ViaSec

PRVÁ SLOVENSKÁ CERTIFIKAČNÁ AUTORITA
(PSCA)

Pravidlá na výkon služby poskytovania časovej pečiatky ACA PSCA

Obsah

1. Úvod

Pri tvorbe hodnoverných a v praxi overiteľných digitálnych dôkazov je nevyhnutnosťou mať dohodnutý spôsob priradenia časových údajov k danému konaniu tak, že tieto časové údaje môžu byť navzájom v neskoršej dobe porovnávané. Kvalita týchto dôkazov je založená na postupoch pri vytváraní a správe údajových štruktúr, ktoré reprezentujú danú udalosť, a na kvalite parametrických údajov, ktoré ich pevne spájajú s reálnym svetom. V tomto prípade to budú časové údaje a spôsob, ako budú využité.

Na dôvažok, v prípade overovania elektronického podpisu, môže byť nevyhnutné preukázať, že elektronický podpis podpisovateľa bol zhotovený v čase platnosti certifikátu podpisovateľa. Toto je nevyhnutné v dvoch prípadoch:

- počas doby platnosti certifikátu podpisovateľa môže dôjsť ku kompromitácii súkromného kľúča podpisovateľa a tento certifikát je z uvedeného dôvodu zrušený,
- po ukončení doby platnosti certifikátu podpisovateľa.

Na riešenie uvedeného problému je možné použiť **elektronickú časovú pečiatku**. 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

Pravidlá na výkon kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok, (ďalej len časová pečiatka) Prvej Slovenskej Certifikačnej Autority (ďalej ACA PSCA) je dokument, ktorý upresňuje a konkretizuje požiadavky na zriadenie a výkon služby časových pečiatok, ktoré špecifikuje dokument „Politika časovej pečiatky ACA PSCA“. Zaoberá sa pravidlami, ktoré ustanovujú použiteľnosť časovej pečiatky pre definovaný okruh používateľov časových pečiatok a triedy aplikácií so spoločnými bezpečnostnými požiadavkami. Definuje účastníkov procesu vydávania časových pečiatok, ich zodpovednosti, práva a rozsah použitia časových pečiatok.

Tento dokument nastoľuje zásady prevádzkovania a riadenia služby časovej pečiatky, ktoré vytvárajú ich primeranú dôveru k tejto činnosti PSCA.

Požiadavky tohto dokumentu sú zamerané na službu časových pečiatok použitú na podporu kvalifikovaných elektronických podpisov alebo na ľubovoľnú aplikáciu vyžadujúcu dôkaz, že informácia existovala pred daným časom.

Požiadavky tohto dokumentu sú založené na použití kryptografie verejných kľúčov, certifikátov verejných kľúčov a spoľahlivom časovom zdroji.

2. Základné pojmy a skratky

2.1. Pojmy

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 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 spätne odvodiť digitálny dokument

Digitálny odtlačok (dokumentu resp. súboru) – číslo (funkčná hodnota) vypočítané hash funkciou 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. skrátene žiadosť) – dátová štruktúra obsahujúca digitálny odtlačok dokumentu, na ktorý sa má vyhotoviť časová pečiatka, vytvorený žiadateľom pomocou schválenej hash funkcie.

Zdokonalený elektronický podpis – v zmysle Nariadenie eIDAS čl. 3 bod 11 je elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26 Nariadenia eIDAS.

2.2. Skratky

ACA – Akreditovaná certifikačná autorita

CA – Certifikačná autorita

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

NBÚ – Národný bezpečnostný úrad

PSCA – Prvá Slovenská Certifikačná Autorita

TSA – Vydavateľ časovej pečiatky (Time Stamp Authority)

UTC – Univerzálny svetový čas (Coordinated Universal Time)

3. Odkazy

Tento dokument vychádza z:

1) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len Nariadenie eIDAS).
2) ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI);General Policy Requirements for Trust Service Providers
3) ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
4) ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI);Time-stamping protocol and time-stamp token profiles
5) ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
6) IETF RFC 3161 (2001) "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".
7) IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".
8) Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu Národný bezpečnostný úrad. verzia 1.3.
9) 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)

4. Všeobecné ustanovenia

4.1. Služba poskytovania časovej pečiatky

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

- poskytovanie časovej pečiatky – zložka, ktorá vytvára samotné časové pečiatky,
- radenie 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 PSCA.

Druhá zložka služby je zároveň zodpovedná za inštalovanie a odinštalovanie služby poskytovania časovej pečiatky.

4.2. Vydavateľ časovej pečiatky

Vydavateľom časovej pečiatky v zmysle týchto pravidiel je:

Adresa:	**Viasec, s.r.o.**
	Prvá Slovenská Certifikačná Autorita (PSCA)
	Borská 6
	841 04 Bratislava 4
e-mail:	**support@psca.sk**
www:	**http://www.psca.sk**
telefón	**+421 2 35000100**
fax:	**+421 2 35000799**

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

PSCA preberá plnú zodpovednosť za poskytovanie služby časovej pečiatky, tak ako je definovaná v ods. 4.1. Na vytvorenie časovej pečiatky je použitý privátny kľúč TSA PSCA a v tele časovej pečiatky je identifikácia TSA PSCA ako vydavateľa časovej pečiatky.

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

Na poskytovanie časovej pečiatky využíva TSA PSCA zariadenie certifikované podľa štandardu FIPS 140-2 level 3 prípadne EAL 4+.

Všetky zmeny týkajúce sa kontaktných údajov budú okamžite zverejnené na webovej stránke PSCA.

4.3. 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 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.

5. Politika a pravidlá na výkon služby poskytovania časovej pečiatky

5.1. Prehľad

Politika časovej pečiatky je súhrn pravidiel, ktoré ustanovujú použiteľnosť časovej pečiatky pre definovaný okruh používateľov a/alebo triedy aplikácií so spoločnými bezpečnostnými požiadavkami.

Pravidlá na výkon služby poskytovania časovej pečiatky upresňujú a konkretizujú požiadavky na zriadenie a výkon služby časovej pečiatky, ktoré špecifikuje dokument „Politika časovej pečiatky ACA PSCA“, konkrétne definuje požiadavky na TSA PSCA, ktorá vydáva časové pečiatky používajúc certifikáty vydané certifikačnou autoritou poskytujúcou kvalifikované dôveryhodné služby (ďalej len ako „vydávajúca CA“).

5.2. Identifikácia

Pravidlá na výkon služby poskytovania časovej pečiatky ACA PSCA (tento dokument) sú identifikované nasledovným identifikátorom (OID):

1.3.6.1.4.1.16043.3.4.1

odvodeným od objektového identifikátora Viasec s.r.o. v nasledujúcej hierarchii príslušného podstromu:

1 – ISO assigned OIDs
1.3 – ISO Identified Organization
1.3.6 – US Department of Defense
1.3.6.1 – OID assignments from 1.3.6.1 – Internet
1.3.6.1.4 – Internet Private
1.3.6.1.4.1 – IANA-registered Private Enterprises
1.3.6.1.4.1. 16043 – Viasec s.r.o.
1.3.6.1.4.1. 16043.3 – ACA PSCA
1.3.6.1.4.1. 16043.3.4 – prevádzková smernica služby časovej pečiatky
1.3.6.1.4.1. 16043.3.4.1 – verzia 1

5.3. Používatelia a platnosť

Tento dokument má za cieľ vyhovieť požiadavkám na službu časovej pečiatky pre kvalifikovaný elektronický podpis v súlade s požiadavkami čl. 42 Nariadenia eIDAS a zákona o dôveryhodných službách.

Tento dokument je použiteľný pre službu časovej pečiatky určenú pre žiadateľov zo širokej verejnosti alebo službu časovej pečiatky pre uzatvorenú skupinu.

Službu časovej pečiatky poskytuje TSA PSCA v rámci ACA PSCA ako platenú službu.

5.4. Zhoda

TSA PSCA bude používať vo vyhotovovaných časových pečiatkach identifikáciu svojej politiky časových pečiatok v zmysle ods. 5.2.

TSA, ktorá je v zhode s touto smernicou, musí byť schopná preukázať, že si plní povinnosti v zmysle ods. 6.1 a má zavedené kontroly v zmysle ods. 7.

6. Povinnosti a zodpovednosť

6.1. Povinnosti poskytovateľa služby časovej pečiatky

6.1.1. Všeobecne

TSA PSCA ako poskytovateľ služby časovej pečiatky sa zaväzuje:

- uskutočňovať všetky príslušné požiadavky na TSA uvedené v ods. 7.,
- zabezpečiť súlad praxe TSA s procedúrami predpísanými týmito pravidlami a ďalšími súvisiacimi dokumentmi.

6.1.2. Povinnosti poskytovateľa služby časovej pečiatky voči žiadateľovi

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

6.1.3. Dôveryhodné roly a ich povinnosti

TSA PSCA z personálno-organizačného hľadiska pozostáva z rolí. Pod pojmom rola sa rozumie skupina osôb, ktoré vykonávajú buď tie isté činnosti alebo činnosti z nejakého aspektu príbuzné.

Pri niektorých zvlášť dôležitých činnostiach sa môže vyžadovať, aby pri ich vykonávaní bolo prítomných viacero osôb zastávajúcich danú rolu (tzv. princíp “k” z “n”). Dôvodom tu je bezpečnostné hľadisko – prítomné osoby sa navzájom kontrolujú – týmto sa minimalizuje tak možnosť úmyselného zneužitia právomoci nejakou osobou ako aj pravdepodobnosť neúmyselnej chyby alebo omylu.

Osoby zastávajúce rovnakú rolu sú v značnej miere navzájom zastupiteľné a nie je medzi nimi vzťah podriadenosti.

Vzťahy podriadenosti sú definované medzi jednotlivými rolami. Tieto vzťahy medzi rolami potom samozrejme definujú vzťahy medzi jednotlivými osobami, ktoré dané roly zastávajú.

V rámci TSA PSCA sú definované nasledovné dôveryhodné role:

- Administrátor TSA
- Operátor TSA
- Audítor TSA

6.1.3.1. Povinnosti administrátora TSA

Administrátori sú autorizovaní na inštaláciu, konfiguráciu a údržbu systému TSA PSCA.

Administrátor TSA je povinný najmä:

- riadiť sa ustanoveniami politiky časových pečiatok a tohto dokumentu a pokynmi vedenia PSCA, svoju činnosť koordinovať podľa potreby s ostatnými pracovníkmi TSA PSCA,
- organizovať správu páru kľúčov TSA PSCA uložených v kryptografickom module (napr. generovanie kľúčov, ich zálohovanie, obnova zo zálohy, ničenie exspirovaného súkromného kľúča),
- vykonávať inštaláciu, konfiguráciu a údržbu systému TSA PSCA vrátane kryptografického modulu a potrebného zálohovania,
- vykonávať inštaláciu, konfiguráciu a údržbu zdroja presného času,
- vykonávať správu, údržbu a zálohovanie počítača tej časti webu PSCA, ktorá sa týka služby časovej pečiatky,
- robiť záznamy o zálohovaní a iných závažných udalostiach z pohľadu správy a údržby systému TSA PSCA, a o manipulácii s párom kľúčov TSA PSCA uložených v kryptografickom module (napr. generovanie kľúčov, ich zálohovanie, obnova zo zálohy, ničenie exspirovaného súkromného kľúča) v Knihe prevádzky TSA PSCA,
- robiť obnovu systému TSA PSCA a podieľať sa na obnove webu PSCA v prípade havárie,
- prezerať záznamy (logy) vytvárané operačným systémom na počítačových systémoch TSA PSCA.

6.1.3.2. Povinnosti operátora TSA

Operátor TSA je zodpovedný za každodennú dôveryhodnú prevádzku systému TSA PSCA. Je autorizovaný na vykonávanie zálohovania dát vytváraných systémom TSA (napr. logov).

Operátor TSA je povinný najmä:

- riadiť sa ustanoveniami politiky časových pečiatok a tohto dokumentu a pokynmi vedenia PSCA, svoju činnosť koordinovať podľa potreby s ostatnými pracovníkmi TSA PSCA,

- na výzvu administrátora TSA sa podieľať na správe páru kľúčov TSA PSCA uložených v kryptografickom module (napr. generovanie kľúčov, ich zálohovanie, obnova zo zálohy, ničenie exspirovaného súkromného kľúča), najmä v prípadoch, keď sa vyžaduje pri činnosti s kryptografickým modulom prítomnosť a autorizácia viacerých osôb,
- dohliadať na správnu činnosť systému TSA vrátane zdroja presného času,
- viesť záznamy o mimoriadnych udalostiach, stavoch a problémoch v činnosti systému TSA prostredníctvom Knihy prevádzky TSA PSCA.

6.1.3.3. Povinnosti audítora TSA

Audítor TSA je autorizovaný na nahliadanie do archívov a do Knihy prevádzky TSA a môže vykonávať audit záznamov TSA PSCA.

Pri svojej činnosti audítor má právo kontrolovať všetky bezpečnostné aspekty prevádzky TSA.

Právom audítora je tiež kontrolovať súlad každodennej praxe TSA s ustanoveniami politiky časových pečiatok, tohto dokumentu a prípadných iných relevantných dokumentov.

Audítor upozorní vedenie PSCA na zistené problémy a nedostatky v činnosti TSA. O zistených problémoch a nedostatkoch v činnosti TSA môže audítor urobiť záznam do Knihy prevádzky TSA.

6.1.3.4. Nezlučiteľnosť rolí

Nezlučiteľnosť rolí minimalizuje možné riziko zneužitia systému jedným pracovníkom. V rámci TSA je nezlučiteľná rola administrátora TSA alebo operátora TSA s audítorom TSA. Výkon role administrátor TSA a operátor TSA jedným pracovníkom je povolený.

6.2. Povinnosti žiadateľa

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

Žiadateľovi sa odporúča po získaní digitálneho odtlačku dokumentu, ktorý je opatrený časovou pečiatkou, overiť si, že táto časová pečiatka 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 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 PSCA.

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.

6.3. Povinnosti spoliehajúcich sa strán

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

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

6.4. Zodpovednosť

Právna zodpovednosť ACA PSCA 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 PSCA, 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.

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

Akákoľvek žiadosť o náhradu škody musí byť podaná písomne.

7. Požiadavky na výkon služby poskytovania časovej pečiatky (TSA)

Poskytovateľ časovej pečiatky TSA PSCA musí zaviesť systém riadenia spĺňajúci nižšie uvedené požiadavky.

Požiadavky poukazujú na úlohy v oblasti bezpečnosti nasledované viac špecifickými 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 ACA PSCA v závislosti na úrovni dohodnutej služby so zákazníkom.

7.1. Prehlásenie o výkone služby a zverejňovaných informáciách

7.1.1. Prehlásenie o výkone služby

TSA PSCA zabezpečí nevyhnutnú spoľahlivosť pri poskytovaní služby časovej pečiatky nasledovnými opatreniami:

- vypracovaním procedúr resp. pracovných postupov používaných na naplnenie všetkých požiadaviek určených v tejto smernici,
- poskytnutím príslušných častí tohto dokumentu a ďalších náležitých dokumentov všetkým žiadateľom o služby časovej pečiatky ako aj spoliehajúcim sa stranám,

  Poznámka: TSA PSCA nemusí sprístupniť všetky detailné informácie o svojej praxi pri výkone TSA.

- zverejnením podmienok týkajúcich sa použitia služieb časovej pečiatky v zmysle ods. 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 ACA PSCA,
- zabezpečením prostredníctvom vedenia ACA PSCA riadneho zavedenia a používania všetkých postupov a praktík TSA PSCA,
- 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.

7.1.2. Zverejňované informácie

TSA PSCA sprístupní všetkým žiadateľom a spoliehajúcim sa stranám podmienky poskytovania služieb časovej pečiatky.

Zverejňované informácie budú obsahovať:

a) kontaktné informácie,
b) používanú politiku časových pečiatok,
c) používaný hash algoritmus

d) životnosť kľúčov používaných na vyhotovovanie časovej pečiatky, pričom doba platnosti certifikátu TSA PSCA nesmie prekročiť dobu platnosti certifikátu CA (ktorá vydáva certifikát TSA PSCA),
e) presnosť času vo vyhotovovaných časových pečiatkach 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 uchovávania záznamov (logov) TSA PSCA,
k) príslušné právne predpisy,
l) obmedzenia zodpovednosti,
m) postupy podávania sťažností a urovnávania sporov,
n) či bola TSA PSCA posudzovaná vzhľadom k svojej politike časových pečiatok, a ak áno, kým.

Hore uvedené informácie budú k dispozícii trvale prostredníctvom webu ACA PSCA. Bude ich možné získať v elektronickej podobe stiahnutím z web stránok ACA PSCA.

7.2. Manažment životného cyklu kľúčov

7.2.1. Generovanie kľúčov a získanie certifikátu TSA PSCA

Všetky kryptografické kľúče TSA a certifikáty TSA používané pri výkone služby časovej pečiatky sú generované za kontrolovaných okolností, pričom sa dodržia nasledovné požiadavky:

a) generovanie podpisových kľúčov je vykonávané vo fyzicky bezpečnom prostredí (pozri časť 7.4.4),
b) tvorba podpisových kľúčov je vykonávaná pomocou kryptografického zariadenia Document Sealing Engine 200 (v skratke DSE 200), ktorého výrobcom je firma nCipher Corporation Ltd., a ktoré spĺňa požiadavky dané štandardom FIPS 140-2 level 3,
c) kľúče resp. ním zodpovedajúci certifikát TSA budú mať nasledujúce parametre:
   - algoritmus generovania kľúčov: RSA,
   - dĺžka podpisových kľúčov: 2 048 bit,
   - algoritmus podpisovania používaný pre podpisové kľúče časových pečiatok: sha256RSA,
d) pri príprave, rozdelení a inicializácii operátorských kariet patriacich k zariadeniu je potrebné postupovať v súlade s rozhodnutím vedenia PSCA o počte operátorských kariet, ktoré sa použijú, a o zvolených konkrétnych

hodnotách konštánt „k“ a „n“ pre uplatňovanie autorizačného princípu „k“ z „n“ v rámci sady kariet,

e) generovanie podpisových kľúčov sa vykonáva za prítomnosti a pod kontrolou aspoň troch poučených osôb určených vedením PSCA, spravidla pracovníkov ACA PSCA - osôb zastávajúcich dôveryhodné roly v rámci TSA PSCA,
f) určené osoby budú prítomné na tejto ceremónii počas celej potrebnej doby, vrátane nevyhnutných prípravných prác, ktoré sú tesne spojené s vlastným procesom generovania páru kľúčov TSA do kryptografického zariadenia a ktoré musia tomuto procesu predchádzať ako napr. inštalácia ovládačov zariadenia a softvéru na jeho správu, príprava, rozdelenie a inicializácia operátorských kariet patriacich k zariadeniu,
g) poverené osoby musia byť zaviazané, aby tento výkon urobili v súlade s týmto dokumentom a príslušnou technickou dokumentáciou,
h) generovanie páru kľúčov TSA vykonáva administrátor TSA. Okrem páru kľúčov TSA vygeneruje aj žiadosť o certifikát TSA vo formáte PKCS#10 zodpovedajúcu vygenerovaným kľúčom TSA. Táto žiadosť o certifikát sa vo forme súboru archivuje na prenositeľnom médiu a použije sa v procese vydania certifikátu vydávajúcou CA.
i) Po vydaní certifikátu TSA administrátor TSA osobne prevezme daný certifikát TSA od pracovníka vydávajúcej CA a nainštaluje ho do vybavenia TSA.
j) Po ukončení generovania páru kľúčov TSA sa vykoná o ceremónii generovania páru kľúčov záznam do Knihy prevádzky TSA. Záznam do Knihy prevádzky TSA sa vykoná aj o inštalovaní certifikátu TSA do vybavenia TSA.

7.2.2. Ochrana súkromného kľúča TSA

TSA PSCA zabezpečuje, že jej súkromný kľúč zostane tajný a zostane zachovaná jeho integrita nasledovne:

a) súkromný podpisový kľúč TSA PSCA je generovaný, uchovávaný a používaný v kryptografickom module zariadenia DSE 200, ktoré spĺňa požiadavky dané štandardom FIPS 140-2 level 3,
b) v prípade zálohovania súkromného kľúča je tento kopírovaný, uchovávaný a obnovovaný len dôveryhodnými a kvalifikovanými oprávnenými osobami za prítomnosti a pod kontrolou minimálne dvoch osôb,
c) jednou z osôb, ktorá vykonáva tieto činnosti, je administrátor TSA PSCA,
d) poverené osoby robia dané výkony v súlade s týmto dokumentom a príslušnou technickou dokumentáciou.
e) po ukončení akejkoľvek manipulácie so súkromným kľúčom TSA sa vykoná o danej činnosti (napr. zálohovanie, kopírovanie alebo obnova súkromného kľúča) záznam do „Knihy prevádzky TSA PSCA“.

7.2.3. Distribúcia verejného kľúča TSA PSCA

TSA PSCA zaručuje, že integrita a dôveryhodnosť verejného verifikačného kľúča TSA PSCA je zachovaná počas jeho distribúcie k spoliehajúcim sa stranám nasledovne:

a) verejný verifikačný kľúč TSA PSCA je k dispozícii pre spoliehajúce sa strany prostredníctvom certifikátu verejného kľúča,
b) tento certifikát TSA PSCA je vydaný ako kvalifikovaný certifikát a je vydaný certifikačnou autoritou, ktorej certifikačná politika poskytuje rovnakú alebo vyššiu úroveň bezpečnosti ako má tento dokument.

7.2.4. Obnovovanie kľúča TSA PSCA

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

7.2.5. Ukončenie životnosti kľúčov TSA PSCA

TSA PSCA zaisťuje, že súkromný podpisový kľúč TSA nie je používaný po ukončení jeho životnosti nasledovne:

a) po exspirácii aktuálneho kľúča je vygenerovaný a používaný nový kľúč a k nemu patriaci nový certifikát TSA,
b) exspirovaný súkromný kľúč TSA PSCA, vrátane všetkých jeho prípadných kópií, je zničený takým spôsobom, ktorý znemožní jeho obnovu,
c) zničenie exspirovaného súkromného kľúča TSA sa vykoná dôveryhodnými a kvalifikovanými oprávnenými osobami za prítomnosti a pod kontrolou minimálne dvoch osôb,
d) jednou z osôb, ktoré vykonáva tieto činnosti, bude administrátor TSA,
e) poverené osoby sú zaviazané, aby tieto výkony robili v súlade s týmto dokumentom a príslušnou technickou dokumentáciou,
f) o zničení exspirovaného súkromného kľúča TSA sa vykoná záznam do „Knihy prevádzky TSA“,
g) systém generovania časovej pečiatky zaisťuje, že akýkoľvek pokus o vyhotovenie časovej pečiatky použitím exspirovaného súkromného kľúča TSA bude neúspešný.

7.2.6. Manažment životného cyklu kryptografického modulu používaného na podpisovanie časových pečiatok

TSA PSCA zabezpečuje bezpečnosť kryptografického hardvéru (hardvérový modul na podpisovanie časových pečiatok) počas celej jeho životnosti nasledovne:

a) garantuje, že do hardvérového modulu na podpisovanie časových pečiatok sa nebude svojvoľne zasahovať resp. s ním nedovolene manipulovať počas jeho prípadnej prepravy,
b) garantuje, že do hardvérového modulu na podpisovanie časových pečiatok sa nebude svojvoľne zasahovať resp. s ním nedovolene manipulovať v priebehu jeho uschovávania, skladovania a prevádzkového využívania,
c) inštalácia, aktivácia a prípadné zálohovanie podpisových kľúčov TSA v kryptografickom module sa vykonáva len dôveryhodnými a kvalifikovanými oprávnenými osobami za prítomnosti a pod kontrolou minimálne dvoch osôb, a vo fyzicky bezpečnom prostredí, pričom jednou z týchto osôb je administrátor TSA,
d) garantuje, že hardvérový modul na podpisovanie časových pečiatok funguje korektne,
e) v prípade vyradenia hardvérového modulu z prevádzky je z neho vymazaný súkromný kľúč TSA,
f) vymazanie súkromného kľúča TSA PSCA je vykonané dôveryhodnými a kvalifikovanými oprávnenými osobami za prítomnosti a pod kontrolou minimálne dvoch osôb, a vo fyzicky bezpečnom prostredí, pričom jednou z týchto osôb je administrátor TSA PSCA

7.3. Vytváranie časových pečiatok

7.3.1. Časové pečiatky

TSA PSCA zabezpečuje, že časové pečiatky sú vydávané bezpečne, a že obsahujú správny čas nasledovne:

a) časová pečiatka obsahuje identifikátor politiky časovej pečiatky,
b) každá časová pečiatka má jedinečné identifikačné číslo,
c) hodnoty času, ktoré sa dávajú do vyhotovovaných časových pečiatok, sú odvodené z hodnôt reálneho času poskytovaných prostredníctvom UTC (ako spoľahlivého časového zdroja),
d) čas, ktorý je dávaný do vyhotovovaných časových pečiatok, je synchronizovaný s hodnotou UTC v rámci presnosti definovanej v tomto dokumente,
e) v prípade, že je zistená odchýlka hodín TSA prekračujúca presnosť deklarovanú týmto dokumentom, TSA PSCA nevydáva časové pečiatky,
f) časová pečiatka zahŕňa hodnotu hash funkcie, ktorú poskytol žiadateľ, aplikovanú na dáta, ku ktorým sa má vyhotoviť časová pečiatka,
g) časová pečiatka je podpisovaná kľúčom TSA PSCA, ktorý je používaný len na tento účel,
h) Časová pečiatka bude obsahuje
   - identifikáciu Slovenskej republiky ako krajiny, v ktorej pôsobí TSA PSCA,
   - identifikáciu TSA PSCA,

- identifikáciu zariadenia, ktorým sa vyhotovila časová pečiatka.

7.3.2. Vyhotovenie a overenie časovej pečiatky

7.3.2.1.

Žiadateľ zašle (prostredníctvom dohodnutého rozhrania) TSA PSCA ako vydavateľovi časovej pečiatky žiadosť o vyhotovenie časovej pečiatky. Žiadosť obsahuje digitálny odtlačok dokumentu, na ktorý sa má vyhotoviť časová pečiatka, vytvorený pomocou schválenej hash funkcie.

Dohodnutým rozhraním môže byť:

- web rozhranie (protokoly http resp. https) servera TSA PSCA
- rozhranie, ktoré na strane klienta poskytuje klientský softvér dohodnutý s ACA PSCA resp. schválený ACA PSCA

7.3.2.2.

Ak je žiadosť v schválenom formáte a nie sú prekážky na vyhotovenie časovej pečiatky zo strany TSA PSCA, TSA PSCA pomocou bezpečného zariadenia na vyhotovovanie časových pečiatok a zdroja času vyhotoví časovú pečiatku na predložený digitálny odtlačok dokumentu a pošle ju žiadateľovi v režime on-line.

7.3.2.3.

Ak žiadosť o vyhotovenie časovej pečiatky nemá schválený formát alebo ak u TSA PSCA vznikli prekážky vyhotovenia časovej pečiatky (napr. sa zistila odchýlka času mimo deklarovanú presnosť), TSA PSCA časovú pečiatku na predložený digitálny odtlačok dokumentu nevyhotoví.

7.3.2.4.

Overenie platnosti časovej pečiatky vykonáva spoliehajúca sa strana na základe danej časovej pečiatky a dokumentu, na ktorý bola daná časová pečiatka vyhotovená, a politiky časových pečiatok, ktorá sa na danú časovú pečiatku vzťahuje.

7.3.2.5.

Časová pečiatka je platná, ak

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

7.3.3. Synchronizácia času s UTC

TSA PSCA zabezpečuje, že čas ňou používaný je synchronizovaný s UTC s deklarovanou presnosťou 500 milisekúnd nasledovne:

a) kalibrácia hodín TSA PSCA je vykonávaná tak, že očakávaná odchýlka času nebude mimo deklarovanú presnosť,
b) hodiny zariadenia TSA PSCA sú chránené proti hrozbám, ktoré by mohli viesť k nezistiteľným zásahom do hodín, ktoré by mohli mať za následok ich odchýlku od kalibrácie, pričom pod pojmom hrozba sa myslí napr. neoprávnený zásah (neautorizovanej) osoby alebo elektromagnetické rušenie.
c) TSA PSCA zabezpečí, že v prípade, že sa čas, ktorý by bol uvedený v časovej pečiatke, odchýli od synchronizácie s UTC, zastaví vydávanie časových pečiatok,

TSA PSCA zabezpečí, že bude vykonaná synchronizácia hodín v prípade, že bude notifikovaná oprávneným orgánom o výskyte opravnej sekundy.

7.4. Manažment a prevádzka TSA PSCA

7.4.1. Manažment bezpečnosti

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

a) TSA PSCA preberá plnú zodpovednosť za všetky aspekty poskytovania služby časovej pečiatky popisované vo svojej politike,
b) TSA PSCA poskytne smernice o informačnej bezpečnosti prostredníctvom svojho vedenia, ktoré je zodpovedné za definovanie informačnej bezpečnosti,
c) s týmto dokumentom sú oboznámení všetci pracovníci, ktorých sa týka,
d) infraštruktúra informačnej bezpečnosti nevyhnutná pre zabezpečenie bezpečnosti v rámci TSA PSCA je udržiavaná počas celej doby činnosti TSA PSCA.
e) akékoľvek zmeny, ktoré by mohli ovplyvniť úroveň bezpečnosti, sú odsúhlasené vedením ACA PSCA,
f) bezpečnostné opatrenia a pracovné postupy TSA PSCA, systémové a informačné aktíva poskytujúce služby časovej pečiatky sú dokumentované, zavedené a udržiavané.

7.4.2. Klasifikácia a manažment aktív

TSA PSCA zabezpečuje, že jej informačné a ďalšie aktíva sú chránené na požadovanej úrovni, a že TSA PSCA má zoznam všetkých aktív a ich klasifikáciu z pohľadu požiadaviek na ochranu, ktoré sú v súlade s vykonanou analýzou rizík.

7.4.3. Personálna bezpečnosť

TSA PSCA zabezpečuje, že postupy personálnej práce a prijímania do zamestnania podporujú jej dôveryhodnosť nasledovne:

a) TSA PSCA zamestnáva pracovníkov, ktorí majú zodpovedajúce znalosti, skúsenosti a nevyhnutnú kvalifikáciu pre poskytované služby, a ktorí sú vhodní pre danú pracovnú pozíciu,
b) mechanizmus dôveryhodných rolí a ich zodpovednosti sú popísané v ods. 6.1.3 tohto dokumentu,
c) dôveryhodné role, na ktorých je závislá bezpečnosť TSA PSCA, sú jasne identifikované,
d) jednotlivé dôveryhodné role v rámci TSA PSCA majú popisy práce definované z hľadiska rozdelenia povinností a minimálnych privilégií, 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. 7.4.1)

Pre manažment služby časovej pečiatky sú aplikované nasledovné princípy:

a) je zamestnávaný manažérsky personál, ktorý:
   - má znalosť technológie časovej pečiatky,
   - má znalosť technológie elektronického podpisu,
   - má znalosť mechanizmu kalibrácie a synchronizácie hodín TSA s UTC,
   - je oboznámený s postupmi pre osoby so zodpovednosťou v bezpečnostnej oblasti,
   - má skúsenosti v informačnej bezpečnosti a odhade rizika,

b) všetci pracovníci TSA PSCA v dôveryhodných rolách sú mimo akéhokoľvek konfliktu záujmov, ktorý by mohol ovplyvniť ich nestrannosť,
c) pracovníci TSA PSCA sú menovaní do dôveryhodných rolí vedúcim pracovníkom zodpovedným za bezpečnosť,
d) TSA PSCA nenavrhuje do dôveryhodnej roly pracovníka, ktorý bol odsúdený za trestný čin, prípadne sú známe iné skutočnosti, ktoré ovplyvňujú jeho vhodnosť na danú pozíciu.

7.4.4. Fyzická a priestorová bezpečnosť

TSA PSCA zabezpečuje, že fyzický prístup k jej kritickým aktívam je kontrolovaný a riziko neoprávneného fyzického prístupu je minimalizované nasledovne:

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. 7.2.1 a 7.2.2.
c) technické vybavenie používané na poskytovanie služby časovej pečiatky je prevádzkované v prostredí, ktoré ho fyzicky chráni 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.

7.4.5. Prevádzkový manažment

TSA PSCA zabezpečuje, že systémové komponenty sú bezpečné a pracujú správne, s minimálnym rizikom poruchy nasledovne:

a) integrita systémových komponentov TSA PSCA je chránená proti vírusom, škodlivému a neautorizovanému softvéru,
b) zaznamenávanie incidentov a postupy reakcií na incidenty je zavedené takým spôsobom, ktoré minimalizuje škody z bezpečnostných incidentov a zlyhaní,
c) s médiami používanými v rámci dôveryhodného TSA PSCA systému sa zaobchádza takým spôsobom, aby sa predišlo ich poškodeniu, odcudzeniu, neautorizovanému prístupu k nim a zastaraniu,
d) médiá obsahujúce citlivé informácie, ktoré nie sú už potrebné, sú vymazané a bezpečným spôsobom likvidované,
e) pre všetky dôveryhodné role sú ustanovené a zavedené postupy ktoré majú vplyv na poskytovanie služby časovej pečiatky.

7.4.6. Manažment prístupu k systému

TSA PSCA zabezpečuje že k prístup k systému je vyhradený len autorizovaným osobám nasledovným spôsobom:

a) je implementovaný firewall, aby sa zabránilo neautorizovanému prístupu cez sieť,
b) firewall je nakonfigurovaný tak, aby sa zabránilo používaniu všetkých protokolov a prístupov (napr. portov), ktoré nie sú potrebné na prevádzku TSA,

c) TSA PSCA zaisťuje efektívnu administráciu prístupu používateľov (vrátane používateľov v dôveryhodných rolách) na udržiavanie bezpečnosti systému, včítane manažovania používateľských kont, auditovania a dočasnej modifikácie alebo odopretia prístupu,
d) TSA PSCA zaisťuje, že prístup k funkciám informačného a aplikačného systému je obmedzený v zmysle politiky prístupových práv, a že systém používaný TSA PSCA poskytuje dostatočnú kontrolu počítačovej bezpečnosti na oddelenie dôveryhodných rolí, tak ako sú určení v týchto pravidlách,
e) pracovníci TSA PSCA sa náležite identifikujú a autentizujú pred použitím kritických aplikácií,
f) pracovníci TSA PSCA musia byť sú zodpovední za svoje aktivity, napr. prostredníctvom uchovávania záznamov o aktivitách (logov) sa dá dokázať zodpovednosť konkrétnej osoby za danú aktivitu,
g) TSA PSCA zaisťuje, že sieťové komponenty (napr. smerovače) sú prevádzkované vo fyzicky bezpečnom prostredí a že ich konfigurácie sa periodicky preverujú na súlad s požiadavkami TSA,
h) nepretržite je používané monitorovacie a poplašné vybavenie, na detekciu a registrovanie neautorizovaných pokusov o prístup k systémom TSA,
i) sú spracované postupy pre prípady pokusov o neautorizovaný prístup k systémom TSA, ktoré umožňujú vhodným spôsobom na ne reagovať.

7.4.7. Nasadenie a údržba dôveryhodných systémov

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

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

Nasadenie používaného softvéru do prevádzky a vykonávanie jeho zmien je v kompetencii administrátora TSA.

7.4.8. Kompromitácia služieb TSA PSCA

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

a) „Plán obnovy PSCA“ sa zaoberá kompromitáciou alebo podozrením na kompromitáciu privátneho podpisového kľúča TSA PSCA alebo stratou kalibrácie hodín TSA PSCA, ktoré môžu ovplyvniť už vydané časové pečiatky,
b) v prípade kompromitácie alebo podozrenia z kompromitácie alebo pri strate kalibrácie dá TSA PSCA k dispozícii všetkým žiadateľom a spoliehajúcim sa stranám popis zistenej kompromitácie,

c) v prípade kompromitácie činnosti TSA PSCA, podozrenia z kompromitácie alebo straty kalibrácie TSA PSCA nevydáva časové pečiatky až do času, keď sa prijmú opatrenia na obnovu po kompromitácii,

d) v prípade závažnej kompromitácie činnosti TSA PSCA alebo straty kalibrácie, sprístupní TSA PSCA, pokiaľ je to možné, všetkým žiadateľom a spoliehajúcim sa stranám informáciu, ktorá by im mala napomôcť identifikovať časové pečiatky, ktoré by mohli byť ovplyvnené, s výnimkou, keď by to viedlo k porušeniu súkromia používateľov služby časovej pečiatky alebo bezpečnosti služby TSA PSCA

7.4.9. Ukončenie činnosti TSA PSCA

TSA PSCA zabezpečuje, že prípadné narušenie služieb žiadateľom a spoliehajúcim sa stranám v dôsledku zastavenia služby poskytovania časovej pečiatky bude minimalizované a obzvlášť zaisťuje následnú podporu vo forme informácií požadovaných na overenie správnosti časových pečiatok nasledovným spôsobom:

a) pred ukončením poskytovania služby časovej pečiatky sa vykoná minimálne nasledovné:

- TSA PSCA poskytne všetkým potenciálnym žiadateľom a spoliehajúcim sa stranám informácie týkajúce sa ukončenia jej činnosti,
- TSA PSCA prenesie na spoľahlivý subjekt svoje záväzky týkajúce sa udržiavania záznamov (logov) a archívu pre audit nevyhnutných pre dokazovanie správnej činnosti TSA PSCA po primeranú dobu,
- TSA PSCA prenesie na spoľahlivý subjekt svoje záväzky, aby bol k dispozícii počas primeranej doby jej verejný verifikačný kľúč prostredníctvom certifikátu pre spoliehajúce sa strany,
- súkromný podpisový kľúč TSA vrátane všetkých jeho kópií je zničený takým spôsobom, že nie je možná jeho obnova,
- zničenie súkromného kľúča TSA je vykonané pod dohľadom viacerých kvalifikovaných osôb a o zničení súkromného kľúča TSA je spísaný protokol dokladujúci jeho zničenie,

b) TSA PSCA prijme všetky kroky na zrušenie svojich certifikátov.

7.4.10. Súlad s právnymi požiadavkami

TSA PSCA 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).

TSA PSCA zabezpečuje, že:

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

b) v rámci TSA PSCA 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 ACA PSCA,
c) informácie poskytnuté žiadateľmi o služby TSA PSCA sú chránené pred ich zverejnením, s výnimkou, že na to dá súhlas žiadateľ, alebo to prikáže sú, alebo iný kompetentný štátny orgán.

7.4.11. Zaznamenávanie údajov týkajúcich sa výkonu služby poskytovania časovej pečiatky

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

a) TSA PSCA dokumentuje, ktoré konkrétne prípady a údaje sú zaznamenávané,
b) je udržiavaná dôvernosť 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 TSA PSCA, manažmentu kľúčov a synchronizácie času,
f) záznamy týkajúce sa činnosti služby časovej pečiatky sú uchovávané počas primeranej doby po vypršaní platnosti podpisového kľúča TSA PSCA, aby bola možné poskytnúť právny dôkaz a ako je to uvedené v prehlásení o zverejňovaní informácií (pozri ods. 7.1),
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 (min. 10 rokov),
h) akékoľvek informácie o žiadateľovi sú uchovávané ako dôverné, okrem prípadov, keď existuje súhlas žiadateľa s ich publikovaním alebo prípadov uvedených v ods.7.4.10 c),
i) sú uchovávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k životnému cyklu kľúčov TSA,
j) sú uchovávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k životnému cyklu certifikátov TSA,
k) sú uchovávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k synchronizácii hodín TSA,
l) sú uchovávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k detegovaniu straty synchronizácie hodín.

7.5. Organizačné aspekty

TSA PSCA zaisťuje, že jej organizácia je spoľahlivá, pričom zdôrazňuje že:

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