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

Na osnovu člana 12 stav 2 i člana 33 stav 2 Zakona o elektronskom potpisu (“Službeni list RCG”, br. 55/03), Sekretarijat za razvoj donosi

PRAVILNIK

O MJERAMA I POSTUPCIMA UPOTREBE I ZAŠTITE ELEKTRONSKOG POTPISA, SREDSTAVA ZA IZRADU ELEKTRONSKOG POTPISA I SISTEMA CERTIFIKOVANJA

I OPŠTE ODREDBE

Član 1

Ovim Pravilnikom utvrđuju se mjere, postupci i oblici zaštite elektronskog potpisa i naprednog elektronskog potpisa, sredstava za izradu elektronskih potpisa, zaštite sistema certifikovanja i podataka o potpisniku, kao i postupci provjere identiteta potpisnika prilikom izdavanja elektronskih certifikata u Republici Crnoj Gori (u daljem tekstu: Republika).

Član 2

Postupci za izradu elektronskog potpisa, kriterijumi koje treba da ispunjavaju sredstva za izradu i provjeru elektronskog potpisa, kao 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) standardima EESSI SG (European Electronic Signatures Standardisation Initiative Steering Group);
4) IETF RFC (Request for Comments) dokumentima;
5) PKCS (Publik Key Criptographic Standards) dokumentima i preporukama kompanije RSA Data Security;
6) evropskim standardima Common Criteria (for Information Technology Security Evaluation) u odjeljku EAL (Evaluation Assurance Level);
7) 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.

II ELEKTRONSKI POTPIS

Član 3

Potpisnik izrađuje i koristi elektronski potpis i napredni elektronski potpis u skladu sa uslovima utvrdjenim Zakonom o elektronskom potpisu (u daljem tekstu: Zakon) , ovim pravilnikom, kao i uslovima utvrdjenim ugovorom sa davaocem usluga certifikovanja.

Član 4

Podaci za izradu elektronskog potpisa ne čine sastavni dio elektronskog potpisa.

Potpisnik je dužan zaštiti podatke za izradu elektronskog potpisa od neovlašćenog pristupa, otuđivanja i nepravilne upotrebe. Zaštita se mora dodatno obezbijediti primjenom

lozinke, biometrijskih postupaka ili drugim zaštitnim tehnikama.

Član 5

Podaci za izradu elektronskog potpisa moraju se u potpunosti razlikovati od podataka za provjeru elektronskog potpisa.

Postupak izrade elektronskog potpisa ne smije izmijeniti podatke koji se potpisuju niti spriječiti prikaz tih podataka potpisniku prije čina potpisivanja.

Potpisnik u elektronski potpis ugrađuje osnovne podatke o postupku, algoritmu i sadržaju potpisa kako bi korisnik elektronskog potpisa mogao provjeriti potpis na osnovu iste ili slične tehnologije i postupaka.

Napredni elektronski potpis mora se izrađivati primjenom standardizovanih algoritama iz grupe RSA (rsagen1) odnosno DSA (dsagen1).

Kod izrade naprednog elektronskog potpisa obvezno se koristi hash funkcija iz grupe SHA-1 (Secure Hash Algorithm), odnosno RIPEMD 160.

Član 6

Korisnik elektronskog potpisa (udaljem tekstu: korisnik) sprovodi provjeru elektronskog potpisa u skladu sa uputstvima potpisnika.

Ako je uz potpis ugrađen i certifikat,korisnik provjeru sprovodi u skladu sa uputstvima davaoca usluga certifikovanja koji je izdao certifikat, odnosno drugog davaoca usluga certifikovanja koji punopravno odgovara i priznaje certifikat.

Korisnik prilikom provjere naprednog elektronskog potpisa , pored podataka o potpisniku, mora provjeriti:

1) podatke o davaocu usluga certifikovanja koji je izdao kvalifikovani certifikat;

2) rok važenja kvalifikovanog certifikata;

3) valjanost certifikata u odnosu na davaoca usluga koji je izdao kvalifikovani certifikat (*certification path up to a trust point,* vidjeti RFC 2459 ili RFC 3280 Certification Path Validation);

4) nepostojanje u registru opozvanih certifikata.

III SREDSTVA ZA IZRADU ELEKTRONSKOG POTPISA

Član 7

Potpisnik je dužan zaštititi sredstva za izradu elektronskog potpisa od neovlašćenog pristupa, krađe i oštećenja.

U slučajevima kada sredstva za izradu elektronskog potpisa sadrže podatke za izradu naprednog elektronskog potpisa potrebno je sredstva za izradu elektronskog potpisa uskladiti sa zahtjevima za zaštitu i sigurnost opreme neophodne za izradu naprednog elektronskog potpisa.

Usklađivanje iz stava 2 ovog člana mora se sprovoditi primjenom najmanje jednog od zajedničkih međunarodnih obrazaca zaštite sredstava za izradu naprednog elektronskog potpisa:

1) ISO/IEC 15408-1:1999 – opšti sistem mjera zaštite uređaja i opreme koje su zajednički prihvatili međunarodno (ISO) i evropsko (IEC) tijelo u oblasti standardizacije, kojim je definisan skup uslova za funkcionalnost i sigurnost sredstava za izradu elektronskog potpisa u dokumentu “ Common Criteria 2.1” u odjeljku EAL 4+ (5), kojim se posebno utvrđuju sigurnosni zahtjevi na najvišem nivou, i kojima mora odgovarati funkcionisanje sredstava za izradu naprednog elektronskog potpisa (SOF-high);

2) CEN/ISSS SSCD-PP (Secure Signature Creation Device-Protection Profile) opšti obrazac zaštite sredstava za izradu naprednog elektronskog potpisa koji je Evropska unija prihvatila saglasno preporukama sadržanim u Smjernicama o elektronskom potpisu (Directive 1999/93) u dodatku II kojim se bliže opisuju zahtjevi koje moraju ispunjavati sredstva za izradu naprednog elektronskog potpisa kroz dokument CWA 14169;

3) opšti obrazac za sigurnost kriptografskih modula FIPS 140-1, dovoljno visokog nivoa – ne nižeg od nivoa 3.

Član 8

Kod izrade naprednog elektronskog potpisa u slučaju primjene sistema dva kriptografska ključa, dužina ključa za izradu naprednog elektronskog potpisa mora biti najmanje 1024 bita, uz primjenu kriptografskih algoritama iz grupe RSA/DSA i usklađeno sa međunarodnim standardom PKCS#1 (najmanje v (verzija) 2.1.).

Kriptografski moduli moraju se zasnivati na algoritmima i parametrima koji predstavljaju radno okruženje za izradu naprednog elektronskog potpisa saglasno trenutno važećim obrascima ugrađenim u dokument Algorithms and Parameters for Secure Electronic Signatures (najmanje v 2.1, 2001-10), koji za potrebe Evropske unije izrađuje EESSI/SG .

Kod ugrađivanja kriptografskih algoritama u sredstvo za izradu naprednog elektronskog potpisa mora se obezbijediti modularnost kojom se omogućava naknadna ugradnja novih algoritama.

Član 9

Programska oprema kojom se sprovodi provjera elektronskog potpisa mora u potpunosti onemogućiti dobijanje podataka za izradu elektronskog potpisa, pomoću podataka za njegovu provjeru.

Programska oprema koja generiše podatke za izradu elektronskog potpisa mora obezbijediti zaštitu tih podataka od neželjenog ili neovlašćenog pristupa, primjenom postojeće tehnologije.

Član 10

Programska oprema za izradu naprednog elektronskog potpisa mora imati ugrađene osnovne oblike zaštite, saglasno dokumentima o osnovnim pravilima zaštite i sigurnosti sredstva za izradu naprednog elektronskog potpisa – CWA 14168 i 14169 defined a Common Criteria Protection Profile (PP) for secure signature creation devices (SSCDs) , odnosno EAL4+ preporukama.

Član 11

Potpisnik koji izgubi ili mu je otuđeno sredstvo za izradu elektronskog potpisa, kao i u slučajevima kada mu je onemogućen pristup podacima za izradu elektronskog potpisa, dužan je o tome odmah obavijestiti davaoca usluga certifikovanja i zahtijevati opoziv certifikata.

Davalac usluga certifikovanja dužan je, odmah po prijemu zahtjeva iz stava 1 ovog člana, postupiti po utvrđenim pravilima opoziva izdatih certifikata, u skladu sa internim Pravilnikom o postupcima izdavanja certifikata, na osnovu kojeg vrši usluge certifikovanja.

IV SISTEM CERTIFIKOVANJA

Poslovna politika, organizacija radnih procesa i pružanje usluga certifikovanja

Član 12

Davalac usluga certifikovanja prije početka rada mora donijeti Opšta pravila pružanja usluga certifikovanja, koja korisnicima usluga obezbjedjuju neophodne informacija za odluku o prihvatanju usluga .

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate, istovremeno sa Opštim pravilima iz stava 1 ovog člana, mora donijeti Pravilnik o postupcima izdavanja certifikata i Pravilnik o zaštiti sistema certifikovanja, kojima će utvrditi postupke i mjere koje primjenjuje prilikom izdavanja i rukovanja certifikatima.

Član 13

Opšta pravila pružanja usluga certifikovanja , Pravilnik o postupcima izdavanja certifikata i Pravilnik o zaštiti sistema certifikovanja moraju biti izradjeni u skladu sa RFC 2527, odnosno međunarodno prihvaćenim obrascem ETSI TS 101 456 – Policy Requirements for Certification Authorities Issuing Qualified Certificates.

Opšti akti iz stava 1 ovog člana, zavisno od oblasti koju uređuju, u svojoj strukturi obavezno sadrže segmente:

1) *uvodne napomene i osnovni podaci* (opis usluga; identifikacioni podaci i OID oznaka; korisnici i područje primjene usluga;adresni podaci);
2) *opšte odredbe* (obaveze davaoca usluga, potpisnika i korisnika;odgovornost;finansijska odgovornost;usklađenost sa zakonom;naknada za usluge; objava i opoziv certifikata;provjera usklađenosti;povjerljivost i tajnost poslovanja i podataka;zaštita intelektualne svojine/autorstva);
3) *identifikacija i potvrđivanje identiteta potpisnika* (registracija potpisnika; plansko obnavljanje certifikata; obnavljanje nakon opoziva;zahtjevi za opoziv certifikata);
4) *osnovni zahtjevi u radu sa certifikatima* (prijem zahtjeva za izdavanje certfikata; izdavanje certifikata; dostavljanje/prihvat certifikata; opoziv certifikata; postupci provjere sigurnosnih mjera; arhiviranje certifikata i podataka; zamjena certifikata; postupci otklanjanja posljedica šteta i nezgoda; prestanak rada);
5) *kontrola sigurnosti opreme, postupaka i osoblja* (kontrola prostora, opreme i sredstava; kontrola postupaka i radnih procesa; kontrola osoblja – broj, stručnost, ovlašćenja);
6) *kontrola tehničke sigurnosti rada sistema certifikovanja* (izrada sopstvenog certifikata; zaštita podataka za izradu sopstvenog elektronskog potpisa; upravljanje podacima za izradu elektronskog potpisa; podaci za pristup potpisu davaoca usluga; kontrola sigurnosti računarskog sistema; kontrola sigurnosti radnog vijeka sistema; kontrola sigurnosti mrežnog sistema; kontrola sigurnosti kriptografskih modula);
7) *sadržaj certifikata i liste opozvanih certifikata* (sadržaj/obrazac certifikata; sadržaj liste opozvanih certifikata);
8) *postupci sa dokumentacijom* (postupak kod promjene sadržaja dokumentacije;objavljivanje dokumentacije;postupk prihvatanja/odobravanja dokumentacije).

Član 14

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate,pored opštih akata iz člana 13 ovog pravilnika, mora izraditi i interna pravila kojima se obezbjedjuje ispravno sprovođenje zaštitnih i sigurnosnih mjera u sistemu certifikovanja.

Internim pravilima iz stava 1 ovog člana dodatno se uređuju:

1) postupak pristupa i kretanja kroz poslovni prostor davaoca usluga certifikovanja;

2) postupak i tehnike dopunske zaštite informacionog sistema, upotrebe telekomunikacione opreme u radu sa podacima u sistemu certifikovanja;

3) postupci i radnje u vanrednim situacijama,naročito u slučaju požara i drugih nepogoda, nepredvidivih upada u poslovni prostor davaoca usluga certifikovanja, odnosno u informacioni sistem;

4) pravila vođenja evidencije o prisustvu zaposlenih u sistemu certifikovanja i pristupu sistemu certifikovanja.

Član 15

Interna pravila iz člana 14 ovog pravilnika predstavljaju poslovnu tajnu i dostupna su ovlašćenom službenom licu koje vrši nadzor nad radom davaoca usluga certifikovanja, u skladu sa Zakonom.

Član 16

U slučaju prigovora u vezi sa odstupanjem sadržaja usluga u odnosu na utvrđena pravila sadržana u dokumentima davaoca usluga certifikovanja, odgovorno lice davaoca usluga dužno je otkloniti odstupanja.

Ako odgovorno lice u roku od sedam radnih dana nije u mogućnosti obezbijediti otklanjanje odstupanja, postupak se može povjeriti trećem licu radi arbitraže, uz saglasnost strana u sporu.

Ako arbitraža nije moguća, strane se radi rješenja spora mogu obratiti nadležnom sudu.

Infrastruktura

Član 17

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate mora primjenjivati smjernice Evropske unije i Evropske standarde koji se odnose na postupke osiguranja i zaštite opreme i prostora.

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate mora obavljanje usluga certifikovanja prilagoditi novim standardima, odlukama i preporukama iz stava 1 ovog člana, koje se donesu nakon njihovog upisa u registar.

Ispunjenje određenog uslova iz stava 1 ovog člana može uslijediti i poslije upisa u registar, a prije početka rada, naročito kada su potrebna veća ulaganja u specijalizovani prostor ili opremu ili je neophodno zaposliti osoblje određene specijalnosti. U tom slučaju, uz zahtjev treba priložiti uvjerljiv dokaz da je određeni uslov moguće ostvariti u predloženom roku.

Član 18

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate usluge certifikovanja mora obavljati svojim sredstvima za rad i stalno zaposlenim osobljem.

Postupke sa najsloženijom opremom (software, hardware) koji se mogu sprovesti jedino od strane proizvođača te opreme, davalac usluga certifikovanja koji izdaje kvalifikovane certifikate može obaviti uz odgovarajuće učešće osoblja proizvođača te opreme i uz pomoć njihove opreme.

Član 19

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate za obavljanje usluga certifikovanja mora posjedovati sopstveni poslovni prostor ili poslovni prostor zakupljen na rok duži od pet godina u odnosu na dan podnošenja zahtjeva za upis u evidenciju. Veličina i struktura poslovnog prostora mora biti prikladna za smještaj opreme i rad osoblja koje obavlja usluge certifikovanja.

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate, poslove generisanja kriptografskih ključeva i izrade certifikata mora obavljati u specijalizovanom prostoru izdvojenom za tu namjenu.

Pristup prostoru u kojem se obavljaju poslovi iz stava 2 ovog člana mogu imati samo ovlašćena lica. O svakom pristupu prostoru mora se voditi evidencija.

Tehnička i programska oprema

Član 20

Davalac usluga certifikovanja za tehničku i programsku opremu kojom obavlja usluge certifikovanja mora primjenjivati domaće standarde, standarde ETSI, kao i odluke i preporuke

RFC grupe, ISO protokole i standarde.

Član 21

Davalac usluga certifikovanja mora obezbijediti fizičku zaštitu tehničke i procesne opreme i sprovoditi stalni nadzor pristupa računarskim resursima i poslovnom prostoru u kome su smješteni resursi sistema certifikovanja.

Pristup se može sprovoditi isključivo uz prisustvo najmanje dva ovlašćena lica koja imaju pravo pristupa informacionom sistemu davaoca usluga certifikovanja.

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate mora obezbijediti da pristup prostoru u kome se nalaze resursi sistema certifikovanja ima isključivo osoblje koje radi u tom sistemu.

Član 22

Informacioni sistem davaoca usluga certifikovanja koji izdaje kvalifikovane certifikate mora biti izgrađen od računarske opreme i odgovarajućih softverskih programa namijenjenih isključivo za poslove certifikovanja.

Član 23

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate opremu za provjeru i rad sistema certifikovanja mora uskladiti sa tehničkim standardom FIPS 140-1 dovoljno visokog nivoa – najmanje nivoa 3, odnosno sa utvrđenim zajedničkim obrascem zaštite programsko-tehničke i informatičke opreme i sistema "Common Criteria 2.1" zasnovanog na standardu ISO 15408-1:1999.

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate postupke i oblike zaštite sistema za cijelo vrijeme pružanja usluga certifikovanja mora usklađivati sa trenutno važećim preporukama i standardima u oblasti zaštite i sigurnosti rada informatičkih sredstava i sistema.

Osoblje

Član 24

Osoblje zaposleno u sistemu certifikovanja poslove i operativne zadatke u sistemu certifikovanja sprovodi kroz odvojene organizacione jedinice (službe, odjeljenja i slično) za upravljanje informacionim sistemom, sistemom upravljanja certifikatima, poslovima zaštite i kontrole, kao i poslovima pravne zaštite i nadzora nad radom sistema certifikovanja.

Član 25

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate mora imati zaključen ugovor o radu na neodredjeno vrijeme najmanje sa:

1) dva stručnjaka sa visokom stručnom spremom matematičkog, informatičkog ili tehničkog smjera, specijalizovanih za rad sa kriptografskim tehnologijama;

2) tri stručnjaka sa visokom stručnom spremom tehničkog smjera za zaštitu računarskih sistema i informacionih baza , kao i sa iskustvom u radu na sistemima izdavanja, opoziva i održavanja certifikata;

3) jednog pravnika sa visokom stručnom spremom koji poznaje sistem zaštite ličnih podataka, upotrebe i pravne usklađenosti elektronskog potpisa.

Član 26

Davalac usluga certifikovanja mora obezbijediti da zaposleno osoblje posjeduje stručna znanja za rad sa tehnologijom certifikovanja i postupke zaštite računarske opreme i programa koji su primijenjeni u sistemu certifikovanja, kao i permanentno usavršavanje znanja i vještina potrebnih za rad u sistemu certifikovanja.

Član 27

Zaposleni kod jednog davaoca usluga certifikovanja ne može biti u radnom, odnosno poslovnom odnosu sa drugim davaocima usluga certifikovanja.

Finansijski resursi

Član 28

Davalac usluga certifikovanja mora posjedovati finansijske resurse koji obezbjeđuju nesmetano pružanje usluga certifikovanja bez obzira na broj korisnika usluga i za cijelo vrijeme obavljanja usluga certifikovanja.

Davalac usluga certifikovanja mora posjedovati žiro račun i garanciju poslovne banke na tekuće poslovanje, vidljivo kroz javno dostupan godišnji poslovni izvještaj.

Certifikati i podaci (izdavanje i opoziv certifikata, provjera identiteta potpisnika)

Član 29

Davalac usluga certifikovanja mora obezbijediti jedinstvenost podataka za provjeru elektronskog potpisa na način koji omogućava nedvosmislenu identifikaciju potpisnika.

Član 30

Potpisnik koji želi uslugu certifikovanja mora lično u prijavnoj službi davaoca usluga certifikovanja podnijeti zahtjev za izdavanje certifikata.

Potpisnik mora obezbijediti tačnost i ispravnost podataka u zahtjevu i za to odgovara pravno i materijalno.

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate dužan je razmotriti sve podatke koje je potpisnik predao u zahtjevu za izdavanje certifikata i sprovesti njegovu fizičku identifikaciju na osnovu lične karte ili drugih relevantnih dokumenata sa fotografijom potpisnika (pasoš, vozačka dozvola), kojima se potvrđuje istinitost podataka sadržanih u zahtjevu za izdavanje certifikata.

Identifikacija se potvrđuje usklađivanjem priložene fotografije potpisnika i dopunski se usklađuje sa ispravnim i potpunim izgovaranjem i pisanjem imena i prezimena potpisnika.

Član 31

Podaci ispravnih i odobrenih zahtjeva za izdavanje certifikata arhiviraju se u informacionom sistemu davaoca usluga certifikovanja.

Sadržaj certifikata upisuje se u Registar izdatih certifikata.

Član 32

Potpisnik kojem je odobreno izdavanje certifikata mora lično, kod davaoca usluga certifikovanja ili na drugom za te poslove određenom mjestu, preuzeti izdati certifikat.

Izdavanje certifikata može obavljati isključivo lice koje je ovlašćeno za te poslove i ima zaključen ugovor o radu na neodređeno vrijeme sa davaocem usluga certifikovanja koji izdaje kvalifikovane certifikate.

Član 33

Sadržaj kvalifikovnog certifikata mora biti usklađen sa tehničkom specifikacijom ETSI TS 101 862 (najmanje v 1.3.2 , 2004-06 ili novije) – Qualified Certificate Profile i zasnovan na Qualified Certificate Profile obrascu RFC 3739.

Certifikat obavezno sadrži:

1) serijski broj (jedinstven, neponovljiv broj);

2) identifikaciju davaoca usluga certifikovanja;

3) kriptografski algoritam primijenjen kod izrade elektronskog potpisa;

4) elektronski potpis davaoca usluga certifikovanja;

5) ime davaoca usluga certifikovanja koji je izdao certifikat;

6) identifikacione elemente potpisnika neophodne za jednoznačnu identifikaciju;

7) podatke neophodne za postupak provjere elektronskog potpisa potpisnika na kojeg se odnosi certifikat;

8) podatke za provjeru elektronskog potpisa;

9) datum izdavanja i rok važenja certifikata;

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

11) oznaku da se radi o kvalifikovanom certifikatu.

Član 34

Izdati certifikat se opoziva:

1) na zahtjev potpisnika;

2) na službeni zahtjev od strane suda, nadležnog organa državne uprave, odnosno pravnog lica kod kojeg je potpisnik zaposlen u trenutku podnošenja zahtjeva za opoziv certifikata;

3) na zahtjev davaoca usluga certifikovanja u slučajevima neispunjavanja tehničkih uslova, odnosno ako se pri upotrebi elektronskog potpisa ne postupa na propisani način.

Opozvani certifikati upisuju se u listu opozvanih certifikata, koja mora biti dostupna svim subjektima koji imaju pristup uslugama davaoca usluga certifikovanja.

Lista opozvanih certifikata mora se odmah obnoviti kod svake nastale promjene, odnosno ako nije bilo promjena u roku od 48 sati.

Član 35

Lista opozvanih certifikata obavezno sadrži:

1) redni broj radne verzije liste;

2) kriptografski algoritam korišćen pri izradi elektronskog potpisa davaoca usluga certifikovanja;

3) elektronski potpis davaoca usluga certifikovanja;

4) ime davaoca usluga certifikovanja;

5) datum izrade liste.

Svaki opozvani certifikat u Listi opozvanih certifikata obavezno sadrži:

1) serijski broj dodijeljen certifikatu kod izdavanja;

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

Član 36

Davalac usluga certifikovanja utvrđuje vremenski period važenja izdatog kvalifikovanog certifikata, odnosno dan do kada se priznaje važenje izdatog certifikata.

Period iz stava 1 ovog člana za kvalifikovane certifikate mora se utvrditi u trajanju do pet godina, za ključeve dužine najmanje 1024 bita.

Član 37

Podaci o potpisnicima, izdati certifikati, statusi certifikata, kao i tehnički podaci nastali evidentiranjem rada sistema certifikovanja moraju se arhivirati na medije koji obezbjeđuju trajnost zapisa najmanje 20 godina.

U cilju čuvanja zapisa obavezno se izrađuju i sigurnosne kopije koje moraju biti smještene na drugoj lokaciji, izdvojeno od sistema certifikovanja u upotrebi.

Član 38

Arhivirani podaci moraju se čuvati i zaštititi od neovlašćenog pristupa i eventualnih gubitaka u zapisu.

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate mora u cilju očuvanja čitljivosti i ispravnosti zapisa na medijima, sprovoditi postupke provjere i, po potrebi, osvježivanje zapisa na medijima najmanje dva puta godišnje.

Član 39

Potpisnik može zatražiti od davaoca usluga certifikovanja povremeno provjeravanje podataka za provjeru elektronskog potpisa.

Potpisnik zahtjev za provjeru, u smislu stava 1 ovog člana, podnosi lično kod davaoca usluga certifikovanja, a može i u elektronskom obliku, ako je takav zahtjev ispravno elektronski potpisan od strane podnosioca zahtjeva.

Član 40

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate, podatke za izradu svog elektronskog potpisa mora odvojeno rasporediti na najmanje dvije osobe koje zajedno izrađuju elektronski potpis.

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate podatke za izradu svog elektronskog potpisa mora fizički i elektronski zaštititi u skladu sa utvrđenim pravilima i standardima u cilju sprečavanja fizičkog ili elektronskog pristupa od strane neovlašćenih lica.

Zaštita ličnih podataka

Član 41

Davalac usluga certifikovanja podatke o potpisnicima mora prikupljati, čuvati, koristiti i brisati u skladu sa odgovarajućim propisima o zaštiti ličnih podataka, uz poštovanje i zaštitu privatnosti korisnika sistema certifikovanja.

Podaci o potpisniku mogu se pribavljati isključivo neposredno od potpisnika , u obimu i sadržaju koji su neophodni za postupak izdavanja certifikata.

Potpisnik ima pravo uvida u podatke koji se o njemu vode kod davaoca usluga certifikovanja, u cilju provjere ili potrebnih dopuna i ispravki.

Zahtjev za uvid u podatke može se dostaviti i u elektronskom obliku i potpisan sa elektronskim potpisom podnosioca zahtjeva.

Davalac usluga certifikovanja mora dostaviti tražene podatke najkasnije u roku od pet radnih dana od dana prijema zahtjeva.

Član 42

Davalac usluga certifikovanja ne smije pružati povjerljive podatke, osim u slučajevima kada to traži sud ili državni tužilac, odnosno kada to dozvoli vlasnik podataka.

Osoba koja kod davaoca usluga certifikovanja sprovodi provjeru rada sistema certifikovanja ima pravo uvida u povjerljive podatke, izuzev u kriptografske podatke (podaci za izradu elektronskog potpisa davaoca usluga certifikovanja), ali ih ne smije iznositi izvan sistema niti objavljivati u izvještajima. Ta osoba se ugovorom dodatno obavezuje na držanje u potpunoj tajnosti povjerljivih podataka u koje je imala uvid za vrijeme postupaka provjere rada sistema certifikovanja.

V OPŠTI POSTUPCI ZAŠTITE SISTEMA CERTIFIKOVANJA

Član 43

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate dužan je izraditi jedinstveni sistem zaštite i sigurnosti vršenja usluga.

Izradu i održavanje jedinstvenog sistema iz stava 1 ovog člana, davalac usluga mora vršiti u skladu sa internim Pravilnikom o zaštiti sistema certifikovanja.

Član 44

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate mora , redovno svake godine i nakon značajnih promjena u sistemu za vrijeme vršenja usluga, sprovoditi provjeru svih segmenata sistema u odnosu na sigurnost, pouzdanost i kvalitet rada, u skladu sa Pravilnikom o zaštiti sistema certifikovanja.

Vremenski period između dva postupka provjere ne može biti duži od 12 mjeseci.

Član 45

Davalac usluga certifikovanja može nastaviti sa pružanjem usluga certifikovanja, ako se utvrdi da je sistem u potpunosti usklađen sa zahtjevima sadržanim u Pravilniku o zaštiti sistema certifikovanja.

Član 46

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate za poslove zaštite sistema certifikovanja mora zaposliti kvalifikovano osoblje za poslove :

1) kontrole fizičkog pristupa računarskoj opremi;

2) ugradnje i konfiguracije programskog rješenja zaštite, kao i sistemsko mijenjanje kriptografskih ključeva;

3) analize rada u svima fazama, evidentiranje i arhiviranje tih podataka i obavještavanje;

4) upravljačke funkcije i operacije otklanjanja problema u funkcionisanju utvrdjenih mjera zaštite;

5) izvještavanja o pokušajima narušavanja propisanih mjera zaštite i identifikaciju subjekata koji vrše narušavanje.

Član 47

Provjera, u smislu člana 44 ovog pravilnika, mora se obavezno sprovesti za:

1) sistem certifikovanja (informacioni sistem);

2) tehnologiju kriptozaštite;

3) radni prostor , računarsku i mrežnu opremu;

4) relevantne zakonske i druge propise u Republici i Evropskoj uniji.

Član 48

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate sistem certifikovanja i informacioni sistem mora uskladiti sa zahtjevima sigurnosti rada informacionih sistema, saglasno obrascima ISO/IEC 17799:2000 (Code of Practice for Information Security Management) i BS 7799-2:1999 (British Standard for Information Security Management – Specification for Information Security Management System).

Sistem certifikovanja mora sadržati odvojene radne cjeline, pri čemu osoblje koje radi na poslovima upravljanja računarskim sistemom ili provjere identiteta i registracije potpisnika ne može vršiti poslove koji se odnose na izdavanje i opoziv certifikata.

Član 49

Svi podaci za izradu naprednog elektronskog potpisa davaoca usluga certifikovanja, moraju biti kriptografski zaštićeni uz primjenu:

1) sredstava za izradu naprednog elektronskog potpisa saglasno FIPS 140-1 (dovoljno visokog nivoa – ne nižeg od nivoa 3) i sa kojima je moguća upotreba posebnih pristupnih tehnika za 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, i SHA-1 ili RIPEMD – 160 algoritma za kriptovanje sadržaja;

3) kriptografskih algoritama (3DES algoritma – 128 bitni ili AES tehnika) radi zaštite pristupa podacima.

Član 50

Davalac usluga certifikovanja podatke za izradu svog elektronskog potpisa mora čuvati u najmanje dva primjerka na odvojenim lokacijama, u za to namjenski uređenom prostoru zaštićenom od oštećenja u slučaju požara, poplave i drugih štetnih uticaja, kao i obezbijediti razdvajanje osnovnog skupa podataka za izradu elektronskog potpisa u najmanje dva dijela.

Dostupnost podataka za izradu naprednog elektronskog potpisa davaoca usluga certifikovanja koji izdaje kvalifikovane certifikate, mora biti jednokratna i to samo za vrijeme izrade elektronskog potpisa i mora prestati nakon svake izrade elektronskog potpisa.

Član 51

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate rad sa računarskom i programskom opremom mora povjeriti isključivo osoblju sa visokom stručnom spremom i specijalističkim znanjima u rukovanju opremom koja je ugrađena u sistem certifikovanja.

Davalac usluga certifikovanja koji izdaje kvalifikovane certifikate, fizički pristup računarskom sistemu kojim se sprovode usluge certifikovanja može omogućiti isključivo osoblju koje neposredno radi sa računarskim sistemom.

Osoblje za održavanje higijene prostora u kojem se nalazi računarski sistem svoj dio posla može vršiti isključivo uz prisustvo osoblja koje neposredno radi sa računarskim sistemom.

U slučaju neovlašćenog pristupa računarskoj i programskoj opremi, odnosno informacionom sistemu, davalac usluga certifikovanja mora obustaviti normalan rad i sprovesti mjere predviđene za rad u vanrednim situacijama, sve do potpunog otkrivanja uzroka i otklanjanja mogućih šteta.

Centralni računarski sistem mora imati obezbijeđeno trajno napajanje energijom, uz potreban radni ambijent, kao što su dozvoljeni stepen vlažnosti i temperature, dozvoljeni nivo zračenja i ostale vrijednosti specifične za računarski sistem u funkciji.

Računarski sistem mora biti smješten u prostoru koji je obezbijeđen od poplave, uz adekvatnu protivpožarnu zaštitu.

VI ZAVRŠNE ODREDBE

Član 52

Danom stupanja na snagu ovog pravilnika prestaje da važi Pravilnik o mjerama i postupcima upotrebe i zaštite elektronskog potpisa, sredstava za izradu elektronskog potpisa i sistema certifikovanja, br. 051-04-851/1-04 od 5. jula 2004.godine ("Službeni list RCG",br. 53/04).

Član 52

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

Broj: 051-04- 460/1-05
Podgorica, 04. aprila 2005.godine

SEKRETAR
Dušan Simonović, s.r.