

# PRAVILNIK

## O TEHNIČKO-TEHNOLOŠKIM POSTUPCIMA ZA FORMIRANJE KVALIFIKOVANOG ELEKTRONSKOG POTPISA I KRITERIJUMIMA KOJE TREBA DA ISPUNE SREDSTVA ZA FORMIRANJE KVALIFIKOVANOG ELEKTRONSKOG POTPISA

("Sl. glasnik RS", br. 26/2008 i 13/2010)

### Član 1

Ovim pravilnikom propisuju se tehničko-tehnološki postupci za formiranje kvalifikovanog elektronskog potpisa i kriterijumi koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa.

### Član 2

Tehničko-tehnološki postupci za formiranje kvalifikovanog elektronskog potpisa, kao i kriterijumi koje treba da ispunjavaju sredstva za formiranje i proveru kvalifikovanog elektronskog potpisa moraju biti u skladu sa odgovarajućim međunarodnim standardima i preporukama, odnosno drugim standardima, dokumentima i preporukama, koje se odnose na formiranje i proveru kvalifikovanog elektronskog potpisa, utvrđenim ovim pravilnikom.

### Član 3

Kvalifikovani elektronski potpis, pored uslova iz člana 7. Zakona o elektronskom potpisu (u daljem tekstu: Zakon), mora da zadovolji i sledeće bliže uslove, i to:

- 1) da je formiran primenom sredstva za formiranje kvalifikovanog elektronskog potpisa (SSCD);
- 2) da se proverava na osnovu kvalifikovanog elektronskog sertifikata potpisnika - koji je validan u trenutku formiranja kvalifikovanog elektronskog potpisa.

### Član 4

Kvalifikovani elektronski potpis formira se primenom jednog od standardizovanih asimetričnih kriptografskih algoritama, i to:

- 1) RSA (*Rivest Shamir Adleman*) primenom standarda PKCS#1 uz minimalnu dužinu RSA modulusa  $n$  od 1024 bita;
- 2) DSA (*Digital Signature Algorithm*) sa minimalnim dužinama parametara  $p$  i  $q$  od 1024 i 160 bita, respektivno;
- 3) ECDSA (*Elliptic Curve Digital Signature Algorithm*) sa minimalnim dužinama parametara  $p$  i  $q$  od 192 i 160 bita, respektivno.

## Član 5

Pri formiranju kvalifikovanog elektronskog potpisa primenjuju se i *hash* funkcije za dobijanje otisaka poruke fiksne veličine (najmanje 160 bita).

*Hash* funkcije iz stava 1. ovog člana realizuju se primenom standardizovanih *hash* algoritama, i to:

- 1) SHA-1 (*Secure Hash Algorithm*) - *hash* vrednost veličine 160 bita;
- 2) RIPEMD-160 - *hash* vrednost veličine 160 bita;
- 3) SHA-224, SHA-256, SHA-384 i SHA-512.

## Član 6

Skup standardnih algoritama iz čl. 4. i 5. ovog pravilnika kombinovani sa zahtevima u vezi izbora parametara, kao i lista standardnih kombinacija primenjenih algoritama u formi algoritamskih veza ("*signature suites*"), moraju biti u skladu sa dokumentom ETSI ESI SR 002 176 "*Algorithms and Parameters for Secure Electronic Signatures*".

## Član 7

Sredstvo za formiranje kvalifikovanog elektronskog potpisa mora imati svojstva koja omogućavaju naknadnu ugradnju novih algoritama u skladu sa daljim razvojem kriptografskih tehnika i standarda.

## Član 8

Potpisana elektronska dokumenta kvalifikovanim elektronskim potpisom razmenjuju se u formatu dokumenata u kojima su ugrađeni osnovni podaci o postupku, algoritmu i kvalifikovanom elektronskom sertifikatu potpisnika, kako bi primalac elektronskog dokumenta mogao proveriti kvalifikovani elektronski potpis na bazi usaglašene tehnologije i postupaka.

## Član 9

Format elektronskog dokumenta koji je potpisan kvalifikovanim elektronskim potpisom mora biti usklađen sa nekim od dokumenata: PKCS#7 preporuka, RFC 3852 "*Cryptographic Message Syntax (CMS)*", ETSI ESI TS 101 733 "*CMS Advanced Electronic Signatures (CAAdES)*", RFC 3275 XMLDSIG, ETSI ESI TS 101 903 "*XML Advanced Electronic Signatures (XAdES)*" ili ETSI ESI TS 102 778 "*PDF Advanced Electronic Signatures (PAdES)*".

## Član 10

Kvalifikovani elektronski sertifikat mora biti usklađen sa preporukom ITU-T X.509 i dokumentima ETSI ESI TS 101 862 "*Qualified Certificate Profile*", RFC 3739 "*Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*", RFC 3280 "*Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL) Profile*" i ETSI TS 102 280 "*X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons*".

Postupci za formiranje kvalifikovanog elektronskog potpisa treba da budu u skladu sa dokumentom ETSI ESI TR 102 272 "ASN.1 *format for signature policies*" ili sa dokumentom ETSI ESI TR 102 038 "XML *format for signature policies*".

## Član 11

Polje "*subject*" kvalifikovanog elektronskog sertifikata mora da ima atribut "*commonName*".

U atribut "*commonName*" treba da je upisano puno ime i prezime potpisnika, jedinstveni identifikator potpisnika unutar sertifikacionog tela i opciono JMBG. Podaci se upisuju sledećim redom: ime, razmak, prezime, razmak, jedinstveni identifikator unutar sertifikacionog tela i na kraju, opciono, crtica i JMBG. Za atribut "*commonName*" treba koristiti UTF8*String* kodiranje, tako da sva slova iz imena i prezimena budu verno predstavljena odgovarajućim karakterima.

Sertifikaciono telo je dužno da korisniku jasno stavi do znanja da li će sertifikat sadržati JMBG.

Sertifikati koji se koriste u opštenju organa, opštenju organa i stranaka, dostavljanju i izradi odluke organa u elektronskom obliku u upravnom, sudskom i drugom postupku pred državnim organom, treba da sadrže JMBG. Sertifikate koji sadrže JMBG ili lični broj sertifikaciono telo ne sme učiniti javno dostupnim.

## Član 12

Postupak provere kvalifikovanog elektronskog potpisa obuhvata i postupak provere kvalifikovanog elektronskog sertifikata potpisnika, koji se sastoji od:

- 1) provere roka važnosti datog sertifikata;
- 2) provere podataka o sertifikacionom telu koje je izdalo kvalifikovani elektronski sertifikat potpisnika;
- 3) provere da li se dati sertifikat nalazi na listi opozvanih sertifikata.

Moguće je izvršiti i dodatne provere u odnosu na stav 1. ovog člana ukoliko je to definisano u Pravilima nadležnog sertifikacionog tela koje je izdalo kvalifikovani elektronski sertifikat.

## Član 13

Formiranje i provera kvalifikovanog elektronskog potpisa se vrši primenom:

- 1) sredstva za formiranje kvalifikovanog elektronskog potpisa (SSCD);
- 2) bezbedne aplikacije za formiranje i proveru kvalifikovanog elektronskog potpisa (SSCA i SSVA, respektivno);
- 3) tehničkih komponenata sertifikacionih tela;
- 4) kvalifikovanog elektronskog sertifikata.

## Član 14

Sredstva za formiranje kvalifikovanog elektronskog potpisa, pored uslova iz člana 8. Zakona, moraju da ispune sledeće kriterijume, i to:

- 1) da se podaci za formiranje kvalifikovanog elektronskog potpisa generišu u samom sredstvu za formiranje kvalifikovanog elektronskog potpisa i da ga nikad ne napuštaju;
- 2) da se kvalifikovani elektronski potpis formira u samom sredstvu za formiranje kvalifikovanog elektronskog potpisa;
- 3) da se obezbedi korišćenje sredstva za formiranje kvalifikovanog elektronskog potpisa isključivo od strane potpisnika uz prethodno realizovanu pouzdanu proceduru autentikacije;
- 4) da sredstvo mora biti takvo da je potpisnik u mogućnosti da ga koristi u različitim aplikacijama i informatičko-tehnološkim okruženjima.

## Član 15

Bezbedna aplikacija za izradu kvalifikovanog elektronskog potpisa (SSCA - *Secure Signature Creation Application*) se koristi zajedno i neodvojivo od SSCD.

SSCA u sebi može da sadrži i bezbednu aplikaciju za proveru kvalifikovanog elektronskog potpisa (SSVA - *Secure Signature Verification Application*) i validaciju kvalifikovanog elektronskog sertifikata potpisnika, kao i prikaz rezultata.

## Član 16

Tehničke komponente iz delatnosti sertifikacionih tela jesu softverski i hardverski proizvodi koji:

- 1) kreiraju podatke za formiranje kvalifikovanog elektronskog potpisa i prenose ih u odgovarajući hardverski uređaj sa karakteristikama koje su u skladu sa ovim pravilnikom, ili ih generišu direktno na datom hardverskom uređaju;
- 2) čine raspoloživim kvalifikovane sertifikate korisnika (uz saglasnost korisnika i bez JMBG-a i ličnog broja) i statuse sertifikata, odnosno liste opozvanih sertifikata za naknadnu verifikaciju i proveru statusa opozvanosti i, ako je potrebno, za preuzimanje od strane zainteresovanih strana.

## Član 17

Sredstvo za formiranje kvalifikovanog elektronskog potpisa (SSCD) iz člana 14. ovog pravilnika mora biti u skladu sa jednim od sledećih standarda:

- 1) preferirano CEN *Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)"*;
- 2) FIPS 140-2 (*Federal Information Processing Standard*) nivoa 2 ili viših.

## Član 18

Aplikacija za izradu kvalifikovanog elektronskog potpisa (SSCA) iz člana 15. stav 1. ovog pravilnika treba da bude u skladu sa sledećim standardom CEN *Workshop Agreement 14170 "Security requirements for signature creation applications"*.

## Član 19

Aplikacija za proveru kvalifikovanog elektronskog potpisa (SSVA) iz člana 15. stav 2. ovog pravilnika treba da bude u skladu sa sledećim standardom CEN *Workshop Agreement 14171 "General guidelines for electronic signature verification"*.

## Član 20

Tehničke komponente sertifikacionog tela iz člana 16. ovog pravilnika moraju biti u skladu sa sledećim standardima:

1) Za generisanje asimetričnih kriptografskih ključeva u sertifikacionom telu u skladu sa nekim od standarda:

- (1) CEN *Workshop Agreement 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Modules for CSP Key Generation Services - Protection Profile (CMCKG-PP)"*,
- (2) CEN *Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)"*,
- (3) FIPS 140-2 (*Federal Information Processing Standard*) nivoa 3 ili viši;

2) Za generisanje kvalifikovanih sertifikata u skladu sa nekim od standarda:

- (1) CEN *Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection profile (MCSO-PP)"*,
- (2) CEN *Workshop Agreement 14167-4: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic Module for CSP Signing Operations - Protection profile (CMCSO-PP)"*,
- (3) CEN *Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)"*,
- (4) FIPS 140-2 (*Federal Information Processing Standard*) nivoa 3 ili viši.

## Član 21

Programska oprema i postupci primenom kojih se vrši provera kvalifikovanog elektronskog potpisa moraju u potpunosti omogućiti dobijanje podataka za formiranje kvalifikovanog elektronskog potpisa pomoću podataka za njegovu proveru.

## Član 22

Potpisnik je dužan da zaštiti podatke za formiranje kvalifikovanog elektronskog potpisa od neovlašćenog pristupa, otuđivanja i nepravilne upotrebe.

Zaštita iz stava 1. ovog člana dodatno obuhvata primenu lozinki ili PIN kodova, biometrijskih postupaka ili drugih zaštitnih tehnika.

## Član 23

Stupanjem na snagu ovog pravilnika prestaje da važi Pravilnik o tehničko-tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijumima koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa ("Službeni glasnik RS", br. 48/05, 82/05 i 116/05).

## Član 24

Ovaj pravilnik stupa na snagu osmog dana od dana objavljivanja u "Službenom glasniku Republike Srbije".

<b>Tip dokumenta:</b>	Propis
<b>Naslov:</b>	<b>PRAVILNIK O TEHNIČKO-TEHNOLOŠKIM POSTUPCIMA ZA FORMIRANJE KVALIFIKOVANOG ELEKTRONSKOG POTPISA I KRITERIJUMIMA KOJE TREBA DA ISPUNE SREDSTVA ZA FORMIRANJE KVALIFIKOVANOG ELEKTRONSKOG POTPISA ("Sl. glasnik RS", br. 26/2008 i 13/2010)</b>
<b>Rubrika:</b>	X-2 - Standardizacija i akreditacija i sertifikacija/Postupak akreditacije i sertifikacije i nadzora
<b>Nivo dokumenta:</b>	Republike Srbije
<b>Glasil:</b>	<b>Službeni glasnik RS, broj 13/2010 od 12/03/2010</b>
<b>Vrsta propisa:</b>	Pravilnici
<b>Propis na snazi:</b>	22/03/2008 -
<b>Verzija na snazi:</b>	20/03/2010 -
<b>Osnov za donošenje:</b>	Na osnovu člana 11. Zakona o elektronskom potpisu ("Službeni glasnik RS", broj 135/04), Ministar za telekomunikacije i informaciono društvo donosi PRAVILNIK O IZMENAMA PRAVILNIKA O TEHNIČKO-TEHNOLOŠKIM POSTUPCIMA ZA FORMIRANJE KVALIFIKOVANOG ELEKTRONSKOG POTPISA I KRITERIJUMIMA KOJE TREBA DA ISPUNE SREDSTVA ZA FORMIRANJE KVALIFIKOVANOG ELEKTRONSKOG POTPISA
<b>Donosilac:</b>	Ministarstvo za telekomunikacije i informaciono društvo
<b>Natpropis:</b>	ZAKON O ELEKTRONSKOM POTPISU ("Sl. glasnik RS", br. 135/2004)

<b>Uneto u bazu:</b>	16/03/2010
<b>Komentar urednika:</b>	-
<b>Komentar korisnika:</b>	-