KCCKB Verejné

Druh dokumentu: Politika

CERTIFIKAČNÁ POLITIKA PRE KVALIFIKOVANÚ DÔVERYHODNÚ SLUŽBU VYHOTOVOVANIA KVALIFIKOVANÝCH ELEKTRONICKÝCH ČASOVÝCH PEČIATOK

Číslo: 21

Verzia: 2

Zverejnený: 27.5.2024

Účinný od: 27.5.2024

Záväzný pre: *VŠETCI ZAMESTNANCI*

Prístupný pre: *VEREJNOSŤ*

Vydal útvar: *Odbor auditu a autorizovaných činností*

Autori: Tomáš Hettych

Spoluautori:

Schválil: Ivan Makatura, generálny riaditeľ

1 ÚVOD

Tento dokument popisuje politiku poskytovania dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok (v ďalšom aj „CP TSA“) a bezpečnostné požiadavky, ktoré sa týkajú prevádzkovej praxe a postupov pri poskytovaní tejto služby.

Tento dokument obsahuje pravidlá na výkon certifikačných činností TSP KCCKB (CPS) a informácie pre používateľov a spoliehajúce sa tretie strany ako podklad pre posúdenie dôveryhodnosti certifikátu.

Účelom tohto dokumentu je definovať prezentovať metodiku, záväzné postupy a zodpovednosti poskytovateľa pri vydávaní časových pečiatok, definovať úlohy, povinnosti a zodpovednosť zúčastnených strán pri používaní časových pečiatok.

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

Poskytovateľom tejto dôveryhodnej služby je:

Názov poskytovateľa	Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
Sídlo	Na družstvo 125, 916 25 Brunovce
Korešpondenčná adresa	Budatínska 32, 851 06 Bratislava
IČO	52 839 052
Telefón	+421 905 531 652
E-mail	doveryhodne.sluzby@cybercompetence.sk
Webové sídlo	www.cybercompetence.sk

(ďalej len „KCCKB“), prostredníctvom svojho systému autority časovej pečiatky (TSA KCCKB).

Táto politika môže byť použitá pre verejnú službu poskytovanie časových pečiatok ako aj na použitie v uzavretých komunitách.

Tento dokument môže byť použitý nezávislými orgánmi ako základ pre potvrdenie, že KCCB je dôveryhodný na vyhotovovanie časových pečiatok.

Služby časovej pečiatky identifikované v tomto dokumente sú využívané v okruhu TSA zriadenej a prevádzkovanej Kompetenčným a certifikačný centrom kybernetickej bezpečnosti.

TSA KCCKB nepublikuje samostatné vyhlásenie o zverejnení (Disclosure statement), potrebné informácie sú uvedené v nasledujúcich bodoch.

1.1 Prehľad

Táto CP TSA sa týka poskytovania dôveryhodnej služby vyhotovovania kvalifikovanej elektronickej časovej pečiatky v zmysle ustanovení Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 3. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS“), a vypracovanej podľa normy ETSI EN 319 421 V1.2.1 Policy and security requirements for Trust Service Providers issuing time stamps.

Vyhotovované kvalifikované elektronické pečiatky sú podpisované s využitím súkromných kľúčov jednotiek vyhotovujúcich časové pečiatky (ďalej aj „TSU“), ktorých certifikáty môžu byť vydané výhradne týmito certifikačnými autoritami:

Vydavateľ
KCA NBU SR 3

1.2 Názov dokumentu a jeho identifikácia

Politika časových pečiatok je identifikovaná nasledovným identifikátorom odvodeným od objektového identifikátora KCCKB:

1.3.158.52839052.0.1.4

kde jednotlivé zložky OID majú nasledovný význam:

1	ISO
3	ISO Identified Organization
158	Slovakia
52839052	jedinečný identifikátor KCCKB (IČO)
0	poskytovanie dôveryhodných služieb
1	Certifikačné politiky
4	Certifikačná politika pre dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok

1.3 Účastníci PKI

V rámci poskytovania dôveryhodných služieb vyhotovovania kvalifikovaných elektronických časových pečiatok sú účastníkmi infraštruktúry verejného kľúča Poskytovateľa uvedení v tejto časti.

1.3.1 Jednotka vyhotovovania časových pečiatok

Jednotka vyhotovovania časových pečiatok:

- je entita, ktorá poskytuje kvalifikované dôveryhodné služby vyhotovovania kvalifikovaných elektronických časových pečiatok používateľom (Orgány verejnej moci, Spoliehajúce sa strany),
- má celkovú zodpovednosť za poskytovanie kvalifikovaných dôveryhodných služieb špecifikovaných v odstavci 1.1,
- je uvádzaná vo vydaných časových pečiatkach ako vydavateľ a jej súkromné kľúče sú používané pri vyhotovovaní podpisu týchto časových pečiatok,
- zaručuje, že všetky aspekty jej služieb, operácií a infraštruktúry zviazanej s časovými pečiatkami vydanými podľa tejto politiky sú vykonávané v súlade s jej požiadavkami a ustanoveniami a v súlade s týmto dokumentom.

TSU KCCKB sú súčasťou hierarchickej PKI:

KCA NBÚ SR 3 -> TSU

TSA KCCKB môže prevádzkovať v rámci podriadenosti pod certifikačnou autoritou KCA3 viaceré TSU poskytujúce dôveryhodné služby vyhotovovania časovej pečiatky.

1.3.2 Registračná autorita

Žiadne ustanovenia – nie je relevantné.

1.3.3 Klient

O vyhotovenie časovej pečiatky môže žiadať:

1. Národný bezpečnostný úrad SR
2. KCCKB

Žiadatelia o službu časovej pečiatky sú povinní:

- postupovať pri žiadosti o vydanie časovej pečiatky spôsobom predpísaným v tomto dokumente,
- používať predpísaný formát a protokol žiadosti o vydanie časovej pečiatky,
- preveriť platnosť vydanej časovej pečiatky bezprostredne po jej príjme spôsobom definovaným v týchto zásadách,
- riešiť nezrovnalosti pri vydaní časovej pečiatky s kontaktnou osobou KCCKB bez zbytočných prieťahov.

1.3.4 Spoliehajúca sa strana

Spoliehajúca sa strana je ľubovoľná právnická alebo fyzická osoba, prípadne technologické zariadenie a to ako so sídlom v SR tak aj v zahraničí, ktorá na základe overovania časovej pečiatky skúma (overuje alebo verifikuje), či údaje ku ktorým existuje časová pečiatka objektívne existovali v určitom (určiteľnom) čase.

Spoliehajúce sa strany sú povinné postupovať pri overovaní časovej pečiatky v zmysle inštrukcií tohto dokumentu o overovaní časových pečiatok.

1.3.5 Iní účastníci

Poskytovateľ pre zabezpečenie funkčnosti služby využíva infraštruktúru Národného bezpečnostného úradu (ďalej aj NBÚ)

1.4 Použiteľnosť časovej pečiatky

Časové pečiatky vyhotovené v rámci poskytovania dôveryhodnej služby vyhotovovania časových pečiatok popísanej v tejto politike môžu orgány verejnej moci a Spoliehajúce sa strany používať bez obmedzenia všade, kde je vyžadovaná časová pečiatka definovaná v článku 42 Nariadenia eIDAS

1.5 Správa politiky

Táto politika spĺňa požiadavky štandardu ETSI TS 102 023.

1.5.1 Organizácia zodpovedná za správu dokumentu

Tento dokument je spravovaný Odborom *auditu a autorizovaných činností* KCCKB.

Kontaktná adresa:
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
Budatínska 32,
851 05 Bratislava,
Slovenská republika,

www.cybercompetence.sk

1.5.2 Kontaktná osoba

Bezpečnostný správca TSA KCCKB
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
Budatínska 32,
851 05 Bratislava,

Telefón: +421 905 531 652
e-mail:
doveryhodne.sluzby@cybercompetence.sk

1.5.3 Osoba rozhodujúca o CP

Vo všetkých záležitostiach a aspektoch týkajúcich sa TSA a jej činnosti s konečnou platnosťou rozhoduje riaditeľ odboru auditu a autorizovaných činností.

1.5.4 Postupy schvaľovania CP a externej politiky

Ešte pred začiatkom prevádzky má mať TSA schválený svoju CP a CPS a musí spĺňať všetky jeho požiadavky.

CP a CPS musia byť aktualizované najmä v nasledujúcich prípadoch:
- pri zmene prevádzkových podmienok,
- pri zmene procesov,
- pri zmene rizikového profilu alebo ako reakcia na bezpečnostné incidenty,

alebo minimálne raz za 2 roky.

Za ich aktualizáciu zodpovedá vlastník dokumentu.

Obsah CP a CPS schvaľuje riaditeľ odboru auditu a autorizovaných činností.

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

1.6 Definície a skratky

1.6.1 Definície

Žiadateľ	Orgány verejnej moci, ktorým sú poskytované služby časových pečiatok na základe vzájomnej dohody.
Spoliehajúca sa strana	Ľubovoľná právnická alebo fyzická osoba, ktorá na základe overovania časovej pečiatky skúma (overuje alebo verifikuje) či údaje ku ktorým existuje časová pečiatka objektívne existovali v určitom (určiteľnom) čase.
Univerzálny koordinovaný čas	Časový údaj v „svetovom čase“ odvodený od slnečného času nultého poludníka.

1.6.2 Skratky

UTC	Univerzálny koordinovaný čas
TST	Telo časovej pečiatky (Time Stamp Token)
TSA	Vydavateľ časových pečiatok (Time Stamp Authority)

KCCKB	Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
NBÚ	Národný bezpečnostný úrad
KCA	Koreňová certifikačná autorita NBÚ
TAC	Čas na dokončenie (Time At Completion)
PMA	Autorita pre správu poriadkov (Policy Management Authority)

2 ÚLOŽISKÁ

Webové sídlo poskytovateľa uvedené v bode 1 slúži ako Úložisko. Úložisko je prístupné Klientom, Spoliehajúcim stranám a verejnosti.

2.1 Zverejňovanie informácií o TSA

Na Úložisko sú ukladané minimálne tieto informácie:

- Všetky vydané CRL od začiatku činnosti vyhotovovania časových pečiatok,
- Vlastné certifikáty všetkých TSU, ktoré sú využívané pri poskytovaní činnosti vyhotovovania časových pečiatok,
- Tento dokument.

2.2 Frekvencia zverejňovania informácií

Zoznam zrušených certifikátov (CRL) musí byť publikovaný ako je špecifikované v aktuálnom CP pre vyhotovovanie kvalifikovaných certifikátov. Informácie o zrušenom certifikáte TSU musia byť dostupné na webovom sídle (pozri kapitola 0), ktorý slúži ako jeho úložisko.

CP TSA sa musí zverejniť čo najskôr po ich schválení a vydaní.

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

2.3 Kontroly prístupu

V záujme ochrany informácií uložených v úložisku, ktoré nie sú určené na verejné rozšírenie musí TSA KCCKB:

- vynaložiť maximálne úsilie na to, aby zaistil integritu, dôvernosť a dostupnosť dát vyplývajúcich s poskytovaných dôveryhodných služieb,
- vykonať logické a bezpečnostné opatrenia, aby zabránil neautorizovanému prístupu k úložisku osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v úložisku.

3 VŠEOBECNÉ USTANOVENIA

Služba časových pečiatok poskytuje žiadateľovi časový údaj logicky prepojený s údajmi vo formáte časovej pečiatky, pre ktorý sa časová pečiatka požaduje.

Poskytnutím časovej pečiatky KCCKB ako poskytovateľ časových pečiatok osvedčuje, že údaje ku ktorým bola časová pečiatka vyhotovená existovali v čase uvedenom v časovej pečiatke.

3.1 Všeobecné ustanovenia politiky

Právne záruky a obmedzenia záruk v rámci tohto dokumentu vyplývajú zo zákonných predpisov platných v SR.

Spory budú riešené v zmysle platných zákonov a ostatných všeobecne záväzných predpisov SR.

V rámci tohto dokumentu nie je stanovená žiadna finančná zodpovednosť. V prípade jej vzniku bude finančná zodpovednosť jednotlivých strán určená právnymi predpismi platnými v Slovenskej republike.

3.2 Služby súvisiace s časovou pečiatkou

Služby súvisiace s časovou pečiatkou je možné z pohľadu naplnenia požiadaviek rozdeliť na dve samostatné služby, ktorými sú:

- poskytovanie časovej pečiatky – táto služba vytvára samotnú časovú pečiatku,
- manažment časovej pečiatky – táto služba monitoruje a riadi procesy vyhotovovania časovej pečiatky, aby sa zaistilo, že služba je poskytovaná v súlade s touto CP TSA. Súčasťou tohto manažmentu je proces aktivácie resp. de-aktivácie služby vyhotovovania časovej pečiatky. Manažment časovej pečiatky napríklad okrem iného zabezpečuje, aby čas použitý pri vyhotovovaní časových pečiatok bol správne synchronizovaný s UTC.

3.3 Vydavateľ časových pečiatok

Poskytovateľ dôveryhodnej služby vyhotovovania časovej pečiatky pre potreby klientov v zmysle tejto CP TSA je KCCKB prostredníctvom TSA KCCKB.

KCCKB musí niesť celkovú zodpovednosť za poskytovanie služieb súvisiacich s časovou pečiatkou ako sú definované v odstavci 3.2.

Zodpovednosť TSA KCCKB za vyhotovovanie časových pečiatok je identifikovateľná (pozri bod 6.7.1)

TSA KCCKB môže prevádzkovať niekoľko identifikovateľných nezávislých jednotiek na vyhotovovanie časovej pečiatky (TSU).

3.4 Používateľ časovej pečiatky

Používateľom služby vyhotovovania elektronickej časovej pečiatky sú Klienti uvedení v bode 1.3.3.

4 ÚVOD DO POLITIKY ČASOVEJ PEČIATKY A PLNENIE VŠEOBECNÝCH POŽIADAVIEK

4.1 Všeobecne

Tento dokument „Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok“ je verejným dokumentom.

Činnosť TSA KCCKB pri vydávaní časových pečiatok sa riadi prevádzkovými a bezpečnostnými smernicami TSA KCCKB.

4.2 Cieľoví používatelia a použitie

4.2.1 Správna prax uplatňovania politiky vyhotovovania časových pečiatok

Táto politika môže byť použitá pre verejnú službu poskytovanie časových pečiatok ako aj na použitie v uzavretých komunitách.

5 POLITIKY A PRAVIDLÁ

5.1 Ohodnotenie rizík

Pravidlá a zásady pre hodnotenie rizík sú definované v Politike poskytovania dôveryhodných služieb, kap. 4. Posúdenie rizík

5.2 Pravidlá pre praktický výkon dôveryhodných služieb

Všeobecné pravidlá pre praktický výkon dôveryhodných služieb sú uvedené v dokumente Politika poskytovania dôveryhodných služieb.

5.3 Všeobecné podmienky

Všeobecné podmienky sú uvedené v dokumente Politika poskytovania dôveryhodných služieb, odstavec 5.2.

5.4 Politika informačnej bezpečnosti

Politika informačnej bezpečnosti je uvedená v dokumente Politika poskytovania dôveryhodných služieb, odstavec 5.3, pričom dôveryhodnosť systému je zaistená:

- zavedenými bezpečnostnými pravidlami a procedúrami,
- spôsobom riadenia bezpečnosti TSA,
- dohľadom nad bezpečnosťou vykonávanie obslužných činností a prevádzkových rutín,
- pravidelným vnútorným a externým auditom bezpečnosti,
- súladom so štandardami definujúcimi požiadavky na bezpečnosť dôveryhodných systémov.

5.5 Záväzky TSA KCCKB

5.5.1 Všeobecne

TSA KCCKB ako poskytovateľ služieb časových pečiatok sa zaväzuje:

1. zabezpečiť plnenie požiadaviek v zmysle kapitoly 6 a 7;
3. používať bezpečnostné systémy ktoré zaisťujú primeranú technickú úroveň ochrany, vrátane použitia kryptografických opatrení;
4. vykonávať prijaté postupy bezpečným a spoľahlivým spôsobom,
5. zabezpečiť súlad hodín servera časových pečiatok s časom UTC v proklamovanej presnosti,

6. zabezpečiť sledovateľnosť spracovania žiadostí o vydanie časových pečiatok,
7. zabezpečiť ochranu kľúčov používaných na vydávanie časových pečiatok,
8. zabezpečiť zverejňovanie údajov nutných na overovanie vydaných časových pečiatok v podobe certifikátov verejného kľúča prislúchajúceho súkromnému kľúču používanému pri podpisovaní časových pečiatok,
9. zverejňovať informácie o:
    - spôsobe poskytovania služieb časovej pečiatky,
    - spôsobe prijímania žiadostí o časové pečiatky,
    - spôsobe overovania časových pečiatok.
10. zabezpečiť, aby prax vyhotovovania časovej pečiatky zodpovedala procedúram popísaným v tejto CP TSA a v súlade s CPS TSA.

5.5.2 Záväzky TSA KCCKB ku Klientom

TSA KCCKB ako poskytovateľ služieb časových pečiatok je povinný:

1. zaistiť spracovanie žiadostí o vydanie časovej pečiatky doručených v predpísanom formáte,
2. odpovedať na platnú žiadosť o vydanie časovej pečiatku vydaním časovej pečiatky (pokiaľ tomu nebránia technické problémy),
3. zverejňovať údaje nutné na overovanie vydaných časových pečiatok v podobe certifikátov verejného kľúča prislúchajúceho súkromnému kľúču používanému pri podpisovaní časových pečiatok.

5.6 Informácie pre spoliehajúce sa strany

TSA KCCKB ako poskytovateľ služieb časových pečiatok je vo vzťahu k Spoliehajúcim sa stranám povinný zaistiť podmienky na overenie časových pečiatok zverejňovaním údajov nutných na overovanie vydaných časových pečiatok v podobe certifikátov verejného kľúča prislúchajúceho súkromnému kľúču používanému pri podpisovaní časových pečiatok.

TSA KCCKB musí sprístupniť pre Spoliehajúce sa strany nasledovné:

1. povinnosť overenia, že časová pečiatka bola správne podpísaná a že súkromný kľúč použitý na podpis časovej pečiatky nebol do času overovania kompromitovaný,
2. počas platnosti certifikátu vydávajúcej TSU musí byť platnosť jeho podpisového kľúča overená na základe aktuálneho stavu jeho platnosti na základe údajov publikovaných TSA KCCKB,
3. všetky obmedzenia pre použitie časovej pečiatky podľa tejto politiky,
4. všetky ďalšie obmedzenia uvedené v dohodách alebo kdekoľvek inde.

6 RIADENIE A PREVÁDZKA TSA

6.1 Úvod

Riadenie a prevádzka TSA musia byť vykonávané tak, aby prijaté bezpečnostné opatrenia a nástroje na kontrolu ich plnenia poskytli nevyhnutnú dôveru, že budú naplnené.

Poskytovanie časovej pečiatky ako odpoveď na požiadavku je na rozhodnutí TSA KCCKB a závisí na dohode o úrovni poskytovaných služieb s príslušným orgánom verejnej moci.

6.2 Vnútorná organizácia

Poskytovateľ:

- je právnická osoba, podliehajúca legislatíve Slovenskej republiky,
- riadi informačnú bezpečnosť primerane pre poskytované služby vyhotovovania časových pečiatok,
- má k dispozícii dostatočný počet osôb, ktoré majú nevyhnutné vzdelanie, školenia, technické znalosti a skúsenosti vzhľadom na typ, rozsah a množstvo práce nevyhnutnej na poskytovanie služieb vyhotovovania časovej pečiatky.

6.3 Personálna bezpečnosť

Manažment kľúčov môže vykonávať len k tomu poverený pracovník v rámci svojej role. Tieto role pracovníkov sú jednoznačne definované dokumentáciou TSA. Každý pracovník je preukázateľne poučený o svojich povinnostiach, bezpečnostných a pracovných postupoch požadovaných pri plnení úloh vyplývajúcich z jeho role.

Osoby zabezpečujúce činnosti v prevádzke TSA sú preverované v zmysle Vyhlášky NBÚ č. 331/2004 Z.z. o personálnej bezpečnosti.

Externé organizácie, ktoré vystupujú ako zmluvní dodávatelia činností pre TSA, sú preverované v zmysle Vyhlášky NBÚ č. 325/2004 Z.z. o priemyselnej bezpečnosti.

6.4 Správa aktív

Požiadavky pre oblasť správy aktív sú uvedené v dokumente Politika poskytovania dôveryhodných služieb, odstavec 6.3.

6.5 Riadenie prístupu

Požiadavky pre oblasť riadenia prístupu sú uvedené v dokumente Politika poskytovania dôveryhodných služieb, odstavec 6.4.

Navyše:

- na vykonanie kritických činností na kryptografickom module (napr. generovanie, záloha súkromného kľúča TSA, obnova kľúčov, obnova zariadení) je nutný prístup dvoch určených pracovníkov TSA KCCKB (princíp štyroch očí),
- kľúče servera časových pečiatok určené na podpisovanie a overovanie časových pečiatok sú generované v kryptografickom module TSA. Procedúra generovania kľúčov sa vykonáva len pod dozorom komisie na to poverenej.

6.6 Kryptografické opatrenia

6.6.1 Všeobecne

Na správu všetkých kryptografických kľúčov a zariadení sú počas ich životného cyklu použité primerané bezpečnostné prvky a opatrenia.

6.6.2 Generovanie kľúčov pre TSU

Generovanie kľúčov pre jednotlivé TSU spĺňa nasledovné:

a) je vykonané vo fyzicky bezpečnom prostredí (pozri odstavec 6.8) osobami zaradenými v dôveryhodných rolách (pozri odstavec 6.3) za účasti minimálne dvoch oprávnených osôb. Okruh osôb autorizovaných vykonávať túto funkciu je obmedzený len na osoby v rolách vymenované v dokumente CPS TSA.

b) Generovanie TSU podpisového kľúča je vykonávané v bezpečnom kryptografickom zariadení, ktoré je dôveryhodný systém, ktorý spĺňa úroveň EAL 4+ resp. FIPS-140-3.

c) Algoritmus vytvárania TSU kľúča, výsledná dĺžka kľúča a podpisový algoritmus použitý na podpisovanie časových pečiatok je v súlade s požiadavkami normy ETSI TS 119 312.

d) Podpisový kľúč TSU nie je možné importovať do iného kryptografického modulu bez rozhodnutia bezpečnostného správcu a za účasti stanoveného počtu oprávnených osôb.

e) V kryptografických moduloch jednotlivých TSU sú rôzne podpisové kryptografické kľúče.

f) TSU má v danom čase k dispozícii len jeden aktívny kľúč na podpisovanie časovej pečiatky.

6.6.3 Ochrana súkromného kľúča TSU

Súkromné kľúče TSU zostávajú dôverné a ich integrita je udržiavaná minimálne s nasledovnými požiadavkami:

a) Súkromný podpisový kľúč TSU je uložený a používaný v kryptografickom module, ktorý je dôveryhodný systém zabezpečený na úrovni EAL 4+ v zmysle normy ISO/IEC 15408. resp. spĺňa požiadavky FIPS 140-3.

b) Súkromné kľúče TSU sú zálohované, kopírované, ukladané a obnovované len personálom v dôveryhodných rolách, za dodržania podmienky stanoveného počtu oprávnených osôb a vo fyzicky bezpečnom prostredí. Autorizované osoby na vykonávanie týchto činností sú len tie, ktoré podliehajú pravidlám, ktoré sú uvedené v dokumente CPS TSA.

c) Akékoľvek záložné kópie súkromných podpisových kľúčov nachádzajúce sa mimo TSU sú chránené, tak že je zabezpečená ich integrita a dôvernosť.

6.6.4 Certifikát verejného kľúča TSU

TSA KCCKB zaručuje integritu a autenticitu verejného kľúča TSU pre overenie podpisu nasledovne:

a) Verejný kľúč TSU, ktorý slúži na overenie podpisu je dostupný spoliehajúcim sa stranám v certifikáte verejného kľúča.

b) Certifikát verejného kľúča TSU pre overenie podpisu je vydaný certifikačnou autoritou poskytujúcou služby v zmysle normy ETSI EN 319 411-1.

c) TSU nevyhotoví časovú pečiatku pred tým ako jej certifikát verejného kľúča pre overenie podpisu je načítaný v kryptografickom zariadení TSU.

Keď TSA KCCKB prevezme certifikát verejného kľúča, ktorý slúži na overenie podpisu pre jednotlivé TSU, overí, že tento certifikát bol správne podpísaný, vrátane overenia celej certifikačnej cesty k dôveryhodnej certifikačnej autorite.

6.6.5 Prepísanie kľúča TSU

Životnosť certifikátu TSU nie je dlhšia ako doba, počas ktorej sú zvolený algoritmus a dĺžka kľúča uznané ako vhodné pre tento účel.

6.6.6 Manažment životného cyklu podpisového kryptografického hardvéru

Aplikované sú nasledovné požiadavky:

d) Do kryptografického hardvéru, určeného na podpisovanie časových pečiatok, nesmie byť svojvoľne zasahované počas jeho prepravy.

e) Do kryptografického hardvéru, ktorý podpisuje časové pečiatky, nesmie byť svojvoľne zasahované počas jeho skladovania.

f) Inštalácia, aktivácia a duplikácia podpisových kľúčov TSU v kryptografickom hardware je vykonávaná iba osobami v dôveryhodných roliach, s minimálne dvojitou kontrolou a vo fyzicky bezpečnom prostredí (pozri odstavec 6.8).

g) Súkromné podpisové kľúče TSU uložené v kryptografickom module TSU sú v prípade vyradenia modulu vymazané takým spôsobom, že je prakticky nemožné ich obnovenie.

6.6.7 Ukončenie životného cyklu kľúča TSU

Životný cyklus kľúčov TSA je ukončený:

- vypršaním platnosti certifikátu,
- zrušením platnosti certifikátu v prípade mimoriadnej udalosti.

Zrušenie certifikátu je avizované vydaním CRL a jeho zverejnením publikačnými prostriedkami TSA KCCKB.

Neplatné kľúče TSA (kľúče, ktorých životný cyklus bol ukončený) sú nahradené vygenerovaním nového kľúčového páru, certifikáciou verejného kľúča a zverejnením certifikátu na publikačných prostriedkoch.

Zrušené certifikáty zverejnené v CRL je možné používať aj po ich zrušení na overovanie časových pečiatok, ktoré boli vydané pred zrušením certifikátu (čas vydania časovej pečiatky je nižší, ako čas zrušenia certifikátu).

6.7 Vyhotovenie časovej pečiatky

Formát vydávaných časových pečiatok zodpovedá štandardom RFC 3161 a ETSI TS 101 861.

Na vyžiadanie časových pečiatok sa používa proprietárny protokol so zvýšenou ochranou, odvodený od protokolu RFC 3161.

Vyžiadanie časovej značky prebieha v nasledujúcich fázach:

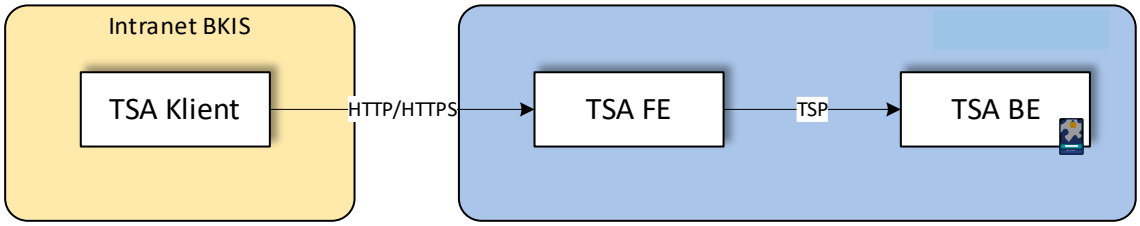
- vygenerovanie žiadosti o pridelenie časovej značky,
- odoslanie žiadosti o pridelenie časovej značky,
- prijatie odpovede na žiadosť o časovú značku (TSR).

Na hašovanie pri vydávaní časových pečiatok je použitý algoritmus SHA256. Na podpisovanie časových pečiatok (šifrovanie produktu hašovania) je použitý algoritmus RSA s dĺžkou kľúča 2048 bitov.

Časový údaj časovej pečiatky je udaný v čase UTC. Časový údaj časovej pečiatky má presnosť 1 sekunda, alebo menej.

6.7.1 Vydanie časovej pečiatky

6.7.1.1 Architektúra časovej pečiatky



6.7.1.1.1 Funkčná dekompozícia komponentov

Nasledovná tabuľka popisuje základné komponenty služby.

Funkčná dekompozícia komponentov

Systém	Funkcia
Systém TSP klient-a	Server/pracovná stanica s nainštalovanou klientskou aplikáciou schopná komunikovať pomocou protokolu TSP (TCP/HTTP/HTTPs)
TSA front-end	Front-end služba vydávania časovej pečiatky pridávajúca HTTP/HTTPS vrstvu pre TSP protokol: - HTTP server - Modul, sprostredkúvajúci službu TSA - Aplikačné vybavenie pre kontrolu dostupnosti poskytovanej služby
TSA back-end	Samotný server vydávania časovej pečiatky, ktorý na svoj chod využíva jednotlivé komponenty ako: - Systém kontroly presnosti času - Databázový systém - HSM (bezpečné uloženie kryptografických kľúčov TSA) - Úložisko logov - Synchronizácia času voči referenčnému zdroju času

6.7.1.1.2 Popis logických funkčných komponentov

6.7.1.1.2.1 Klientska aplikácia

Klientska aplikácia je ľubovoľná aplikácia tretej strany schopná komunikovať pomocou protokolu TSP definovaného v RFC 3161. Táto aplikácia vygeneruje zo zvoleného dokumentu hash, zakomponuje ho do žiadosti o vydanie časovej pečiatky a zašle ho systémom TSA. Prijatú odpoveď môže ďalej spracovávať ľubovoľným spôsobom.

6.7.1.1.2.2 Modul sprostredkúvajúci službu TSA

Modul sprostredkúvajúci službu TSA slúži ako brána medzi protokolmi TSP/HTTP(s) a TSP/TCP (špecifikované v RFC 3161). Zabezpečuje teda prijatie žiadosti o vydanie časovej pečiatky ako HTTP požiadavku, preposlanie žiadosti aplikácii Disig TSA Signer (protokol TCP) a vrátenie odpovede klientovi.

6.7.1.1.2.3 Disig TSA Signer (TSAD)

Disig TSA Signer je prezentovaný aplikačným servisom TSAD, čo je aplikácia obsluhujúca požiadavky o vydanie časovej pečiatky prichádzajúce na port 318/TCP. Podporovaný transportný mechanizmus je zjednodušeným variantom protokolu „Socket Based Protocol“ definovaného v sekcii 3.3. v RFC 3161. Využíva komunikáciu prostredníctvom TCP socketu typu request-response bez možností pooling-u.

Nakoľko servis TSAD predstavuje samotné jadro aplikácie, pokrýva aj viacero bezpečnostných funkcií systému. Modul pri každom svojom spustení načíta konfiguráciu z vopred pripraveného a elektronicky podpísaného konfiguračného súboru. Ďalej už s konfiguračným súborom nemusí pracovať, čo zabezpečí, že jeho prípadná zmena nijak neovplyvní beh samotnej aplikácie. Požiadavka na elektronický podpis konfiguračného súboru oprávnenou osobou zároveň zvyšuje bezpečnosť celého procesu konfigurácie. Tým je splnená bezpečnostná funkcia manažmentu konfigurácie.

Servis TSAD z celého svojho behu od spustenia, cez vydávanie časových pečiatok až po ukončenie behu neustále generuje auditné záznamy pokrývajúce všetky dôležité udalosti. Generované auditné záznamy navyše elektronicky podpisuje s možnosťou využívania kľúčov z bezpečné úložiska. V neposlednom rade sa modul stará o posielanie podpísaných logov do bezpečného úložiska logov. Tým modul pokrýva celú bezpečnostnú funkciu generovania auditných záznamov.

Základnou úlohou aplikácie a jej hlavného modulu – servisu TSAD je vydávanie časových pečiatok. Z bezpečnostného hľadiska je v prvom rade dôležité spracúvať len správne žiadosti o vydanie. Aplikácia teda žiadosti spracúva, overí ich platnosť a podľa platnej politiky aj vydáva časové pečiatky. Všetky tieto časti plne pokrývajú všetky aspekty bezpečnostnej funkcionality vydávania časových pečiatok. Ďalšou bezpečnostnou funkciou, ktorá je TSAD pokrytá je požiadavka, aby nebolo možné celý proces vydávania časových pečiatok obísť, alebo časť z neho vynechať – bezpečnostná funkcia zabezpečeného chodu. Táto požiadavka je splnená tým, že navrhovaný servis TSAD je uzavretým modulom bez možnosti externej zmeny jeho vstavanej funkcionality.

6.7.1.1.2.4 Databázový systém

TSAD využíva databázový systém na ukladanie informácií o prijatých žiadostiach o vydanie časovej pečiatky a tiež informácií o vybavení týchto žiadostí. Udržiavaním záznamov o prijatých požiadavkách a odoslaných odpovediach tento systém čiastočne pokrýva požiadavku vytvárania a spracovania auditných záznamov, hoci je časť ukladania záznamov pokrytá aj v module Úložisko logov.

6.7.1.1.2.5 Bezpečné úložisko kľúčov (HSM)

Bezpečné úložisko kľúčov uchováva privátny kľúč TSA. V tomto prípade sa jedná o špecializované hardvérové kryptografické zaradenie HSM, ktoré modul TSAD využíva na vykonávanie kryptografických operácií medzi, ktoré patrí najmä podpisovanie časových pečiatok. Z bezpečnostného hľadiska tento modul zabezpečuje najmä podporné úlohy – poskytovanie kľúčov pre elektronický podpis, ktoré sú potrebné pre správnu a bezpečnú aplikáciu generovania a spracúvania auditných záznamov a vytvárania časových pečiatok.

6.7.1.1.2.6 Úložisko logov

Subsystém spracúvajúci auditné správy vygenerované servisom TSAD. Správy s vyššou prioritou sú elektronicky podpísané samostatným kľúčom určeným na tento účel. Toto úložisko plne pokrýva požiadavku

na spracovanie a uchovávanie auditných záznamov, navyše ošetrenie elektronickým podpisom zvyšuje bezpečnosť logov a zabezpečuje ich autenticitu.

6.7.1.1.2.7 Referenčný zdroj času

Referenčný zdroj času je systém, ktorý má k dispozícii údaj o presnom čase a je schopný ho sprostredkovať ostatným systémom prostredníctvom protokolu NTP. Modul disponuje informáciou o presnom čase, ktorá je kľúčová pre správnu funkčnosť systému autority časovej pečiatky.

6.7.1.1.2.8 NTPD

Úlohou služby NTPD je synchronizácia systémového času s referenčným zdrojom času. Synchronizácia sa vykonáva prostredníctvom protokolu NTP a tento servis je štandardnou súčasťou operačného systému. Z bezpečnostného hľadiska tento modul zabezpečuje synchronizáciu systémového času voči času poskytovanému referenčným zdrojom času. Systémový čas sa používa nielen vo vydávaných časových pečiatkach ale i vo vytváraných auditných záznamoch.

6.7.1.1.2.9 Systém kontroly času

Systém kontroly presnosti času porovnáva systémový čas s časovým údajom získaným z referenčného zdroja času. Rozdiel medzi týmito dvoma časovými údajmi zapisuje do vyhradenej časti operačnej pamäte, ktorú zdieľa so servisom TSAD. Servis TSAD používa rozdiel v procese vydávania časových pečiatok na určenie, či je odchýlka systémového času od referenčného zdroja akceptovateľná alebo nie. Modul sa nepriamo podieľa na obmedzení vydávania časových pečiatok v prípade, keď sa systémový čas odchýli od referenčného zdroja času.

6.7.1.2 Podanie žiadosti o vydanie časovej pečiatky

Žiadosť o pridelenie časovej značky vygeneruje klient TS vo formáte TSQ. Žiadosť vo formáte TSQ klient zapuzdri do formátu PKCS #7 (na umožnenie autentizácie).

Klient TS odošle vygenerovanú žiadosť o pridelenie časovej značky (súbor PKCS #7) protokolom HTTP serveru TSA.

Ako potvrdenie prijatia žiadosti o pridelenie časovej značky server TSA odošle klientovi TS identifikátor, pod ktorým klient preberie vygenerovanú časovú značku.

6.7.1.3 Generovanie časových pečiatok

Odpoveď na žiadosť o časovú pečiatku TSR je generovaná na základe údajov zo žiadosti. TSR obsahuje status odpovedi a vlastnú časovú pečiatku (TST). Telo časovej pečiatky TST obsahuje informácie zaslané žiadateľom v žiadosti, doplnené o jedinečné sériové číslo, informáciu o dátume a čase vydania časovej pečiatky (UTC čas) a o informačné údaje o časovej pečiatke. Údaje tela TST sú podpísané hašovaním algoritmom SHA256 a zakryptovaním produktu hašovania súkromným kľúčom TSA. Pri prípadnom rozsynchronizovaní hodín TSA je žiadosť odmietnutá. Vygenerované časové pečiatky sú odovzdané žiadateľom na internetovej stránke, na ktorej bola podaná žiadosť o časovú pečiatku.

6.7.1.4 Prijatie odpovede na žiadosť o časovú pečiatku

Proces prevzatia časovej pečiatka je asynchrónny. Klient TS prevezme vygenerovanú časovú pečiatku pri novom HTTP volaní pri ktorom sa identifikuje identifikátorom.

Prevzatá časová pečiatka má štandardný formát podľa RFC 3161.

6.7.1.5 Overovanie časových pečiatok

Overovanie časových pečiatok sa musí vykonať v nasledovných krokoch:

- overenie platnosti certifikátu verejného kľúča TSA proti CRL,
- overenie platnosti certifikátu verejného kľúča TSA preverením podpisu certifikátu,
- overenie platnosti časovej pečiatky na základe overenia elektronického podpisu časovej pečiatky.

Pokiaľ ktorékoľvek z vymenovaných overení nebolo overené s pozitívnym výsledkom, je časová pečiatka pokladaná za neplatnú.

6.7.2 Synchronizácia hodín s UTC

Hodiny TSA používané ako zdroj času pre časové pečiatky sú synchronizované od zdroja presného času služby Sovereign Time.

Synchronizácia času zaručuje presnosť lepšiu ako 1 sekunda.

6.8 Fyzická a objektová bezpečnosť

Pravidlá a zásady pre zaistenie fyzickej a objektovej bezpečnosti sú definované v Politike poskytovania dôveryhodných služieb, kap. 6.6 Fyzická a objektová bezpečnosť.

Navyše platí:

a) Na kryptografický modul musí byť aplikované riadenie prístupu v súlade s odstavcom 6.5.

b) Na správu vyhotovovania časových pečiatok musia byť aplikované nasledovné dodatočné opatrenia:

- Technické prostriedky na vyhotovovanie časových pečiatok musia byť prevádzkované v prostredí, ktoré fyzicky a logicky chráni služby pred kompromitáciou, ktorá môže byť spôsobená neautorizovaným prístupom k systémom alebo údajom.
- Každý vstup do fyzicky bezpečnej oblasti musí podliehať nezávislému dohľadu a neautorizovaná osoba musí byť sprevádzaná autorizovanou osobou pokiaľ je v bezpečnej oblasti. Každý vstup a prítomnosť musí byť zaznamenaná.

- Fyzická ochrana musí byť dosiahnutá vytvorením jasne definovanej bezpečnostnej hranice (perimetrom, fyzickou bariérou) okolo správy vyhotovovania časovej pečiatky. Akékoľvek časti objektu zdieľané s inými organizáciami musia byť mimo tohto perimetra.
- Fyzické a objektové bezpečnostné opatrenia musia chrániť objekty, kde sú umiestnené systémy, samotné systémové zdroje a objekty použité na podporu ich prevádzky. Bezpečnostné opatrenia týkajúce sa fyzickej a objektovej bezpečnosti TSA musia pokrývať minimálne fyzické riadenie prístupu, ochranu pred prírodnými katastrofami, ochranu pred požiarom, výpadok podporných rozvodov (napr. elektrina, telekomunikácie), zrútenie štruktúry, úniky z potrubí, ochranu proti odcudzeniu, vlámaniu, a obnovu po pohrome.
- Prijaté opatrenia musia chrániť zariadenia, informácie, médiá a softvér týkajúcich sa služieb vyhotovovania časových pečiatok pred vynesením bez autorizácie.

6.9 Prevádzková bezpečnosť

Bezpečnosť prevádzky TSA je riadená v rámci manažmentu bezpečnosti TSA KCCKB.

Na zabezpečovanie akreditovaných certifikačných služieb používa TSA KCCKB produkty na elektronický podpis s medzinárodne uznávanou certifikáciou ISO/IEC 15408 a FIPS 140-1. Na dosiahnutie certifikácie ISO/IEC 15408 a FIPS 140-1 museli produkty pre elektronický podpis splniť príslušné požiadavky na zabezpečenie vývoja, ktoré tieto štandardy stanovujú.

Pri vývoji špecializovaného programového vybavenia sa uplatňujú ustanovenia interných bezpečnostných smerníc, ktoré predpisujú zásady bezpečnosti vývoja programového vybavenia a riadenie bezpečnosti pri poskytovaní certifikačných služieb.

Kľúče servera časových pečiatok určené na podpisovanie určené na podpisovanie a overovanie časových pečiatok sú generované v kryptografickom module TSA. Generovanie kľúčov sa vykonáva v bezpečnom prostredí.

Procedúra generovania kľúčov sa vykonáva pod dozorom komisie na to poverenej. Po ukončení platnosti certifikátu pre TSS bude záloha súkromného kľúča zničená.

Súkromné kľúče servera časových pečiatok určené na podpisovanie časových pečiatok sú uchovávané v kryptografickom module servera časových pečiatok a za žiadnych okolností neopúšťajú kryptografický modul.

Kryptografický modul servera časových pečiatok zodpovedá požiadavkám štandardu FIPS 140-1 level 4.

6.10 Sieťová bezpečnosť

Systém a pravidlá na zaistenie sieťovej bezpečnosti sú popísané v Politike poskytovania dôveryhodných služieb, kap. 6.8 Sieťová bezpečnosť.

Ďalej platí, že:

c) TSA KCCKB musí udržiavať a chrániť všetky TSU v bezpečnej zóne,

d) všetky systémy TSU musia byť nakonfigurované tak, že budú mať odstránené a/alebo zakázané všetky účty, aplikácie, služby, protokoly a porty, ktoré nie sú používané pre ich prevádzku,

e) do bezpečných zón a vysoko bezpečných zón môžu mať prístup len dôveryhodné roly.

6.11 Riadenie bezpečnostných incidentov

Systém riadenia bezpečnostných incidentov je popísaný v Politike poskytovania dôveryhodných služieb, kap. 6.9 Riadenie bezpečnostných incidentov.

6.12 Zber dôkazov

Všeobecné požiadavky na zber dôkazov sú popísané v Politike poskytovania dôveryhodných služieb, kap. 6.10 Zber dôkazov.

V súvislosti s poskytovaním služby časovej pečiatky je zber dôkazov zabezpečovaný zaznamenávaním a bezpečným uchovávaním informácií súvisiacich s poskytovaním služby časovej pečiatky.

Procesy pri poskytovaní časových pečiatok zaznamenávajú auditné stopy, z ktorých je možné spätne analyzovať priebeh vydania časovej pečiatky.

Auditné záznamy sa uchovávajú po dobu 5 rokov.

Na zaznamenávanie informácií súvisiacich s poskytovaním služby časovej pečiatky slúži databáza servera TSA, ktorá bude slúžiť na ukladanie:

- zoznamu vydaných časových pečiatok,
- zoznamu vydaných odpovedí,
- informácií o mimoriadnych udalostiach v systéme používanom v manažmente časových pečiatok,
- informácií o dôležitých udalostiach v prostredí vydavateľa časových pečiatok, manažmente kryptografických kľúčov a v synchronizácii zdrojov času vrátane presných časových údajov:
  - riadenie životného cyklu kľúčov TSU;
  - riadenie životného cyklu certifikátov TSU;
  - synchronizácia hodín TSU s UTC. Toto musí zahŕňať aj informácie týkajúce sa normálnej re-kalibrácie alebo synchronizácie hodín použitých pri vyhotovovaní časových pečiatok;
  - zistené straty synchronizácie.

Takýmito záznamami sú:

- všetky časové pečiatky (bez ohľadu na to, ktoré boli vyzdvihnuté a ktoré nie),
- záznamy o štarte a zastavení DB Klienta (aj neúspešnom, napr. ak sa nepodarí pripojiť k DBŽ),

- záznamy o odmietnutí vydať časovú pečiatku (napr. z dôvodu vypršania TAC, nedostupnosti TimeStamp servera, atď.),
- záznamy o prekročení maximálneho počtu vlákien (threadov), ku ktorému môže dôjsť pri nadmernom zaťažení služby časovej pečiatky.

6.13 Riadenie kontinuity činnosti organizácie

Pre prípad vzniku pohromy má TSA KCCKB definovaný a udržiavaný plán kontinuity. V prípade pohromy (vrátanie kompromitácie súkromného kľúča alebo iných citlivých údajov TSA musí byť prevádzka TSA obnovená v rámci oneskorenia definovaného v pláne kontinuity.

6.14 Ukončenie činnosti TSA KCCKB a plány ukončenia činnosti

Postup ukončenia činnosti TSA je popísaný v Politike poskytovania dôveryhodných služieb, kap. 6.12 Ukončenie činnosti TSP KCCKB a plány ukončenia činnosti.

Ukončenie činnosti TSA bude oznámené:

- žiadateľom služieb časovej pečiatky,
- verejne ohlásené verejnými oznamovacími prostriedkami.

Okrem toho, v prípade ukončenia služieb TSA, musia byť zrušené všetky certifikáty vydané pre jednotlivé TSU.

6.15 Zhoda

Poskytovanie služby vyhotovovania kvalifikovaných elektronických časových pečiatok sa riadia:

- Nariadením 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,
- Zákonom č. 272/2016 Z.z. o dôveryhodných službách,
- ostatnými všeobecne platnými nariadeniami platnými v SR, vzťahujúcimi sa k výkonu tejto činnosti.

7 PLNENIE POŽIADAVIEK PRE KVALIFIKOVANÉ ELEKTRONICKÉ ČASOVÉ PEČIATKY PODĽA NARIADENIA EIDAS

7.1 Certifikát verejného kľúča TSU

Pre kvalifikované elektronické časové pečiatky (v zmysle eIDAS) musí byť certifikát verejného kľúča TSU, ktorý slúži na overenie podpisu kvalifikovanej elektronickej časovej pečiatky, vydaný certifikačnou autoritou prevádzkovanou v zmysle politiky, ktorá vychádza z normy ETSI EN 319 411-2.

7.2 Vyhotovovanie nekvalifikovaných a kvalifikovaných elektronických časových pečiatok podľa Nariadenia eIDAS

Ak TSU zahrnutá v systéme TSA vyhotovuje časové pečiatky, ktoré sú vyhlasované ako kvalifikované elektronické pečiatky podľa eIDAS, táto TSU nesmie vyhotovovať nekvalifikované elektronické časové pečiatky.

V prípade vyhotovovania nekvalifikovaných elektronických časových pečiatok musí TSA používať rôzne inú TSU s rozdielnym názvom subjektu certifikátu verejného kľúča. Služba takejto TSU musí byť prístupná cez iný samostatný prístupový bod.