

# **Podpisová politika**

**pre použitie zaručeného elektronického podpisu v  
bežnom styku**

# Obsah

<b>1</b>	<b>ÚVOD</b>	<b>4</b>
1.1	PREHLAD	4
1.2	IDENTIFIKÁCIA DOKUMENTU	4
1.3	APLIKOVATELNOSŤ PODPISOVEJ POLITIKY	4
1.4	ZÚČASTNENÉ STRANY	4
1.5	KONTAKTNÉ INFORMÁCIE	5
<b>2</b>	<b>PODPOROVANÉ TYPY ZÁVÄZKOV</b>	<b>5</b>
2.1	ROLE PODPISOVATEĽA	6
<b>3</b>	<b>POVINNOSTI A ZODPOVEDNOSŤ ÚČASTNÍKOV</b>	<b>6</b>
3.1	POVINNOSTI PODPISOVATEĽA	6
3.1.1	<i>Ochrana súkromného kľúča podpisovateľa</i>	6
3.1.2	<i>Použitie certifikátu a príslušného kľúča podpisovateľa</i>	7
3.1.3	<i>Prostredie pre vytvorenie podpisu</i>	7
3.1.4	<i>Atribúty a obsah podpisu</i>	7
3.1.5	<i>Role podpisovateľa</i>	7
3.2	POVINNOSTI OVEROVATEĽA	7
3.2.1	<i>Overovanie podpisu</i>	7
3.2.2	<i>Prostredie pre overenie podpisu</i>	8
3.3	POVINNOSTI SPOLIEHAJÚCEJ SA STRANY	8
3.3.1	<i>Konanie na základe podpisu</i>	8
3.3.2	<i>Atribúty a obsah podpisu</i>	8
3.3.3	<i>Role podpisovateľa</i>	8
<b>4</b>	<b>PRAVIDLÁ PLATNOSTI ZARUČENÉHO ELEKTRONICKÉHO PODPISU</b>	<b>8</b>
4.1	OBDOBIE PODPISOVANIA	9
4.2	FORMÁTY PODPISOVANÝCH DOKUMENTOV	9
4.3	FORMÁTY ZARUČENÉHO ELEKTRONICKÉHO PODPISU	9
4.3.1	<i>Vyžadované podpísané atribúty</i>	9
4.3.2	<i>Vyžadované nepodpísané atribúty</i>	10
4.3.3	<i>Zakázané podpísané atribúty</i>	10
4.4	CERTIFIKÁT VEREJNÉHO KĽÚČA PODPISOVATEĽA	11
4.4.1	<i>Certifikačná cesta</i>	11
4.4.2	<i>Akceptovateľné koreňové certifikáty</i>	11
4.4.3	<i>Formát certifikátov</i>	11
4.4.4	<i>Akceptovateľné certifikačné poriadky</i>	11
4.4.5	<i>Mená subjektov</i>	12
4.4.6	<i>Mechanizmy zrušovania certifikátov</i>	12
4.4.7	<i>Platnosť certifikátov</i>	12
4.5	ATRIBÚTOVÉ CERTIFIKÁTY	12
4.6	ZAZNAMENÁVANIE ČASU	12
4.6.1	<i>Čas vytvorenia podpisu</i>	12
4.6.2	<i>Maximálna doba do získania časovej pečiatky</i>	13
4.6.3	<i>Formát časovej pečiatky</i>	13
4.6.4	<i>Akceptovateľné authority časových pečiatok</i>	13
4.6.5	<i>Akceptovateľné politiky časových pečiatok</i>	13
4.6.6	<i>Certifikát authority časových pečiatok</i>	13
4.7	ROLE PODPISOVATEĽA	14
4.7.1	<i>Role uvedené podpisovateľom</i>	14



D. Trust Certifikačná Autorita, a.s.

Podpisová politika pre použitie elektronického podpisu v bežnom styku

Verzia 2.0

4.7.2	<i>Certifikované role</i> .....	14
4.8	ALGORITMY A DĹŽKY KĹÚČOV .....	14
4.9	OPĀTOVNĀ KONTROLA PLATNOSTI.....	15
<b>5</b>	<b>VIACERĚ PODPISY</b> .....	<b>15</b>
<b>6</b>	<b>ADMINISTRĀCIA DOKUMENTU</b> .....	<b>15</b>
6.1	PUBLIKĀCIA A ARCHIVĀCIA .....	15
6.2	PROCES ZMIEN DOKUMENTU .....	15
6.3	OZNAMOVANIE ZISTENÝCH NEDOSTATKOV .....	16
6.4	AUTORSKĚ PRĀVA .....	16
<b>7</b>	<b>REFERENCIE</b> .....	<b>16</b>

# 1 Úvod

## 1.1 Prehľad

Tento dokument predstavuje podpisovú politiku pre použitie zaručeného elektronického podpisu v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise (ďalej len ZoEP) v bežnom styku. Táto podpisová politika definuje pravidlá zaručujúce jednoznačné určenie platnosti zaručeného elektronického podpisu pre účely jeho použitia v bežnom styku a povinnosti pre podpisovateľov a overovateľov pri vytváraní a overovaní platnosti zaručených elektronických podpisov. Použitie tejto podpisovej politiky je rozhodnutím podpisovateľa na základe jeho predchádzajúcej dohody alebo požiadaviek predpokladaných strán spoliehajúcich sa na ním vytvorený zaručený elektronický podpis.

## 1.2 Identifikácia dokumentu

Názov dokumentu: Podpisová politika pre použitie elektronického podpisu v bežnom styku

Verzia: 2.0

Dátum vydania dokumentu: 24.08.2005

URI dokumentu: [http://uri.dtca.sk/signature\\_policies/common/v2.0](http://uri.dtca.sk/signature_policies/common/v2.0)

OID dokumentu: 1.3.6.1.4.1.19725.3.1.2

## 1.3 Aplikovateľnosť podpisovej politiky

Táto podpisová politika určuje pravidlá zaručujúce jednoznačnosť určenia platnosti zaručeného elektronického podpisu. Túto podpisovú politiku je možné použiť v bežnom styku t.j. pre potreby podpisovania vyžadujúce zaručený elektronický podpis v obchodnom alebo administratívnom styku, v zmysle ZoEP, v otvorených i uzavretých systémoch pre typy záväzkov uvedené v tejto podpisovej politike.

## 1.4 Zúčastnené strany

Pre účely tejto podpisovej politiky sú zúčastnenými stranami :

- **vydavateľom** tejto podpisovej politiky autorita, ktorá je zodpovedná za definovanie obsahu tohto dokumentu, jeho aktualizáciu, správu a publikáciu,
- **podpisovateľom** fyzická osoba, ktorá je vlastníkom kvalifikovaného certifikátu vydaného k párovým údajom (súkromnému a verejnému kľúču), pomocou ktorých je vytváraný alebo bol vytvorený elektronický podpis,
- **overovateľom** osoba zisťujúca platnosť elektronického podpisu v zmysle tejto podpisovej politiky,

- **spoliehajúcou sa stranou** osoba zakladajúca svoje ďalšie konanie na obdržaní platného zaručeného elektronického podpisu v súlade s touto podpisovou politikou,
- **účastníkom** podpisovateľ, overovateľ alebo spoliehajúca sa strana.

Rozhodnutie o použití tejto podpisovej politiky pre vytvorenie konkrétneho elektronického podpisu je výlučným právom podpisovateľa. Podpisovateľ musí toto rozhodnutie urobiť počas procesu podpisovania, čo potvrdí vložení referencie na túto podpisovú politiku do ním vytvoreného elektronického podpisu v súlade s bodom 4.3.1.1. Vložení tejto referencie do elektronického podpisu podpisovateľ potvrdzuje, že je zoznámený s touto podpisovou politikou, akceptuje jej ustanovenia a preberá na seba všetky záväzky ňou ustanovené.

Ak elektronický podpis neobsahuje referenciu na túto podpisovú politiku v súlade so schválenými formátmi pre zaručený elektronický podpis nie je podpisovateľ touto podpisovou politikou viazaný a to ani na základe predchádzajúcej dohody so spoliehajúcou sa stranou.

## 1.5 Kontaktné informácie

Vydavateľom tejto podpisovej politiky je:

Názov organizácie: D. Trust Certifikačná Autorita, a.s.  
Sídlo organizácie: Plynárska 7/C, 821 09 Bratislava 2  
IČO: 35840005  
Registrácia: Obchodný register Okresného súdu Bratislava I, oddiel: Sa, vložka číslo: 2986/B

Vydavateľa je možné kontaktovať:

telefonicky: +421 2 58222153

faxom: +421 2 58222777

e-mailom: [info@dtca.sk](mailto:info@dtca.sk)

a na vyššie uvedenej poštovej adrese.

Ďalšie informácie o tejto podpisovej politike a jej vydavateľovi je možné získať prostredníctvom webových stránok prístupných na adrese <http://www.dtca.sk>

## 2 Podporované typy záväzkov

Táto podpisová politika podporuje jediný typ záväzku, ktorým je schválenie dokumentu. Podpisovateľ vytvorením podpisu podľa tejto podpisovej politiky potvrdzuje, že je

zoznámený s obsahom podpisovaného dokumentu, že s ním súhlasí a preberá na seba záväzky z dokumentu preňho vyplývajúce.

## 2.1 Role podpisovateľa

Podpisovateľ môže svoj kvalifikovaný certifikát použiť pre podpisovanie v rôznych roliach. Rola podpisovateľa určuje v koho mene a s akými právomocami podpisovateľ koná.

Ak podpisovateľ neuvedie v podpise rolu, v ktorej koná a podpisovateľ a spoliehajúca sa strana sa vopred písomne nedohodli v akej roli v tomto prípade podpisovateľ koná, koná podpisovateľ v roli, ktorá jednoznačne vyplýva z povahy alebo obsahu podpisovaného dokumentu. Ak rola dokumentom nie je určená, koná podpisovateľ výlučne za seba ako za fyzickú osobu.

## 3 Povinnosti a zodpovednosť účastníkov

Táto kapitola definuje povinnosti účastníkov pri vytváraní a overovaní platnosti zaručených elektronických podpisov vytvorených podľa tejto podpisovej politiky. Nesplnením si povinnosti ustanovenej v tejto časti preberá účastník, ktorému bola táto povinnosť uložená, plnú zodpovednosť za škody spôsobené iným účastníkom svojím konaním.

### 3.1 Povinnosti podpisovateľa

Porušenie povinností podpisovateľa ustanovených v tomto bode nezakladá dôvod pre pokladanie ktoréhokoľvek zaručeného elektronického podpisu podpisovateľa, spĺňajúceho všetky podmienky ustanovené v bode 4, za neplatný.

#### 3.1.1 Ochrana súkromného kľúča podpisovateľa

Podpisovateľ je povinný venovať ochrane svojho súkromného kľúča primeranú pozornosť. Podpisovateľ je povinný najmä:

- uchovávať svoj súkromný kľúč výlučne v bezpečnom zariadení certifikovanom na tento účel NBÚ,
- neposkytnúť svoj súkromný kľúč ani jeho časti ani k nim neumožniť prístup certifikačnej autorite ani inej strane pre účely jeho zálohovania, uchovávania alebo akéhokoľvek iné účely,
- chrániť bezpečné zariadenie pred jeho zneužitím inými osobami,
- neprezradiť autentifikačné údaje potrebné pre prístup k súkromnému kľúču inej osobe,
- nezaznamenávať si autentifikačné údaje potrebné pre prístup k súkromnému kľúču spôsobom, pri ktorom hrozí ich prezradenie inej osobe,

- pravidelne meniť autentifikačné údaje potrebné pre prístup k súkromnému kľúču.

### **3.1.2 Použitie certifikátu a príslušného kľúča podpisovateľa**

Podpisovateľ smie svoj súkromný kľúč a kvalifikovaný certifikát, ktorý používa pre vytváranie elektronických podpisov podľa tejto podpisovej politiky, použiť len pre účely vytvárania zaručených elektronických podpisov. Ich používanie na vytváranie iných typov podpisov, šifrovanie, autentifikáciu alebo iné účely nie je prípustné.

### **3.1.3 Prostredie pre vytvorenie podpisu**

Podpisovateľ je povinný vytvárať zaručené elektronické podpisy podľa tejto podpisovej politiky v prostredí spĺňajúcom bezpečnostné požiadavky určené ZoEP. Podpisovateľ je pre tento účel povinný najmä:

- presvedčiť sa v rámci svojich možností, že prostriedky a zariadenia, ktoré používa nie sú zmanipulované alebo inak poškodené,
- podľa svojich možností používať zariadenia a prostriedky pre vytváranie elektronického podpisu, ktorým bola udelená certifikácia NBÚ,
- dodržiavať postupy pre vytváranie zaručeného elektronického podpisu pre prostriedky a zariadenia, ktoré používa,
- nevytvárať podpisy na verejne prístupných zariadeniach, ktoré nie sú výslovne určené pre tento účel.

### **3.1.4 Atribúty a obsah podpisu**

Podpisovateľ nesmie do podpisu zahrnúť podpísané atribúty, ktorých významu nerozumie alebo s ním nesúhlasí. Podpisovateľ nesie plnú zodpovednosť za porušenie tejto povinnosti. Podpisovateľ nesie plnú zodpovednosť za hodnoty uvedené v podpísaných atribútoch. Ak podpisovateľ uviedol v podpísanom atribúte hodnotu, ktorá sa nezhoduje so skutočnosťou a spoliehajúca strana konala v dobrej viere na základe tejto hodnoty, nesie podpisovateľ plnú zodpovednosť za škody vzniknuté spoliehajúcej sa strane.

### **3.1.5 Role podpisovateľa**

Podpisovateľ smie uviesť v podpise len také role, v ktorých má právo konať.

## **3.2 Povinnosti overovateľa**

### **3.2.1 Overovanie podpisu**

Overovateľ je povinný pri overovaní podpisu overiť, či boli splnené všetky požiadavky ustanovené bodom 4. Ak niektorá z požiadaviek splnená nebola resp. overovateľ ju nie je schopný overiť musí vyhlásiť podpis za neplatný resp. pokladať podpis za neplatný.

### **3.2.2 Prostredie pre overenie podpisu**

Overovateľ je povinný overovať zaručené elektronické podpisy podľa tejto podpisovej politiky v prostredí spĺňajúcom bezpečnostné požiadavky určené ZoEP. Podpisovateľ je pre tento účel povinný najmä:

- presvedčiť sa v rámci svojich možností, že prostriedky a zariadenia, ktoré používa nie sú zmanipulované alebo inak poškodené,
- podľa svojich možností používať zariadenia a prostriedky pre overovanie elektronického podpisu, ktorým bola udelená certifikácia NBÚ,
- dodržiavať postupy pre overenie zaručeného elektronického podpisu pre prostriedky a zariadenia, ktoré používa.

## **3.3 Povinnosti spoliehajúcej sa strany**

### **3.3.1 Konanie na základe podpisu**

Spoliehajúca sa strana je pred konaním, ktoré zakladá na predpoklade platnosti podpisu podľa tejto podpisovej politiky, povinná overiť jeho platnosť. Ak je podpis neplatný alebo nemožno jeho platnosť overiť je spoliehajúca sa strana povinná zdržať takéhoto konania.

Spoliehajúca sa strana môže overiť platnosť elektronického podpisu podľa tejto podpisovej politiky sama alebo využiť služby inej dôveryhodnej osoby. Zodpovednosť za overenie podpisu v oboch prípadoch nesie spoliehajúca sa strana.

### **3.3.2 Atribúty a obsah podpisu**

Spoliehajúca sa strana smie konať na jeho základe zaručeného elektronického podpisu platného podľa tejto podpisovej politiky len ak rozumie významu a obsahu všetkých podpísaných atribútov uvedených v podpise.

### **3.3.3 Role podpisovateľa**

Ak podpisovateľ uviedol v podpise rolu alebo viaceré role, v ktorej koná a spoliehajúca sa strana si nie je jednoznačne istá o akú rolu ide alebo či táto rola postačuje pre účel vytvorenia podpisu, nesmie konať na jeho základe.

## **4 Pravidlá platnosti zaručeného elektronického podpisu**

Táto kapitola definuje pravidlá platnosti zaručených elektronických podpisov vytvorených podľa tejto podpisovej politiky. Zaručený elektronický podpis je platný vtedy a len vtedy ak spĺňa všetky podmienky, pravidlá a požiadavky ustanovené v tejto kapitole a je platný v zmysle ZoEP.

## 4.1 Obdobie podpisovania

Zaručené elektronické podpisy je podľa tejto podpisovej politiky povolené vytvárať len v období od 1.9.2005 do 1.1.2007. Mimo toto obdobie nie je možné vytvárať zaručené elektronické podpisy v súlade s touto podpisovou politikou a takéto zaručené elektronické podpisy sú považované za neplatné.

## 4.2 Formáty podpisovaných dokumentov

Dokumenty podpisované podľa tejto podpisovej politiky smú byť uložené vo formátoch definovaných prílohou č. 3 k vyhláške č. 542/2002 Z.z.

## 4.3 Formáty zaručeného elektronického podpisu

Zaručený elektronický podpis vytvorený podľa tejto podpisovej politiky musí byť uložený vo formáte schválenom Národným bezpečnostným úradom Slovenskej republiky (ďalej tiež NBÚ) v súlade so ZoEP a prípustnom podľa tejto podpisovej politiky.

Formát podpisu zvolený podpisovateľom pri vytvorení podpisu v súlade s vyššie uvedenými požiadavkami a použitý pre uloženie podpisu bude ďalej nazývaný len použitým formátom podpisu.

Táto podpisová politika pripúšťa v súlade s použitým formátom podpisu uloženie podpisu:

- samostatne a nezávisle od podpisovaného dokumentu,
- ako súčasť podpisovaného dokumentu,
- spolu s dokumentom v na to určenej dátovej štruktúre.

Podpisovateľ musí do podpisu zahrnúť podpísané a nepodpísané atribúty podľa nižšie uvedených požiadaviek. Podpisovateľ môže do podpisu zahrnúť i iné podpísané a nepodpísané atribúty podľa vlastného uváženia.

Podpisovateľ resp. spoliehajúce sa strany smú do podpisu zahrnúť resp. spoliehať sa na uvedenie a naplnenie podpísaného atribútu len ak jeho formát, použitie a význam boli definované v tejto podpisovej politike alebo v špecifikácii použitého formátu elektronického podpisu.

### 4.3.1 Vyžadované podpísané atribúty

Podpisovateľ je povinný do podpisu, vytvoreného podľa tejto podpisovej politiky, zahrnúť ako podpísané atribúty všetky atribúty uvedené v tomto bode a súčasne všetky atribúty, ktorých zahrnutie do podpisu ako podpísané atribúty vyžaduje použitý formát podpisu. Podpis, ktorý neobsahuje všetky vyžadované podpísané atribúty je neplatný.

#### **4.3.1.1 Identifikátor podpisovej politiky**

Táto podpisová politika vyžaduje explicitné uvedenie referencie na podpisovú politiku v elektronickom podpise podľa nej vytvoreného. Používanie elektronických podpisov bez uvedenia referencie podpisovej politiky nie je prípustné.

Podpisovateľ zahmie do podpisu podpísaný atribút určený na uloženie referencie podpisovej politiky definovaný použitým formátom podpisu. Do referencie musí podpisovateľ zahrnúť identifikátor tejto podpisovej politiky, digitálny odtlačok tejto podpisovej politiky a URI z ktorého je možné získať túto podpisovú politiku. Ako identifikátor podpisovej politiky v atribúte musí byť uvedený príslušný identifikátor definovaný v bode 1.2. Digitálny odtlačok uvedený v atribúte musí byť spočítaný jedným z algoritmov SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 alebo RIPEMD-160 s dátovou formou tejto podpisovej politiky zverejnenej vydavateľom v súlade s bodom 6.1. V atribúte musí byť uvedené URI, z ktorého účastníci môžu získať túto podpisovú politiku t.j. URI, na ktorom vydavateľ zverejňuje túto podpisovú politiku podľa bodu 6.1.

#### **4.3.1.2 Referencia podpisového certifikátu**

Podpisovateľ zahrnie do na to určeného atribútu podpisu definovaného použitým formátom digitálny odtlačok kvalifikovaného certifikátu verejného kľúča, pomocou ktorého má byť overovaná platnosť tohto podpisu, a prípadne ďalšie identifikačné údaje tohto certifikátu.

Podpis musí byť overiteľný na základe certifikátu a verejného kľúča v ňom uloženého, digitálny odtlačok ktorého je zhodný s digitálnym odtlačkom uvedeným v tomto atribúte.

#### **4.3.2 Vyžadované nepodpísané atribúty**

Podpisovateľ je povinný do podpisu vytvoreného podľa tejto podpisovej politiky zahrnúť ako nepodpísané atribúty všetky atribúty uvedené v tomto bode a súčasne všetky atribúty, ktorých zahrnutie do podpisu ako nepodpísané atribúty vyžaduje použitý formát podpisu.

##### **4.3.2.1 Podpisový certifikát**

Podpisovateľ zahrnie do na to určeného atribútu podpisu definovaného príslušným formátom kvalifikovaný certifikát verejného kľúča, pomocou ktorého má byť overovaná platnosť tohto podpisu. Digitálny odtlačok tohto certifikátu sa musí zhodovať s odtlačkom v atribúte uvedenom podľa bodu 4.3.1.2.

#### **4.3.3 Zakázané podpísané atribúty**

Podpisovateľ nesmie do podpisu zahrnúť ako podpísaný atribút žiaden z atribútov uvedených v tomto bode. Podpis obsahujúci jeden alebo viac takýchto atribútov atribút je neplatný.

#### 4.3.3.1 Typ záväzku

Podpis nesmie obsahovať štandardný atribút definovaný príslušným formátom elektronického podpisu určujúci typ záväzku podpisovateľa. Typ záväzku je jednoznačne určený touto podpisovou politikou.

### 4.4 Certifikát verejného kľúča podpisovateľa

Certifikát verejného kľúča podpisovateľa vydaný akreditovanou certifikačnou autoritou na verejný kľúč tvoriaci pár so súkromným kľúčom použitým podpisovateľom na podpisovanie podľa tejto podpisovej politiky a uvedený v atribúte podpisu podľa bodu 4.3.1.2, musí byť kvalifikovaným certifikátom fyzickej osoby v zmysle ZoEP §7 ods. 2. Tento certifikát bude pre účely tohto bodu nazývaný aj podpisovým certifikátom.

#### 4.4.1 Certifikačná cesta

Úplná certifikačná cesta k podpisovému certifikátu vždy začína kvalifikovaným koreňovým certifikátom koreňovej certifikačnej autority NBÚ (ďalej len KCA) (viď bod 4.4.2) a končí príslušným kvalifikovaným podpisovým certifikátom fyzickej osoby. Certifikačná cesta môže obsahovať medzi týmito certifikátmi aj ďalšie certifikáty spĺňajúce požiadavky stanovené ZoEP, najmä kvalifikovaný certifikát akreditovanej certifikačnej autority vydaný KCA.

#### 4.4.2 Akceptovateľné koreňové certifikáty

Jedinými akceptovateľnými koreňovými certifikátmi tvoriacimi vrchol každej certifikačnej cesty sú certifikáty koreňovej certifikačnej autority NBÚ, ktoré sú vydané a zverejnené NBÚ.

#### 4.4.3 Formát certifikátov

Všetky certifikáty v certifikačnej ceste musia spĺňať požiadavky podľa normy [X509] pre certifikáty verzie 3, požiadavky kladené na príslušné kvalifikované certifikáty ZoEP a musia byť uložené a naplnené v súlade s formátmi pre kvalifikované certifikáty schválenými NBÚ.

Podpisový certifikát musí obsahovať štandardné rozšírenie `crlDistributionPoints` obsahujúce najmenej dva distribučné body pre zoznamy zrušených certifikátov verejne prístupné pomocou protokolu HTTP alebo HTTPS.

Podpisový certifikát nesmie obsahovať žiadne kritické rozšírenia obmedzujúce alebo upravujúce záväzky podpisovateľa.

#### 4.4.4 Akceptovateľné certifikačné poriadky

Táto podpisová politika akceptuje ako certifikačný poriadok, podľa ktorého bol vydaný podpisový certifikát, ľubovoľný certifikačný poriadok používaný akreditovanou certifikačnou autoritou pre vydávanie kvalifikovaných certifikátov.

#### **4.4.5 Mená subjektov**

Táto podpisová politika nekladie žiadne podmienky na mená subjektov a vydavateľov vyskytujúc sa v podpisovom certifikáte alebo iných certifikátoch v certifikačnej ceste vedúcej k nemu nad rámec podmienok stanovených formátmi certifikátov.

#### **4.4.6 Mechanizmy zrušovania certifikátov**

Táto podpisová politika podporuje zrušovanie certifikátov pred ukončením ich plánovanej doby platnosti len pomocou mechanizmu publikovania zoznamov zrušených certifikátov (ďalej len CRL). Táto podpisová politika nepodporuje používanie rozdielových CRL (Delta CRL).

#### **4.4.7 Platnosť certifikátov**

Každý z certifikátov v certifikačnej ceste k podpisovému certifikátu musí byť v čase vytvorenia podpisu, v zmysle bodu 4.6.1, platný v zmysle podmienok ustanovených ZoEP.

Certifikát je k danému času platný ak sú splnené všetky nasledovné podmienky:

- Certifikát je podpísaný platným elektronickým podpisom vydavateľa tohto certifikátu.
- Certifikát je k danému času v dobe svojej platnosti uvedenej v ňom.
- Certifikát nebol k tomuto času zrušený.

Certifikát je k danému času pokladaný za zrušený, ak sa nachádza na príslušnom zozname zrušených certifikátov platnom k danému času.

#### **4.5 Atribútové certifikáty**

Táto podpisová politika v súlade so ZoEP nepripúšťa používanie atribútových certifikátov.

#### **4.6 Zaznamenávanie času**

Ak overovanie platnosti podpisu alebo jeho archivácia vyžadujú zaznamenávanie času, musí byť tento zaznamenaný v súlade s ustanoveniami tohto bodu pomocou platnej časovej pečiatky.

Autoritou časových pečiatok je pre účely tohto bodu akreditovaná certifikačná autorita poskytujúca službu vydávania časových pečiatok.

##### **4.6.1 Čas vytvorenia podpisu**

Časom vytvorenia podpisu podľa tejto podpisovej politiky je najskorší čas, kedy je dôveryhodne doložená existencia príslušného podpisu pomocou časovej pečiatky platnej podľa tejto podpisovej politiky.

Ak podpisovateľ získal časovú pečiatku dôveryhodne dokladajúcu čas vytvorenia podpisu, je povinný doručiť túto overovateľovi. Ak tak podpisovateľ neurobí musí overovateľ predpokladať, že čas vytvorenia podpisu nie je dôveryhodne doložený.

Ak overovateľ nemá k dispozícii dôveryhodne doložený čas vytvorenia podpisu je povinný získať časovú pečiatku k tomuto podpisu dokladajúcu aktuálny čas, ktorý sa stáva časom vytvorenia podpisu.

#### **4.6.2 Maximálna doba do získania časovej pečiatky**

Ak podpisovateľ do podpisu vložil atribút definujúci podľa použitého formátu podpisu čas vytvorenia podpisu, musí byť časová pečiatka dokladujúca čas vytvorenia podpisu k podpisu získaná najneskôr do 72 hodín od času uvedeného podpisovateľom.

#### **4.6.3 Formát časovej pečiatky**

Časová pečiatka musí byť uložená vo formáte definovanom normou [TSP] v súlade s formátmi časovej pečiatky schválenými NBÚ.

#### **4.6.4 Akceptovateľné authority časových pečiatok**

Pre potreby tejto podpisovej politiky sú akceptovateľné časové pečiatky vydávané akreditovanými certifikačnými autoritami súlade so ZoEP.

#### **4.6.5 Akceptovateľné politiky časových pečiatok**

Časové pečiatky použiteľné pre potreby tejto podpisovej politiky môžu byť vydané podľa ľubovoľnej politiky časových pečiatok používanej akreditovanou certifikačnou autoritou pre vydávanie časových pečiatok.

#### **4.6.6 Certifikát authority časových pečiatok**

Certifikát authority časových pečiatok, identifikovaný príslušným atribútom časovej pečiatky, určený pre overenie platnosti príslušnej časovej pečiatky musí byť kvalifikovaným certifikátom v zmysle ZoEP.

##### **4.6.6.1 Certifikačná cesta**

Úplná certifikačná cesta k certifikátu authority časových pečiatok vždy začína kvalifikovaným koreňovým certifikátom koreňovej certifikačnej authority NBÚ a končí kvalifikovaným certifikátom authority časových pečiatok. Certifikačná cesta môže obsahovať medzi týmito certifikátmi aj ďalšie certifikáty spĺňajúce požiadavky stanovené ZoEP.

##### **4.6.6.2 Akceptovateľné koreňové certifikáty**

Jedinými akceptovateľnými koreňovými certifikátmi tvoriacimi vrchol každej certifikačnej cesty sú certifikáty koreňovej certifikačnej authority NBÚ, ktoré sú vydané a zverejnené NBÚ.

#### **4.6.6.3 Formát certifikátov**

Všetky certifikáty v certifikačnej ceste musia spĺňať požiadavky podľa normy [X509] pre certifikáty verzie 3, požiadavky kladené na príslušné kvalifikované certifikáty ZoEP a musia byť uložené a naplnené v súlade s formátmi pre kvalifikované certifikáty schválenými NBÚ.

#### **4.6.6.4 Akceptovateľné certifikačné poriadky**

Táto podpisová politika nekladie žiadne podmienky na výber certifikačného poriadku akreditovanej certifikačnej autority, podľa ktorého bol vydaný certifikát autority časovej pečiatky alebo iné certifikáty v certifikačnej ceste vedúcej k nemu.

#### **4.6.6.5 Mechanizmy zrušovania certifikátov a platnosť certifikátov**

Pre mechanizmy zrušovania certifikátov v certifikačnej ceste vedúcej k certifikátu autority časových pečiatok a ich platnosť sa primerane použijú ustanovenia bodov 4.4.6 a 4.4.7.

### **4.7 Role podpisovateľa**

Právomoci vyplývajúce z role podpisovateľa uvedenej v podpise alebo inak určenej touto podpisovou politikou musia byť dostatočné pre prevzatie záväzkov vyplývajúcich z podpisu. Ak nie je možné jednoznačne určiť, či je táto podmienka splnená je podpis neplatný.

#### **4.7.1 Role uvedené podpisovateľom**

Rolu, prípadne viaceré role, v ktorej resp. v ktorých podpisovateľ koná môže uviesť do podpísaného atribútu podpisu určeného na tento účel použitým formátom podpisu. Každá z rolí, v ktorej podpisovateľ vystupuje, musí byť určená jednoznačne a jasne. Ak podpisovateľ koná v mene organizácie musí byť táto organizácia v uvedenej roli jednoznačne určená.

#### **4.7.2 Certifikované role**

Používanie atribútových certifikátov na určenie role podpisovateľa sa nepripúšťa.

### **4.8 Algoritmy a dĺžky kľúčov**

Táto podpisová politika pripúšťa na vytváranie zaručených elektronických popisov použitie algoritmov s parametrami definovanými ktoroukoľvek z platných podpisových schém definovaných vyhláškou č. 537/2002 Z.z.

Dĺžky kľúčov certifikačných autorít, používané pre podpisovanie certifikátov a časových pečiatok, musia byť najmenej 2048 bitov pre šifrovací systém RSA a dĺžky zaručujúcej rovnakú úroveň bezpečnosti pre iné šifrovacie systémy.

## 4.9 Opätovná kontrola platnosti

Táto podpisová politika nevyžaduje uplynutie žiadnej doby od času vytvorenia podpisu, po ktorej je potrebná opätovná kontrola splnenia podmienok platnosti podpisu pred jeho vyhlásením za platný.

## 5 Viaceré podpisy

Ak formát elektronického podpisu pripúšťa uloženie viacerých elektronických podpisov v jednej dátovej štruktúre povoľuje táto podpisová politika použitie takejto vlastnosti. Platnosť každého podpisu a splnenie záväzkov účastníkov sa posudzuje pre každý podpis samostatne. Ak podpisovateľ podpísal, iný, už existujúci podpis, platný podľa tejto podpisovej politiky, je tento jeho podpis rovný podpisu dokumentu samotného.

Viaceré podpisy dokumentu môžu byť uložené i v samostatných dátových štruktúrach.

Ak je konanie spoliehajúcej sa strany podmienené viacerými podpismi dokumentu musí mať spoliehajúca sa strana pred začatím svojho konania k dispozícii všetky potrebné podpisy platné podľa tejto podpisovej politiky.

## 6 Administrácia dokumentu

### 6.1 Publikácia a archivácia

Vydavateľ sa zaväzuje sprístupniť tento dokument účastníkom prostredníctvom svojich webových stránok na adrese [http://repository.dtca.sk/2004/common\\_sp-v2\\_0.pdf](http://repository.dtca.sk/2004/common_sp-v2_0.pdf). Vydavateľ na tejto adrese uverejní tento dokument vo formáte Adobe Portable Document Format (PDF) verzia 1.3. Dokument v tomto formáte je považovaný za finálnu dátovú formu tejto podpisovej politiky pre účely vypočítania digitálneho odtlačku podpisovej politiky. Vydavateľ sa zaväzuje poskytnúť túto podpisovú politiku účastníkom na základe žiadosti i na vhodnom prenosnom dátovom médiu. Žiadateľ je povinný uhradiť vydavateľovi skutočné náklady vzniknuté pri vybavovaní jeho žiadosti ak o to vydavateľ požiada.

Vydavateľ sa zväzuje po zverejnení podpisovej politiky nemeniť žiadnym spôsobom jej zverejnenú formu. Vydavateľ sa zaväzuje pomocou svojich stránok sprístupňovať podpisovú politiku minimálne po dobu 5 rokov od jej vydania a na základe žiadosti minimálne 20 rokov od jej vydania. Vydavateľ zabezpečí dlhodobé uchovávanie tejto podpisovej politiky v archíve prístupnom účastníkom.

### 6.2 Proces zmien dokumentu

Vydavateľ je oprávnený aktualizovať a meniť túto podpisovú politiku a to najmä na základe požiadaviek účastníkov a zmien v prostredí, v ktorom je používaná. Pri akejkoľvek zmene tejto podpisovej politiky, či už obsahového, editoriálneho,



D. Trust Certifikačná Autorita, a.s.

Podpisová politika pre použitie elektronického podpisu v bežnom styku

Verzia 2.0

typografického alebo iného charakteru je vydavateľ povinný vydať novú verziu podpisovej politiky odlišujúcu sa od ostatných verzií číslom verzie, URI a identifikátorom objektu (OID).

Vydavateľ je povinný zverejniť navrhovanú verziu podpisovanej politiky na svojich webových stránkach a to najmenej 7 dní pred plánovaným nadobudnutím jej platnosti. Účastníci a odborná verejnosť majú v tejto lehote možnosť vyjadriť k navrhovanej podpisovej politike svoje pripomienky ich zaslaním na kontaktné adresy vydavateľa uvedené v bode 1.5. Akceptovanie pripomienok a úprava navrhovanej verzie podpisovanej politiky na základe získanej odozvy je výlučne vecou rozhodnutia a plne v kompetencii vydavateľa.

Vydaním novej verzie podpisovanej politiky nie je dotknutá použiteľnosť a platnosť žiadnej z jej predchádzajúcich verzií.

### 6.3 Oznamovanie zistených nedostatkov

Ak vydavateľ zistí pred ukončením obdobia podpisovania ustanoveného v bode 4.1 nedostatky alebo chyby, ktoré by mohli mať za následok nejednoznačnosť výsledku overenia platnosti elektronického podpisu alebo by iným spôsobom mohli spochybniť túto podpisovú politiku ako celok, je povinný o zistených nedostatkoch informovať účastníkov prostredníctvom svojich webových stránok. Spolu s informáciou o zistených nedostatkoch je povinný uviesť odporúčanie, či je naďalej možné používať politiku alebo jej ďalšie použitie nie je vhodné spolu.

Zverejnenie informácie o zistených nedostatkoch ani odporúčanie ďalej nepoužívať podpisovú politiku nezakladá dôvod pre akékoľvek zmeny v právach a povinnostiach účastníkov ustanovených touto podpisovou politikou vyplývajúcich z jej použitia pred alebo po dátume zverejnenia takéhoto oznámenia.

### 6.4 Autorské práva

Vlastníkom všetkých autorských práv k tomuto dokumentu je vydavateľ. Vydavateľ týmto dáva všeobecný súhlas k vytváraniu kópií a distribúcii tohto dokumentu v jeho kompletnej a nezmenenej forme a jeho používaniu v súlade s jeho účelom.

## 7 Referencie

- |      |   |
|------|---|
| X509 | ITU-T Recommendation X.509 : “Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks“ |
| TSP  | RFC 3161 : “Internet X.509 Public Key Infrastructure Time Stamping Protocol (TSP)”  |