POLITIKA

poskytovania dôveryhodnej služby vyhotovovania kvalifikovaných elektronických **časových pečiatok**

Disig, a.s.

Vypracoval	Ing. Peter **Miškovič**
Dátum platnosti	10.5.2017
Verzia	4.0
Typ	POLITIKA
Schválil	Ing. **Ľuboš Batěk**

Obsah

1.	Úvod	4
1.1	Prehľad	4
1.2	Názov dokumentu a jeho identifikácia	5
1.3	Účastníci PKI	5
1.3.1	Jednotka vyhotovovania časových pečiatok	5
1.3.2	Registračná autorita	6
1.3.3	Zákazník	7
1.3.4	Spoliehajúca sa strana	7
1.3.5	Iní účastníci	7
1.4	Použiteľnosť časovej pečiatky	8
1.5	Správa politiky	8
1.5.1	Organizácia zodpovedná za správu dokumentu	8
1.5.2	Kontaktná osoba	8
1.5.3	Osoba rozhodujúca o súlade CP s certifikačnou politikou	9
1.5.4	Postupy schvaľovania CP a externej politiky	9
1.6	Definície a skratky	9
1.6.1	Definície	9
1.6.2	Skratky	10
2.	Úložiská	11
2.1	Zverejňovanie informácií o TSA	11
2.2	Frekvencia zverejňovania informácií	11
2.3	Kontroly prístupu	12
3.	Všeobecné ustanovenia	13
3.1	Všeobecné ustanovenia politiky	13
3.2	Služby súvisiace s časovou pečiatkou	13
3.3	Vydavateľ časových pečiatok	13
3.4	Používateľ časovej pečiatky	14
4.	Úvod do politiky **časovej pečiatky** a plnenie všeobecných požiadaviek	15
4.1	Všeobecne	15
4.2	Cieľoví používatelia a použitie	15
4.2.1	Správne prax uplatňovania politiky vyhotovovania časových pečiatok	15
5.	Politiky a pravidlá	16

5.1	Ohodnotenie rizík	16
5.2	Pravidlá pre praktický výkon dôveryhodných služieb	16
5.3	Všeobecné podmienky	16
5.4	Politika informačnej bezpečnosti	16
5.5	Záväzky Poskytovateľa	16
5.5.1	Všeobecne	16
5.5.2	Záväzky Poskytovateľa k Zákazníkovi	16
5.6	Informácie pre spoliehajúce sa strany	17
6.	Manažment a prevádzka TSA **Poskytovateľa**	18
6.1	Úvod	18
6.2	Vnútorná organizácia	18
6.3	Personálna bezpečnosť	18
6.4	Správa aktív	18
6.5	Riadenie prístupu	18
6.6	Kryptografické opatrenia	19
6.6.1	Všeobecne	19
6.6.2	Generovanie kľúčov pre TSU	19
6.6.3	Ochrana súkromného kľúča TSU	19
6.6.4	Certifikát verejného kľúča TSU	20
6.6.5	Prepísanie kľúča TSU	20
6.6.6	Manažment životného cyklu podpisového kryptografického hardvéru	20
6.6.7	Ukončenie životného cyklu kľúča TSU	20
6.7	Vyhotovenie časovej pečiatky	21
6.7.1	Vydanie časovej pečiatky	21
6.7.2	Synchronizácia hodín s UTC	22
6.8	Fyzická a objektová bezpečnosť	22
6.9	Prevádzková bezpečnosť	23
6.10	Sieťová bezpečnosť	23
6.11	Riadenie bezpečnostných incidentov	24
6.12	Zber dôkazov	24
6.13	Riadenie kontinuity činnosti organizácie	24
6.14	Ukončenie činnosti Poskytovateľa a plány ukončenia činnosti	25
6.15	Zhoda	25
7.	Plnenie požiadaviek pre kvalifikované elektronické **časové pečiatky podľa** Nariadenia eIDAS	26
7.1	Certifikát verejného kľúča TSU	26
7.2	Vyhotovovanie nekvalifikovaných a kvalifikovaných elektronických časových pečiatok podľa Nariadenia eIDAS	26

8. Odkazy 27

1. Úvod

Tento dokument definuje politiku a plnenie bezpečnostných požiadaviek, ktoré sa týkajú prevádzkovej praxe a postupov riadenia poskytovania dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok (ďalej len „časová pečiatka“). Poskytovateľom tejto dôveryhodnej služby je spoločnosť Disig, a.s., so sídlom Záhradnícka 151, 821 08 Bratislava, IČO: 35975946, zapísaná v Obchodnom registri OS BA I, odd. Sa, vložka č. 3794/B (ďalej len „Poskytovateľ“), prostredníctvom svojho systému autority časovej pečiatky (TSA Disig).

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

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

1.1 Prehľad

Táto CP TSA sa týka poskytovania dôveryhodnej služby vyhotovovania:

- kvalifikovanej elektronickej **časovej pečiatky**
  (Identifikátor politiky - A best practices policy for time-stamp (BTSP) v zmysle EN 319411-2 [1]: itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)),

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“) [2] .

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 poskytovateľa:

Názov	Sériové číslo certifikátu	Vydavateľ	DigitalID v SK dôveryhodnom zozname
CA Disig	00F4	KCA NBU SR 3	FX9fXwhpKsZwA6H6UWpNrI1fmFM=
CA Disig QCA	077A	KCA NBU SR 3	9FgiC3T8jAqPjDqlhZcvhFnZHyg=

1.2 Názov dokumentu a jeho identifikácia

Názov:	Politika poskytovania dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok
Skratka názvu:	CP TSA Disig QTS*
Verzia:	4.0
Schválené dňa:	5.5.2017
Platnosť od:	10.5.2017
Tomuto CP TSA je priradený identifikátor objektu (OID):	1.3.158.35975946.0.0.1.0.4

* - v texte tohto dokumentu sa väčšinou používa pri odkaze len skrátená forma CP TSA

Popis použitého identifikátora objektu (OID):

1. – ISO assigned OIDs

1.3. – ISO Identified Organization

1.3.158. – Identifikačné číslo subjektu (IČO)

1.3.158.35975946. – Disig

1.3.158.35975946.0.0.1. - CA Disig – vyhotovovanie kvalifikovaných certifikátov

1.3.158.35975946.0.0.1.0.4 – CP TSA Disig QCS

1.3 Účastníci PKI

V rámci poskytovania dôveryhodných služieb vyhotovovania kvalifikovaných elektronických časových pečiatok sú účastníkmi infraštruktúry verejného kľúča entity uvedené 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 (Zákazníci, 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 pravidlami na výkon certifikačných činností Poskytovateľa.

TSU Poskytovateľa sú súčasťou hierarchickej PKI:

Certifikačná autorita KCA NBÚ SR 3 -> CA Disig resp. CA Disig QCA 3 -> TSU

Poskytovateľ môže prevádzkovať v rámci podriadenosti pod certifikačnými autoritami CA Disig resp. CA Disig QCA 3 viaceré TSU poskytujúce dôveryhodné služby vyhotovovania časovej pečiatky.

1.3.2 **Registračná** autorita

Registračná autorita (ďalej len „RA“) je entita, ktorá koná, na základe zmluvy, v mene Poskytovateľa, pričom vykonáva niektoré vybrané činnosti pri poskytovaní dôveryhodných služieb Poskytovateľa.

RA musí vykonávať svoje aktivity v súlade so schválenou CP TSA a Pravidlami na výkon certifikačných činností (ďalej aj „CPS“) v aktuálnom znení.

Poskytovateľ môže zriadiť RA nasledovných typov:

- **Komerčná** RA – je určená na sprostredkovanie vybraných kvalifikovaných dôveryhodných služieb Poskytovateľa širokej verejnosti a je prevádzkovaná treťou stranou, na základe písomnej zmluvy s Poskytovateľom.
- Firemná RA – je určená na sprostredkovanie vybraných kvalifikovaných dôveryhodných služieb výhradne pre vlastné potreby konkrétnej právnickej osoby resp. pre potreby ňou prevádzkovaných systémov vyžadujúcich použitie KC a je prevádzkovaná, na základe písomnej zmluvy s Poskytovateľom, danou konkrétnou právnickou osobou.
- Interná RA – je prevádzkovaná Poskytovateľom a je určená na poskytovanie kvalifikovaných dôveryhodných služieb pre všetkých záujemcov. Táto RA nie je samostatný právny subjekt.

Poskytovateľ v súčasnej dobe zriaďuje len RA pôsobiace na území Slovenskej republiky, ktoré sú právnym subjektom so sídlom v Slovenskej republike.

1.3.3 Zákazník

Zákazníkom sa rozumie fyzická osoba resp. právnická osoba, ktorej Poskytovateľ poskytuje službu vyhotovenia časovej pečiatky a ten na koho sa viažu záväzky odberateľa .

Podmienky, ktoré musí splniť Zákazník, definuje táto CP TSA.

Ak je Zákazníkom právnická osoba, táto môže zahŕňať niekoľko koncových používateľov alebo jediného koncového používateľa . Niektoré povinnosti, ktoré sa vzťahujú na túto právnickú osobu, sa zároveň vzťahujú aj na týchto koncových používateľov. V každom prípade právnická osoba je plne zodpovedná ak povinnosti dané touto CP TSA nie sú zo strany koncových používateľov správne splnené, a preto je takáto organizácia zodpovedná za vhodnú informovanosť svojich koncových používateľov.

Keď je Zákazník zároveň koncovým používateľom, tak je priamo zodpovedný, ak neplní svoje povinnosti v zmysle tejto CP TSA.

1.3.4 Spoliehajúca sa strana

Spoliehajúcou sa stranou je fyzická alebo právnická osoba, ktorá sa pri svojom konaní spolieha na vyhotovenú časovú pečiatku.

1.3.5 Iní **účastníci**

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

- dohľadu na vytváraním a aktualizáciou CP TSA, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien,
- revízie CPS, aby sa zaručilo, že prax Poskytovateľa vyhovuje príslušnej CP TSA,
- revízie výsledkov auditov, aby sa určilo, či Poskytovateľ zodpovedne dodržiava ustanovenia vydaných CPS,
- vydávanie odporúčaní pre Poskytovateľa týkajúcich sa nápravných a iných vhodných opatrení,
- riadenia a usmerňovania činnosti Poskytovateľa a registračných autorít (ďalej len „RA“),
- výkladu ustanovení vydaných CPS a svojich pokynov pre Poskytovateľa a RA,
- výkonu funkcie interného audítora, pričom touto činnosťou poverí samostatného zamestnanca.

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

1.4 Použiteľnosť časovej pečiatky

Časová pečiatka vyhotovená v zmysle požiadaviek tejto CP TSA je použiteľná všade, kde je vyžadovaná časová pečiatka definovaná v článku 42 Nariadenia eIDAS. [2]

1.5 Správa politiky

1.5.1 Organizácia zodpovedná za správu dokumentu

Tabuľka č. 1 obsahuje údaje Poskytovateľa, ktorý je zodpovedný za prípravu, vytvorenie a udržiavanie tohto dokumentu.

Tabuľka č. 1: Kontaktné údaje Disig

Poskytovateľ	
spoločnosť:	Disig, a.s.
adresa:	Záhradnícka 151, 821 08 Bratislava 2
IČO:	359 75 946
telefón	+421 2 20850140
e-mail:	disig@disig.sk
webové sídlo:	http://www.disig.sk

1.5.2 Kontaktná osoba

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

Tabuľka č. 2 obsahuje kontaktné údaje na zložku zodpovednú za prevádzku TSA

Tabuľka č. 2: Kontaktné údaje TSA

Autorita **časovej pečiatky** CA Disig	
adresa:	Záhradnícka 151, 821 08 Bratislava 2
e-mail:	spravaca@disig.sk;
telefón	+421 2 20850140

fax:	+421 2 20850141
webové sídlo:	http://eidas.disig.sk

1.5.3 Osoba rozhodujúca o súlade CP s **certifikačnou** politikou

Osobou, ktorá je zodpovedná za rozhodovanie o súlade postupov Poskytovateľa, ktoré sú uvedené v tejto CP je osoba menovaná do roly PMA.

1.5.4 Postupy **schvaľovania** CP a externej politiky

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

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

1.6 Definície a skratky

1.6.1 Definície

Pre potreby tohto dokumentu sú použité nasledovné definície prevzaté z Nariadenia eIDAS [2] resp. normy ETSI EN 319 401 [3]:

Univerzálny koordinovaný **čas** (Coordinated Universal Time (UTC)): časová škála založená na sekunde podľa definície v Recommendation ITU-R TF.460-6, „svetový čas“;

Elektronická **časová pečiatka** : 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.

Kvalifikovaná elektronická **časová pečiatka**: elektronická časová pečiatka, ktorá spĺňa požiadavky stanovené v článku 42 Nariadenia eIDAS [2]:

Politika **časovej pečiatky** (Time-stamp policy): definovaný súbor pravidiel ktorý svedčí o použiteľnosti časovej pečiatky pre konkrétnu skupinu a/alebo triedu aplikácií so spoločnými bezpečnostnými požiadavkami;

Autorita **časovej pečiatky** (Time-Stamping Authority (TSA)): TSP poskytujúci služby vyhotovovania časovej pečiatky použitím jednej alebo viacerých TSU

Služba vyhotovovania **časových pečiatok** (Time-stamping service): dôveryhodná služba vyhotovovania časových pečiatok

Jednotka vyhotovovania **časových pečiatok** (Time-Stamping Unit (TSU)): sústava technických a programových prostriedkov, ktorá je spravovaná ako jednotka a má v danom čase aktívny jeden kľúč na podpisovanie časových pečiatok

Poskytovateľ dôveryhodnej služby (Trust Service Provider (TSP)): entita, ktorá poskytuje jednu alebo viac dôveryhodných služieb

Pravidlá na vykonávanie **certifikačných činností** TSA (TSA practice statement): prehlásenie o postupoch, ktoré TSA používa pri vyhotovovaní časových pečiatok, je to špecifický typ prehlásenia o postupoch dôveryhodnej služby ako je definovaný v norme ETSI EN 319 401 [3]

Systém TSA (TSA system): zostava IT produktov a komponentov zorganizovaných na podporu poskytovania služieb vyhotovovania časovej pečiatky

1.6.2 Skratky

BIPM	—	Medzinárodný úrad váh a mier ä Bureau International des Poids et Mesures)
BTSP	—	Osvedčené postupy politiky časových pečiatok (Best practices Time-Stamp Policy)
CA	—	Certifikačná autorita, autorita vyhotovujúca certifikáty verejného kľúča (Certification Authority)
GMT	—	Greenwichský stredný čas, čas greenwichského poludníka (Greenwich Mean Time)
IERS	—	Medzinárodná referenčná služba zemskej rotácie (International Earth Rotation and Reference System Service)
IT	—	informačná technológia (Information Technology)
NBÚ	—	Národný bezpečnostný úrad
TAI	—	Medzinárodný atómový čas (International Atomic Time)
TSA	—	Autorita časovej pečiatky, vydavateľ časovej pečiatky (Time-Stamping Authority)
TSU	—	Samostatná jednotka vytvárajúca časovú pečiatku (Time-Stamping Unit)
QSCD		Kvalifikované zariadenie na vyhotovovanie elektronického podpisu/pečate (Qualified electronic Signature/Seal Creation Device)

2. Úložiská

Úložiská musia byť umiestnené tak, aby boli prístupné Zákazníkom a Spoliehajúcim sa stranám a v súlade s celkovými bezpečnostnými požiadavkami.

Funkciu úložiska Poskytovateľa bude zastávať jeho webové sídlo. Presná URL adresa je uvedené v kapitole 1 Webové sídlo Poskytovateľa je prostredníctvom internetu verejne prístupné Zákazníkom, Spoliehajúcim sa stranám a verejnosti vôbec.

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

2.1 **Zverejňovanie** informácií o TSA

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

- aktuálne CRL ako aj všetky CRL vydané od začiatku činnosti vyhotovovania časových pečiatok,
- vlastné certifikáty jednotlivých TSU Poskytovateľa, ktoré patria k jej verejným kľúčom, ktorých zodpovedajúci súkromný kľúč je využívaný pri podpisovaní vyhotovovaných časových pečiatok

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

2.2 Frekvencia **zverejňovania** informácií

Zoznam zrušených certifikátov (CRL) musí byť publikovaný ako je špecifikované v bode 4.9.7 aktuálneho CP QTSP QCA. Informácie o zrušenom certifikáte TSU musia byť dostupné na webovom sídle Poskytovateľa (pozri kapitola 1), ktorý slúži ako jeho úložisko.

CP TSA a CPS TSA prípadne ich revízie sa musia 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

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

3.1 Všeobecné ustanovenia politiky

Tento dokument nadväzuje na dokument „Politika poskytovania dôveryhodných služieb Disig, a.s.“ [4], kde sú popísané všeobecné pravidlá poskytovaných dôveryhodných služieb.

Požiadavky tejto politiky sú založené na kryptografii verejného kľúča (PKI), certifikátoch verejného kľúča a spoľahlivého zdroja presného času.

Očakáva sa, že odberatelia a spoliehajúce sa strany budú konzultovať podrobnosti spôsobu poskytovania TSA služby priamo s poskytujúcou TSU Poskytovateľa.

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 Zákazníkov v zmysle tejto CP TSA je spoločnosť Disig.

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

Zodpovednosť Poskytovateľa za vyhotovovanie časových pečiatok je identifikovateľná (pozri bod 6.7.1 d))

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

3.4 **Používateľ časovej pečiatky**

Používateľom časovej pečiatky je Zákazník.

4. Úvod do politiky **časovej pečiatky** a plnenie všeobecných požiadaviek

4.1 Všeobecne

Tento dokument definuje politiku časovej pečiatky Poskytovateľa, ktorá vyhotovuje časové pečiatky podporované certifikátmi verejného kľúča s presnosťou líšiacou sa od UTC maximálne o 1000 ms.

4.2 **Cieľoví** používatelia a použitie

4.2.1 Správne prax **uplatňovania** politiky vyhotovovania **časových pečiatok**

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

5. Politiky a pravidlá

5.1 Ohodnotenie rizík

Pozri kapitolu 5 dokumentu [4].

5.2 Pravidlá pre praktický výkon dôveryhodných služieb

Všeobecné pravidlá pre praktický výkon dôveryhodných služieb sú uvedené v [4].

5.3 Všeobecné podmienky

Platia všeobecné podmienky popísané v dokumente [4] odstavec 6.2.

5.4 Politika **informačnej bezpečnosti**

Politika informačnej bezpečnosti je popísaná v dokumente [4] odstavec 6.3. [4]

5.5 Záväzky **Poskytovateľa**

5.5.1 Všeobecne

Poskytovateľ časovej pečiatky sa zaväzuje:

- realizovať všetky požiadavky kladené na Poskytovateľa v zmysle kapitoly 6 a 7;
- používať bezpečné systémy a zaisťovať dostatočnú bezpečnosť postupov, ktoré tieto systémy podporujú vrátane dostatočnej kryptografickej bezpečnosti týchto systémov;
- používať bezpečné systémy pre uchovávanie časových pečiatok;
- zabezpečiť, aby prax vyhotovovania časovej pečiatky zodpovedala procedúram popísaným v tejto CP TSA a v súlade s CPS TSA.

5.5.2 Záväzky **Poskytovateľa** k Zákazníkovi

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

5.6 Informácie pre spoliehajúce sa strany

Všeobecné podmienky dostupné pre spoliehajúce sa strany (pozri odstavec 5.3) musia, zahŕňať, v prípade, že sa spoliehajú na časovú pečiatku, nasledovné:

a) Povinnosť overenia, že časová pečiatka bola správne podpísaná a že súkromný kľúč použitý na podpis časovej pečiatky nebol do času overovania kompromitovaný.

   Počas platnosti certifikátu vydávajúcej TSU musí byť platnosť jeho podpisového kľúča overená na základe aktuálneho stavu jeho platnosti na základe údajov publikovaných Poskytovateľom.

b) Všetky obmedzenia pre použitie časovej pečiatky podľa tejto politiky.

c) Všetky ďalšie obmedzenia uvedené v dohodách alebo kdekoľvek inde.

6. Manažment a prevádzka TSA **Poskytovateľa**

6.1 Úvod

Manažment a prevádzka TSA Poskytovateľa sú vykonávaná 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 Poskytovateľa a závisí na dohode o úrovni poskytovaných služieb so Zákazníkom.

6.2 Vnútorná organizácia

Pre vnútornú organizáciu platia ustanovenia uvedené v dokumente [4] odstavec 7.1 a ďalej tieto:

Poskytovateľ:

a) je právnická osoba podliehajúca legislatíve Slovenskej republiky.
b) má zavedený systém riadenia kvality a informačnej bezpečnosti primeraný pre poskytované služby vyhotovovania časových pečiatok.
c) zamestnáva 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**

Pre personálna bezpečnosť platia ustanovenia uvedené v dokumente [4] odstavec 7.2.

6.4 Správa aktív

Pre správu aktív platia ustanovenia uvedené v dokumente [4] odstavec 7.3.

6.5 Riadenie prístupu

Pre riadenie prístupu platia ustanovenia uvedené v dokumente [4] odstavec 7.4.

6.6 Kryptografické opatrenia

6.6.1 Všeobecne

Vhodné bezpečnostné opatrenia aplikované na manažment akýchkoľvek kryptografických kľúčov a kryptografických zariadení počas ich životnosti sú popísané v dokumente [4] odstavec 7.5.

6.6.2 Generovanie kľúčov pre TSU

Generovanie kľúčov pre jednotlivé TSU spĺňa nasledovné:

a) je vykonané vo fyzicky bezpečnom prostredí (pozri odstavec 7.8) osobami zaradenými v dôveryhodných rolách (pozri odstavec 7.3) 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(ov) 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. [5]

d) Podpisový kľúč TSU nie je možné importovať do iného kryptografického modulu bez rozhodnutia PMA 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. [6] 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 [7].

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

Poskytovateľ 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. [8]

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

Keď Poskytovateľ 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 (pozri bod 7.6.1c).

6.6.6 Manažment životného cyklu podpisového kryptografického hardvéru

Aplikované sú nasledovné požiadavky:

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

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

c) Inštalácia, aktivácia a duplikácia podpisových kľúčov TSU v kryptografickom hardware je vykonávaná iba osobami v dôveryhodných rolách, s minimálne dvojitou kontrolou a vo fyzicky bezpečnom prostredí (pozri odstavec 7.8).

d) 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

Poskytovateľ musí definovať dátum exspirácie kľúčov TSU.

Tento dátum nesmie byť neskorší ako koniec platnosti pridružného certifikátu verejného kľúča, kde musí zohľadňovať životnosť definovanú v „odporúčaných veľkostiach kľúča vzhľadom na čas“ z normy ETSI TS 119 312. [5]

Z dôvodu schopnosti verifikovať počas vhodného intervalu času platnosti časových pečiatok, môže byť platnosť podpisového kľúča TSU redukovaná.

Dátum exspirácie kľúčov TSU môže byť definovaný počas inicializácie kryptografického modulu alebo nastavením periódy použitia súkromného kľúča v certifikáte verejného kľúča TSU.

Súkromný podpisový kľúč TSU nebude použitý po skončení jeho životného cyklu.

TSA Disig zabezpečí predovšetkým, že:

a) budú použité prevádzkové alebo technické postupy, ktoré zabezpečia, aby bol použitý nový kľúč keď kľúč TSU exspiruje,

b) súkromné podpisové kľúče TSU, alebo ľubovoľná časť kľúča, zahrňujúc akékoľvek kópie, budú likvidované tak, aby súkromné kľúče prakticky nebolo možné obnoviť.

6.7 Vyhotovenie **časovej pečiatky**

6.7.1 Vydanie **časovej pečiatky**

Časové pečiatky sa musia zhodovať s profilom časovej pečiatky podľa definície v norme ETSI EN 319 422. [9]

Časové pečiatky musia byť vydhotovované bezpečne a musia obsahovať správny čas.

Predovšetkým:

a) Hodnoty času, ktoré TSU používa v časovej pečiatke, musia byť sledovateľné k minimálne jednej z hodnôt reálneho času distribuovaného laboratóriom UTC(k).

b) Čas zahrnutý do časovej pečiatky musí byť synchronizovaný s UTC s presnosťou definovanou v tejto politike.

c) Ak sa zistí, že hodiny poskytovateľa časových pečiatok (pozri bod 7.7.2 c)) bežia mimo stanovenej presnosti (pozri bod 7.7.1. b)), potom časové pečiatky nesmú byť vyhotovené.

d) Časová pečiatka musí byť podpisovaná s využitím súkromného kľúča vytvoreného len pre tento účel.

e) Systém vyhotovujúci časovú pečiatku musí zamietnuť akýkoľvek pokus o vyhotovenie časovej pečiatky ak podpisový súkromný kľúč niektorej TSU Poskytovateľa exspiroval.

6.7.2 Synchronizácia hodín s UTC

Čas používaný jednotlivými TSU musí byť synchronizovaný s UTC s deklarovanou presnosťou minimálne s nasledovnými požiadavkami:

a) Kalibrácia systémových hodín TSU musí byť udržiavaná tak, aby sa hodiny neodchýlili od deklarovanej presnosti.

b) Deklarovaná presnosť je 1000 ms alebo lepšia.

c) Hodiny TSU musia byť chránené proti hrozbám, ktoré by mohli spôsobiť nedetekovateľnú zmenu hodín tak, že presiahnu kalibráciu.

d) Poskytovateľ musí overovať, či čas zahrnutý do časovej pečiatky je posunutý alebo odchýlený od synchronizácie s UTC.

e) Ak sa zistí, že čas zahrnutý v časovej pečiatke je posunutý alebo odchýlený od synchronizácie s UTC, TSU musí zastaviť vyhotovovanie časovej pečiatky.

f) Synchronizácia hodín musí byť udržiavaná keď nastane priestupná sekunda ktorú oznámila príslušná autorita. Zmena zohľadňujúca priestupnú sekundu nastane počas poslednej minúty dňa, keď je priestupná sekunda naplánovaná. Keď nastane táto zmena, musí byť vytvorený záznam o presnom čase, keď táto zmena nastala.

6.8 Fyzická a objektová **bezpečnosť**

Pre fyzickú a objektová bezpečnosť platia ustanovenia uvedené v dokumente [4] odstavec 8.6 a ďalej tieto:

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 Poskytovateľa 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**

Pre prevádzkovú bezpečnosť platia ustanovenia uvedené v dokumente [4] odstavec 8.7 a ďalej toto:

a) Poskytovateľ musí monitorovať kapacitné možnosti poskytovanej služby a včas projektované do budúcich požiadaviek na kapacitu, aby sa zabezpečil dostupný adekvátny výkon a úložný priestor.

6.10 **Sieťová bezpečnosť**

Pre sieťovú bezpečnosť platia pre Poskytovateľa ustanovenia uvedené v dokumente [4] odstavec 8.8 a ďalej tieto:

a) musí udržiavať a chrániť všetky TSU v bezpečnej zóne,

b) 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,

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

6.11 Riadenie **bezpečnostných** incidentov

Pre riadenie bezpečnostných incidentov platia ustanovenia uvedené v dokumente [4] odstavec 8.9.

6.12 Zber dôkazov

Pre zber dôkazov platia ustanovenia uvedené v dokumente [4] odstavec 8.10 a ďalej musia byť zaznamenávané všetky udalosti týkajúce sa:

a) riadenia životného cyklu kľúčov TSU;

b) riadenia životného cyklu certifikátov TSU;

c) synchronizácie hodín TSU s UTC. Toto musí zahŕňať aj informácie týkajúce sa normálnej re-kalibrácie alebo synchronizácie hodín použitých pri vyhotovovaní časových pečiatok;

d) zistenej straty synchronizácie.

6.13 Riadenie kontinuity **činnosti** organizácie

Pre riadenie kontinuity činnosti organizácie platia ustanovenia uvedené v dokumente [4] odstavec 8.11 a ďalej platí:

a) Plán obnovy po pohrome sa musí zaoberať kompromitáciou prípadne podozrením s kompromitácie súkromného kľúča TSU alebo stratou kalibrácie hodín TSU, čo mohlo mať vplyv na vydané časové pečiatky.

b) V prípade kompromitácie alebo podozrenia z kompromitácie alebo strate kalibrácie pri vyhotovovaní časovej pečiatky musí Poskytovateľ sprístupniť všetkým odberateľom a spoliehajúcim sa stranám popis kompromitácie, ktorá nastala.

c) V prípade kompromitácie prevádzky TSU (napr. kompromitácia kľúča TSU), podozrenia z kompromitácie alebo strate TSU kalibrácie nesmie vyhotovovaťčasové pečiatky pokiaľ nebudú vykonané kroky na obnovu po kompromitácii.

d) V prípade významnej kompromitácie prevádzky Poskytovateľa alebo strate kalibrácie, musí Poskytovateľ sprístupniť všetkým odberateľom a spoliehajúcim sa stranám informáciu, ktorá môže byť použitá na identifikáciu časových pečiatok, ktoré mohli byť ovplyvnené, pokiaľ tým neporuší súkromie používateľov Poskytovateľa alebo bezpečnosť služieb Poskytovateľa.

6.14 **Ukončenie činnosti Poskytovateľa** a plány **ukončenia činnosti**

Pre ukončenie činnosti Poskytovateľa platia ustanovenia uvedené v dokumente [4] odstavec 8.12 a ďalej toto:

a) V prípade ukončenia služieb Poskytovateľa musia byť zrušené všetky certifikáty vydané pre jednotlivé TSU.

6.15 Zhoda

Pre zhodu platia ustanovenia uvedené v dokumente [4] odstavec 8.13.

7. Plnenie požiadaviek pre kvalifikované elektronické **časové pečiatky podľa** Nariadenia eIDAS

7.1 Certifikát verejného **kľúča** TSU

V zmysle Nariadenia eIDAS [2], pre kvalifikované elektronické časové pečiatky 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 [10].

7.2 Vyhotovovanie nekvalifikovaných a kvalifikovaných elektronických **časových pečiatok podľa** Nariadenia eIDAS

Ak TSU zahrnutá v systéme Poskytovateľa vyhotovuje časové pečiatky, ktoré sú vyhlasované ako kvalifikované elektronické pečiatky podľa Nariadenia eIDAS [2], táto TSU nesmie vyhotovovať nekvalifikované elektronické časové pečiatky.

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

8. Odkazy

[1] ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. ETSI EN 319 421.

[2] Nariadenie Európskeho parlamentu a Rady (EÚ) **č.** 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES .

[3] Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. ETSI EN 319 401.

[4] Politika poskytovania dôveryhodných služieb Disig, a.s.

[5] Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. ETSI TS 119 312.

[6] Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model. ISO/IEC 15408-1:2009.

[7] Pravidlá na praktický výkon dôveryhodnej služby **časovej pečiatky.** CPS TSA CA Disig.

[8] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[9] Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles. ETSI EN 319 422.

[10] ETSI EN 319411-2 " Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

[11] RECOMMENDATION ITU-R TF.460-6 Standard-frequency and time-signal emissions. ITU-R TF.460-6 .

[12] RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.

História zmien

Verzia	Dátum	Popis revízie; revidoval
1.0	26.2.0007	Prvá verzia dokumentu; Miškovič
1.1	16.7.2007	Zmena názvu certifikačnej autority; Miškovič
1.2	28.1.2009	Úprava CP v súvislosti s nadobudnutím účinnosti zákona č. 214/2008 Z.z., ktorým sa novelizuje zákon č. 215/2002 Z.z. o elektronickom podpise; Miškovič
2.0	23.12.2009	Zmeny v súvislosti so zmenou podpisového algoritmu vydávaných časových pečiatok a zmenou profilu TSA certifikátu; Miškovič
2.1	31.3.2015	Zmena OID politiky a stanovenie spôsobu žiadania o poskytnutie akreditovanej služby časovej pečiatky s OID v žiadosti (4.2; 5.2); Miškovič
4.0	5.5.2017	Komplexná revízia v súvislosti s nadobudnutím účinnosti Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014; Miškovič