

1345.

Na osnovu člana 12 stav 2 Zakona o elektronskom potpisu ("Službeni list RCG", broj 55/03 i "Službeni list RCG", broj 41/10), Ministarstvo za informaciono društvo i telekomunikacije donijelo je

## **P R A V I L N I K O MJERAMA ZAŠTITE ELEKTRONSKOG POTPISA I NAPREDNOG ELEKTRONSKOG POTPISA**

### Član 1

Ovim pravilnikom propisuju se mjere zaštite elektronskog potpisa i naprednog elektronskog potpisa, mjere provjere identiteta potpisnika od strane potpisnika ili davaoca usluga certifikovanja u Crnoj Gori, tehničko-tehnološki postupci za izradu naprednog elektronskog potpisa i uslovi koje treba da ispune sredstva za izradu naprednog elektronskog potpisa.

### Član 2

Odredbe ovog pravilnika shodno se primjenjuju na vremenski pečat i napredni vremenski pečat.

### Član 3

Mjere zaštite elektronskog potpisa i naprednog elektronskog potpisa, postupci za izradu naprednog elektronskog potpisa, uslovi koje treba da ispunjavaju sredstva za izradu i provjeru naprednog elektronskog potpisa, usklađuju se sa međunarodnim standardima datim u Prilogu, koji je sastavni dio ovog pravilnika.

### Član 4

Radi zaštite elektronskog potpisa i naprednog elektronskog potpisa od neovlašćenog pristupa, krađe i oštećenja, potpisnik koristi lozinke, PIN kodove, i druge vrste zaštite elektronskog potpisa.

### Član 5

Ako potpisnik izgubi ili mu je otuđeno sredstvo za izradu elektronskog potpisa i u slučaju kada je onemogućen pristup podacima za izradu elektronskog potpisa, potpisnik obaviještava davaoca usluga certifikovanja i podnosi zahtjev za opoziv ili suspenziju certifikata.

Zaštita iz člana 3 stav 1 ovog člana, vrši se primjenom mjera u skladu sa Uredbom o mjerama informacione bezbjednosti („Službeni list CG“, broj 58/10).

### Član 6

Čuvanje i zaštita podataka za izradu naprednog elektronskog potpisa davaoca usluga certifikovanja sprovodi se uz primjenu:

- 1) sredstava za izradu naprednog elektronskog potpisa u skladu sa američkim standardima FIPS 140-1 (koje je utvrdilo tijelo za standardizaciju: National Institute of Standards and Technology - Federal Information Processing Standards), dovoljno visokog nivoa – ne nižeg

od nivoa 3 ili standardom FIPS 140-2 koji omogućavaju rad sa podacima za izradu elektronskog potpisa;

- 2) podataka za izradu potpisa primjenom RSA ili DSA algoritma dužine najmanje 2048 bita, odnosno odgovarajućeg nivoa Elliptic Curve algoritma, SHA1 ili SHA-2 (SHA-224, SHA-256, SHA-384 i SHA-512);
- 3) kriptografskih algoritama (3DES algoritma – 128 bitni ili AES tehnika) radi zaštite pristupa podacima.

Podatke za izradu elektronskog potpisa, davalac usluga certifikovanja štiti u skladu sa utvrđenim pravilima i međunarodnim standardima u cilju sprečavanja fizičkog ili elektronskog pristupa od strane neovlašćenih lica.

## Član 7

Davalac usluga certifikovanja obezbijeduje jedinstvenost podataka radi provjere elektronskog potpisa na način koji omogućava identifikaciju potpisnika.

## Član 8

Potpisnik u elektronski potpis i napredni elektronski potpis unosi osnovne podatke o sadržaju, načinu i postupku izrade elektronskog potpisa, kako bi primalac mogao da izvrši provjeru potpisa.

Radi provjere identiteta, primalac prilikom provjere elektronskog potpisa i naprednog elektronskog potpisa kod davaoca usluga certifikovanja provjerava da li je certifikat na listi nevažećih (opozvanih, suspendovanih ili isteklih) certifikata.

## Član 9

Davalac usluga certifikovanja koji prikuplja podatke za izradu elektronskih potpisa podatke o potpisnicima i podatke o poslovnim subjektima prikuplja, čuva, koristi i briše u skladu sa propisima kojima se uređuje zaštita ličnih podataka i podataka o poslovnim subjektima.

## Član 10

Korisnici elektronskog potpisa ili naprednog elektronskog potpisa mogu od davaoca usluga certifikovanja zatražiti provjeravanje podataka na osnovu kojih se vrši provjera elektronskog potpisa.

Korisnici elektronskog potpisa ili naprednog elektronskog potpisa u slučaju iz stava 1 ovog člana, podnose zahtjev davaocu usluga certifikovanja lično ili u elektronskoj formi, ako je zahtjev elektronski potpisan od strane podnosioca zahtjeva.

## Član 11

Podatke za izradu sopstvenog elektronskog potpisa, davalac usluga certifikovanja raspoređuje na najmanje dva lica koja izrađuju elektronski potpis.

Prilikom izrade naprednog elektronskog potpisa ne može se vršiti izmjena podataka koji se potpisuju i onemogućiti njihovo dostavljanje potpisniku prije potpisivanja.

Sadržina elektronskog potpisa se usklađuje sa međunarodnim standardima koji se odnose na izradu i upotrebu elektronskog potpisa i naprednog elektronskog potpisa.

## Član 12

Prilikom izrade naprednog elektronskog potpisa u slučaju primjene sistema asimetrične kriptografije, dužina ključa za izradu naprednog elektronskog potpisa mora biti najmanje 1024 bita, uz primjenu kriptografskih algoritama iz grupe RSA/DSA i usklađena sa međunarodnim standardom PKCS#1 (Verzija 2.1 na više).

Kriptografski moduli zasnivaju se na algoritmima i parametrima koji predstavljaju radno okruženje za izradu naprednog elektronskog potpisa u skladu sa obrascima koje sadrži dokument - Algoritmi i parametri sigurnog elektronskog potpisa (Algorithms and Parameters for Secure Electronic Signatures)- verzija 2.1, 2001-10 ili novija.

## Član 13

Sredstva za izradu naprednog elektronskog potpisa, koja sadrže podatke za izradu naprednog elektronskog potpisa treba da ispunjavaju međunarodne zahtjeve za zaštitu i sigurnost opreme neophodne za izradu naprednog elektronskog potpisa, kao i da primjenjuju jedan od sljedećih obrazaca za zaštitu sredstava za izradu naprednog elektronskog potpisa:

- opšti obrazac zaštite sredstava za izradu naprednog elektronskog potpisa - CEN/ISSS SSCD-PP (Secure Signature Creation Device-Protection Profile) ;
- opšti obrazac za sigurnost kriptografskih modula FIPS 140-1, minimalnog nivoa 3, ili FIPS 140-2, minimalnog nivoa 3 (američko tijelo za standardizaciju - National Institute of Standards and Technology – Federal Information Processing Standard).

## Član 14

Programska oprema za izradu naprednog elektronskog potpisa treba da ima ugrađene osnovne oblike zaštite, u skladu sa propisima o osnovnim pravilima zaštite i bezbjednosti sredstava za izradu naprednog elektronskog potpisa – SSCD/PP odnosno EAL4+ preporukama.

## Član 15

Danom stupanja na snagu ovog pravilnika prestaju da važe čl. 1 do 11 Pravilnika o mjerama i postupcima upotrebe i zaštite elektronskog potpisa, sredstava za izradu elektronskog potpisa i sistema certifikovanja ("Službeni list RCG", broj 25/05).

## Član 16

Ovaj pravilnik stupa na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore".

Broj: 051-01-4041/1-11

Podgorica, 16. decembra 2011. godine

Ministar  
prof. dr. **Vujica Lazović**, s.r.



## Kriterijumi i mjere za izradu i zaštitu elektronskog potpisa

Kriterijumi koje treba da ispunjavaju sredstva za izradu i provjeru naprednog elektronskog potpisa i vremenskog pečata i postupci za izradu naprednog elektronskog potpisa i ugradnju vremenskog pečata, kao i mjere zaštite elektronskog potpisa i naprednog elektronskog potpisa, moraju biti usklađeni sa odgovarajućim međunarodnim standardima, i to:

- 1) tehničkim standardima Evropskih organizacija ETSI (European Telecommunications Standards Institute) i ESI (Elektronic Signatures and Infrastructures);
- 2) standardima CEN/ISSS i dokumentima CWA (CEN Workshop Agreement);
- 3) dokumentima IETF RFC (Request for Comments);
- 4) dokumentima i preporukama kompanije RSA Data Security PKCS (Public Key Cryptographic Standards);
- 5) zajedničkim kriterijumima (for Information Technology Security Evaluation) u odjeljku EAL (Evaluation Assurance Level);
- 6) američkim standardima FIPS 140-1 (koje je utvrdilo tijelo za standardizaciju: National Institute of Standards and Technology - Federal Information Processing Standards), kao i standardima FIPS 140-2.

odnosno:

- ISO/ IEC 15408-1:2005 Informaciona tehnologija - Bezbjednosne tehnike - Kriterijumi za vrednovanje bezbjednosti IT-a – Dio 1: Uvod i opšti model (ISO/IEC 15408-1:2005) (Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model (ISO/IEC 15408-1:2005));
- ISO/IEC 15408-2:2005 Informaciona tehnologija - Bezbjednosne tehnike - Kriterijumi za vrednovanje bezbjednosti IT-a – Dio 2: Funkcionalni zahtjevi za sigurnost (ISO/IEC 15408-2:2005) (Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements (ISO/IEC 15408-2:2005));
- ISO/IEC 15408-3:2005 Informaciona tehnologija - Bezbjednosne tehnike - Kriterijumi za vrednovanje bezbjednosti IT-a – Dio 3: Garantni zahtjevi za sigurnost (ISO/IEC 15408-3:2005) (Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements (ISO/IEC 15408-3:2005));
- ETSI TS 101 733 V.1.7.4.:2008 Elektronski potpisi i infrastrukture (ESI) - CMS usavršeni elektronski potpisi (CAAdES) (ETSI TS 101 733 V.1.7.4.:2008) (Electronic signatures and infrastructures (ESI) - CMS advanced electronic signatures (CAAdES) (ETSI TS 101 733 V.1.7.4.:2008));
- ETSI TS 101 903 V1.4.1:2009 XML napredni elektronski potpisi (XAdES) (ETSI TS 101 903 V1.4.1:2009) (XML advanced electronic signatures (XAdES) (ETSI TS 101 903 V1.4.1:2009));
- ETSI TS 102 778 V.1.1.1:2009 Elektronski potpisi i infrastrukture (ESI)-Profili PDF naprednog elektronskog potpisa-CMS profil na osnovu ISO 32000-1 (ETSI TS 102778 V.1.1.1:2009) (Electronic signatures and infrastructures (ESI)-PDF advanced electronic signature profiles-CMS profile based on ISO 32000-1 (ETSI TS 102778 V.1.1.1:2009));
- ETSI TS 102 778-1 V.1.1.1:2009 Elektronski potpisi i infrastrukture (ESI)-Profili PDF naprednog elektronskog potpisa- Dio 1: PAdES pregled-Okvirni dokument za PadES (ETSI TS 102 778-1 V.1.1.1:2009) (Electronic signatures and infrastructures (ESI)-PDF advanced electronic signature profiles-Part 1: PAdES overview-A framework document for PadES (ETSI TS 102 778-1 V.1.1.1:2009));
- ETSI TS 102 778-2 V.1.2.1:2009 Elektronski potpisi i infrastrukture (ESI)-Profili PDF naprednog elektronskog potpisa-Dio 2: Osnovni PadES-Profil na osnovu ISO 32000-1 (ETSI TS 102 778-2 V.1.2.1:2009) (Electronic signatures and infrastructures (ESI)-PDF advanced electronic signature profiles-Part 2: PadES basic - Profile based on ISO 32000-1 (ETSI TS 102 778-2 V.1.2.1:2009));
- ETSI TS 102 778-3 V.1.1.1:2009 Elektronski potpisi i infrastrukture (ESI)-Profili PDF naprednog elektronskog potpisa-Dio 3: Pobjoljšani PAdES-Profil PAdES-BES i PAdES-EPES (ETSI TS 102 778-3 V.1.1.1:2009) (Electronic signatures and infrastructures (ESI) - PDF advanced electronic signature profiles-Part 3: PAdES enhanced-PAdES-BES and PAdES-EPES profiles (ETSI TS 102 778-3 V.1.1.1:2009));
- ETSI TS 102 778-4 V.1.1.1:2009 Elektronski potpisi i infrastrukture (ESI)-Profili PDF naprednog elektronskog potpisa-Dio 4: Dugotrajni PAdES – Profil PAdES-LTV (ETSI TS 102 778-4 V.1.1.1:2009) (Electronic signatures and

infrastructures (ESI)-PDF advanced electronic signature profiles-Part 4: PAdES Long term-PAdES-LTV profile ETSI TS 102 778-4 V.1.1.1:2009));

- ETSI TS 102 778-5 V.1.1.1:2009 ETSI TS 102 778-5 V.1.1.1:2009 Elektronski potpisi i infrastrukture (ESI)-Profili PDF naprednog elektroničkog potpisa-Dio 5:PadES za XML sadržaj-Profili za potpise XadES (ETSI TS 102 778-5 V.1.1.1:2009) (Electronic signatures and infrastructures (ESI)-PDF advanced electronic signature profiles- PadES for XML content-Profiles for XadES signatures (ETSI TS 102 778-5 V.1.1.1:2009)).