Certifikačná autorita CA Disig

Certifikačný poriadok pre autoritu časovej pečiatky (TSA)

Vypracoval	**Ing. Peter Miškovič**
Dátum	**23.12.2009**
Verzia	**2.0**
Typ	**Poriadok**
Schválil	**Ing. Ľuboš Batěk**

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

Obsah

1. Úvod

Autorita časovej pečiatky certifikačnej autority CA Disig (ďalej len „CA Disig“), ktorú prevádzkuje spoločnosť Disig, a.s. (ďalej len „Disig“) vydáva časovú pečiatku, ktorá priraďuje dátum a čas k dokumentu v elektronickej podobe v prísnom kryptografickom režime.

Časovú pečiatku je možné v neskoršej dobe použiť na preukázanie skutočnosti, že elektronický dokument (alebo elektronický podpis) existoval pred určitým konkrétnym časovým momentom uvedeným v časovej pečiatke. Elektronický dokument a časová pečiatka spolu tvoria nezvratný dôkaz v prípade akejkoľvek snahy o spochybnenie existencie duševného vlastníctva uvedeného v dokumente v danom čase.

Certifikačný poriadok (ďalej len „CP“) CA Disig:

- je súhrn pravidiel, ktoré ustanovujú použiteľnosť časovej pečiatky pre definovaný okruh používateľov a triedy aplikácií so spoločnými bezpečnostnými požiadavkami,
- definuje účastníkov procesu vydávania časovej pečiatky, ich zodpovednosti, práva a rozsah použitia časovej pečiatky.
- poskytuje žiadateľovi a spoliehajúcej sa strane zásady prevádzkovania a riadenia služby časovej pečiatky, ktoré vytvárajú ich primeranú dôveru k činnosti CA Disig v tejto oblasti.

Požiadavky CP sú zamerané na akreditovanú službu časovej pečiatky použitú na podporu zaručeného elektronického podpisu alebo na ľubovoľnú aplikáciu vyžadujúcu dôkaz, že informácia existovala pred daným časom, pričom sú tieto založené na použití kryptografie verejných kľúčov, certifikátov verejných kľúčov a spoľahlivom časovom zdroji.

2. Použité skratky a pojmy

2.1. Skratky

CA Disig	-	Certifikačná autorita prevádzkovaná spoločnosťou Disig, a.s.
NBÚ	-	Národný bezpečnostný úrad
TSA	-	Vydavateľ časovej pečiatky (Time Stamp Authority)
UTC	-	Univerzálny svetový čas (Coordinated Universal Time)

2.2. Pojmy

Časová pečiatka – informácia pripojená alebo inak logicky spojená s elektronickým dokumentom spĺňajúca požiadavky § 9 Zákona č. 215/2002 Z. z. o elektronickom podpise, ktorá umožňuje preukázať, že elektronický dokument (alebo elektronický podpis) existoval pred určitým konkrétnym časovým momentom uvedeným v časovej pečiatke. Časová pečiatka je dátový objekt, ktorý zväzuje reprezentáciu informácie s konkrétnym časom, čím sa vytvorí dôkaz, že daná informácia (napr. elektronický dokument, elektronický podpis) existovala pred daným konkrétnym časom.

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 službu vydávania časových pečiatok, označuje sa skratkou TSA (Time Stamp Authority). V zmysle zákona č. 215/2002 o elektronickom podpise ju môže vyhotoviť iba akreditovaná certifikačná autorita 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 (Vyhláška NBÚ č. 537/2002 Z. z.)

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.

3. Všeobecné ustanovenia

3.1. Služba poskytovania časovej pečiatky

Služba poskytovania časovej pečiatky vydavateľom časovej pečiatky (ďalej len „TSA CA Disig“) 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 CA Disig.

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

3.2. Vydavateľ časovej pečiatky

Vydavateľom časovej pečiatky v zmysle tohto CP je:

Certifikačná autorita CA Disig	
Adresa:	**Záhradnícka 151, 821 08 Bratislava 2**
e-mail:	**operatorca@disig.sk**
telefón	**+421 2 20850140**
fax:	**+421 2 20850141**
www:	**http://www.disig.sk**

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

CA Disig preberá plnú zodpovednosť za poskytovanie služby časovej pečiatky, tak ako je definovaná v ods. 3.1.

Na vytvorenie časovej pečiatky je použitý privátny kľúč TSA CA Disig a v tele časovej pečiatky je identifikácia TSA CA Disig ako vydavateľa časovej pečiatky.

TSA CA Disig nevyužíva žiadnu ďalšiu stranu pri poskytovaní služieb časovej pečiatky.

Na poskytovanie časovej pečiatky využíva TSA CA Disig zariadenie certifikované podľa štandardu FIPS 140-2 level 3.

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

3.3. Používateľ časovej pečiatky

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

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

Ak je používateľom právnická osoba zastupujúca niekoľkých koncových používateľov, je táto zodpovedná za to že povinnosti dané organizácii sú koncovými používateľmi dodržiavané a očakáva sa, že organizácia ich bude vhodným spôsobom o tejto skutočnosti informovať.

4. Certifikačný poriadok autority časovej pečiatky

4.1. Prehľad

CP 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 poriadok TSA CA Disig a prostredníctvom nej požiadavky na TSA CA Disig, ktorá poskytuje akreditovanú službu vydávania časových pečiatok (ďalej aj „služba časových pečiatok“).

4.2. Identifikácia

CP TSA CA Disig je identifikovaná nasledovným identifikátorom (OID):

1.3.158.35975946.0.0.1.0.4.2.0

odvodeným od objektového identifikátora C v nasledujúcej hierarchii príslušného podstromu

1. – ISO assigned OIDs

1.**3**. – ISO Identified Organization

1.3.**158**. – Identifikačné číslo subjektu (IČO)

1.3.158.**35975946**. – **Disig, a.s.**

1.3.158.35975946.0.0.**1**.0.– **ACA Disig**

1.3.158.35975946.0.0.1.0.**4.** – **CP TSA ACA Disig**

1.3.158.35975946.0.0.1.0.4.**2.0** CP TSA ACA Disig **verzia 2.0**

4.3. Oznamovanie bezpečnostných incidentov

Tento CP má za cieľ vyhovieť požiadavkám na akreditovanú službu vydávania časovej pečiatky v súlade s požiadavkami Zákona č. 215/2002 Z. z. o elektronickom podpise v znení zákona č. 76/2009 Z. z. a jeho vykonávacích vyhlášok (ďalej len „Zakon č. 215/2002 Z. z.“).

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

Akreditovanú službu časovej pečiatky poskytuje TSA CA Disig v rámci akreditovaných služieb certifikačnej autorityCA Disig.

4.4. Zhoda

TSA CA Disig používa pri vyhotovovaných časových pečiatkach identifikáciu politiky časových pečiatok v zmysle ods. 4.2 a je schopná preukázať, že si plní povinnosti v zmysle ods. 5.1 a má zavedené kontroly v zmysle ods. 6.

5. Povinnosti a zodpovednosť

5.1. Povinnosti poskytovateľa služby časovej pečiatky

5.1.1. Všeobecne

TSA CA Disig ako poskytovateľ služby časovej pečiatky sa zaväzuje:

- uskutočňovať všetky príslušné požiadavky na TSA uvedené v ods. 6,
- zabezpečiť súlad praxe TSA s procedúrami predpísanými touto politikou a ďalšími súvisiacimi dokumentmi,
- poskytovať službu časovej pečiatky v súlade s prevádzkovou smernicou TSA a ďalšími súvisiacimi dokumentmi.

5.1.2. Povinnosti poskytovateľa služby časovej pečiatky voči žiadateľovi

TSA CA Disig si plní svoje záväzky v súlade s podmienkami poskytovania služby časovej pečiatky tak, že služba je dostupná pre definovaných užívateľov a je vykonávaná s maximálnou dôslednosťou.

5.2. Povinnosti žiadateľa

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

Žiadateľovi sa odporúča po získaní digitálneho odtlačku dokumentu 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 a oprávnený žiadať o vyhotovenie časovej pečiatky len prostredníctvom rozhrania alebo softvérovej aplikácie umožňujúceho získať časovú pečiatku na adrese definovanej CA Disig.

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.

5.3. Povinnosti spoliehajúcich sa strán

Spoliehajúce sa strany majú nasledovné povinnosti, ktoré musia vykonať, ak sa chcú spoliehať na časovú pečiatku:

- overiť si, že časová pečiatka je správne podpísaná, a že súkromný kľúč použitý na podpis digitálneho odtlačku dokumentu nebol kompromitovaný v čase jeho podpísania,
- brať do úvahy všetky obmedzenia používania časovej pečiatky uvedené v tomto CP,
- brať do úvahy všetky ďalšie predpísané bezpečnostné opatrenia.

5.4. Zodpovednosť

Právna zodpovednosť TSA CA Disig je daná platnou legislatívou Slovenskej republiky.

Finančnú zodpovednosť a z nej vyplývajúce plnenie je možné uznať len za predpokladov, že užívateľ 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 CA Disig, urobil všetko, aby prípadnej škode zabránil.

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

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

Akákoľvek žiadosť o náhradu škody musí byť podaná písomne.

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

Poskytovateľ časovej pečiatky TSA CA Disig má zavedený systém poskytovania služby spĺňajúci požiadavky zákona č. 215/2002 Z.z. o elektronickom podpise a jeho vykonávacích predpisov.

6.1. Prehlásenie o výkone služby a zverejňovaných informáciách

6.1.1. Prehlásenie o výkone služby

TSA CA Disig zabezpečuje nevyhnutnú spoľahlivosť pri poskytovaní služby časovej pečiatky nasledovnými opatreniami:

- má vypracované pravidlá na výkon služby časovej pečiatky a procedúry resp. pracovné postupy používané na naplnenie všetkých požiadaviek určených v tomto poriadku,
- poskytuje príslušné časti svojich pravidiel na výkon služby časovej pečiatky a ďalšie náležité dokumentov všetkým žiadateľom o službu časovej pečiatky ako aj spoliehajúcim sa stranám,

Poznámka:	TSA CA Disig nemusí sprístupniť detailné informácie o svojej praxi pri výkone TSA.

- zverejňovaním podmienok týkajúcich sa použitia služieb časovej pečiatky v zmysle časti 6.1.2 pre všetkých žiadateľov a potenciálne spoliehajúce sa strany,
- schvaľovaním všetkých dokumentov popisujúcich pravidlá pre výkon činností spojených so službou časovej pečiatky zodpovednými pracovníkmi vedenia Disig
- zabezpečením prostredníctvom vedenia Disig riadneho zavedenia a používania všetkých postupov a praktík TSA CA Disig,
- definovaním postupov preskúmania praktík TSA CA Disig vrátane zodpovedností pri udržiavaní úrovne poskytovaných služieb,
- sprístupnením všetkých zmien týkajúcich sa pravidiel na výkon činností súvisiacich s poskytovaním služieb časovej pečiatky, okamžite po schválení zodpovednými pracovníkmi, všetkým dotknutým stranám.

6.1.2. Zverejňované informácie

TSA CA Disig sprístupňuje všetkým žiadateľom a spoliehajúcim sa stranám podmienky poskytovania služieb časovej pečiatky.

Zverejňované informácie obsahujú:

- kontaktné informácie,

- používaný CP TSA CA Disig,
- používaný algoritmus hašovacej funkcie,
- životnosť kľúčov používaných na vyhotovovanie časovej pečiatky,
- presnosť času vo vyhotovovanej časovej pečiatke s ohľadom na UTC,
- akékoľvek obmedzenia týkajúce sa používania služby časovej pečiatky,
- povinnosti žiadateľa,
- povinnosti spoliehajúcich sa strán,
- informácie o spôsobe overovania časovej pečiatky tak, aby spoliehajúca sa strana mohla túto považovať za „primerane spoľahlivú“ a akékoľvek obmedzenia trvania platnosti
- dobu uchovávania záznamov TSA CA Disig,
- príslušné právne predpisy,
- obmedzenia zodpovednosti,
- postupy podávania sťažností a urovnávania sporov,
- či bola TSA CA Disig posudzovaná vzhľadom k svojej politike časových pečiatok.

Hore uvedené informácie sú k dispozícii trvale prostredníctvom webu CA Disig.

Je ich možné získať v elektronickej podobe stiahnutím z web stránok CA Disig.

Za ich základný zdroj sa považuje tento dokument.

6.2. Manažment životného cyklu kľúčov

6.2.1. Generovanie kľúčov

TSA CA Disig zaisťuje, že všetky kryptografické kľúče používané pri výkone služby časovej pečiatky sú generované za kontrolovaných okolností v bezpečnom zariadení a vo fyzicky bezpečnom prostredí (pozri ods. 6.4.4) dôveryhodnými a kvalifikovanými osobami (pozri ods. 6.4.3) za prítomnosti a pod kontrolou stanoveného počtu osôb.

6.2.2. Ochrana súkromného kľúča TSA CA Disig

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

Súkromný podpisový kľúč TSA CA Disig je generovaný, uchovávaný a používaný v kryptografickom module, ktorý spĺňa požiadavky dané štandardom FIPS 140-2 level 3 a je certifikovaný na NBÚ SR ako produkt pre poskytovateľov certifikačných služieb.

6.2.3. Distribúcia verejného kľúča TSA CA Disig

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

- verejný verifikačný kľúč TSA CA Disig je k dispozícii pre spoliehajúce sa strany prostredníctvom certifikátu verejného kľúča,
- certifikát TSA CA Disig je vydaný akreditovanou CA Disig,
- certifikát je vydaný certifikačnou autoritou, ktorej certifikačný poriadok poskytuje rovnakú, alebo vyššiu úroveň bezpečnosti, ako má tento CP TSA.

6.2.4. Obnovovanie kľúča TSA CA Disig

Životnosť certifikátu TSA CA Disig nie je dlhšia ako časový interval, po dobu ktorého zvolený algoritmus a dĺžka kľúča sú vhodné pre daný účel.

6.2.5. Ukončenie životnosti kľúčov TSA CA Disig

TSA CA Disig sa zaručuje, že súkromný podpisový kľúč TSA nebude používaný po ukončení jeho životnosti.

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

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

6.3. Vytváranie časovej pečiatky

6.3.1. Časová pečiatka

TSA CA Disig zabezpečuje, že časová pečiatka je vydávaná bezpečne, a že obsahuje správny čas.

Predovšetkým:

- časová pečiatka obsahuje identifikátor CP časovej pečiatky,
- časová pečiatka má jedinečné identifikačné číslo,
- hodnota času, ktorá sa dávajú do vyhotovovanej časovej pečiatky, je odvodená z hodnoty reálneho času poskytovaného prostredníctvom UTC (ako spoľahlivého časového zdroja),

- čas, ktorý je dávaný do vyhotovovanej časovej pečiatky, je synchronizovaný s hodnotou UTC v rámci presnosti definovanej v tomto CP,
- časová pečiatka zahŕňa hodnotu hašovacej funkcie, ktorú poskytol žiadateľ, aplikovanú na údaje, ku ktorým sa má vyhotoviť časová pečiatka,
- časová pečiatka je podpisovaná kľúčom TSA CA Disig, ktorý je používaný len na tento účel.

6.3.2. Vyhotovenie a overenie časovej pečiatky

Žiadateľ zašle na adresu služby TSA CA Disig 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 CA Disig, 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 CA Disig vznikli prekážky vyhotovenia časovej pečiatky, TSA CA Disig časovú pečiatku, na predložený digitálny odtlačok dokumentu, nevyhotoví.

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

Časová pečiatka je platná, ak:

- elektronický podpis časovej pečiatky je platný,
- časová pečiatka je v súlade s použitým CP TSA.

6.3.3. Synchronizácia času s UTC

TSA CA Disig zabezpečuje že čas ňou používaný je synchronizovaný s UTC s deklarovanou presnosťou 500 milisekúnd, a to predovšetkým nasledovnými opatreniami:

- kalibrácia hodín TSA CA Disig je vykonávaná tak, že očakávaná odchýlka času nie je mimo deklarovanú presnosť,
- hodiny zariadenia TSA CA Disig sú chránené proti hrozbám, ktoré by mohli viesť k nezistiteľným zásahom do hodín, ktoré by mohli mať za následok ich odchýlku od kalibrácie,
- TSA CA Disig zabezpečuje, že v prípade, že sa čas, ktorý by bol uvedený v časovej pečiatke, odchýli od synchronizácie s UTC, sa táto skutočnosť zistí a časová pečiatka nebude vydaná,

- TSA CA Disig zabezpečuje, že je vykonaná synchronizácia hodín v prípade, že existuje notifikovaná oprávneným orgánom o výskyte opravnej sekundy.

6.3.4. Profil certifikátu časovej pečiatky

Algoritmy a dĺžky kľúčov uplatňované v certifikáte TSA CA Disig:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je 2 048 bitov

Algoritmus fingerprintu (Thumbprint Algorithm)
SHA1

Dĺžka platnosti certifikátu CA Disig
365 dní

Tabuľka č. 1: : Obsah položiek v certifikáte TSA CA Disig

Názov položky	Skratka názvu položky	Hodnota položky
Štát (countryName)	C	**SK**
Mesto (localityName)	L	**Bratislava**
Organizácia (organizationName)	O	**Disig a.s.**
Útvar v organizácii (organizationUnitName)	OU	**ACA-307-2007-2**
Útvar v organizácii (organizationUnitName)	OU	**Akreditovana sluzba vydavania casovej peciatky**
Názov (commonName)	CN	**TSA CA Disig**
Email (emailAddress)	E	**spravaca@disig.sk**

Tabuľka č. 2: Použité rozšírenia v certifikáte TSA CA Disig

Názov rozšírenia	Hodnota rozšírenia	Kritickosť
authorityKeyIdentifier	KeyID=15 7f 5f 5f 08 69 2a c6 70 03 a1 fa 51 6a 4d ac 8d 5f 98 53 Certificate Issuer: Directory Address: CN=KCA NBU SR 3 OU=SIBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Certificate SerialNumber=00 f4	nekritické
subjectKeyIdentifier	určí sa výpočtom	nekritické
keyUsage	Non-Repudiation	nekritické
certificatePolicies	[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.2 [3]Certificate Policy: Policy Identifier=1.3.158.35975946.0.0.1.0.1.2.0 [3,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.disig.sk/_pdf/cp_aca2.pdf [4]Certificate Policy: Policy Identifier=1.3.158.35975946.0.0.1.0.4.2.0 [4,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.disig.sk/_pdf/cp_tsa_aca2.pdf	nekritické
BasicConstraints	Subject Type=End Entity Path Length Constraint=None	kritické
Extended Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)	kritické
crlDistributionPoints	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.disig.sk/aca2/crl/aca2_disig.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.disig.sk/aca2/crl/aca2_disig.crl	nekritické
AuthorityInfoAccess	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://aca-ocsp.disig.sk [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.disig.sk/aca2/cert/aca2_disig.p7c [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	nekritické

	Alternative Name: URL=http://ca.disig.sk/aca2/cert/aca2_disig.p7c	

6.4. Manažment a prevádzka TSA CA Disig

6.4.1. Manažment bezpečnosti

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

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

6.4.2. Klasifikácia a manažment aktív

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

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

6.4.3. Personálna bezpečnosť

Disig zabezpečuje, že postupy personálnej práce podporujú jej dôveryhodnosť.

Predovšetkým:

- prevádzkou TSA CA Disig sú poverení pracovníci, ktorí majú zodpovedajúce znalosti, skúsenosti a nevyhnutnú kvalifikáciu na poskytované služby, a ktorí sú vhodní pre danú pracovnú pozíciu,
- TSA CA Disig 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 vyžaduje, aby pri ich vykonávaní bolo prítomných viacero osôb zastávajúcich danú rolu (tzv. princíp “k” z “n”),

- dôveryhodné roly a ich zodpovednosti sú popísané v prevádzkových smerniciach a prípadne v ďalších dokumentoch a tie roly, na ktorých je závislá bezpečnosť TSA CA Disig, sú jasne identifikované,
- jednotlivé dôveryhodné roly v rámci TSA CA Disig 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,
- pracovníci uplatňujú administratívne a manažérske postupy a procedúry, ktoré sú v súlade s procedúrami manažmentu informačnej bezpečnosti (pozri ods. 6.4.1)

6.4.4. Fyzická a priestorová bezpečnosť

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

Predovšetkým:

- 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,
- je implementovaná kontrola prístupu ku kryptografickému modulu, aby sa zaistili požiadavky na bezpečnosť kryptografického modulu v zmysle ods. 6.2.1 a 6.2.2,
- 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,
- je implementované riadenie fyzickej a priestorovej bezpečnosti, aby sa ochránilo vybavenie, kde sú lokalizované systémové zdroje, samotné systémové zdroje a podporné vybavenie.

6.4.5. Prevádzkový manažment

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

Predovšetkým:

- integrita systémových komponentov TSA CA Disig je chránená proti vírusom, škodlivému a neautorizovanému softvéru,

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

6.4.6. Manažment prístupu k systému

Disig zaisťuje, že k prístup k systému je vyhradený len autorizovaným osobám.

Predovšetkým:

- je implementovaná ochrana, ktorá zabráni neautorizovanému prístupu prostredníctvom sieťového pripojenia,
- Disig zaisťuje efektívnu administráciu prístupu používateľov (vrátane používateľov v dôveryhodných rolách) na udržiavanie bezpečnosti systému,
- 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.

6.4.7. Nasadenie a údržba dôveryhodných systémov

Disig 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.

6.4.8. Kompromitácia služieb TSA DISIG

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

6.4.9. Ukončenie činnosti TSA DISIG

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

6.4.10. Súlad s právnymi požiadavkami

TSA CA Disig zabezpečuje súlad svojej činnosti s právnymi požiadavkami.

Výkon služby časovej pečiatky sa riadi platnou legislatívou Slovenskej republiky so zreteľom na zákon č. 215/2002 Z. z. o elektronickom podpise v aktuálnom znení a súvisiace vyhlášky (vyhlášky NBÚ č. 131/2009 Z. z., 132/2009 Z. z., 133/2009 Z. z., 134/2009 Z. z., 135/2009 Z. z., 136/2009 Z. z.)

Popri tom:

- sú splnené právne požiadavky legislatívy Európskej únie tak, ako sú premietnuté v slovenskej legislatíve,
- v rámci TSA CA Disig 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 CA Disig,
- informácie poskytnuté žiadateľmi o služby TSA CA Disig sú chránené pred zverejnením, pokiaľ na to nedá súhlas žiadateľ alebo to neprikáže súd alebo iný kompetentný štátny orgán.

6.4.11. Zaznamenávanie údajov týkajúcich sa výkonu služby časovej pečiatky

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

Predovšetkým:

- TSA CA Disig dokumentuje, ktoré konkrétne prípady a údaje sa majú zaznamenávať,
- je udržiavaná dôvernosť a celistvosť súčasných a archivovaných záznamov týkajúcich sa činnosti služby časovej pečiatky,
- záznamy týkajúce sa činnosti služby časovej pečiatky sú bezpečne a kompletne archivované v zmysle zverejnených praktík,
- 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,
- je zaznamenávaný presný čas významných udalostí týkajúcich sa prostredia TSA CA Disig, manažmentu kľúčov a synchronizácie času,
- záznamy týkajúce sa činnosti služby časovej pečiatky sú uchovávané počas primeranej doby po vypršaní platnosti podpisového kľúča TSA CA Disig, aby bola možné poskytnúť právny dôkaz a ako je to uvedené v prehlásení o zverejňovaní informácií (pozri ods. 6.1),
- udalosti sú zaznamenávané spôsobom, aby tieto záznamy nemohli byť ľahko zmazané alebo zničené a sú uchovávané počas doby, ktorá je na ich uchovávanie požadovaná,

- akékoľvek informácie o žiadateľovi sa uchovávajú ako dôverné okrem prípadov, keď existuje súhlas žiadateľa s ich publikovaním alebo prípadov uvedených v ods. 6.4.10,
- sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k životnému cyklu kľúčov TSA CA Disig,
- sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k životnému cyklu certifikátov TSA CA Disig,
- sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k synchronizácii hodín TSA CA Disig,
- sú zaznamenávané všetky záznamy týkajúce sa všetkých udalostí majúcich vzťah k detegovaniu straty synchronizácie hodín.

6.5. Organizačné aspekty

Disig zaisťuje, že jej organizácia je spoľahlivá, pričom kladie dôraz na zaistenie, že:

- Poriadky, pravidlá a postupy používané TSA CA Disig nie sú diskriminačné,
- umožní prístup k svojim službám žiadateľom, ktorých aktivity spadajú do oblasti jej pôsobnosti, a ktorí súhlasia dodržovať svoje povinnosti ako sú špecifikované v tomto CP,
- má systém pre manažment kvality a informačnej bezpečnosti vhodný na poskytovanie služieb časovej pečiatky,
- má primerané prostriedky na pokrytie svojej zodpovednosti vyplývajúcej z výkonu svojich činností,
- je finančne stabilná a má zdroje požadované na výkon činností v súlade s týmto poriadkom,
- zamestnáva dostatočný počet pracovníkov, ktorí majú nevyhnutné vzdelanie, zácvik, technické znalosti a skúsenosti týkajúce sa poskytovania služby časovej pečiatky
- má postup na riešenie sťažností a podnetov od žiadateľov alebo iných strán týkajúce sa poskytovania služby časovej pečiatky alebo iných súvisiacich služieb.

7. Odkazy

Tento CP vychádza z:

- ETSI TS 102 023 V1.2.2 (2008-10) Policy requirements for time-stamping authorities“
- RFC 3628, November 2003 „Policy requirements for time-stamping authorities (TSAs)“
- RFC 3161, August 2001 „Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)“
- ETSI TS 101 456 V1.4.3 (2007-05) – Policy requirements for certification authorities issuing qualified certificates.
- Zákon č. 215/2002 Z. z. o elektronickom podpise v znení zákona č. 76/2009 Z. z. a súvisiace vyhlášky (vyhlášky NBÚ č. 131/2009 Z. z., 132/2009 Z. z., 133/2009 Z. z., 134/2009 Z. z., 135/2009 Z. z. a 136/2009 Z. z.)