(Objavljen u “Sl.listu RCG”,br. 25/05)

Na osnovu člana 35 stav 2 Zakona o elektronskom potpisu (“Službeni list RCG”, br. 55/03) Sekretarijat za razvoj donosi

PRAVILNIK

O TEHNIČKIM PRAVILIMA I USLOVIMA POVEZIVANJA SISTEMA CERTIFIKOVNJA ELEKTRONSKIH POTPISA

I OPŠTE ODREDBE

Član 1

Ovim pravilnikom utvrđuju se tehnička pravila i uslovi za obezbjedjenje povezanosti sistema certifikovanja davalaca usluga certifikovanja u Republici Crnoj Gori.

Član 2

Postupci za izradu elektronskog potpisa i izdavanje certifikata moraju biti usklađeni sa odgovarajućim međunarodnim standardima i preporukama, i to:

1) tehničkim standardima Evropske organizacije ETSI (Europen Telecommunications Standards Institute) i ESI (Elektronic Signatures and Infrastructures);
2) evropskim standardima CEN/ISSS i dokumentima CWA (CEN Workshop Agreement);
3) IETF RFC (Request for Comments) dokumentima;
4) PKCS (Publik Key Criptographic Standards) dokumentima i preporukama kompanije RSA Data Security;
5) evropskim standardima Common Criteria (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).

II ELEKTRONSKI POTPIS

Član 3

Struktura elektronskog potpisa zasniva se na ETSI TS 101 733 v (verzija) 1.5.1 (2003-12) – Electronic Signature Formats, kao specifikaciji obrazaca elektronskog potpisa.

Uz specifikaciju iz stava 1 ovog člana, u izradi strukture elektronskog potpisa preuzimaju se obrasci zasnovani na CMS (Cryptographic Message Syntax) modelu utvrđenom u dokumentu RFC 3369 i ESS (Enhanced Security Services for S/MIME) modelu utvrđenom u dokumentu RFC 2634.

Elektronski potpis obavezno sadrži osnovna obilježja utvrđena u CMS, ESS i ETSI TS

101 733 v 1.5.1.

Član 4

Za potrebe automatskog prepoznavanja vrste potpisanih podataka može se koristiti obrazac MIME-encapsulated message (Multipurpose Internet Mail Extensions- RFC 1341).

Član 5

Elektronski potpis koriste potpisnik i primalac u skladu sa utvrđenom politikom upotrebe potpisa.

Politika upotrebe potpisa obavezno se iskazuje u dokumentu čitljivom korisnicima potpisa koji moraju imati mogućnost uvida u obaveze i prava koja proizilaze iz sadržaja koji se potpisuje.

Za potrebe automatske obrade elektronskog potpisa neophodno je izraditi politiku upotrebe potpisa i u formatiranom obliku za potrebe neposrednog preuzimanja od strane računarskih programa (aplikacija).

Formatirani oblik politike upotrebe elektronskog potpisa mora biti izrađen primjenom obrasca ASN.1:1997 (Abstract Syntax Notation One) i mora imati jedinstvenu binarno kodiranu vrijednost dobijenu kodiranjem po BER (Basic Encoding Rules)/X.209 obrascu-ISO/IEC 8825-1 ASN.1 Encoding Rules-BER.

Potpisnik i primalac moraju koristiti istu politiku upotrebe potpisa radi postizanja istovjetnosti potpisa kod njegove izrade i provjere.

Za nesumnjivo identifikovanje politike upotrebe potpisa u potpis se mora ugraditi identifikator ili rezime politike upotrebe potpisa.

Kod računarskih aplikacija koje koriste veliki broj istovrsnih dokumenata sa jednom politikom upotrebe elektronskog potpisa dozvoljeno je unaprijed definisati ugradnju te politike u elektronski potpis ili je ugraditi u aplikaciju.

Član 6

Potpisniku u procesu potpisivanja mora biti prezentiran i opis procedure (postupka) potpisivanja , sa obaveznim skupom podataka:

1) informacija/obavještenje o sadržaju pravnih i drugih činjenica povezanih sa potpisivanjem;

2) izjava potpisnika o prihvatanju politike upotrebe potpisa, kao i da je upoznat sa sadržajem koji potpisuje;

3) dodatni potpisni skup podataka koji čini sastavni dio elektronskog potpisa i dodaje se potpisanom elektronskom zapisu (ime potpisnika, vrijeme, mjesto i svrha potpisivanja).

Član 7

Svaki elektronski potpis obavezno sadrži jedinstveni identifikator (identifikator certifikata kojim je stvoren elektronski potpis) koji mora biti kriptografski zaštićen.

Član 8

Podaci koje sadrži elektronski potpis moraju biti kodirani jednim od obrazaca kodiranja: DER (Definitive Encoding Rules), Base 64, CMS (Cryptographic Message Syntax) – PKCS#7.

Elektronski potpis objedinjuje se (programski zatvara) u omotnicu primjenom najmanje jednog od obrazaca: PKCS #7, ISO/IEC 9796-2 (Digital Signature Schemes), S/MIME (Secure Multipurpose Internet Mail Extensions).

Član 9

Kod sistema koji podržavaju i koriste promet dokumenata i podršku računarskih aplikacija u obrascu XML (Extended Markup Language) može se prihvatiti i upotreba elektronskog potpisa oblikovanog u skladu sa W3C/IETF Recommendation "XML-Signature Syntax and Processing" (RFC 3275) ili XAdES (XML Advanced Electronic Signatures) dokumentom ETSI TS 101 903 v 1.2.2 (2004-04).

Prilikom upotrebe obrasca elektronskog potpisa iz stava 1 ovog člana, elektronski potpis mora uključivati politiku upotrebe elektronskog potpisa i biti izrađen primjenom PKI tehnologije.

III CERTIFIKAT

Član 10

Struktura certifikata zasniva se na obrascu ITU X.509 v 3 i obavezno sadrži:

1) verziju obrasca X.509;

2) serijski broj;

3) oznaku (ID) algoritma izrade elektronskog potpisa (SHA-1/RSA, MD5/RSA);

4) ime davaoca usluga certifikovanja – po strukturi utvrđenoj u obrascu X.500;

5) period važenja certfikata;

6) ime potpisnika (korisnika certifikata) – po strukturi utvrđenoj u obrascu X.500

7) podatke o javnom ključu potpisnika;

8) dodatne atribute (proširenje osnovnog skupa atributa), u skladu sa članom 11 ovog pravilnika;

9) elektronski potpisane prethodne podatke od strane davaoca usluga certifikovanja.

Član 11

Certifikat izrađen na osnovu obrasca X.509 v 3 obavezno sadrži i skup dodatnih atributa:

1) identifikator ključa davaoca usluga certifikovanja;

2) identifikator ključa potpisnika (korisnika certifikata);

3) namjene upotrebe ključa;

4) jednoznačni identifikacioni kod (Object Identifier prema ASN.1) Opštih pravila davaoca usluga certifikovanja (ako je prethodno dobio OID);

5) postupak i mjesto pristupa listi opozvanih certifikata.

Dodatni atributi (proširenje) moraju biti strukturirani u skladu sa dokumentom ETSI 101 862 v 1.3.2 (2004-06)-Qualified Certificate Profile , RFC 3739- Internet X.509 Public Key Infrastructure: Qualified Certificates Profile i RFC 3280 - Internet X.509 Public Key

Infrastructure Certificate and Certificate Revocation List (CRL) Profile, koji obezbjeđuju međusobno povezivanje kvalifikovanih certifikata.

Član 12

Obrazac i sadržaj kvalifikovanih certifikata, u skladu sa odredbama Zakona o elektronskom potpisu (u daljem tekstu: Zakon) i smjernicama Evropske unije, utvrđeni su dokumentom ETSI TS 101 862 v 1.3.2 (2004-06) -Qualified Certificate Profile.

Primjena certifikata u Internet okruženju zasniva se na obrascu RFC 3280- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile izvedenom iz X.509 v 3, uz dodatne obrasce:

1) RFC 2632 – S/MIME v 3 Certificate Handling;
2) RFC 2633 – S/MIME v 3 Message Specification;
3) RFC 3739 Internet X.509 Public Key Infrastructure:Qualified Certificates Profile.

Član 13

Svi podaci sadržani u certifikatu moraju se kodirati putem dva međusobno povezana modula:

1) ASN.1:1997 (Abstract Syntax Notation One) usklađen sa ISO/IEC 8824-1:1998, kojim se opisuju podaci;

2) DER (Definitve Encoding Rules), kojim se opisuje jedinstveni obrazac za čuvanje i razmjenu podataka.

Certifikati i javni ključevi potpisnika (kod primjene sistema javnih ključeva) moraju biti strukturirani u standardnom X.509 v 3 formatu.

IV OPREMA

Član 14

Sva oprema koja se koristi u sistemu certifikovanja mora biti kompatibilna sa opšte prihvaćenim standardima i preporukama.

Član 15

Sva oprema koja se koristi u sistemu certifikovanja mora obezbijediti izdvajanje podataka elektronskog potpisa i certifikata najmanje u jedan od osnovnih obrazaca:

1) DER Encoded Binary X.509 (*.cer);
2) Cryptographic Message Syntax Standard PKCS#7 Certificates (*.p7b);
3) Personal Information Exchange Syntax Standard PKCS#12 (*.pfx).

Član 16

Kod upotrebe smart kartica mora se obezbijediti mogućnost izdvajanja certifikata u jedan od standardnih obrazaca iz člana 15 ovog pravilnika.

Kod upotrebe smart kartica obavezno se primjenjuju ISO/IEC 7816 (1,2,3) i ISO 7816

(4, 5, 6, 7, 8, 9, 10) obrasci za ujednačavanje oblika, veličine i funkcionalnosti kartica i terminala za prihvat kartica.

Kod upotrebe smart kartica u postupcima primjene elektronskih potpisa i certifikata mora se koristiti obrazac PKCS#15 zapisa kriptoključeva, certifikata i drugih podataka (PKCS#15 smart card file format).

Uređaji za čitanje i pisanje zapisa na smart kartice u okruženju personalnih računara moraju imati podršku za tehničke obrasce PC/SC.

Uređaji za upotrebu smart kartica, ključeva i drugih formi (tokeni) moraju obezbijediti priključak u standardne komunikacione interfejse RS232, USB, Firewire, PCMCIA, Bluetooth.

Član 17

Oprema korisnika sistema certifikovanja mora omogućiti:

1) slanje i primanje elektronski potpisanih sadržaja;

2) provjeravanje primljenih certifikata putem liste opozvanih certifikata;

3) provjeravanje primljenih certifikata putem najmanje tri nivoa;

4) primanje i slanje kriptovanih zapisa;

5) upotrebu i provjeru kvalifikovanih certifikata;

6) upotrebu smart kartica i drugih medija za kriptografsku obradu.

Član 18

Kod upotrebe računarske opreme moraju se koristiti API (Application Program Interface) programska rješenja, kojima se obezbjedjuje korišćenje bilo koje vrste smart kartica, PCMCIA (Personal Computer Memory Card International Association) modula, tokena i drugih uređaja.

Oprema sa ugrađenim API programskim rješenjima mora obezbijediti:

1) izradu elektronskog potpisa;

2) provjeru elektronskog potpisa;

3) oblikovanje podataka;

4) komunikaciju uređaja i podataka.

API programska rješenja moraju se zasnivati na kriptografskim obrascima:

1) PKCS#11 (CRYPTOKI, RSA) za ugradnju u uređaje i programe;

2) IDUP-API (Independent Data Unit Protection) za ugradnju u uređaje;

3) GSS-API (General Security Services) za ugradnju u programe;

4) Microsoft CryptoAPI za ugradnju u programe.

Kod upotrebe kartica Fortezza obavezna je primjena RFC 2876 (Use of the KEA and SKIPJACK Algorithms in CMS) obrasca povezivanja procesa kriptovanja i procesa potpisivanja.

Član 19

Sva oprema koja se koristi u sistemu certifikovanja mora omogućiti povezivanje osnovnih obrazaca za izradu i provjeru elektronskog potpisa i izradu kriptovanih zapisa sa:

1) Microsoft Crypto API;

2) Netscape Security Framework;

3) Entrust PKI.

Sva oprema uključena u sistem certifikovanja mora obezbijediti međusobno sinhronizovan rad putem interfejsa PKCS#11 (Public Key Cryptographic Standard 11/Cryptographic Token Interface Standard – Cryptoki) bez obzira na vrstu uređaja i medija kojima se izrađuje, koristi ili provjerava elektronski potpis.

Zapisi, podaci i kriptoelementi ugrađeni u uređaje moraju biti usklađeni sa obrascem PKCS#15 (Cryptographic Token Information Format) i obezbijediti primjenu uređaja nezavisno od vrste interfejsa izrađenog u skladu sa obrascem PKCS#11.

Član 20

Zapisi i elektronski potpisi izrađeni jednom opremom uz primjenu bilo kojeg od odabranih obrazaca moraju biti čitljivi upotrebom druge opreme uz korišćenje istovjetnog algoritma potpisivanja (DSS/DSA) ili kriptovanja (PKCS#1-RSA).

Oprema koja se koristi u sistemu kvalifikovanih certifikata mora biti u skladu sa FIPS PUB 104-1 (CA HSM najmanje nivo 3, korisničke kartice najmanje nivo 2, client software najmanje nivo 1) Validation of Cryptographic Modules obrascem sigurnosti uređaja, programa i zapisa.

Član 21

Oprema koja uključuje biometrijske metode identifikacije potpisnika može se primjenjivati samo ako se pridruži sistemu certifikovanja X.509 i ako se jedinstveno identifikuje sredstvo za izradu elektronskog potpisa, na način koji obezbjeđuje da biometrijski uzorak može biti korišćen samo sa tim sredstvom.

V SISTEM CERTIFIKOVANJA

Usluge certifikovanja

Član 22

Svaki sistem koji pruža usluge certifikovanja mora biti u neprekidnom radu i javno dostupan putem telekomunikacionog sistema.

Sistem certifikovanja obavezno obezbjeđuje vršenje najmanje jedne od usluga:

1) registracija korisnika certifikata;
2) izdavanje, dostava, objavljivanje i opoziv certifikata;
3) objavljivanje statusa certifikata;
4) upravljanje i čuvanje ključeva;
5) vođenje elektronskih imenika.

Član 23

Svaki sistem certifikovanja mora obezbijediti prihvatanje ulaznih podataka (zahtjeva za

izdavanje certifikata) u PKCS#10 obrascu kodiranom u DER ili PEM obliku.

Svaki sistem certifikovanja mora podržavati skup X.509 v 3 obaveznih dodatnih atributa u certifikatima, u skladu sa članom 11 ovog pravilnika.

Član 24

Postupak povezivanja sistema certifikovanja zasniva se na primjeni dogovorenih obrazaca za područja:

1) certifikata;

2) poruka;

3) razmjene certifikata i poruka;

4) prenosa certifikata i poruka.

Certifikat ima dogovorenu obaveznu formu utvrđenu putem obrasca X.509 v 3:1997.

Poruke uključuju:

1) zahtjev za izdavanje certifikata, koji se iskazuje putem obrasca PKCS#10;

2) nepotpisane/potpisane/kriptovane poruke, koje se iskazuju putem obrasca PKCS#7;

3) podatke o potpisniku, koji se iskazuju putem obrasca PKCS#12 (Personal Information Exchange Syntax).

Zahtjev za izdavanje certifikata zasniva se na potpisanoj PKCS#10 oblikovanoj poruci, a odgovor (certifikat) na PKCS#7 nepotpisanoj poruci. Sistemi certifikovanja koji imaju mogućnost tehnološke podrške mogu koristiti i CMP (Certificate Management Protocols).

Prenos certifikata i poruka sprovodi se putem telekomunikacionih sistema, uz obaveznu upotrebu obrasca S/MIME (Secure Multipurpose Internet Mail Extensions), odnosno SSL (Secure Socket Layer) protokola.

Provjera certifikata putem liste opozvanih certifikata

Član 25

Opozvani certifikati moraju se upisati u listu opozvanih certifikata, koja mora biti dostupna svim subjektima (korisnicima i trećim stranama) u sistemu certifikovanja.

Lista opozvanih certifikata oblikuje se u skladu sa obrascem X.509 i RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Član 26

Lista opozvanih certifikata obavezno sadrži:

1) redni broj radne verzije liste;

2) kriptografski algoritam korišćen prilikom izrade elektronskog potpisa davaoca usluga certifikovanja;

3) elektronski potpis davaoca usluga certifikovanja;

4) ime davaoca usluga certifikovanja;

6) datum i vrijeme izrade (izdavanja) liste;

7) datum i vrijeme izrade (izdavanja) nove liste.

Svaki opozvani certifikat u Listi opozvanih certifikata sadrži:

1) serijski broj dodijeljen certifikatu prilikom izdavanja;

2) datum opoziva (od kada certifikat ne važi).

Član 27

Svaki sistem certifikovanja mora obezbijediti trenutan i nesmetan uvid u listu opozvanih certifikata kod potvrđivanja važnosti (od strane primaoca elektronski potpisanog sadržaja) certifikata koje je izdao.

Elektronski imenici

Član 28

Svi potpisnici i subjekti sistema certifikovanja upisuju se u elektronske imenike.

Usluge elektronskih imenika zasnivaju se na primjeni obrasca ITU-T X.500:2001 (Directory Service) – ISO/IEC 9594:2001 ili LDAP v 3 (RFC 2251 Lightweight Directory Access Protocol) putem jedinstvene strukture (DIT-Directory Information Tree).

Nazivi subjekata u elektronskom imeniku (DN) kodiraju se po obrascu ASN.1 i moraju biti izraženi podskupom atributa koji obezbjeđuje jedinstvenost naziva subjekta (DN), sa liste atributa prema RFC 3739 Qualified Certificate Profile:

1) komponenta domena (domainComponent);

2) naziv države (countryName; nazivi i oznake u skladu sa obrascem ISO 3166-1:1997+Alpha 2)

3) uobičajeno ime (commonName);

4) prezime (surname);

8) ime po rođenju (givenName);

9) pseudonim (pseudonym);

10) serijski broj (serialNumber);

11) titula (title);

12) naziv organizacije/pravnog lica (organizationName);

10) naziv organizacione jedinice (organizationalUnitName);

11) naziv Republike (stateOrProvinceName);

12) mjesto/adresa (localityName);

Sadržaj elektronskog imenika mora biti izrađen primjenom obrasca kodiranja ISO/IEC 10646 – 1:2000 Universal Multiple Octet Coded Character Set (UCS) – Basic Multiple Plane (BMP), odnosno u skladu sa obrascem UTF-8.

Član 29

Pristup sadržaju elektronskih imenika mora biti oblikovan u skladu sa LDAP v 3 obrascem pristupa elektronskim imenicima.

LDAP elektronski imenici mogu biti sadržajno ograničeni za jedan sistem certifikovanja.

Svaki sistem certifikovanja mora obezbijediti prosleđivanje pitanja u elektronske imenike drugih sistema certifikovanja. Prosleđivanje pitanja može se sprovoditi upotrebom sopstvenog elektronskog imenika ili usmjeravanjem pitanja davaocu usluga koji za njega vodi elektronski

imenik.

Povezivanje elektronskih imenika koji koriste obrazac LDAP mora se sprovoditi primjenom obrasca LDUP (LDAP Duplication/Replication/Update Protocol) putem osnovnih modula:

1) Replication Information Model:2001;

2) Replication Update Protocol:2001.

Povezivanje elektronskih imenika koji koriste obrazac X.500 može se sprovoditi i primjenom obrasca DISP (Directory Information Shadowing Protocol) putem primjene dogovorene strukture DIT (Directory Information Tree), objedinjene obrascima ISO 9594 odnosno X.520:1988 (Selected Attribute Types) i X.521:1988 (Selected Object Classes).

Član 30

Elektronski imenik obavezno sadrži:

1) skup podataka o davaocu usluga certifikovanja, njegovo jednoznačno ime (DN), njegov certifikat i podatke o listi opozvanih certifikata;

2) skup podataka o potpisniku, njegovo jednoznačno ime (DN) i njegov certifikat.

VI ZAVRŠNA ODREDBA

Član 31

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

Broj: 051-04- 461/1-05
Podgorica, 04. aprila 2005.godine

SEKRETAR
Dušan Simonović, s.r.