu dôkaz, že informácia existovala pred daným časom. Požiadavky tohto vyhlásenia sú založené na použití kryptografie verejných kľúčov, certifikátov verejných kľúčov a spoľahlivom časovom zdroji.

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

1.1 Prehľad

CPS sa týka poskytovania nasledovných kvalifikovaných dôveryhodných služieb:

- **Kvalifikovaná dôveryhodná služba vyhotovovania kvalifikovaných elektronických časových pečiatok**

Certifikačné autority Poskytovateľa pre poskytovanie kvalifikovaných dôveryhodných služieb:

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


1.2 Názov a identifikácia dokumentu

Verzia dokumentu: 1.0

Dátum účinnosti: 10.12.2021

Vyhlásenie o certifikačnej politike NFQES TSA je identifikovaný objektovým identifikátorom OID 1.3.158.52577465.0.0.0.1.6.1, 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)
- 0.0.0.1 CA NFQES
- 6 Dokument „Vyhlásenie o certifikačnej politike NFQES TSA“
- 1 major verzia dokumentu

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	6 z 29

História zmien:

Verzia	Dátum	Popis revízie
1.0	10.12.2021	Prvá schválená verzia dokumentu

1.3 Správa politiky

1.3.1 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@nfqes.sk

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

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

Orgán dohľadu:

Kontakt pre žiadosť o zrušenie Certifikátu:

Mobil: +421 918 022 030

E-mail: info@nfqes.sk

1.3.2 Kontaktná osoba

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

Certifikačná autorita TSA NFQES:

Adresa: Veľký Diel 3323, 010 08 Žilina

Email: ca@nfqes.sk


Telefón: +421 918 022 030

Webové sídlo: <https://nfqes.sk>

Nahlasovanie incidentov: infra@nfqes.sk

1.3.3 Osoba, ktorá určuje vhodnosť CPS pre certifikačnú politiku

Osobou, ktorá je zodpovedná za rozhodovanie o súlade postupov Poskytovateľa, ktoré sú uvedené v CP TSA resp. CPS TSA s touto politikou je PMA.

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	7 z 29

1.3.4 Postupy schvaľovania CPS

Poskytovateľ má schválené CP a CPS ešte pred začiatkom prevádzky a spĺňa všetky jeho požiadavky. Obsah CP a CPS schválila osoba menovaná do role PMA.

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

PMA informuje o svojich rozhodnutiach takým spôsobom, aby boli tieto informácie dobre prístupné stranám spoliehajúcim sa na časové pečiatky.

1.4 Definície a skratky

Elektronická časová pečiatka – sú údaje v elektronickej forme, ktoré viažu iné údaje v elektronickej forme s konkrétnym časom, čím tvoria dôkaz o existencii týchto iných údajov v danom čase a spĺňa požiadavky Nariadenia (EÚ) č. 910/2014 - Nariadenie eIDAS čl. 3 bod 33

Kvalifikovaná elektronická časová pečiatka - elektronická časová pečiatka, ktorá spĺňa požiadavky Nariadenia eIDAS stanovené v článku 42

Spoliehajúca sa strana – príjemca (používateľ) časovej pečiatky spoliehajúci sa na jej presnosť

Referenčný čas – čas, ktorý poskytuje niektoré z referenčných pracovísk

Vydavateľ časovej pečiatky – (Certifikačná) autorita, ktorá poskytuje kvalifikovanú dôveryhodnú službu vydávania časových pečiatok, označuje sa skratkou TSA (Time Stamp Authority). V zmysle zákona č. 272/2016 Z. z. o dôveryhodných službách a Nariadenia eIDAS ju môže vyhotoviť iba kvalifikovaný poskytovateľ dôveryhodných služieb použitím súkromného kľúča určeného na tento účel

Hašovacia (hash) funkcia – matematická transformácia, ktorá digitálnym dokumentom rozličnej dĺžky priradí také čísla vopred ustanovenej nenulovej pevnej dĺžky, že umožňujú overiť integritu digitálneho dokumentu, z ktorého boli odvodené transformáciou a nemožno z nich späť odvodit digitálny dokument

Digitálny odtlačok (dokumentu resp. súboru) – číslo (funkčná hodnota) vypočítané pomocou hašovacej funkcie z dokumentu resp. súboru

Žiadateľ – právnická osoba alebo fyzická osoba, ktorá žiada o vyhotovenie časovej pečiatky prostredníctvom žiadosti zaslanej vydavateľovi časovej pečiatky a ktorá súhlasila s podmienkami poskytovanej služby


Žiadosť o vyhotovenie časovej pečiatky (resp. skrátené žiadosť) – dátová štruktúra obsahujúca digitálny odtlačok dokumentu, na ktorý sa má vyhotoviť časová pečiatka, vytvorený žiadateľom pomocou schválenej hašovacej funkcie

Zdokonalený elektronický podpis - elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26 Nariadenia eIDAS

Skratky:

CA – Certifikačná autorita

eIDAS – skratka pre Nariadenie (EÚ) č. 910/2014

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	8 z 29

- NBÚ** – Národný bezpečnostný úrad
- TSA** – Vydavateľ časovej pečiatky (Time Stamp Authority)
- UTC** – Univerzálny svetový čas (Coordinated Universal Time)

1.5 Používatelia a platnosť


Toto vyhlásenie má za cieľ vyhovieť požiadavkám na službu časovej pečiatky v súlade s požiadavkami čl. 42 Nariadenia eIDAS a zákona č. 272/2016 Z. z. o dôveryhodných službách.

Toto vyhlásenie je použiteľná pre službu časovej pečiatky určenú pre žiadateľov zo širokej verejnosti alebo službu časovej pečiatky pre uzatvorenú skupinu.

Službu časovej pečiatky poskytuje TSA NFQES v rámci NFQES CA ako platenú službu.

1.6 Zhoda

TSA, ktorá je v zhode s touto politikou, musí byť schopná preukázať, že si plní povinnosti v zmysle ods. 3.1 a má zavedené kontroly v zmysle ods. 4.

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	9 z 29

2. Všeobecné ustanovenia

2.1 Služba poskytovania časovej pečiatky

Služba poskytovania časovej pečiatky vydavateľom časovej pečiatky (ďalej TSA NFQES) pozostáva s dvoch neoddeliteľných zložiek, ktorými sú:

- poskytovanie časovej pečiatky – zložka, ktorá vytvára samotnú časovú pečiatku,
- riadenie vyhotovovania časovej pečiatky – zložka, ktorá monitoruje a kontroluje priebeh vyhotovovania časovej pečiatky, aby sa zaistilo, že táto služba je poskytovaná v zmysle pravidiel stanovených TSA NFQES.

2.2 Vydavateľ časovej pečiatky

Vydavateľom časovej pečiatky v zmysle tejto politiky je:

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@nfqes.sk

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

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

Všetky otázky, sťažnosti a reklamácie týkajúce sa poskytovania služby časovej pečiatky je potrebné zasielať písomne na hore uvedenú adresu. NFQES preferuje elektronickú výmenu informácií.

NFQES preberá plnú zodpovednosť za poskytovanie služby časovej pečiatky, tak ako je definovaná v ods. 2.1. Na vytvorenie časovej pečiatky je použitý privátny kľúč TSA NFQES a v tele časovej pečiatky je identifikácia TSA NFQES ako vydavateľa časovej pečiatky.


TSA NFQES nevyužíva žiadnu ďalšiu stranu pri poskytovaní služieb časovej pečiatky.

Na poskytovanie časovej pečiatky využíva TSA NFQES zariadenie certifikované podľa štandardu FIPS 140-2 level 3. Všetky zmeny týkajúce sa kontaktných údajov budú okamžite zverejnené na webovej stránke NFQES.

2.3 Používateľ časovej pečiatky


Používateľom časovej pečiatky môže byť právnická osoba zastupujúca niekoľkých koncových používateľov alebo individuálna fyzická osoba ako koncový používateľ.

V prípade, že používateľom je právnická osoba zastupujúca niekoľkých koncových používateľov, je zodpovedná za to, že niektoré povinnosti danej organizácie budú plnené aj jej koncovými používateľmi. V každom prípade je organizácia zodpovedná za to, že povinnosti dané organizácii sú koncovými

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	10 z 29

používateľmi dodržiavané a očakáva sa, že organizácia ich bude vhodným spôsobom o tejto skutočnosti informovať.

V prípade, že koncovým používateľom časovej pečiatky je individuálna fyzická osoba, je táto priamo zodpovedná za dodržiavanie všetkých stanovených povinností.

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	11 z 29

3. Povinnosti a zodpovednosť

3.1 Povinnosti poskytovateľa služby časovej pečiatky

3.1.1 Všeobecne

TSA NFQES ako poskytovateľ služby časovej pečiatky sa zaväzuje:

- uskutočňovať všetky príslušné požiadavky na TSA uvedené v ods. 4,
- zabezpečiť súlad praxe TSA s procedúrami predpísanými touto politikou a ďalšími súvisiacimi dokumentmi,
- poskytovať služby časovej pečiatky v súlade s prevádzkovou smernicou TSA a ďalšími súvisiacimi dokumentmi.

3.1.2 Povinnosti poskytovateľa služby časovej pečiatky voči žiadateľovi

TSA NFQES si plní svoje záväzky v súlade s podmienkami poskytovania služby časovej pečiatky tak, aby táto služba bola maximálne dostupná a bola vykonávaná s čo najväčšou precíznosťou.

3.2 Povinnosti žiadateľa

V tomto dokumente nie sú definované žiadne ďalšie povinnosti pre žiadateľa služby časovej pečiatky mimo tých, ktoré sú definované v podmienkach poskytovania tejto služby.

Žiadateľovi sa odporúča po získaní digitálneho odtlačku dokumentu opatrenom časovou pečaťou overiť si, že táto časová pečať je správne podpísaná, a že súkromný kľúč použitý na podpis digitálneho odtlačku dokumentu nie je kompromitovaný.

Žiadateľ je povinný platiť dohodnutú cenu dohodnutým spôsobom a v dohodnutých termínoch (lehotách) za prístup k službe časovej pečiatky a za časové pečiatky, ktoré mu boli vyhotovené.


Žiadateľ je povinný a oprávnený žiadať o vyhotovenie časovej pečiatky len prostredníctvom rozhrania alebo softvérovej aplikácie, ktoré boli dohodnuté medzi ním a NFQES.

Po prijatí časovej pečiatky, o ktorú žiadateľ požiadal, sa žiadateľ stáva automaticky spoliehajúcou sa stranou a teda sa na neho vzťahujú aj povinnosti spoliehajúcich sa strán.

3.3 Povinnosti spoliehajúcich sa strán

Podmienky poskytovania služieb časovej pečiatky, ktoré sú k dispozícii spoliehajúcim sa stranám, obsahujú povinnosti, ktoré musí vykonať, keď sa spolieha na časovú pečať:

- a) overiť si, že časová pečať je správne podpísaná, a že súkromný kľúč použitý na podpis digitálneho odtlačku dokumentu nebol kompromitovaný v čase jeho podpisania,
- b) brať do úvahy všetky obmedzenia používania časovej pečiatky uvedené v politike časovej pečiatky,
- c) brať do úvahy všetky ďalšie predpísané bezpečnostné opatrenia.

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	12 z 29

3.4 Zodpovednosť


Právna zodpovednosť NFQES TSA je daná platnou legislatívou Slovenskej republiky.

Finančnú zodpovednosť z nej vyplývajúce plnenie je možné uznať len za predpokladov, že zákazník neporušil svoje povinnosti (hlavne overiť si, že časová pečiatka je správne podpísaná) a že každý, kto sa v danom prípade spoliehal na časovú pečiatku vydanú TSA NFQES, urobil všetko, aby prípadnej škode zabránil.

Neoverenie časovej pečiatky sa kvalifikuje ako hrubé porušenie povinností vyplývajúcich z tohto dokumentu, dôsledkom čoho zanikajú akékoľvek nároky na prípadné uplatňovanie si ľubovoľnej náhrady.

NFQES a ani zriaďovateľ NFQES nemajú žiadnu finančnú zodpovednosť za prípadné škody, ktoré by vznikli žiadateľovi alebo spoliehajúcej sa strane v súvislosti s používaním časových pečiatok vydaných TSA NFQES s nejakou konkrétnou aplikáciou resp. hardvérom alebo v súvislosti s tým, že časové pečiatky vydané TSA NFQES nie je možné používať s nejakou konkrétnou aplikáciou resp. hardvérom.

Akákoľvek žiadosť o náhradu škody musí byť podaná písomne.

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	13 z 29

4. Požiadavky na výkon služby časovej pečiatky (TSA)

Poskytovateľ časovej pečiatky TSA NFQES má zavedený systém riadenia spĺňajúci nižšie uvedené požiadavky.

Požiadavky poukazujú na úlohy v oblasti bezpečnosti nasledované špecifickejšími požiadavkami na riadenie, zabezpečujúce splnenie týchto podmienok za účelom preukázania nevyhnutnej dôvery, že tieto úlohy budú splnené.

Poskytovanie služby časovej pečiatky na požiadanie je na uvážení NFQES CA v závislosti na úrovni dohodnutej služby so zákazníkom.

4.1 Prehlásenie o výkone služby a zverejňovaných informáciách

4.1.1 Prehlásenie o výkone služby

TSA NFQES má zabezpečenú nevyhnutnú spoľahlivosť pri poskytovaní služby časovej pečiatky nasledovnými opatreniami:


- vypracovaním pravidiel na výkon služby časovej pečiatky a procedúr resp. pracovných postupov používaných na naplnenie všetkých požiadaviek určených v tejto politike,
- poskytnutím príslušných častí svojich pravidiel na výkon služby časovej pečiatky činností TSA a ďalších náležitých dokumentov všetkým žiadateľom o služby časovej pečiatky ako aj spoliehajúcim sa stranám,
Poznámka: TSA NFQES nemusí sprístupniť všetky detailné informácie o svojej praxi pri výkone TSA.
- zverejnením podmienok týkajúcich sa použitia služieb časovej pečiatky v zmysle časti 7.1.2 pre všetkých žiadateľov a potenciálne spoliehajúce sa strany,
- schvaľovaním všetkých dokumentov popisujúcich pravidlá pre výkon činností spojených so službou časovej pečiatky zodpovednými pracovníkmi vedenia TSA NFQES,
- zabezpečením prostredníctvom vedenia NFQES CA riadneho zavedenia a používania všetkých postupov a praktík TSA NFQES,
- definovaním postupov preskúmania praktík TSA vrátane zodpovedností pri udržiavaní úrovne poskytovaných služieb,
- okamžite po schválení zodpovednými pracovníkmi sprístupnením všetkých zmien týkajúcich sa pravidiel na výkon činností súvisiacich s poskytovaním služieb časovej pečiatky všetkým dotknutým stranám.

4.1.2 Zverejňované informácie

TSA NFQES má sprístupnené všetkým žiadateľom a spoliehajúcim sa stranám podmienky poskytovania služieb časovej pečiatky.

Zverejňované informácie obsahujú:

- a) kontaktné informácie,
- b) používanú politiku časovej pečiatky,
- c) používaný algoritmus hašovacej funkcie,

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	14 z 29

- d) životnosť kľúčov používaných na vyhotovovanie časovej pečiatky,
- e) presnosť času vo vyhotovovanej časovej pečiatke s ohľadom na UTC,
- f) akékoľvek obmedzenia týkajúce sa používania služby časovej pečiatky,
- g) povinnosti žiadateľa,
- h) povinnosti spoliehajúcich sa strán,
- i) informácie o spôsobe overovania časovej pečiatky tak, aby spoliehajúca sa strana mohla túto považovať za „primerane spoľahlivú“ a akékoľvek obmedzenia trvania platnosti
- j) dobu uchovávanía záznamov TSA NFQES,
- k) príslušné právne predpisy,
- l) obmedzenia zodpovednosti,
- m) postupy podávania sťažností a urovnávania sporov,
- n) či bola TSA NFQES posudzovaná vzhľadom k svojej politike časových pečiatok.

Hore uvedené informácie sú k dispozícii trvale prostredníctvom webu TSA NFQES.

Je možné ich získať v elektronickej podobe stiahnutím z web stránok TSA NFQES. Za ich základný zdroj sa považuje tento dokument.

4.2 Manažment životného cyklu kľúčov

4.2.1 Generovanie kľúčov

TSA NFQES zaisťuje, že všetky kryptografické kľúče používané pri výkone služby časovej pečiatky sú generované za kontrolovaných okolností v bezpečnom zariadení a vo fyzicky bezpečnom prostredí (pozri ods. 4.4.4) dôveryhodnými a kvalifikovanými osobami (pozri ods. 4.4.3) za prítomnosti a pod kontrolou stanoveného počtu osôb.

4.2.2 Ochrana súkromného kľúča TSA

TSA NFQES zabezpečuje, že jej súkromný kľúč zostane tajný a zostane zachovaná jeho integrita.

Súkromný podpisový kľúč TSA NFQES je generovaný, uchovávaný a používaný v kryptografickom module, ktorý spĺňa požiadavky dané štandardom FIPS 140-2 level 3.


4.2.3 Distribúcia verejného kľúča TSA NFQES

TSA NFQES zaručuje, že integrita a dôveryhodnosť verejného verifikačného kľúča TSA NFQES budú zachované počas jeho distribúcie k spoliehajúcim sa stranám to najmä:

- verejný verifikačný kľúč TSA NFQES je k dispozícii pre spoliehajúce sa strany prostredníctvom certifikátu verejného kľúča,
- certifikát je vydaný certifikačnou autoritou, ktorej certifikačná politika poskytuje rovnakú, alebo vyššiu úroveň bezpečnosti, ako má táto politika časovej pečiatky.

4.2.4 Obnovovanie kľúča TSA NFQES

Obnovovanie kľúča TSA NFQES a následne certifikátu TSA vyplýva zo zásady, že životnosť certifikátu TSA NFQES je konečná, avšak súčasne pritom doba platnosti certifikátu TSA NFQES neprekračuje dobu platnosti certifikátu vydávajúcej CA (ktorá vydala certifikát TSA NFQES).

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	15 z 29

4.2.5 Ukončenie životnosti kľúčov TSA NFQES

TSA NFQES zaisťuje, že súkromný podpisový kľúč TSA nebude používaný po ukončení jeho životnosti.

4.2.6 Manažment životného cyklu kryptografického modulu používaného na podpisovanie časových pečiatok

TSA NFQES zabezpečuje bezpečnosť kryptografického hardvéru (hardvérový modul na podpisovanie časovej pečiatky) počas celej jeho životnosti.

4.3 Vytváranie časovej pečiatky

4.3.1 Časová pečiatka

NFQES TSA zabezpečuje, že časová pečiatka je vydávaná bezpečne a že obsahuje správny čas. Predovšetkým:


- b) časová pečiatka obsahuje identifikátor politiky časovej pečiatky,
- c) časová pečiatka má jedinečné identifikačné číslo,
- d) hodnota času, ktorá sa dáva do vyhotovovanej časovej pečiatky, bude odvodená z hodnoty reálneho času poskytovaného prostredníctvom UTC (ako spoľahlivého časového zdroja),
- e) čas, ktorý je dávaný do vyhotovovanej časovej pečiatky, je synchronizovaný s hodnotou UTC v rámci presnosti definovanej v tejto politike,
- f) ak je zistená odchýlka hodín TSA prekračujúca touto politikou deklarovanú presnosť, TSA NFQES časovú pečiatku nevydá,
- g) časová pečiatka zahŕňa hodnotu hašovacej funkcie, ktorú poskytol žiadateľ, aplikovanú na údaje, ku ktorým sa má vyhotoviť časová pečiatka,
- h) časová pečiatka je podpísaná kľúčom TSA NFQES, ktorý je používaný len na tento účel

4.3.2 Vyhotovenie a overenie časovej pečiatky

Žiadateľ zašle (prostredníctvom dohodnutého rozhrania) TSA NFQES ako vydavateľovi časovej pečiatky žiadosť o vyhotovenie časovej pečiatky. Žiadosť obsahuje digitálny odtlačok dokumentu, na ktorý sa má vyhotoviť časová pečiatka, vytvorený pomocou schválenej hašovacej funkcie. Ak je žiadosť v schválenom formáte a nie sú prekážky na vyhotovenie časovej pečiatky zo strany TSA NFQES, táto pomocou bezpečného zariadenia na vyhotovovanie časovej pečiatky a zdroja času vyhotoví časovú pečiatku na predložený digitálny odtlačok dokumentu a pošle ju žiadateľovi v režime on-line. Ak žiadosť o vyhotovenie časovej pečiatky nemá schválený formát, alebo ak u TSA NFQES vznikli prekážky vyhotovenia časovej pečiatky (napr. sa zistila odchýlka času mimo deklarovanú presnosť), TSA NFQES časovú pečiatku na predložený digitálny odtlačok dokumentu nevyhotoví a o tejto skutočnosti a jej príčine informuje žiadateľa v režime on-line. Overenie platnosti časovej pečiatky vykonáva spoliehajúca sa strana na základe danej časovej pečiatky a dokumentu, na ktorý bola daná časová pečiatka vyhotovená, a politiky časovej pečiatky, ktorá sa na danú časovú pečiatku vzťahuje.

Časová pečiatka je platná, ak:

- zdokonalený elektronický podpis časovej pečiatky je platný,
- časová pečiatka je v súlade s použitou politikou časových pečiatok.

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	16 z 29

4.3.3 Synchronizácia času s UTC

TSA NFQES zabezpečuje, že čas ňou používaný je synchronizovaný s UTC s deklarovanou presnosťou menej ako 1 sekunda, a to predovšetkým nasledovnými opatreniami:

- kalibrácia hodín TSA NFQES je vykonávaná tak, že očakávaná odchýlka času nebude mimo deklarovanú presnosť,
- hodiny zariadenia TSA NFQES sú chránené proti hrozbám, ktoré by mohli viesť k nezistiteľným zásahom do hodín, ktoré by mohli mať za následok ich odchýlku od kalibrácie,
- TSA NFQES zabezpečuje, že v prípade, že sa čas, ktorý by bol uvedený v časovej pečiatke, odchýli od synchronizácie s UTC, sa to sa zistí a časová pečiatka nebude vydaná,
- TSA NFQES zabezpečuje, že bude vykonaná synchronizácia hodín v prípade, že bude notifikovaná oprávneným orgánom o výskyte opravnej sekundy.

4.4 Manažment a prevádzka TSA NFQES

4.4.1 Manažment bezpečnosti

TSA NFQES zabezpečuje uplatňovanie takých manažérskych a administratívnych postupov, ktoré sú vhodné a v súlade s najlepšou profesionálnou praxou tak, že:

- TSA NFQES preberá plnú zodpovednosť za všetky aspekty poskytovania služby časovej pečiatky popisované v tejto politike,
- TSA NFQES poskytuje smernice o informačnej bezpečnosti prostredníctvom svojho vedenia, ktoré je zodpovedné za definovanie informačnej bezpečnosti.
- s touto politikou sú oboznámení všetci pracovníci, ktorých sa uvedená politika týka,
- infraštruktúra informačnej bezpečnosti nevyhnutná pre zabezpečenie bezpečnosti v rámci TSA NFQES je udržiavaná počas celej doby činnosti TSA NFQES,
- akékoľvek zmeny, ktoré by mohli ovplyvniť úroveň bezpečnosti, budú odsúhlasené vedením TSA NFQES,
- bezpečnostné opatrenia a pracovné postupy TSA NFQES, systémové a informačné aktíva poskytujúce služby časovej pečiatky sú dokumentované, zavedené a udržiavané.


4.4.2 Klasifikácia a manažment aktív

TSA NFQES zabezpečuje, že jej informačné a ďalšie aktíva sú chránené na požadovanej úrovni, a to predovšetkým:

- TSA NFQES má zoznam všetkých aktív a ich klasifikáciu z pohľadu požiadaviek na ochranu, ktoré sú v súlade s vykonanou analýzou rizík.

4.4.3 Personálna bezpečnosť

TSA NFQES zabezpečuje, že postupy personálnej práce a prijímania do zamestnania podporujú jej dôveryhodnosť. Predovšetkým:

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	17 z 29

- a) TSA NFQES zamestnáva pracovníkov, ktorí majú zodpovedajúce znalosti, skúsenosti a nevyhnutnú kvalifikáciu pre poskytované služby, a ktorí sú vhodní pre danú pracovnú pozíciu,
- b) TSA NFQES z organizačného hľadiska pozostáva z rolí, kde pod pojmom rola sa rozumie skupina osôb, ktoré vykonávajú buď tie isté činnosti alebo činnosti z nejakého aspektu príbuzné, pričom pri niektorých zvlášť dôležitých činnostiach sa môže vyžadovať, aby pri ich vykonávaní bolo prítomných viacero osôb zastávajúcich danú rolu (tzv. princíp "k" z "n", ktorý je nastavený na hodnotu 4 z 8),
- c) dôveryhodné roly a ich zodpovednosti sú popísané v prevádzkových smerniciach a prípadne v ďalších dokumentoch a tie roly, na ktorých je závislá bezpečnosť TSA NFQES, sú jasne identifikované,
- d) jednotlivé dôveryhodné roly v rámci TSA NFQES majú popisy práce definované z hľadiska rozdelenia povinností a minimálnych privilégii, stanovenia citlivosti pozície z hľadiska zodpovednosti a úrovne prístupových práv, ich predchádzajúcej praxe a úrovne zaškolenia a povedomia,
- e) pracovníci uplatňujú administratívne a manažérske postupy a procedúry, ktoré sú v súlade s procedúrami manažmentu informačnej bezpečnosti (pozri ods. 4.4.1)

4.4.4 Fyzická a priestorová bezpečnosť

TSA NFQES zabezpečuje, že fyzický prístup k jej kritickým aktívam je kontrolovaný a riziko neoprávneného fyzického prístupu je minimalizované.

Predovšetkým:


- a) pre poskytovanie aj pre manažovanie časovej pečiatky:
 - fyzický prístup do priestorov týkajúcich sa služby časovej pečiatky je umožnený len autorizovaným osobám,
 - je zavedená kontrola, ktorá zabráni stratám, poškodeniu alebo kompromitácii aktív a prerušeniu obchodných aktivít,
 - je zavedená kontrola, ktorá zabráni prezradeniu alebo odcudzeniu informácií alebo zariadení spracujúcich alebo obsahujúcich informácie,
- b) je implementovaná kontrola prístupu ku kryptografickému modulu, aby sa zaistili požiadavky na bezpečnosť kryptografického modulu v zmysle ods. 4.2.1 a 4.2.2.,
- c) všetko vybavenie používané na poskytovanie služby časovej pečiatky je prevádzkované v prostredí, ktoré fyzicky chráni toto vybavenie pred kompromitáciou prostredníctvom neautorizovaného prístupu k systémom alebo k dátam,
- d) je implementované riadenie fyzickej a priestorovej bezpečnosti, aby sa ochránilo vybavenie, kde sú lokalizované systémové zdroje, samotné systémové zdroje a podporné vybavenie.

4.4.5 Prevádzkový manažment

TSA NFQES zabezpečuje, že systémové komponenty sú bezpečné a pracujú správne, s minimálnym rizikom poruchy.

Predovšetkým:

- a) integrita systémových komponentov TSA NFQES je chránená proti vírusom, škodlivému a neautorizovanému softvéru,

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	18 z 29

- b) zaznamenávanie incidentov a postupy reakcií na incidenty sú zavedené takým spôsobom, aby sa minimalizovali škody z bezpečnostných incidentov a zlyhaní,
- c) s médiami používanými v rámci dôveryhodného TSA NFQES systému sa zaobchádza takým spôsobom, aby sa predišlo ich poškodeniu, odcudzeniu, neautorizovanému prístupu k nim a ich zastaraniu.

4.4.6 Manažment prístupu k systému

TSA NFQES zaisťuje, že k prístupu k systému je vyhradený len autorizovaným osobám.

Predovšetkým:

- a) je implementovaná ochrana, ktorá zabráni neautorizovanému prístupu cez sieť,
- b) TSA NFQES zaisťuje efektívnu administráciu prístupu používateľov (vrátane používateľov v dôveryhodných rolách) na udržiavanie bezpečnosti systému,
- c) nepretržite je používané monitorovacie a poplašné vybavenie, aby bolo možné detegovať a registrovať neautorizované pokusy o prístup k systémom TSA a vhodným spôsobom na ne reagovať.

4.4.7 Nasadenie a údržba dôveryhodných systémov

TSA NFQES používa dôveryhodné systémy a produkty, ktoré sú chránené pred modifikáciou.

Pre vykonávanie zmien (napr. aktualizácie, patche, fixy a pod.) používaného softvéru sa používajú ustálené procedúry alebo postupy odporúčané výrobcom softvéru.

4.4.8 Kompromitácia služieb TSA NFQES

TSA NFQES zabezpečuje, že v prípade udalosti, ktorá ovplyvní jej služby, vrátane kompromitácie privátneho kľúča TSA alebo zistenia odchýlky od kalibrácie, budú príslušné informácie k dispozícii všetkým žiadateľom a spoliehajúcim sa stranám.

4.4.9 Ukončenie činnosti TSA NFQES

TSA NFQES zabezpečuje, že prípadné narušenie služieb žiadateľom a spoliehajúcim sa stranám v dôsledku zastavenia služby poskytovania časovej pečiatky bude minimalizované a obzvlášť zaisťí následnú podporu vo forme informácií požadovaných na overenie platnosti časových pečiatok.


4.4.10 Súlad s právnymi požiadavkami

TSA NFQES zabezpečuje súlad svojej činnosti s právnymi požiadavkami.

Výkon služby časovej pečiatky sa riadi platnou legislatívou Slovenskej republiky so zreteľom na Nariadenie eIDAS a Zákona o dôveryhodných službách a súvisiace vyhlášky (vyhlášky NBÚ v aktuálnom znení).

Popri tom:

- a) sú splnené právne požiadavky legislatívy Európskej únie tak, ako sú premietnuté v legislatíve Slovenskej republiky,

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	19 z 29

- b) v rámci TSA NFQES sú uplatňované príslušné technické a organizačné opatrenia proti neoprávnenému a nezákonnému spracovávaniu osobných údajov a proti náhodnej strate, poškodeniu alebo zničeniu osobných údajov, ktoré uplatňuje TSA NFQES,
- c) informácie poskytnuté žiadateľmi o služby TSA NFQES sú chránené pred zverejnením, pokiaľ na to nedá súhlas žiadateľ alebo to neprikáže súd alebo iný kompetentný štátny orgán.

4.4.11 Zaznamenávanie údajov týkajúcich sa výkonu služby časovej pečiatky

TSA NFQES zabezpečuje, že všetky dôležité informácie týkajúce sa výkonu služby časovej pečiatky sú zaznamenávané a uchovávané počas stanovenej doby, najmä za účelom poskytnutia dôkazov pre účely prípadných právnych konaní.


Predovšetkým:

- a) TSA NFQES dokumentuje, ktoré konkrétne prípady a údaje sa majú zaznamenávať,
- b) je udržiavaná dôvernosc a celistvosť súčasných a archivovaných záznamov týkajúcich sa činnosti služby časovej pečiatky,
- c) záznamy týkajúce sa činnosti služby časovej pečiatky sú bezpečne a kompletne archivované v zmysle zverejnených praktík,
- d) záznamy týkajúce sa činnosti služby časovej pečiatky sú k dispozícii v prípade požiadavky na poskytnutie dôkazov správnosti výkonu činnosti služby časovej pečiatky pre prípady právnych úkonov,
- e) je zaznamenávaný presný čas významných udalostí týkajúcich sa prostredia:
 - a) TSA NFQES, manažmentu kľúčov a synchronizácie času,
- f) záznamy týkajúce sa činnosti služby časovej pečiatky sú uchovávané počas primeranej doby po vypršaní platnosti podpisového kľúča TSA NFQES, aby bola možné poskytnúť právny dôkaz a ako je to uvedené v prehlásení o zverejňovaní informácií (pozri ods. 4.1),
- g) udalosti sú zaznamenávané spôsobom, aby tieto záznamy nemohli byť ľahko zmazané alebo zničené a sú uchovávané počas doby, ktorá je na ich uchovávanie požadovaná,
- h) akékoľvek informácie o žiadateľovi sa uchovávajú ako dôverné okrem prípadov, keď existuje súhlas žiadateľa s ich publikovaním alebo prípadov uvedených v ods. 4.4.10,
- i) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k životnému cyklu kľúčov TSA NFQES,
- j) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k životnému cyklu certifikátov TSA NFQES,
- k) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k synchronizácii hodín TSA NFQES,
- l) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k detegovaniu straty synchronizácie hodín.


4.5 Organizačné aspekty

TSA NFQES zaistuje, že jej organizácia je spoľahlivá, pričom kladie dôraz, že:

- a) politika a postupy používané TSA NFQES nie sú diskriminačné,
- b) umožní prístup k svojim službám žiadateľom, ktorých aktivity spadajú do oblasti jej pôsobnosti, a ktorí súhlasia dodržiavať svoje povinnosti ako sú špecifikované v tomto dokumente,
- c) je právnická osoba v zmysle práva Slovenskej republiky,

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	20 z 29

- d) má systém pre manažment kvality a informačnej bezpečnosti vhodný pre poskytovanie služieb časovej pečiatky,
- e) má primerané prostriedky na pokrytie svojej zodpovednosti vyplývajúcej z výkonu svojich činností,
- f) je finančne stabilná a má zdroje požadované na výkon činností v súlade s touto politikou,
- g) zamestnáva dostatočný počet pracovníkov, ktorí majú nevyhnutné vzdelanie, zácvik, technické znalosti a skúsenosti týkajúce sa poskytovania služby časovej pečiatky,
- h) má postup na riešenie sťažností a podnetov od žiadateľov alebo iných strán týkajúce sa poskytovania služby časovej pečiatky alebo iných súvisiacich služieb.

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	21 z 29

5. AUDIT SÚLADU A ĎALŠIE HODNOTENIA

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

5.1 Frekvencia alebo okolnosti posudzovania

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

5.2 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.

5.3 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.

5.4 Témy, ktorých sa hodnotenie týka

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

5.5 Opatrenia prijaté v dôsledku nedostatku


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

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

5.6 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.

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	22 z 29

6. OSTATNÉ OBCHODNÉ A PRÁVNE VECI

6.1 Poplatky

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

Poplatky za kvalifikované dôveryhodné služby poskytované Poskytovateľom uhrádza Zákazník.

6.1.1 Poplatky za vydanie časovej pečiatky

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

Ceny časových pečiatok 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.

6.1.2 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.

6.1.3 Pravidlá vrátenia peňazí

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

6.2 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.

6.2.1 Poistné krytie

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


6.3 Dôvernosť obchodných informácií

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

6.3.1 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, súkromné kľúče Poskytovateľa,

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	23 z 29

- súkromné kľúče TSA, používané na vyhotovovanie kvalifikovaných elektronických časových pečiatok

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.

6.3.2 Informácie, ktoré nespádajú 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.


6.3.3 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 informácií, ktorej obsahom sú aj vyššie uvedené povinnosti.

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

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

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	24 z 29

6.4 Ochrana osobných údajov

6.4.1 Plán ochrany osobných údajov

Poskytovateľ pri spracovaní osobných údajov dodržiava požiadavky Predpisov o ochrane osobných údajov.

Poskytovateľ zabezpečuje dôvernosc a integritu osobných údajov získaných v rámci procesu vyhotovovania kvalifikovanej časovej pečiatky, a to aj v prípade ich prenosu medzi Zákazníkom a Poskytovateľom či medzi jednotlivými komponentmi systému Poskytovateľa.

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

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

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

6.4.2 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.

6.4.3 Informácie, ktoré sa nepovažujú za súkromné


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

6.4.4 Zodpovednosť za ochranu súkromných informácií

Poskytovateľ bezpečne ochraňuje a uchováva osobné údaje spracúvané v súvislosti s vyhotovovaním kvalifikovaných časových pečiatok. Tieto údaje chráni prijatím vhodných bezpečnostných opatrení, a to najmä pred neautorizovaným prístupom, prezradením alebo zmenou.

6.4.5 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.

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	25 z 29

6.5 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.

6.6 Vyhlásenia a záruky

Poskytovateľ prostredníctvom tejto CPS vyjadruje právne predpoklady používania vydaných kvalifikovaných časových pečiatok.

6.6.1 Vyhlásenia a záruky TSA

Pokiaľ ide o poskytované dôveryhodné služby Poskytovateľ neposkytuje žiadne záruky ani vyhlásenia s výnimkou prípadov uvedených v tejto CPS 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 CPS resp. vydaných CPS deklaruje:

- dodržiavanie svojich povinností v zmysle tejto CPS, vydaných CPS ako aj ďalších publikovaných postupov a politik, vrátane politiky informačnej bezpečnosti,
- plnenie svojich povinností v zmysle Nariadenia eIDAS a platnej legislatívy SR,
- okamžité informovanie dotknutých subjektov v prípade kompromitácie svojich súkromných kľúčov v súlade s touto CPS,
- zavedenie bezpečnostných mechanizmov, vrátane mechanizmov pri generovaní a ochrane súkromného kľúča, týkajúcich sa ochrany svojej PKI infraštruktúry,
- dostupnosť tlačenej resp. elektronickej verzie tejto CPS a ďalších publikovaných politik online,
- dodržiavanie Predpisov na ochranu osobných údajov pri zaobchádzaní s osobnými údajmi Zákazníkov.


6.6.2 Vyhlásenia a záruky účastníkov

Ak nie je v tejto CPS alebo príslušnej zmluve so Zákazníkom uvedené inak, Zákazníkom je výlučne zodpovedný za:

- poskytnutie presných a správnych informácií v komunikácii s Poskytovateľom,
- oboznámenie sa a súhlas so všetkými podmienkami danými v tejto CPS a s ňou spojenými politikami, ktoré sú dostupné v úložisku Poskytovateľa (pozri kapitola 1),
- používanie vydaných časových pečiatok len na právne účely a účely v súlade s touto CPS,

6.6.3 Vyhlásenia a záruky spoliehajúcich sa strán

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

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	26 z 29

6.6.4 Vyhlásenia a záruky ostatných účastníkov

Žiadne ustanovenia.

6.7 Zrieknutie sa záruk

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

6.8 Obmedzenia zodpovednosti

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

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


- a) porušenia povinností Zákazníkom 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 časových pečiatok a pri spoliehaní sa na časové pečiatky;
- b) neposkytnutia potrebnej súčinnosti zo strany Zákazníka;
- c) technickými vlastnosťami, nekompatibilitou, konfiguráciou, nevhodnosťou alebo inými vadami nimi použitých softvérových alebo hardvérových prostriedkov;
- d) nedoručenia alebo omeškania požiadaviek na vyhotovenie časových pečiatok, z dôvodov, ktoré nie sú na strane Poskytovateľa (najmä prípady nedostupnosti alebo preťaženia siete internet alebo vady zariadenia alebo technického vybavenia používaného overovateľom);
- e) neposkytnutia niektorej z dôveryhodných služieb alebo jej nedostupnosti v priebehu plánovanej údržby alebo reorganizácie oznámenej na webovom sídle Poskytovateľa;
- f) pôsobenia vyššej moci;

Poskytovateľ nezodpovedá za škody, ktoré vznikli spoliehajúcej sa strane z dôvodu, že pri spoliehaní sa na dôveryhodné služby Poskytovateľa nepostupovala podľa kapitoly 10. Všeobecných podmienok a v zmysle tejto CPS. resp. v zmysle Informácie pre spoliehajúcu sa stranu.

6.9 Odškodnenie

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z tejto CPS, 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 CPS, 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.

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	27 z 29

6.10 Trvanie a ukončenie

6.10.1 Termín

Tato verzia CPS platí odo dňa nadobudnutia jej platnosti t. j. 10.12.2021 až do jej nahradenia novou verziou. Podrobnosti o histórii zmien tejto CPS sú uvedené na začiatku dokumentu v časti „História zmien“.

6.10.2 Ukončenie

Platnosť tejto verzie CPS skončí dňom publikovania novej verzie s vyšším číslom ako je 1.0, prípadne ukončením činnosti poskytovania kvalifikovaných dôveryhodných služieb Poskytovateľom v čase jej platnosti. Všetky revízie CP a CPS ktoré sú uvedené v histórii zmien pre daný dokument musia byť k dispozícii Zákazníkom resp. Spoliehajúcim sa stranám.

6.10.3 Účinok ukončenia a prežitia

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

6.11 Zmeny a doplnenia

6.11.1 Postup pri zmene a doplnení

Aktualizácia CPS 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 CPS sa musia oznámiť kontaktu uvedenému v bode 1.3.2. Takáto komunikácia musí obsahovať opis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje resp. navrhuje.

Všetky schválené zmeny CPS 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 CPS musí byť očíslovaná a evidovaná, tak že novšia verzia musí mať vyššie číslo verzie ako tá, ktorú nahradzuje.

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

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	28 z 29

6.11.2 Mechanizmus a obdobie oznamovania

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

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

6.11.3 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 CPS zostáva nezmenený.

6.12 Ustanovenia o riešení sporov

Zákazník má právo zaslať Poskytovateľovi sťažnosť, podnet alebo reklamáciu na poskytnutú kvalifikovanú dôveryhodnú službu emailom na info@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 Zákazníkom. V prípade, že Zákazník je spotrebiteľom, prípadný spor môže riešiť taktiež mimosúdnu cestou.

V takomto prípade je oprávnený kontaktovať subjekt mimosúdného 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; 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.


6.13 Rozhodné právo

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

Práva a povinnosti zmluvných strán výslovne neupravené v zmluve uzatvorenej medzi Poskytovateľom a Zákazníkom, Všeobecnými podmienkami a touto CPS 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.

6.14 Dodržiavanie platných právnych predpisov

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

 NFQES	Verzia:	1.0
OID: 1.3.158.52577465.0.0.0.1.6.1	Strana:	29 z 29

7. 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
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing TimeStamps.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Timestamping protocol and time-stamp token profiles
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
- IETF RFC 3161 (2001) "Internet X.509 Public Key Infrastructure: TimeStamp Protocol (TSP)"