# VÚ 8116 Trenčín ODBOR INFORMAČNEJ BEZPEČNOSTI

# Použitie zaručeného elektronického podpisu v praxi

(Pomôcka pre používateľov)

#### 2013 VÚ 8116 Trenčín

Vypracoval: Skupina bezpečnosti technických prostriedkov Centrum informačnej bezpečnosti Trenčín Spracované na základe dokumentácie Certifikačnej autority MOSR a používateľskej príručky QSign 3.4.1

Informácie v tomto dokumente nesmú byť menené bez písomného súhlasu **Odboru informačnej bezpečnosti.** Všetky práva sú vyhradené.

Táto brožúra je určená výhradne pre potreby Ozbrojených síl Slovenskej republiky.

Dokument neprešiel jazykovou úpravou.

#### Ochranné známky:

Mená produktov uvádzané v tomto dokumente môžu byť registrované ochranné známky príslušných firiem.

Pripomienky k tomuto dokumentu môžete posielať na adresu: pki@mil.sk

# **OBSAH**

1.	Ζ	ákladný opis aplikácie
2.	Р	rihlásenie užívateľa do aplikácie Q-Sign 5
3.	Z	ákladné funkcie
3	.1.	Podpisovanie dokumentov
3	.2.	Viacnásobný podpis14
3	.3.	Ako uzatvoriť podpis17
3	.4.	Overovanie prijatých podpísaných dokumentov18
4.	Г	Definícia stavu podpisu certifikátu22

## 1. Základný opis aplikácie

Základnou podmienkou platnosti dokumentu podpísaného zaručeným elektronickým podpisom (ZEP) je použitie bezpečnej aplikácie určenej na tvorbu a overenie zaručeného elektronického podpisu, certifikovanej Národným bezpečnostným úradom SR. Takouto aplikáciou je **QSign**.



Obrázok 1 Štart aplikácie Qsign

Aplikácia QSIGN je primárne určená na podpisovanie a overovanie dokumentov pomocou zaručeného elektronického podpisu v zmysle legislatívy Slovenskej republiky. Je určená pre operačný systém Microsoft Windows ako univerzálny prostriedok na podpisovanie dokumentov. Umožňuje zabezpečiť a overiť autenticitu a integritu elektronických dokumentov.

Základom integrity a autenticity elektronických dokumentov je zabezpečiť, aby údaje, ktoré sú zobrazené na obrazovke, boli zhodné s tými, ktoré používateľ svojim podpisom potvrdzuje ("What you see is what you sign" "Podpisuješ to čo vidíš") a navyše dokument v sebe neskrýval ďalšie údaje, o ktorých podpisovateľ nevie, alebo ich môže ľahko prehliadnuť ("What you see is what you trust"- "Čo vidíš tomu môžeš veriť").

Tento dokument slúži iba ako pomôcka pre použitie aplikácie QSign na okamžité podpísanie dokumentu resp. pre overenie podpisu. Podrobné informácie o používaní aplikácie sú uvedené v používateľskej príručke, ktorá je umiestnená v ponuke "ŠTART- PROGRAMY-ARDACO-QSIGN-QSIGN DOKUMENTÁCIA"

Návod k používaniu aplikácie QSign je implementovaný aj v aplikácii pod názvom **Pomocník** a je dostupný z menu ovládania. Okrem podrobného popisu postupu inštalácie a ovládania vysvetľuje aj základné pojmy z oblasti zaručeného elektronického podpisu.

## 2. Prihlásenie užívateľa do aplikácie Q-Sign

Pre podpisovanie dokumentov si aplikácia vyžaduje prihlásenie používateľa.

1. Pred procesom prihlásenia je potrebné sa presvedčiť, či je čipová karta s kvalifikovaným certifikátom pre ZEP korektne vložená do čítacieho zariadenia (čítačka čipových kariet)

EN 🛠	9 🖻	ی 🕼	7:45 AM	

Obrázok 2 Korektné pripojenie čítačky a čipovej karty

2. Prihlasovacie okno je dostupné cez ovládacie menu aplikácie. Pravým tlačidlom myši kliknite na ikonu **Q** na paneli úloh

	QSign	
∫ SK	\$ 0.5	8:18 AM

Obrázok 3 Aplikácia Qsign v oznamovacej oblasti

3. Zo zobrazenej ponuky menu QSign kliknite na voľbu Prihlásiť



Obrázok 4 Menu aplikácie

4. Po zobrazení prihlasovacieho okna a načítaní pripojených zariadení je potrebné zadať PIN k čipovej karte.

Q, QSign - Pril	hlásenie	×
	Aplikácia je spustená v ONLINE režime	
Typ zariader	nia	
2	Q QSign	- <del>6</del>
Zariadenie OMNIKEY Ca	Autorizácia používateľa	<b>-</b> 0
Certifikát	Používateľ: SmartCard User	
Menovka	PIN:	
	OK Zrušiť	
,	Zobraziť Prihlásiť	Zrušiť
Načítavanie užív	vateľských certifikátov	

Obrázok 5 Autorizácia používateľa

5. Následne sa vo výberovom okne dialógu "**Certifikáty**" zobrazia všetky certifikáty nainštalované na vybranom zariadení, ktorými je možné sa prihlásiť. V prípade, že je pripojené práve jedno zariadenie, po Vašej autorizácii sa dostupné certifikáty načítajú automaticky.



Obrázok 6 Prihlasovanie používateľ

6. Po označení požadovaného certifikátu sa môžete prihlásiť stlačením tlačidla **Prihlásiť** a potvrdiť dôveryhodnosť Certifikátu KCA NBU SR 3:

QSign	×
?	Pre účel overovania platnosti elektronického podpisu je potrebné potvrdiť dôveru koreňového certifikátu: Certifikát: KCA NBU SR 3
	Odtlacok (nash) SHA-1: 21 F7 3B 27 BB BF 28 11 BB EA B4 F1 79 9E 7D D8 92 F3 FE 85
	Uvedený certifikát overte prostredníctvom jeho odtlačku (hash) hodnoty.
	V prípade overovania v súlade s platnou legislatívou SR ide o jeden z koreňových certifikátov Národného bezpečnostného úradu, ktoré sú zverejnené na adrese <u>http://ep.nbusr.sk/kca/certifikat.html</u> .
	Je tento certifikát dôveryhodný?
	Zobraziť Áno Nie

Obrázok 4 Kontrola dôveryhodnosti certifikátu KCA NBU

## 3. Základné funkcie

Medzi najdôležitejšie funkcie, ktoré aplikácia poskytuje používateľovi patrí:

#### 1. Podpisovanie dokumentov

Zahŕňa jednoduché podpisovanie dokumentov, viacnásobné podpisovanie, uzatváranie podpisu alebo archívne podpisovanie s nastaveniami, ktoré používateľovi umožňujú vytvoriť podpis presne podľa jeho požiadaviek.

#### 2. Overovanie podpisov

Overovanie ľubovoľného externého elektronického podpisu v medzinárodnom formáte ETSI (CMS - PKCS7), alebo uloženého v ZEP (ZIP) type súboru.

#### 3. História overovania

Zjednodušuje používateľovi spravovanie overovaných dokumentov. Jednotlivé podpisy je možné dopĺňať o časové pečiatky alebo na archívne podpisy. Umožňuje overovať podpisy bez časovej pečiatky.

#### 3.1. Podpisovanie dokumentov

Aplikácia umožňuje podpísanie ľubovoľného dokumentu na Vašom počítači. Pre inicializovanie podpisovania máte na výber nasledujúce možnosti:

- Podpisovanie pomocou ovládacieho menu aplikácie
- Podpisovanie pomocou kontextového menu
- Podpisovanie pomocou virtuálnej tlačiarne

#### 3.1.1. Podpisovanie pomocou ovládacieho menu aplikácie

- 1. Otvorte ovládacie menu aplikácie
- 2. Vyberte položku Podpísať dokument



Obrázok 8 Podpis dokumentu z menu aplikácie

3. V otvorenom okne aplikácie stlačte tlačidlo **Vybrať** a zadajte cestu k podpisovanému dokumentu.

Q QSign		
Podpisovanie Náhľad dokumentu		
	Dokument na podpísanie Cesta k súboru	<u>U</u> /brať
		<u>Z</u> rušiť

Obrázok 9 Súbor na podpis

 Zobrazí sa podpisové okno – Náhľad dokumentu. Tlačidlo Podpísať nie je prístupné, pred podpisom je potrebné zväčšiť a skontrolovať obsah dokumentu. Po skontrolovaní dokumentu pripraveného na Váš podpis kliknite na lupu pre zmenšenie náhľadu



Obrázok 10 Náhľad dokumentu

5. Kliknite na Nastavenie dokumentu a zašktnite Vložiť časovú pečiatku

ainewania		
	Nastavenie parametrov výstupných dokumentov	
0	Nazov cieloveho dokumentu	
Nebra d	C:\Users\Documents\Dokument_1	l.zep
dokumentu		Zmenit'
4	Tup elektropického podpisu	
Nastavenie	Typ zaheznečenja: Zaručený elektronichý podpis	
dokumentu	Typ podpisu: Bez časovej pečiatky	
S	Vložiť časovú pečiatku podpisu	
Podpisová		
Certifikačné		
oorannaono		
cesty		
cesty		
cesty	Priložiť sprievodné dokumenty	
cesty ? Pomocník	Priložiť sprievodné dokumenty     Zoznam priložených dokumentov	
cesty ? Pomocník	Priložiť sprievodné dokumenty     Zoznam priložených dokumentov	Možiť
Pomocník	Priložiť sprievodné dokumenty     Zoznam priložených dokumentov	<u>M</u> ožiť… Odobrať
Cesty Pomocník	Priložiť sprievodné dokumenty Zoznam priložených dokumentov	
Pomocník	Priložiť sprievodné dokumenty Zoznam priložených dokumentov	 Odobrat'
Pomocník	Priložiť sprievodné dokumenty Zoznam priložených dokumentov  Vloženie časovej pečiatky obsahu podpisovaného dokumentu	<u>M</u> ožit' Odobrat'
cesty Pomocník	Priložiť sprievodné dokumenty Zoznam priložených dokumentov Vloženie časovej pečiatky obsahu podpisovaného dokumentu	<u>M</u> ožiť… Odobrať
cesty Pomocník	Priložiť sprievodné dokumenty Zoznam priložených dokumentov  Vloženie časovej pečiatky obsahu podpisovaného dokumentu Vytvoriť Vložiť zo súboru	Možiť Odobrať
Pomocník	Priložiť sprievodné dokumenty Zoznam priložených dokumentov Vloženie časovej pečiatky obsahu podpisovaného dokumentu Vytvoriť Vložiť zo súboru	Možiť Odobrať
Pomocnik	Priložiť sprievodné dokumenty Zoznam priložených dokumentov Vloženie časovej pečiatky obsahu podpisovaného dokumentu Vloženie časovej pečiatky obsahu podpisovaného dokumentu Vloženie časovej pečiatky obsahu podpisovaného dokumentu Votvoriť Vytvoriť Vložiť zo súboru Segure časového počiatek	 Odobrať
Pomocnik	Priložiť sprievodné dokumenty Zoznam priložených dokumentov Vloženie časovej pečiatky obsahu podpisovaného dokumentu Vytvoriť Vložiť zo súboru Server časových pečiatok	Možiť… Odobrať
Pomocník	Priložiť sprievodné dokumenty Zoznam priložených dokumentov Vloženie časovej pečiatky obsahu podpisovaného dokumentu Vytvoriť Vložiť zo súboru Server časových pečiatok salmilsk OID politiky pre časovú pečiatku	Oožit' Odobrat'
Pomocnik	Priložiť sprievodné dokumenty Zoznam priložených dokumentov Vloženie časovej pečiatky obsahu podpisovaného dokumentu Vloženie časovej pečiatky obsahu podpisovaného dokumentu Vloženie časovej pečiatky obsahu podpisovaného dokumentu Votvoriť Vložiť zo súboru Server časových pečiatok Server časových pečiatok Sel milsk OID politiky pre časovú pečiatku	↓ Odobrať

Obrázok 11 Nastavenie časovej pečiatky

6. Stlačením tlačidla **Podpísať** dokument podpíšete

#### 3.1.2. Podpisovanie pomocou kontextového menu

Operácia podpisovanie dokumentov vyžaduje prihlásenie používateľa

- 1. Kliknúť pravým tlačidlom myši nad dokumentom zobrazíte menu
- 2. V menu vyberte položku QSign Podpíš súbor

<b>Otvoriť</b> Upraviť Nové	
Tlačiť 7-Zip 🛃 Edit with Notepad++	•
Skontrolovať pomocou ESET Endpoint Security Ďalšie možnosti	•
Open with Share with	•
QSign	Over súbor
SmartFTP Restore previous versions	Podpíš súbor
Send to	•
Cut Copy	
Create shortcut Delete Rename	

Obrázok 12 Podpis dokumentu z kontextoveho menu

- 3. V prípade, že ste sa pred podpísaním dokumentu neprihlásili do QSign, aplikácia Vám oznámi, že nie ste prihlásený.
- 4. Po Vašej autorizácii sa načítajú dostupné certifikáty. Po označení požadovaného certifikátu sa môžete prihlásiť stlačením tlačidla **Prihlásiť**.
- 5. Ďalší postup je rovnaký ako v prípade podpisu prostredníctvom menu aplikácie.

#### 3.1.3. Podpisovanie pomocou virtuálnej tlačiarne

Táto voľba je dostupná z ľubovoľného programu nainštalovaného na vašom počítači, ktorý umožňuje tlač dokumentov. Pred tlačou je potrebné vybrať virtuálnu *Tlačiareň pre ZEP* a nechať dokument vytlačiť do prostredia Aplikácie pre ZEP.

1. Otvorte dokument na podpísanie v aplikácií MS Word alebo iný.

2. Vyberte položku menu *Súbor* > *Tlač*.



Obrázok 13 Tlač dokumentu

3. Zo zoznamu tlačiarní vyberte *Tlačiareň pre ZEP*.

Print	? ×
Printer	
Name: 🍓 Tlaciaren pre ZEP	✓ Properties
Status: Idle Type: Tlaciaren pre ZEP Where: ZEP001 Comment:	Fin <u>d</u> Printer
Page range  C All  Current page C Selection  Pages:  Type page numbers and/or page ranges separated by commas counting from the start of the document or the section. For example, type 1, 3, 5–12 or p1s1, p1s2, p1s3–p8s3	Copies Number of copies: 1
Print what:     Document       Print:     All pages in range	Zoom Pages per sheet: 1 page Scale to paper size: No Scaling
Options	OK Cancel

Obrázok 14 Podpis dokumentu cez tlačiareň ZEP

## 3.2. Viacnásobný podpis

#### 3.2.1. Použitie viacnásobného podpisu

V praxi sa vyskytujú prípady, v ktorých je potrebné dokument podpísať viacerými osobami, napr. dokument podliehajúci schvaľovaciemu procesu v štruktúre organizácie alebo zmluva medzi viacerými zmluvnými stranami. V týchto prípadoch je vhodné využiť pri podpisovaní elektronického dokumentu možnosť vytvorenia viacnásobného podpisu.

#### 3.2.2. Ako vytvoriť viacnásobný podpis

Viacnásobný podpis sa vytvorí podpísaním súboru ZEP s jednoduchým podpisom. Podpíše sa tak dokument, ktorého podpis je uložený v súbore ZEP a vznikne ďalší jednoduchý podpis. Ten sa uloží spolu s predchádzajúcim podpisom do súboru ZEP. Viacnásobný podpis je teda tvorený viacerými jednoduchými podpismi v súbore ZEP.

Na vytvorenie viacnásobného podpisu <u>nemôžete použiť podpísanie pomocou virtuálnej</u> tlačiarne.

Môžete použiť kontextové menu po stlačení pravého tlačidla myši nad už existujúcim súborom ZEP s jednoduchým podpisom. Prípadne cez ovládacie menu aplikácie, voľbou **Podpísať dokument**.

1. Pred podpísaním už podpísaného dokumentu aplikácia QSign ponúkne možnosť overenia už existujúceho podpisu. V prípade voľby **Áno** sa výsledok overenia zobrazí v overovacom okne. V prípade voľby **Nie** pokračujte krokom **3**.

	okumentu: D2013042310	43042\M20130423104304	z.em
Podpisovateľ	Výsledný stav podpisu	Typ podpisu	Časová pečiatka
	veupine overenie	ZEP's casovou peciatikou	23. 4. 2013 12:45
Upozomenia:			
Overenie platnosti	certifikátu podľa CRL		
Overenie platnosti PKI 2	certifikátu podľa CRL		•
Overenie platnosti PKI 2 Podpisová politika	certifikátu podľa CRL		E
Overenie platnosti PKI 2 Podpisová politika Identifikátor politik	certifikátu podľa CRL ty: 1 3 158 30845572 1 7	11	

Obrázok 15 Výsledok overenia elektronického podpisu

- 2. Pre zatvorenie overovacieho okna stlačte tlačidlo Zatvoriť
- Zobrazí sa podpisové okno Náhľad dokumentu. Tlačidlo Podpísať nie je prístupné, pred podpisom je potrebné zväčšiť a skontrolovať obsah dokumentu. Po skontrolovaní dokumentu pripraveného na Váš podpis kliknite na lupu pre zmenšenie náhľadu

Q QSign		- 0 <b>x</b>
Podpisovanie         Náhľad         Náhľad         dokumentu         Image: Contract of the second		
	Uzatvoriť Podpísať	Zatvoriť

Obrázok 16 Kontrola a potvrdenie obsahu dokumentu

4. V časti **Nastavenie dokumentu** sa môžete presvedčiť (viď šípka), či ide o viacnásobný podpis, a ku ktorému dokumentu pripájate časovú pečiatku (názov cieľ ového dokumentu).

Q QSign	
Podpisovanie Náhľad dokumentu	Nastavenie parametrov výstupných dokumentov Názov cieľového dokumentu C:\Users\Documents\Dokument_1.zep Zmeniť
Nastavenie dokumentu Podpisová politika	Typ elektronického podpisu Typ zabezpečenia: <b>Zaručený elektronický podpis</b> Typ podpisu: <b>Sčasovou pečiatkou</b> Vložiť časovú pečiatku podpisu Vlacnásobný podpis no formáte ETSI Integritný podpis
Certifikačné cesty Pomocník	Priložiť sprievodné dokumenty  Zoznam priložených dokumentov  Vložiť  Odobrať
	Vloženie časovej pečiatky obsahu podpisovaného dokumentu  Vytvoriť  Vložiť zo súboru  Server časových pečiatok  OID politiky pre časovú pečiatku
	Uzatvoriť Podpísať Zatvoriť

Obrázok 17 Podpísanie dokumentu

Stlačením tlačidla Podpísať dokument podpíšete

## 3.3. Ako uzatvorit' podpis

Viacnásobný, ale aj jednoduchý podpis je možné uzatvoriť. To znamená, že sa nepodpisuje dokument, ale všetky jednoduché a uzatváracie podpisy v archíve.

Postup pri vytváraní uzatváracieho podpisu je zhodný s postupom pri vytváraní jednoduchého či viacnásobného podpisu. Namiesto tlačidla **Podpísať** je však potrebné použiť tlačidlo **Uzatvoriť**.



Obrázok 18 Uzatvorenie dokumentu

Súbor ZEP s uzatváracím podpisom je možné znovu podpísať alebo aj ďalej uzatvoriť, ak je to potrebné. Pred uzatvorením podpisu musia byť všetky podpisy doplnené na úplnú informáciu.

# <u>POZOR: Pred podpísaním dokumentu si vždy dôkladne preštudujte, čo podpisujte.</u>

#### 3.4. Overovanie prijatých podpísaných dokumentov

Overiť podpísaný dokument môže každý, kto:

- 1. má spustenú aplikáciu QSign v režime "Online".
- 2. je pripojený na Internet.

Postup overovania podpisu pomocou kontextového menu je nasledovný:

 v prostredí Prieskumníka otvoríte kontextové menu nad súborom, ktorý chcete overiť, v menu vyberte položku QSign > Over súbor

-	7-Zip	•	1	
okumen 🔘	Skontrolovať pomocou ESET Endpoint Antivirus Ďalšie možnosti	•		
	Otvoriť v programe			
	Zdieľať s	•		
	QSign	•	3	Over súbor
	Obnoviť predchádzajúce verzie		2	Podpíš súbor
	Odoslať kam	+		
	Vystrihnúť		L .	
	Kopírovať		L .	
	Vytvoriť odkaz		L .	
	Odstrániť		L .	
	Premenovať		L .	
	10			

Obrázok 19 Overenie dokumentu cez kontextové menu

- Po stlačení tlačidla Over súbor aplikácia overí platnosť podpisu pomocou informácií získaných z dôveryhodných internetových zdrojov. Vykonanie operácie vyžaduje určitý čas (približne 30 sekúnd)
- 3. Po dokončení operácie overovania sa zobrazí výsledok overenia

QSign				
Overovanie	Názov overeného	dokumentu: D201304	29104504Z\M201	30429104504Z.eml
	Podpisovateľ	Výsledný stav podpisu	Typ podpisu	Časová pečiatka
Wisledok	······ 24	Neúplné overenie	ZEP s časovou	29. 4. 2013 12:4
overenia				
<b>P</b>				
Share a				
podpisov				
100				
Náhľad dokumentu				
História	112000000000000000000000000000000000000			
	Upozomenia:			
2				
Pomocník				
	Overenie platnos	ti certifikátu podľa CRL		
	PKI 2			
	Podpisová politik	a	701711	
	identifikator polit	uky.  1 3 156 308455	/21/11	9/
	SK: ZEP v súlad accordance with Defence of the S	le s legislatívou SR určen n legislation in the Slovak I Slovak Republic purposes	ý pre potreby MO SR Republic dedicated fo	. EN: QES in or Ministry of
L			Overiť	Zatvoriť

Obrázok 20 Výsledok overenia

V prípade zobrazenia stavu "**Neúplné overenie**" je potrebné pre úplnosť overenia zopakovať overenie podpisu podľa uvedeného postupu, znovu po uplynutí 12-24 hodín. Možné stavy podpisov, certifikátov a typy podpisov sú uvedené v bode **4** tejto pomôcky.

4. V záložke Stav podpisov na ľavej strane sú zobrazené detaily certifikátu a certifikačnej cesty

Stav podpisov	pisu 🔻 🔙 Zot	orazit' certifikát	Zobra	ziť politiku		
Podpisovateľ	Тур ро	dpisu Sta	v podpisu	Stav certifik	ačnej cesty	Dátum podpisu
B 20130429104504Z	52013 Jednod	luchý				
é.	ZEPs	časovou Plat	ný	Neúplné ov	erenie	29. 4. 2013 1
Časová pečiatk	a podp	Plat	ný	Neúplné ov	erenie	29. 4. 2013 1
Stav certifikátov podpisove	j certifikačnej ce	sty				
Certifikát 1	Typ certifikátu	Stav certifikátu	Pozr	námka		
8-91	(valifikovaný	Staré CRL				
GAMOSR2 CAMOSR2	CA	Staré CRL				
🦾 🚮 KCA NBU 🖇	Self-signed CA	Staré CRL				
Atribúty podpisu Detaily cert CA 22 9B B3 5D B Deklarovaný čas 29. 4. 2013 12:45: Podpisová politil Id politiky: 13 158 Algoritmus: SHA.22 Hash politiky: 04 72 1D C0 CC Adresa: http://www Organizácia: ou=B	ifikátu Podpisov a 3 C0 57 CC EE D s podpisu 04 ca 30845572 1 7 1 1 56 3 2B 8B 7E 99 DE w nburs.sk/archiv ezpecnostny urad ca: SK: ZEP v súk	rá politika CRL z 0 72 FB D4 9B BA 8 EB 04 35 79 D6 e/201012010000 MO SR.o=Minister MO SR.o=Minister	áznam k ci 44 5F 0C 94 56 56 2 <u>00zsignatu</u> rstvo obrar rstvo obrar	ertifikátu 06 C3 63 C0 2 29 75 C9 F6 AC repolicy.der ny SRJ-Bratisl, pre potreby M	27 7E D5 65 4 C 26 19 EC A ava.c=SKČís SR. EN: Q	4C AF 95 E9 21 B 08 73 75 E9 lo poznámky: 1

Obrázok 21 Podrobné informácie o certifikátoch

5. Kliknutím na záložku Náhľad dokumentu na ľavej strane si môžete dokument pozrieť, uložiť alebo vytlačiť



Obrázok 22 Náhľad dokumentu pri overovaní

Podrobný popis overovacieho okna a možností jeho použitia obsahuje **Pomocník** aplikácie QSign (dostupný z menu ovládania na paneli úloh).

# 4. Definícia stavu podpisu certifikátu

Po overení dokumentu sa vám v overovacom okne zobrazí časť "Výsledok overenia". Dôležitou položkou je "Výsledný stav podpisu" (viď obrázok vyššie).

Možné stavy	Presnejší opis
Platný	Podpis ostane platný pokiaľ obsahuje platnú časovú pečiatku. Tento stav je pri overovaní zvýraznený Zelenou farbou - Platný. <b>Upozornenie</b> : Pokiaľ podpis neobsahuje časovú pečiatku a je zobrazený tento stav, tak časom môže dôjsť k zmene tohto stavu, pretože podpis bol overovaný k systémovému času z histórie overovania
Neplatný	Pokiaľ bol nejaký podpis vyhlásený za neplatný jeho stav sa už nemôže zmeniť. Tento stav je pri overovaní zvýraznený Červenou farbou - Neplatný.
Neúplne overenie	Nie je k dispozícií CRL záznam s ktorým je možno rozhodnúť platnosť podpisu. CRL záznam nemusí byť ešte vydaný alebo nebol importovaný do aplikácie. Tento stav je pri overovaní zvýraznený Modrou farbou. Neúplné overenie neznamená, že podpis nie je platný. V čase overovania podpisu aplikácia nie je schopná jednoznačne rozhodnúť o platnosti podpisu nakoľko nemá dostupné CRL k danému momentu. Avšak po získaní nového CRL (t.j. v rozsahu maximálne 12-24 hodín) doplní uvedenú informáciu na úplné overenie a teda rozhodne o platnosti, resp. neplatnosti podpisu.
Nemožno rozhodnúť	Vzhľadom na Slovenskú legislatívu sa nedá rozhodnúť o platnosti podpisu. Podpis bol vytvorený v dobe, kedy sa nedá automaticky, aplikačne rozhodnúť či bol certifikát podpisovateľa zneplatnený. Tento stav nemôže nastať pri overovaní podľa PKI alebo PKI 2. Tento stav je pri overovaní zvýraznený Modrou farbou - Nemožno rozhodnúť. Upozornenie: V takomto prípade musíte požiadať certifikačnú autoritu, ktorá vydala príslušný certifikát o určenie, či v čase vytvorenia podpisu bol certifikát platný.