# ViaSec

**PRVÁ SLOVENSKÁ CERTIFIKAČNÁ AUTORITA**
**(PSCA)**


# Politika 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

Politika časovej pečiatky Prvej Slovenskej Certifikačnej Autority (ďalej PSCA) je súhrn pravidiel, ktoré ustanovujú použiteľnosť časovej pečiatky pre definovaný okruh jej používateľov a triedy aplikácií so spoločnými bezpečnostnými požiadavkami. Definuje účastníkov procesu vydávania časovej pečiatky, ich zodpovednosti, práva a rozsah použitia časovej pečiatky.

Politika popísaná v tomto dokumente poskytuje žiadateľovi a spoliehajúcej sa strane zásady prevádzkovania a riadenia služby časovej pečiatky, ktoré vytvárajú ich primeranú dôveru k tejto činnosti PSCA.

Požiadavky tejto politiky 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 tejto politiky 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 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. skrátene 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

## 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

Táto politika vychádza z:

- 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 ).
- 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)".
- IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".
- Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu Národný bezpečnostný úrad. verzia 1.3
- 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 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 PSCA.

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

## 4.2. Vydavateľ časovej pečiatky

Vydavateľom časovej pečiatky v zmysle tejto politiky 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 3Všetky 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 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.

Tento dokument definuje politiku TSA PSCA a prostredníctvom nej 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

Politika časovej pečiatky ACA PSCA je identifikovaná 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 – Politika časových pečiatok
1.3.6.1.4.1. 16043.3.4.1. – verzia 1

## 5.3. Používatelia a platnosť

Táto politika má za cieľ vyhovieť požiadavkám na službu časovej pečiatky pre kvalifikovaný elektronický podpis v súlade s požiadavkami čl. 42 Nariadenia eIDAS a zákona č. 272/2016 Z. z. o dôveryhodných službách.

Táto politika je použiteľná 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 používa vo vyhotovovaných časových pečiatkach identifikáciu politiky časových pečiatok v zmysle ods. 5.2

TSA, ktorá je v zhode s touto politikou, 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 touto politikou a ďalšími súvisiacimi dokumentmi,
- poskytovať služby časovej pečiatky v súlade s prevádzkovou smernicou TSA a ďalšími súvisiacimi dokumentmi.

### 6.1.2. Povinnosti poskytovateľa služby časovej pečiatky voči žiadateľovi

TSA PSCA 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.

## 6.2. 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 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 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 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 jeho podpísania,
b) brať do úvahy všetky obmedzenia používania časovej pečiatky uvedené v politike časovej pečiatky
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 časovej pečiatky (TSA)

Poskytovateľ časovej pečiatky TSA PSCA 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 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 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 PSCA 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 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 časovej pečiatky,
c) používaný algoritmus hašovacej funkcie,
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 uchovávania záznamov 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.

Hore uvedené informácie sú k dispozícii trvale prostredníctvom webu ACA PSCA.

Bude ich možné získať v elektronickej podobe stiahnutím z web stránok ACA PSCA.

Za ich základný zdroj sa považuje tento dokument.

## 7.2. Manažment životného cyklu kľúčov

### 7.2.1. Generovanie kľúčov

TSA PSCA zaistí, 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. 7.4.4) dôveryhodnými a kvalifikovanými osobami (pozri ods. 7.4.3) za prítomnosti a pod kontrolou stanoveného počtu osôb.

### 7.2.2. Ochrana súkromného kľúča TSA

TSA PSCA zabezpečí, že jej súkromný kľúč zostane tajný a zostane zachovaná jeho integrita.

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

### 7.2.3. Distribúcia verejného kľúča TSA PSCA

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

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

### 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 zaistí, že súkromný podpisový kľúč TSA nebude používaný po ukončení jeho životnosti.

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

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

## 7.3. Vytváranie časovej pečiatky

### 7.3.1. Časová pečiatka

TSA PSCA zabezpečí, že časová pečiatka je vydávaná bezpečne, a že obsahuje správny čas.

Predovšetkým:

a) časová pečiatka obsahuje identifikátor politiky časovej pečiatky,
b) časová pečiatka má jedinečné identifikačné číslo,

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

### 7.3.2. Vyhotovenie a overenie časovej pečiatky

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 hašovacej funkcie.

Ak je žiadosť v schválenom formáte a nie sú prekážky na vyhotovenie časovej pečiatky zo strany TSA PSCA, 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 PSCA vznikli prekážky vyhotovenia časovej pečiatky (napr. sa zistila odchýlka času mimo deklarovanú presnosť), TSA PSCA 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.

### 7.3.3. Synchronizácia času s UTC

TSA PSCA zabezpečí, že čas ňou používaný bude synchronizovaný s UTC s deklarovanou presnosťou 500 milisekúnd, a to predovšetkým nasledovnými opatreniami:

a) kalibrácia hodín TSA PSCA bude vykonávaná tak, že očakávaná odchýlka času nebude mimo deklarovanú presnosť,
b) hodiny zariadenia TSA PSCA budú chránené proti hrozbám, ktoré by mohli viesť k nezistiteľným zásahom do hodín, ktoré by mohli mať za následok ich odchýlku od kalibrácie,

c) TSA PSCA zabezpečí, 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,
d) 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 zabezpečí 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 v tejto politike,
b) TSA PSCA poskytne smernice o informačnej bezpečnosti prostredníctvom svojho vedenia, ktoré je zodpovedné za definovanie informačnej bezpečnosti.
c) s touto politikou budú oboznámení všetci pracovníci, ktorých sa uvedená politika týka,
d) infraštruktúra informačnej bezpečnosti nevyhnutná pre zabezpečenie bezpečnosti v rámci TSA PSCA bude udržiavaná počas celej doby činnosti TSA PSCA,
e) akékoľvek zmeny, ktoré by mohli ovplyvniť úroveň bezpečnosti, budú 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 zabezpečí, že jej informačné a ďalšie aktíva sú chránené na požadovanej úrovni, a to predovšetkým:

a) 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 zabezpečí, že postupy personálnej práce a prijímania do zamestnania podporujú jej dôveryhodnosť.

Predovšetkým:

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) TSA PSCA 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”),
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 PSCA, sú jasne identifikované,
d) jednotlivé dôveryhodné roly 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)

### 7.4.4. Fyzická a priestorová bezpečnosť

TSA PSCA zabezpečí, 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. 7.2.1 a 7.2.2.,
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.

### 7.4.5. Prevádzkový manažment

TSA PSCA zabezpečí, že systémové komponenty sú bezpečné a pracujú správne, s minimálnym rizikom poruchy.

Predovšetkým:

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

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 PSCA systému sa zaobchádza takým spôsobom, aby sa predišlo ich poškodeniu, odcudzeniu, neautorizovanému prístupu k nim a ich zastaraniu.

### 7.4.6. Manažment prístupu k systému

TSA PSCA zaistí, že k prístup k systému je vyhradený len autorizovaným osobám.

Predovšetkým:

a) je implementovaná ochrana, ktorá zabráni neautorizovanému prístupu cez sieť,
b) TSA PSCA zaistí 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.

### 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 procedúry alebo postupy odporúčané výrobcom softvéru.

### 7.4.8. Kompromitácia služieb TSA PSCA

TSA PSCA zabezpečí, 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.

### 7.4.9. Ukončenie činnosti TSA PSCA

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

### 7.4.10. Súlad s právnymi požiadavkami

TSA PSCA zabezpečí 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,
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 zverejnením, pokiaľ na to nedá súhlas žiadateľ alebo to neprikáže súd alebo iný kompetentný štátny orgán.

### 7.4.11. Zaznamenávanie údajov týkajúcich sa výkonu služby časovej pečiatky

TSA PSCA zabezpečí, 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 PSCA dokumentuje, ktoré konkrétne prípady a údaje sa majú zaznamenávať,
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,
h) akékoľvek informácie o žiadateľovi sa uchovávajú ako dôverné okrem prípadov, keď existuje súhlas žiadateľa s ich publikovaním alebo prípadov uvedených v ods. 7.4.10,
i) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k životnému cyklu kľúčov TSA PSCA,
j) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k životnému cyklu certifikátov TSA PSCA,
k) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k synchronizácii hodín TSA PSCA,
l) sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k detegovaniu straty synchronizácie hodín.

## 7.5. Organizačné aspekty

TSA PSCA zaistí, že jej organizácia je spoľahlivá, pričom kladie dôraz, 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 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