215

Na temelju članka 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", br. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08) i članka 26. stavak (1) Zakona o elektroničkom potpisu ("Službeni glasnik BiH", broj 91/06), na prijedlog ministra komunikacija i prometa Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine na 88. sjednici, održanoj 18. siječnja 2017. godine, donijelo je

PRAVILNIK
O BLIŽIM UVJETIMA ZA IZDAVANJE KVALIFICIRANIH POTVRDA

POGLAVLJE I – Opće odredbe

Članak 1.
(Predmet Pravilnika)

Ovim Pravilnikom propisuju se bliži uvjeti za izdavanje kvalificiranih potvrda i uvjeti koje ovjeritelj mora ispunjavati za izdavanje kvalificiranih potvrda.

Članak 2.
(Primjena međunarodnih standarda)

(1) Prilikom izdavanja kvalificiranih potvrda primjenjuju se međunarodni standardi i preporuke, kao i drugi odgovarajući standardi, dokumenata i preporuka.
(2) Ovjeritelj za izdavanje kvalificiranih potvrda (u daljnjem tekstu: ovjeritelj) izdaje kvalificirane potvrde korisnicima sukladno 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 and Certificate Revocation List (CRL) Profile" i ETSI TS 102 280 "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".

POGLAVLJE II – Pouzdano obavljanje usluga izdavanja kvalificiranih potvrda

Članak 3.
(Način formiranja sigurnog elektroničkog potpisa)

Ovjeritelj izdaje kvalificirane potvrde formiranjem sigurnog elektroničkog potpisa na temelju svog privatnog ključa i asimetričnog kriptografskog algoritma, na način propisan Pravilnikom o tehničko-tehnološkim postupcima za formiranje sigurnog elektroničkog potpisa i uvjetima i kriterijumima, koje treba da ispune sredstva za formiranje sigurnog elektroničkog potpisa.

Članak 4.
(Usluge certifikacije)

(1) Ovjeritelj je dužan osigurati potpunu uslugu certifikacije koja uključuje sljedeće servise, i to:
   a) registraciju korisnika;
   b) formiranje kvalificiranih potvrda;
   c) distribuciju kvalificiranih potvrda korisnicima;
   d) upravljanje životnim vijekom (obnavljanje, suspenzija, opoziv) kvalificiranih potvrda;
   e) osiguravanje pouzdanog i javno dostupnog servisa za provjeru statusa opozvanosti kvalificiranih potvrda.
(2) Ovjeritelj može, pored servisa iz stavka (1) ovoga članka, da osigura i formiranje asimetričnog para ključeva za korisnike, kao i distribuciju privatnog ključa i potvrde korisniku na siguran način, ukoliko je to propisano u politici certificiranja datog ovjeritelja.

Članak 5.
(Opći akti ovjeritelja)

(1) Ovjeritelj, prije početka rada, donosi opća interna pravila pružanja usluge certifikacije (u daljnjem tekstu: opća pravila) koja korisnicima pružaju dovoljno informacija na temelju kojih se mogu odlučiti o prihvaćanju usluga i o obujmu usluga.
(2) Opća pravila funkcioniranja ovjeritelja treba da budu sukladna dokumentima RFC 3647 "Internet X.509 Public Key Infrastructure. Certificate Policy and CertificationPractices Framework" i ETSI TS 101 456 "Policy Requirements for Certification Authorities Issuing Qualified Certificates".
(3) Na temelju općih pravila ovjeritelj donosi sljedeće opće akte:
   a) Politiku certifikacije (engl. Certificate Policy);
   b) Praktična pravila pružanja usluge certifikacije (engl. Certification Practices Statement) (u daljnjem tekstu: praktična pravila).

Članak 6.
(Politika certifikacije i praktična pravila)

(1) Politika certifikacije i praktična pravila su javni dokumenti.
(2) Politika certifikacije definira predmet rada i zahtjeve poslovanja ovjeritelja.
(3) Praktična pravila definiraju procese i način njihovog korištenja pri formiranju i upravljanju kvalificiranim potvrdama, operativne procedure u cilju ispunjenja tih zahtjeva i način na koji ovjeritelj ispunjava tehničke, organizacijske i proceduralne zahtjeve poslovanja koji su identificirani u politici certifikacije.
(4) Politikom certifikacije i praktičnim pravilima uređuju se sljedeće oblasti:
   a) opće odredbe o radu ovjeritelja:
      1) pojam ovjeritelja,
      2) certifikacijske usluge,
      3) obuhvat dokumenta politika certifikacije,
      4) obuhvat dokumenta praktičnih pravila pružanja usluge certifikacije,
      5) korisničke usluge certifikacije.
   b) uvodne odredbe o politici izdavanja kvalificiranih potvrda;
   c) obveze i odgovornosti ovjeritelja i korisnika;
   d) funkcionalne zahtjeve za rad ovjeritelja: operativne procedure rada ovjeritelja i procedure upravljanja životnim ciklusom kriptografskih ključeva:
      1) generiranje ključa ovjeritelja,
      2) procedure čuvanja i formiranja rezervnih preslika ključeva ovjeritelja,
      3) distribuciju javnog ključa ovjeritelja,
      4) korištenje ključa ovjeritelja,
      5) kraj životnog ciklusa ključa ovjeritelja,
      6) upravljanje životnim ciklusom kriptografskog hardvera koji se koristi za generiranje kvalificiranih potvrda,
      7) upravljanje ključevima korisnika za identificiranje,
      8) proceduru primjene sredstava za formiranje sigurnog elektroničkog potpisa.
   e) procedure upravljanja životnim ciklusom certifikata:
      1) metode registracije korisnika,
      2) izdavanje potvrda,
      3) distribuciju potvrda,
      4) obnavljanje potvrda,
      5) suspenziju potvrda,
      6) opoziv potvrda,
      7) način publikacije liste opozvanih potvrda;
   f) upravljanje operativnim radom ovjeritelja:
      1) upravljanje sukladno sa sigurnosnim principima,
      2) upravljanje i klasifikacija najvažnijih informacija i podacima unutar ovjeritelja,
      3) kadrovski resursi,

4) sustav fizičke sigurnosti i sigurnosti okruženja,
5) upravljanje radom ovjeritelja,
6) upravljanje sustavom kontrole pristupa,
7) uporabu i održavanje sigurnih kriptografskih sustava,
8) upravljanje procedurama kontinualnog poslovanja u incidentnim situacijama,
9) prestanak rada ovjeritelja,
10) usaglašenost rada sa kriterijumima za rad ovjeritelja koji izdaju kvalificirane potvrde sukladne članku 8. Zakona i ovim Pravilnikom,
11) formiranje i čuvanje dokumentacije koja se odnosi na kvalificirane potvrde.

g) organizaciju rada ovjeritelja.

Članak 7.
(Sposobnost za osiguranje usluge)

Ovjeritelj demonstrira sposobnost za osiguranje usluge izdavanja kvalificiranih potvrda, ukoliko:

a) posjeduje praktična pravila, i u njima definirane procedure, u kojima se specificira način ispunjenja svih zahtjeva za izdavanjem kvalificiranih potvrda koji su identificirani u politici certifikacije;
b) učini dostupnim praktična pravila svim korisnicima i drugim zainteresiranim strankama;
c) učini dostupnim svim korisnicima i potencijalnim zainteresiranim stranama uvjete korištenja kvalificiranih potvrda;
d) posjeduje upravnu strukturu najviše razine koja ima konačnu autorizaciju i odgovornost za objavljivanje praktičnih pravila ovjeritelja;
e) posjeduje upravnu strukturu operativne razine u ovjeritelju koja je odgovorna za ispravnu primjenu praktičnih pravila;
f) definira postupak periodične analize i revizije praktičnih pravila;
g) posjeduje sve izmjene praktičnih pravila, javno objavljene i odobrene od strane upravne strukture najviše razine.

Članak 8.
(Posebna interna pravila)

(1) Ovjeritelj utvrđuje i posebna interna pravila rada ovjeritelja i zaštite sustava certifikacije (u daljnjem tekstu: posebna pravila) u kojima su sadržani i detaljno opisani postupci i mjere koje se primjenjuju prilikom izdavanja i postupanja kvalificiranim potvrdama.
(2) Posebna pravila su privatni dokument i predstavljaju poslovnu tajnu ovjeritelja.

Članak 9.
(Posebna pravila)

Posebna pravila sadrže odredbe kojim se bliže uređuje:

a) sustav fizičke kontrole pristupa u pojedine prostorije ovjeritelja;
b) sustav logičke kontrole pristupa računalskim resursima ovjeritelja;
c) sustav čuvanja privatnog ključa ovjeritelja;
d) sustav dodijeljene odgovornosti pri aktivaciji privatnog ključa ovjeritelja i
e) postupci i radnje u izvanrednim situacijama (požari, poplave, zemljotresi, druge vremenske nepogode, zlonamjerni upadi u prostorije ili informacijski sustav ovjeritelja).

Članak 10.
(Organizacija rada)

Ovjeritelj osigurava pouzdanu organizaciju rada tako što:

a) donosi pravila i operativne procedure koje nisu diskriminatorske;
b) čini dostupnim svoje servise svim korisnicima čije su aktivnosti sukladne objavljenim općim pravilima;
c) posluje kao pravna osoba sukladna propisima;
d) ima sustav kvaliteta i sustav sigurnog upravljanja kvalificiranim potvrdama sukladno uslugama certifikacije koje pruža;
e) posjeduje osiguranje od odgovornosti za štetu, koja može da proistekne u vršenju njegovih aktivnosti sukladno politici certifikacije;
f) ima financijsku stabilnost i dovoljne resurse koji se zahtijevaju u pružanju usluga certifikacije sukladno politici certifikacije;
g) ima dovoljan broj stalno uposlenih na poslovima certifikacije sa neophodnim obrazovanjem, razinom obučenosti, tehničkim znanjima i iskustvom;
h) učinkovito postupa prilikom rješavanja žalbi i sporova sa korisnicima ili drugim zainteresiranim strankama u svezi pružanja usluga certifikacije;
i) pruža neovisnost dijelova ovjeritelja uključenih u poslove generiranja kvalificiranih potvrda od drugih vanjskih organizacija u sferi pružanja usluga certifikacije. Posebno upravne strukture ovjeritelja, kao i uposlenih sa sigurnosnim funkcijama, moraju biti zaštićeni od bilo kakvih financijskih i drugih pritisaka koji mogu utjecati na povjerenje u usluge certifikacije koje pruža ovjeritelj;
j) ima propisno dokumentiranu strukturu dijelova ovjeritelja povezanih sa generiranjem kvalificiranih potvrda radi odiguravanja nepristrasnosti u pružanju usluga certifikacije, sukladno općim i posebnim pravilima.

Članak 11.
(Osiguranje od odgovornosti za štetu)

Ovjeritelj je dužan osigurati najniži iznos osiguranja od rizika odgovornosti za štetu nastalu vršenjem usluga izdavanja elektroničkih potvrda, tako da:

a) osigurana suma na koju mora biti ugovoreno osiguranje po jednom štetnom događaju ne može iznositi manje od 50.000 KM, podrazumijevajući pritom kao štetni događaj pojedinačnu štetu nastalu uporabom jedne kvalificirane potvrde u jednom aktu u pravnom prometu;
b) ukupna osigurana suma na koju mora biti ugovoreno osiguranje od odgovornosti ovjeritelja kumulativno na godišnjoj razini, po svim štetnim događajima, ne može biti niža od 1.500.000,00 KM.

Članak 12.
(Postupanje ovjeritelja u slučaju izvanrednih okolnosti)

Ovjeritelj osigurava da u slučaju izvanrednih okolnosti operativni rad bude obnovljen što je moguće prije a sukladan općim i posebnim pravilima. U slučaju kompromitiranja svog asimetričnog privatnog ključa, ovjeritelj:

a) prestaje sa izdavanjem kvalificiranih potvrda;
b) informira sve korisnike i druge zainteresirane stranke o kompromitiranju privatnog ključa;
c) javno objavljuje informacije o tome da izdane kvalificirane potvrde, kao i informacije o statusu opozvanosti kvalificiranih potvrda, više nisu važeće;
d) vrši opoziv svih izdanih kvalificiranih potvrda odmah a najkasnije u roku od 24 sata sukladno članku 10. Zakona o elektroničkom potpisu ("Službeni glasnik BiH", broj 91/06, u daljnjem tekstu: Zakon).

Članak 13.
(Evidencija izdanih kvalificiranih potvrda)

(1) Ovjeritelj vodi ažurnu, točnu i sigurnu evidenciju izdanih kvalificiranih potvrda koja može biti javno dostupna, osim u slučajevima kada vlasnik potvrde izričito zahtijeva da njegovi podaci ne budu javno dostupni.
(2) Ovjeritelj vodi ažurnu i sigurnu evidenciju opozvanih i suspendiranih kvalificiranih potvrda i mora za svaku potvrdu koju je izdalo, informaciju o njegovoj validnosti učiniti javno dostupnom.
(3) Za točnost i validnost evidencija iz st. (1) i (2) ovoga članka garantira ovjeritelj, svojom kvalificiranom potvrdom.

Članak 14.
(Određivanje vremena izdavanja i opoziva)

(1) Za određivanje vremena izdavanja i opoziva kvalificiranih potvrda, ovjeritelj osigurava izvor točnog vremena koji je sinhroniziran sa izvorom referentnog vremena kojeg odredi Nadzorno tijelo i objavljuje na službenoj Internet stranici Nadzornog tijela.
(2) Vrijeme izdavanja kvalificirane potvrde ovjeritelj upisuje u izdanu kvalificiranu potvrdu.
(3) Vrijeme izdavanja i opoziva kvalificiranih potvrda ovjeritelj čuva u evidenciji izdanih i opozvanih potvrda iz članka 13. ovoga Pravilnika.

POGLAVLJE III - Registracija korisnika

Članak 15.
(Registracija korisnika)

(1) Ovjeritelj vrši pouzdanu identifikaciju i autentikaciju korisnika u cilju izdavanja kvalificirane potvrde, te vodi registar potvrda.
(2) Postupke registracije iz stavka (1) ovoga članka vrši ovlašteni službenik ovjeritelja.

Članak 16.
(Obveze ovjeritelja u postupku registracije korisnika)

U postupku registracije korisnika, ovjeritelj je dužan osigurati da:

a) se korisnik identificira kao fizička osoba sa specifičnim atributima koji mogu označavati organizacionu jedinicu ili ulogu u organizaciji gdje je uposlen;
b) prije uspostave ugovornog odnosa sa korisnikom, javno informira korisnika na jasan i nedvosmislen način o svim relevantnim uvjetima korištenja kvalificiranih potvrda;
c) se u postupku registracije, identitet korisnika fizičke osobe, utvrđuje neposrednim uvidom u važeći identifikacijski dokument u prisustvu podnositelja zahtjeva;
d) ukoliko se radi o korisniku, pravnoj osobi se izvrši uvid u:
   1) izvod iz sudskog registra iz kojeg se može utvrditi ko je odgovorna osoba u pravnoj osobi,
   2) akt kojim je korisnik ovlašten od strane te pravne osobe ili organizacije za dobivanje kvalificirane potvrde;
e) se u izuzetnom slučaju utvrđuje svaki specifični atribut korisnika kome se izdaje kvalificirana potvrda;
f) informacije sadržane u kvalificiranoj potvrdi budu pouzdane i točne;
g) korisnik dostavi točne i pouzdane informacije o fizičkoj adresi, ili drugim atributima, koji opisuju kako se korisnik može kontaktirati;
h) se čuvaju sve informacije korištene za verifikaciju identiteta korisnika i dokumentaciju korištenu za identificiranje, kao i bilo koja ograničenja njene važnosti;
i) se zaključi ugovor sa korisnikom kojim se regulira sljedeće:
   1) obveza korisnika da koristi sredstvo za formiranje sigurnog elektroničkog potpisa koje osigurava ovjeritelj sukladno općim pravilima,
   2) obveza ovjeritelja da čuva podatke korištene u registraciji korisnika i sve informacije o životnom ciklusu izdane kvalificirane potvrde korisnika;
   3) uvjeti pod kojima se objavljuje potvrda,
   4) klauzulu o točnosti podataka sadržanih u potvrdi;
j) ako asimetrični par ključeva korisnika nije generiran od strane ovjeritelja, proces generiranja zahtijeva za kvalificiranom potvrdom u cjelosti osigurava da korisnik posjeduje privatni ključ koji je matematički povezan sa javnim ključem koji je prezentiran za certifikaciju. U tom slučaju korisnik mora osigura da se asimetrični par ključeva generira isključivo u sredstvu za formiranje sigurnog elektroničkog potpisa;
k) se poštuju odredbe važećih propisa kojima je uređena oblast zaštite osobnih podataka.

POGLAVLJE IV - Kadrovski resursi i upravljanje operativnim radom ovjeritelja

Članak 17.
(Funkcioniranje ovjeritelja)

Ovjeritelj je dužan osigurati pouzdano, sigurno i nesmetano obavljanje poslova izdavanja kvalificirane potvrde.

Članak 18.
(Ljudski resursi)

(1) Ovjeritelj osigurava da uposleni u ovjeritelju posjeduju neophodno potrebnu kvalifikaciju, iskustvo i ekspertsko znanje, za obavljanje poslova ovjeritelja, i to:
   a) potreban broj uposlenih sa visokom školskom spremom iz oblasti informacijsko-komunikacijskih tehnologija,
   b) radno iskustvo uposlenih od najmanje 3 godine na poslovima održavanja i sigurnosti informacijskih sustava,
   c) položen ispit iz oblasti sigurnosti informacijskih sustava,
   d) posjedovanje specifičnih vještina i iskustva,
   e) da posjeduju ekspertizu u tehnologiji elektroničkog potpisa, da su dobro upoznati sa sigurnosnim procedurama za uposlene i sa odgovornostima u domeni sigurnosti, kao i da imaju odgovarajuća iskustva u primjeni sigurnih informacijskih sustava i procjeni rizika.
(2) Ovjeritelj je dužan osigurati sljedeće sigurnosne funkcije u ovjeritelju za:
   a) glavnog administratora sigurnosti - sveukupnu odgovornost za administriranje i implementaciju sigurnosnih funkcija i procedura, kao i upravljanje aktivnostima na dodanom unapređenju poslova generiranja, opoziva i suspenzije kvalificiranih potvrda,
   b) sustav administratore - autoriziranu odgovornost za instalaciju, konfiguriranje i održavanje sigurnih sustava ovjeritelja za registraciju korisnika, generiranje kvalificiranih potvrda, osigurava sredstava za formiranje sigurnog elektroničkog potpisa za korisnike i upravljanje opozivom kvalificiranih potvrda,

c) sustav operatore - odgovornost za rad sigurnih sustava ovjeritelja u tekućem radu na dnevnoj razini i autoriziranu odgovornost za implementaciju sustava za formiranje rezervnih preslika i procedure oporavka,
d) sustav evidentičare - autoriziranu odgovornost za pregledanje i održavanje arhiva i log fajlova sigurnih sustava ovjeritelja;

(3) Odgovorna osoba u ovjeritelju, vršiteljima poslova iz stavka (2) ovoga članka, posebnim aktom utvrđuje sigurnosne funkcije.
(4) U opisu svakog radnog mjesta u ovjeritelju, uloga i stupanj sigurnosti utvrđene u općim pravilima, moraju biti jasno i precizno navedene, sa naglaskom na stupanj povjerljivosti.
(5) Uposleni u ovjeritelju koji imaju određen stupanj sigurnosne funkcije ne smiju biti u sukobu interesa koji mogu utjecati na nepristrasnost rada ovjeritelja.
(6) Sigurnosne funkcije ne mogu se dodijeliti osobi koja je osuđivana za radnje koje su u svezi sa poslovima koje obavljaju kod ovjeritelja. Pristup sigurnosnim funkcijama osigurava se po okončanju propisanih provjera.

POGLAVLJE V - Pouzdani i sigurni kriptografski sustavi

Članak 19.
(Korištenje sigurnih sustava)

Ovjeritelj koristi sigurne sustave i proizvode koji su zaštićeni od neovlaštenih modifikacija.

Članak 20.
(Analiza rizika)

Ovjeritelj vrši analizu rizika kojom identificira kritične servise koji zahtijevaju korištenje sigurnih sustava i visoke razine sigurnosti:

a) prije početka obavljanja usluga certifikacije,
b) tijekom operativnog rada po potrebi, a najmanje svakih šest mjeseci.

Članak 21.
(Sigurno i korektno funkcioniranje sustava)

Ovjeritelj osigurava sigurno i korektno funkcioniranje svojih sustava, sa minimalnim rizikom od kvarova, a naročito:

a) zaštitu integriteta sustava ovjeritelja i informacija od virusa, malicioznog i neautoriziranog softvera;
b) minimalan rizik od štete uslijed mogućih incidenata korištenjem procedura izvješćivanja, brzim i koordiniranim reagiranjem na sigurnosne incidente u cilju smanjenja utjecaja sigurnosnih upada;
c) sigurno korištenje memorijskih medija sukladno unaprijed specificiranim shemama klasifikacije informacija. Mediji koji nisu u operativnom radu, sigurnosno osjetljive podatke moraju sigurno arhivirani;
d) uspostaviti i implementirati procedure za sve sigurne i administrativne funkcije koje imaju utjecaj na pružanje usluga certifikacije. Odgovorna osoba ovjeritelja je odgovorna za planiranje i učinkovitu implementaciju općih pravila;
e) stalnim nadzorom tekućih i planiranih potreba za kapacitetom sustava ovjeritelja radi osiguranja adekvatne procesne snage i memorijskih kapaciteta.

Članak 22.
(Asimetrični ključevi)

(1) Asimetrični ključevi mogu biti javni i privatni;
(2) Ovjeritelj osigurava da se njegovi asimetrični ključevi generiraju u strogo kontroliranim i sigurnim uvjetima, a naročito da se:
a) generiranje asimetričnih ključeva vrši u fizički zaštićenom okruženju od strane i uz minimalan broj autoriziranih uposlenih (najmanje dvije uposlene osobe) za izvršavanje ove funkcije a prema zahtjevima i procedurama definiranim u praktičnim pravilima;
b) generiranje asimetričnih ključeva vrši u sredstvu koje:
1) zadovoljava zahtjeve iz standarda FIPS PUB 140-2 razina 3 i viši ili
2) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)" ili
3) zadovoljava zahtjeve iz standarda 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)";

(3) Rezervne kopije privatnih ključeva za formiranje sigurnog elektroničkog potpisa kvalificiranih potvrda imaju istu ili višu razinu sigurnosnih kontrola u odnosu na ključeve koji se operativno koriste.
(4) Ovjeritelj osigurava da su izdane kvalificirane potvrde potpisane sigurnim elektroničkim potpisom ovjeritelja.

Članak 23.
(Zaštita tajnosti i integriteta)

Ovjeritelj osigurava zaštitu tajnosti i integritet privatnih ključeva, a naročito:

a) čuvanje i korištenje privatnog ključa za formiranje sigurnog elektroničkog potpisa u sigurnom kriptografskom uređaju koji:
1) zadovoljava zahtjeve iz standarda FIPS PUB 140-2 razina 3 i viši ili
2) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)" ili
3) zadovoljava zahtjeve iz standarda 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)";
b) da su dijelovi za aktivaciju privatnog ključa ovjeritelja, kada se nalaze izvan kriptografskog uređaja šifrovani korištenjem simetričnog algoritma i dužine ključa, i omogućavaju pouzdanu odbranu od kriptoanalitičkih napada;
c) čuvanje dijelova za aktivaciju privatnog ključa, uz osiguranje rezervnih preslika tih dijelova, i aktivacija koju vrše uposleni koji imaju sigurnosne funkcije, uz korištenje najmanje dvostruke kontrole u fizički osiguranom okruženju;
d) da se mjerama logičke kontrole pristupa onemogući neovlašteno aktiviranje kriptografskog uređaja sa privatnim ključem ovjeritelja.

Članak 24.
(Verifikacija sigurnog elektroničkog potpisa)

Ovjeritelj osigurava da njegov javni ključ kojim se verificira sigurni elektronički potpis kvalificiranih potvrda bude raspoloživ svim korisnicima i drugim zainteresiranim strankama na način kojim se osigurava autentičnost i integritet javnog ključa.

Članak 25.
(Javni ključ)

Ovjeritelj dostavlja svoj javni ključ i lokaciju liste opozvanih potvrda korisnicima i drugim zainteresiranim strankama na siguran način u obliku kvalificirane potvrde ili liste opozvanih potvrda.

Članak 26.
(Korištenje privatnog ključa)

(1) Ovjeritelj koristi svoj privatni ključ sukladno općim i posebnim pravilima i osigurava:
   a) da se koristi isključivo za formiranje sigurnog elektroničkog potpisa kvalificiranih potvrda, kao i sigurnog elektroničkog potpisa liste opozvanih potvrda;
   b) da se koristi samo unutar fizički zaštićenih prostorija ovjeritelja.
(2) Ovjerirtelj osigurava da se njegovi privatni ključevi ne koriste nakon isteka njihovog životnog ciklusa, sukladno općim i posebnim pravilima.
(3) Privatni ključevi, iz stavka (2) ovoga članka, uništavaju se na način kojim se osigurava da isti ne može biti ponovo formiran.

Članak 27.
(Sigurnost kriptografskih uređaja)

Ovjeritelj osigurava sigurnost kriptografskih uređaja koji se koriste za generiranje i čuvanje ključeva i formiranje sigurnog elektroničkog potpisa tijekom životnog ciklusa uređaja, sukladno posebnim pravilima, a naročito da:
   a) kriptografski uređaj nije kompromitiran tijekom transporta;
   b) kriptografski uređaj nije kompromitiran za vrijeme čuvanja kod ovjeritelja;
   c) procedure instalacije aktivacije, kreiranja rezervnih preslika i ponovnog formiranja privatnog ključa u kriptografskom uređaju vrši se u prisustvu najmanje dva uposlena kojima je dodijeljena sigurnosna funkcija;
   d) ispravnost funkcionisanja kriptografskog uređaja;
   e) da se privatni ključevi ovjeritelja čuvani u kriptografskom uređaju uništavaju nakon kraja životnog ciklusa ključeva ili uređaja.

POGLAVLJE VI - Zaštita potvrda i tajnosti generiranih ključeva

Članak 28.
(Proces generiranja kvalificiranih potvrda)

Ovjeritelj osigurava siguran proces generiranja kvalificiranih potvrda radi osiguravanja njihove autentičnosti i integriteta.

Članak 29.
(Ostale obveze ovjeritelja)

Ovjeritelj osigurava:
   a) da se kvalificirane potvrde generiraju sukladno formatu definiranom u dokumentima ETSI TS 101 862, RFC 3739, RFC 3280 i ETSI TS 102 280;
   b) da je procedura generiranja kvalificirane potvrde sigurno povezana sa odgovarajućim procedurama registracije korisnika, obnavljanja potvrda uz zadržavanje postojećeg ili generiranje novog para ključeva;
   c) u slučaju da ovjeritelj generira korisnikove ključeve osigurava:
      1) da je procedura generiranja kvalificirane potvrde sigurno povezana sa procedurom generiranja asimetričnog para ključeva od strane ovjeritelja,
      2) da je privatni ključ, odnosno sredstvo za formiranje sigurnog elektroničkog potpisa, sigurno dostavljeno do registriranog korisnika, a da se aktivacijski kod sredstva za formiranje sigurnog elektroničkog potpisa ovlaštenoj osobi dostavi na siguran način drugim putem;
   d) jedinstvenost dodijeljenog imena korisniku unutar domene ovjeritelja;
   e) tajnost i integritet registracijskih podataka, i to posebno u slučajevima razmjene podataka sa korisnikom ili u slučaju razmjene informacija između distribuiranih komponenti ovjeritelja;
   f) verifikaciju dostavljenih registracijskih podataka.

Članak 30.
(Obnavljanje i izdavanje nove kvalificirane potvrdu)

Ovjeritelj osigurava da se na zahtjev korisnika ranije opozvana kvalificirana potvrda obnavlja ili izdaje nova ukoliko su isti kompletni, točni i autorizirani.

Članak 31.
(Zahtjevi za obnavljanje i izdavanje nove kvalificirane potvrde)

(1) Na zahtjev za obnavljanjem potvrda, ovjeritelj unosi ažurirane informacije o korisniku i sve druge izmjene koje su prethodno verificirane na isti način kao i u postupku registracije korisnika, sukladno čl. 15. i 16. ovoga Pravilnika.
(2) Ovjeritelj će izdati novu kvalificiranu potvrdu koristeći prethodno certificirani javni ključ korisnika samo ako je njegova kriptografska sigurnost još uvijek dovoljna za predviđeni novi životni ciklus potvrde i ako ne postoje indikacije da je korisnikov privatni ključ kompromitiran.

POGLAVLJE VII - Odgovornost i osiguranje

Članak 32.
(Odgovornost ovjeritelja u svezi certifikacijskih servisa)

Ovjeritelj je odgovoran da su svi certifikacijski servisi navedeni u politici certificiranja sukladno praktičnim pravilima.

Članak 33.
(Pružanje usluga certificiranja)

(1) Pružanje usluga certificiranja regulira se posebnim ugovorom između ovjerioca i korisnika.
(2) Ugovorom iz stava (1) ovog člana uređuje se sljedeće:
   a) obveza dostave tačnih i kompletnih informacija ovjeritelju sukladno proceduri registracije definiranom u politici certificiranja;
   b) korištenje privatnog ključa za formiranje sigurnog elektroničkog potpisa;
   c) način pristupa svom privatnom ključu;
   d) koristi kvalificiranu potvrdu samo uz siguran elektronički potpis koji je formiran sredstvima za formiranje sigurnog elektroničkog potpisa;
   e) ukoliko zahtijeva kvalificirana potvrda od ovjeritelja koja ispunjava uvjete iz Zakona o elektroničkom potpisu i ovoga Pravilnika, generira par ključeva za formiranje i provjeru sigurnog elektronskog potpisa u sredstvu za formiranje sigurnog elektroničkog potpisa koje je u cjelosti pod njegovom kontrolom;
   f) odmah obavjest ovjerioca ako prije isteka važnosti potvrde koji je naznačen u samoj potvrdi:
      1) korisnikov privatni ključ se izgubi, ukrade ili nastupi osnovana sumnja da je kompromitiran,
      2) prestane kontrola nad korištenjem korisnikovog privatnog ključa iz razloga kompromitiranja aktivacijskih podataka (PIN kod ili lozinka) za sredstvo za formiranje sigurnog elektroničkog potpisa ili drugih razloga,

3) ustanovi netočnost ili izmjenu sadržaja kvalificirane potvrde;

g) prekine korištenje svog privatnog ključa ukoliko postoji osnovana sumnja u kompromitiranje ključa ili kontrolu nad aktivacijskim podacima za sredstvo za formiranje sigurnog elektroničkog potpisa.

Članak 34.

(Obveze zainteresiranih stranaka)

U slučaju suspenzije ili opoziva kvalificirane potvrde, korisnik provjerava statusne informacije u svezi suspenzije ili opoziva potvrde koje je ovjeritelj javno objavio sukladno općim pravilima, uvažavajući sva ograničenja u korištenju kvalificirane potvrde koja su naznačena u samoj potvrdi ili objavljena u općim pravilima.

Članak 35.

(Financijska sposobnost ovjeritelja)

(1) Financijska sredstva ovjeritelja potrebna za obavljanje registrirane djelatnosti se prijavljuju i dokumentiraju Nadzornom tijelu, zajedno sa prijavom otpočinjanja djelatnosti.

(2) Ovjeritelj koji izdaju kvalificirane potvrde ili stavljaju na raspolaganje sigurne elektroničke postupke izrade potpisa, moraju posjedovati temeljni kapital u iznosu od najmanje 600.000,00 KM.

(3) Ovjeritelji koji izdaju kvalificirane potvrde ili stavljaju na raspolaganje sigurne elektroničke postupke izrade potpisa, moraju osim toga, istovremeno sa prijavom otpočinjanja svoje djelatnosti, dokazati Nadzornom tijelu da su zaključili osiguranje od odgovornosti sa minimalnom sumom osiguranja od 1.500.000,00 KM, koje pokriva najmanje tri osiguravajuća slučaja u godini.

(4) Od obveza iz st. (1) i (2) ovoga članka su oslobođeni ovjeritelji koji su zakonom uspostavljeni kao tijela državne uprave u Bosni i Hercegovini.

POGLAVLJE VIII - Čuvanje podataka

Članak 36.

(Čuvanje podataka)

(1) Ovjeritelj osigurava trajno čuvanje svih relevantnih podataka koje se tiču kvalificiranih potvrda.

(2) U svezi sa stavkom (1) ovoga članka, ovjeritelj osigurava:

a) tajnost i integritet tekućih i arhiviranih zapisa o kvalificiranim potvrdama;

b) kompletno i pouzdano arhiviranje podataka o kvalificiranim potvrdama sukladno općim pravilima;

c) da su zapisi u svezi kvalificiranih potvrda, kao i registracijske i druge podatke o korisniku, raspoloživi za potrebe pravnih poslova kao dokaz izvršene certifikacije;

d) pouzdano arhiviranje točnog vremena značajnih događaja u ovjeritelju;

e) da se podaci u svezi kvalificiranih potvrda čuvaju onoliko vremena koliko je potrebno da se koriste u pravnim poslovima vezanim za elektroničke potpise;

f) evidentiranje svih događaja na način da se ne mogu lako obrisati ili uništiti (izuzev u cilju prijenosa na dugotrajne medije za čuvanje) unutar vremenskog razdoblja u kome se moraju čuvati;

g) dokumentiranje specifičnih događaja i podataka koji treba da se evidentiraju;

h) evidentiranje svih događaja koji se odnose na registraciju korisnika, uključujući i zahtjeve za obnavljanjem potvrda, a naročito:

1) tip identifikacijskog dokumenta koji je prezentiran od strane korisnika,

2) jedinstveni identifikacijski podatak o korisniku preuzet iz identifikacijskog dokumenta,

3) mjesto čuvanja preslika aplikativnih i identifikacijskih dokumenata, uključujući i potpisan Ugovor sa korisnikom,

4) specifične informacije iz Ugovora sa korisnikom,

5) identitet službenika ovjeritelja koji je izvršio registraciju korisnika,

6) podatke o metodi koja je korištena za provjeru važenja identifikacijskih dokumenata,

i) ime ovjeritelja koje je primilo registracijske informacije;

j) zaštitu privatnosti podataka korisnika i evidentiranje svih događaja u svezi sa životnim ciklusom ključeva ovjeritelja;

k) evidentiranje svih događaja u svezi sa životnim ciklusom kvalificiranih potvrda i ključeva kojima upravlja ovjeritelj, uključujući i korisničke ključeve ako su generirani u ovjeritelju;

l) evidentiranje svih događaja koji se odnose na primjenu sredstava za formiranje sigurnog elektroničkog potpisa;

m) da se svi zahtjevi i izvješća koja se odnose na proceduru opoziva potvrda evidentiraju, uključujući i sve odgovarajuće aktivnosti.

Članak 37.

(Postupanje ovjeritelja u slučaju prestanka rada)

Ovjeritelj osigurava da u slučaju prestanka rada korisnik pretrpi minimalnu moguću štetu tako što će na propisan način čuvati podatake kao dokaz izvršene usluge, a naročito:

a) prije prestanka obavljanja djelatnosti, izvršava sljedeće aktivnosti:

1) informira sve korisnike o prestanku rada,

2) uništava, ili potpuno onemogućava korištenje, svojih privatnih ključeva koji su korišteni za formiranje sigurnog elektroničkog potpisa kvalificiranih potvrda;

b) osigurava neophodna financijska sredstva za realizaciju zahtjeva iz točke a) ovoga stavka;

c) općim pravilima definira proceduru prestanka rada, koja obuhvaća:

1) obavještavanje korisnika,

2) eventualni prijenos obveza drugim ovjeriteljima,

3) proceduru opoziva izdanih kvalificiranih potvrda kojima nije istekao rok važnosti, i prijenos listi opozvanih potvrda drugom ovjeritelju.

POGLAVLJE IX - Osiguranje uvjeta za korisnike za koje se generiraju podaci za formiranje sigurnog elektroničkog potpisa

Članak 38.

(Sredstvo za formiranje sigurnog elektroničkog potpisa)

Ovjeritelj može, uz usluge iz članka 4. ovoga Pravilnika, a sukladno svojim općim i posebnim pravilima, da osigura i sredstvo za formiranje sigurnog elektroničkog potpisa korisnicima i pridruženu lozinku (ili PIN kod) za aktivaciju sredstva, kao i njihovu sigurnu distribuciju do korisnika.

Članak 39.

(Ključevi korisnika)

Ovjeritelj osigurava da su ključevi korisnika koje on generira, generirani sigurno i da je osigurana tajnost privatnog ključa korisnika sve do njegove dostave korisniku i da pri isporuci samo korisnik ima pristup svom privatnom ključu.

Članak 40.

(Asimetrični par korisničkih ključeva)

Ovjeritelj osigurava da:

a) se asimetrični par korisničkih ključeva generira korištenjem algoritma koji je propisan da zadovolji zahtjeve koji se primjenjuju za sigurne elektroničke potpise;
b) su asimetrični ključevi korisnika propisane duljine i korišteni u propisanom asimetričnom kriptografskom algoritmu u cilju da se zadovolje propisani zahtjevi za implementacijom sigurnog elektroničkog potpisa.

Članak 41.

(Uvjeti sigurnosti sredstava za formiranje sigurnog elektroničkog potpisa)

Ukoliko ovjeritelj osigura sredstva za formiranje sigurnog elektroničkog potpisa za korisnike, to čini na siguran način a naročito osigurava da:

a) prijem sredstva za formiranje sigurnog elektroničkog potpisa mora biti sigurno kontroliran od strane ovjeritelja;
b) sredstva za formiranje sigurnog elektroničkog potpisa moraju biti sigurno čuvana i distribuirana;
c) deaktiviranje i reaktiviranje sredstava za formiranje sigurnog elektroničkog potpisa mora biti sigurno kontrolirano od strane ovjeritelja;
d) ukoliko sredstvo za formiranje sigurnog elektroničkog potpisa ima pridružene aktivacijske podatke (PIN kod ili lozinka) isti mora biti sigurno pripremljen i šalju odvojeno u odnosu na sredstvo za formiranje sigurnog elektroničkog potpisa, u različito vrijeme ili na različit način.

Članak 42.

(Tajnost identifikacijskih podataka)

(1) Ovjeritelj koji izdaje kvalificirane potvrde i koji osigurava sredstvo za formiranje sigurnog elektroničkog potpisa (engl. SSCD: Secure Signature – Creation Device) korisnicima garantiraju tajnost identifikacijskih podataka (PIN kod, lozinka), nakon što se ugrade u ista.
(2) Ovlaštena osoba ovjeritelja kvalificiranu potvrdu, uz osiguranje SSCD korisnicima, kvalificiranu potvrdu uručuje osobno korisniku uz svojeručni potpis korisnika o uručenju iste ili istu dostavlja u elektroničkom obliku sigurnim elektroničkim potpisom datog korisnika.
(3) Kvalificirana potvrda iz stavka (1) ovoga članka se verificira i stavlja na raspolaganje trećim osobama tek nakon potvrde primitka SSCD uređaja i odgovarajućih identifikacijskih podataka, uz dopuštenje korisnika.

POGLAVLJE X - Fizička zaštita

Članak 43.

(Kontrola fizičkog pristupa)

Ovjeritelj osigurava kontrolu fizičkog pristupa svojim sigurnosno kritičnim resursima i minimalan rizik u pristupu svojim ključnim elementima sustava.

Članak 44.

(Mjere koje poduzima ovjeritelj)

Ovjeritelj osigurava da:

a) se fizički pristup prostorijama u kojima se obavlja generiranje kvalificiranih potvrda, prijem sredstava za formiranje sigurnog elektroničkog potpisa i upravljanje procedurom opoziva potvrda, ograniči samo na pouzdano autorizirane osobe;
b) su implementirane neophodne mjere u cilju izbjegavanja gubitaka, oštećenja ili kompromitiranja ključnih resursa i eliminiranje mogućnosti prekida poslovnih aktivnosti;
c) se implementiraju odgovarajuće mjere za sprječavanje kompromitiranja ili neovlaštenog preuzimanja informacija i uređaja za procesiranje informacija;
d) su prostorije u kojima se vrši generiranje kvalificiranih potvrda, prijem sredstava za formiranje sigurnog elektroničkog potpisa i upravljanje opozivom, takve da se operativni rad u njima odvija u okruženju koje osigurava fizičku zaštitu certifikacijskih servisa i resursa u slučaju zlouporabe prilikom neautoriziranog pristupa sustavu i podacima;
e) je fizička zaštita uspostavljena kreiranjem jasno definiranih sigurnosnih fizičkih barijera kojima se štite procesi generiranja kvalificiranih potvrda, osiguranje sredstava za formiranje sigurnog elektroničkog potpisa i upravljanje opozivom;
f) su implementirane odgovarajuće fizičke mjere i kontrole sigurnosnog okruženja u cilju zaštite prostorija i sustavskih elemenata ovjeritelja;
g) su implementirane odgovarajuće mjere u cilju zaštite uređaja, informacija, memorijskih medija i softvera od otuđivanja sa lokacije bez propisne autorizacije;
h) se i druge specifične sigurnosne funkcije mogu primijeniti unutar istog sigurnog prostora koji osigurava pristup samo autoriziranim uposlenim osobama.

Članak 45.

(Osiguranje pristupa sustavu certificiranja)

Ovjeritelj je dužan da pristup sustavu certificiranja ograniči isključivo na autorizirane osobe, a naročito osigurava:

a) implementaciju kontrola na mrežnoj razini u cilju zaštite interne mreže ovjeritelja od eksternih mrežnih domena kojima može pristupiti treća strana, uz zabranu svih protokola i pristupa koji se ne koriste u operativnom radu ovjeritelja;
b) pouzdanu zaštitu osjetljivih podataka, koji uključuju i podatke o registraciji korisnika, tijekom prolaska kroz dijelove mreže koji nisu sigurni;
c) učinkovitu i pouzdanu administraciju korisničkih pristupa (uključujući operatore, administratore i bilo koje specifične korisnike koji imaju izravni pristup sustavu) u cilju održavanja sigurnosti sustava, uključujući i upravljanje nalozima korisnika, evidentiranje i mogućnost modificiranja i zabrane pristupa;
d) strogo ograničen pristup informacijama i aplikativnim funkcijama sustava sukladno općim i posebnim pravilima i politikom kontrole pristupa, identificiranom u njima, kao i dovoljnu računalsko-sigurnosnu kontrolu u cilju razdvajanja sigurnosnih funkcija u sustavu koje su identificirane u općim pravilima, uključujući razdvajanje funkcija administratora sigurnosti i operatera, a rad sa korisničkim programima za upravljanje sustavom mora biti posebno ograničen i strogo kontroliran;
e) pouzdanu identifikaciju i autentikaciju uposlenih kod ovjeritelja prije korištenja kritičnih operacija vezanih za procedure upravljanja potvrdama;
f) evidentiranje svih aktivnosti uposlenih kod ovjeritelja na temelju odgovarajućih korisničkih naloga i log fajlova, koji su potpisani sigurnim elektroničkim potpisom;
g) pouzdanu zaštitu sigurnosno osetljivih podataka, koji uključuju i registracijske podatke korisnika, od

neautoriziranog pristupa prethodno obrisanim ili arhiviranim podacima;

h) da se lokalne fizičke mrežne komponente čuvaju u fizički zaštićenom okruženju i da se njihova konfiguracija periodično kontrolira u cilju ispitivanja usklađenosti sa zahtjevima specificiranim u općim i posebnim pravilima;

i) stalno nadziranje i alarmiranje koristeći sustave za detekciju napada i nadziranje kontrole pristupa i alarma u cilju pouzdane detekcije, registracije i reakcije na neautoriziran ili neregularan pokušaj pristupa resursima koji se koriste za pružanje usluga certifikacije;

j) da aplikacija za distribuciju potvrda primijenjuje sustav logičke kontrole pristupa u cilju sprječavanja pokušaja dodavanja ili brisanja odgovarajućih potvrda i izmjene drugih pridruženih informacija;

k) da aplikacija za dobivanje statusa opoziva potvrda primjenjuje sustav logičke kontrole pristupa u cilju sprječavanja pokušaja izmjene informacija o statusu opoziva potvrda.

POGLAVLJE XI - Informacije o uvjetima izdavanja i korištenja potvrda

Članak 46.

(Raspoloživost informacije)

(1) Ovjeritelj osigurava da informacije o uvjetima izdavanja i korištenja kvalificirani potvrda budu raspoložive korisnicima i drugim zainteresiranim strankama.

(2) Raspoloživost informacija iz stavka (1) ovoga članka osigurava se korištenjem jednostavnih vidova komunikacije (Internet i sl.) sa osiguranim integritetom tijekom vremena, da se mogu prenositi elektroničkim putem i da su prikazane na potpuno razumljiv način.

Članak 47.

(Način osiguranja raspoloživosti informacija)

Ovjeritelj osigurava raspoloživost informacija i podataka o svom poslovanju, i to:

a) opća pravila ovjeritelja koja su trenutno važeća;
b) ograničenja u korištenju općih pravila;
c) obveze korisnika;
d) informacije o načinu provjere važnosti kvalificiranih potvrda, uključujući i zahtjeve za provjeru statusa opoziva potvrda;
e) ograničenja odgovornosti koja uključuju slučajeve za koje ovjeritelj prihvata ili odbija odgovornost;
f) vremensko razdoblje čuvanja registracijskih informacija korisnika;
g) vremensko razfoblje čuvanja log fajlova za evidentiranje;
h) proceduru u slučaju podnošenja žalbi;
i) proceduru u slučaju spora;

XII - Upravljanje potvrdama

Članak 48.

(Uvid u kvalificiranu potvrdu)

Ovjeritelj osigurava uvid u status kvalificirane potvrde svim korisnicima i zainteresiranim strankama bez uvida u sadržaj iste.

Članak 49.

(Raspoloživost podataka iz kvalificirane potvrde)

(1) Ovjeritelj osigurava:

a) da je kvalificirana potvrda raspoloživa korisniku kojem je izdana;
b) da je kvalificirana potvrda raspoloživa trećim osobama samo po odobrenju korisnika, a sukladno općim pravilima ovjeritelja;
c) jednostavnu identifikaciju informacija o uvjetima izdavanja i korištenja kvalificiranih potvrda svim zainteresiranim strankama u sustavu;
d) da su informacije navedene pod toč. b) i c) ovoga stavka raspoložive 24 časa na dan, sedam dana u sedmici;

(2) U slučaju pada sustava ili djelimičnog gubitka mogućnosti za osiguranje servisa, ovjeritelj je obvezan poduzeti sve raspoložive mjere u cilju aktiviranja informacijskog servisa, najkasnije do isteka roka predviđenog u općim pravilima.

POGLAVLJE XIII - Provjera ispunjenosti uvjeta za izdavanje kvalificiranih potvrda

Članak 50.

(Provjera ispunjenosti uvjeta)

Provjeru ispunjenosti uvjeta za izdavanje kvalificiranih potvrda vrši Nadzorno tijelo u postupku razmatranja zahtjeva ovjeritelja za upis u Registar ovjeritelja.

Članak 51.

(Ispunjavanje uvjeta)

Provjera ispunjenosti uvjeta za izdavanje kvalificiranih potvrda obuhvaća:

a) provjeru općih pravila i posebnih pravila rada ovjeritelja i njihove usklađenosti sa Zakonom i podzakonskim aktima;
b) provjeru atesta i certifikacije tehničkih i sigurnosnih komponenata koje koristi ovjeritelj za generiranje javnih i privatnih ključeva i izdavanje kvalificiranih potvrda.

Članak 52.

(Provjera operativnog rada ovjeritelja)

Provjera operativnog rada ovjeritelja obuhvaća:

a) proceduru registracije korisnika kome se izdaje kvalificirana potvrda;
b) proceduru prijema zahtjeva za izdavanjem kvalificirane potvrde u registracijskom autoritetu;
c) proceduru dostavljanja zahtjeva do ovjeritelja;
d) proceduru generiranja kvalificirane potvrde;
e) korištenje sigurnih sustava za čuvanje podataka za generiranje kvalificiranih potvrda;
f) korištenje sigurnih hardverskih sredstava za formiranje sigurnog elektroničkog potpisa (hardverski moduli zaštite (HSM - Hardware Security Module));
g) proceduru dostave kvalificirane potvrde, uređaja za generiranje elektroničkog potpisa i identifikacijskih podataka korisnicima;
h) proceduru opoziva potvrde;
i) proceduru obnavljanja potvrde;
j) proceduru suspenzije potvrde;
k) način objavljivanja liste opozvanih i suspendiranih potvrda;
l) sustave fizičke kontrole pristupa u prostorije ovjeritelja;
m) sustave logičke kontrole pristupa računalskim resursima ovjeritelja;
n) sustav za javno objavljivanje temeljnih informacija o pružanju usluga certifikacije, kao i općih pravila rada ovjeritelja.

Članak 53.

(Provjera tehničkih i sigurnosnih komponenti)

Provjera tehničkih i sigurnosnih komponenti koje koristi ovjeritelj obuhvaća:

a) realizaciju sustavskih zahtjeva sigurnosti;
b) izdavanje kvalificiranih potvrda primjenom sigurnog elektroničkog potpisa;

c) sigurno generiranje ključeva ovjeritelja.

Članak 54.
(Operativni rad ovjeritelja)

Operativni rad ovjeritelja se obavlja sukladno standardu CEN WorkshopAgreement 14167-1 (March 2003) "Security Requirements for Trustworthy SystemsManaging Sertificates for Electronic Signatures - Part 1: System Security Requirements".

Članak 55.
(Stupanje na snagu)

Ovaj Pravilnik stupa na snagu narednog dana od dana objave u "Službenom glasniku BiH".

VM broj 14/17
18. siječnja 2017. godine
Sarajevo

Predsjedatelj
Vijeća ministara BiH
Dr. **Denis Zvizdić**, v. r.

На основу члана 17. Закона о Савјету министара Босне и Херцеговине ("Службени гласник БиХ", бр. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 и 24/08) и члана 26. став (1) Закона о електронском потпису ("Службени гласник БиХ", број 91/06), на приједлог министра комуникација и транспорта Босне и Херцеговине, Савјет министара Босне и Херцеговине на 88. сједници, одржаној 18. јануара 2017. године, донио је

ПРАВИЛНИК
О БЛИЖИМ УСЛОВИМА ЗА ИЗДАВАЊЕ КВАЛИФИЦИКОВАНИХ ПОТВРДА

ГЛАВА I – Опште одредбе

Члан 1.
(Предмет Правилника)

Овим Правилником прописују се ближи услови за издавање квалификованих потврда и услови које овјерилац мора испуњавати за издавање квалификованих потврда.

Члан 2.
(Примјена међународних стандарда)

(1) Приликом издавања квалификованих потврда примјењују се међународни стандарди и препоруке, као и други одговарајући стандарди, докумената и препорука.
(2) Овјерилац за издавање квалификованих потврда (у даљем тексту: овјерилац) издаје квалификоване потврде корисницима у складу са документима 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 and Certificate Revocation List (CRL) Profile" i ETSI TS 102 280 "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".

ГЛАВА II – Поуздано обављање услуга издавања квалификованих потврда

Члан 3.
(Начин формирања безбједног електронског потписа)

Овјерилац издаје квалификоване потврде формирањем безбједног електронског потписа на основу свог приватног кључа и асиметричног криптографског алгоритма, на начин прописан Правилником о техничко-технолошким поступцима за формирање безбједног електронског потписа и условима и критеријима, које треба да испуне средства за формирање безбједног електронског потписа.

Члан 4.
(Услуге сертификације)

(1) Овјерилац је дужан обезбиједити потпуну услугу сертификације која укључује сљедеће сервисе, и то:
   а) регистрацију корисника;
   б) формирање квалификованих потврда;
   ц) дистрибуцију квалификованих потврда корисницима;
   д) управљање животним вијеком (обнављање, суспензија, опозив) квалификованих потврда;
   е) обезбјеђивање поузданог и јавно доступног сервиса за провјеру статуса опозваности квалификованих потврда.
(2) Овјерилац може, поред сервиса из става (1) овог члана, да обезбиједи и формирање асиметричног пара кључева за кориснике, као и дистрибуцију приватног кључа и потврде кориснику на безбједан начин, уколико је то прописано у политици сертификације датог овјериоца.

Члан 5.
(Општи акти овјериоца)

(1) Овјерилац, прије почетка рада, доноси општа интерна правила пружања услуге сертификације (у даљем тексту: општа правила) која корисницима пружају довољно информација на основу којих се могу одлучити о прихватању услуга и о обиму услуга.
(2) Општа правила функционисања овјериоца треба да буду у складу са документима RFC 3647 "Internet X.509 Public Key Infrastructure. Certificate Policy and CertificationPractices Framework" и ETSI TS 101 456 "Policy Requirements for Certification Authorities Issuing Qualified Certificates".
(3) На основу општих правила овјерилац доноси сљедеће опште акте:
   а) Политику сертификације (енгл. Certificate Policy);
   б) Практична правила пружања услуге сертификације (енгл. Certification Practices Statement) (у даљем тексту: практична правила).

Члан 6.
(Политика сертификације и практична правила)

(1) Политика сертификације и практична правила су јавни документи.
(2) Политика сертификације дефинише предмет рада и захтјеве пословања овјериоца.
(3) Практична правила дефинишу процесе и начин њиховог коришћења при формирању и управљању квалификованим потврдама, оперативне процедуре у циљу испуњења тих захтјева и начин на који овјерилац испуњава техничке, организационе и процедуралне захтјеве пословања који су идентификовани у политици сертификације.
(4) Политиком сертификације и практичним правилима уређују се сљедеће области:
   а) опште одредбе о раду овјериоца:
      1) појам овјериоца,
      2) сертификационе услуге,
      3) обухват документа политика сертификације,
      4) обухват документа практичних правила пружања услуге сертификације,
      5) корисничке услуге сертификације.
   б) уводне одредбе о политици издавања квалификованих потврда;
   ц) обавезе и одговорности овјериоца и корисника;
   д) функционалне захтјеве за рад овјериоца: оперативне процедуре рада овјериоца и процедуре управљања животним циклусом криптографских кључева:
      1) генерисање кључа овјериоца,
      2) процедуре чувања и формирања резервних копија кључева овјериоца,

3) дистрибуцију јавног кључа овјериоца,
4) коришћење кључа овјериоца,
5) крај животног циклуса кључа овјериоца,
6) управљање животним циклусом криптографског хардвера који се користи за генерисање квалификованих потврда,
7) управљање кључевима корисника за идентификацију,
8) процедуру примјене средстава за формирање безбједног електронског потписа.

е) процедуре управљања животним циклусом сертификата:
1) методе регистрације корисника,
2) издавање потврда,
3) дистрибуцију потврда,
4) обнављање потврда,
5) суспензију потврда,
6) опозив потврда,
7) начин публикације листе опозваних потврда;

ф) управљање оперативним радом овјериоца:
1) управљање у складу са безбједносним принципима,
2) управљање и класификација најважнијих информација и подацима у оквиру овјериоца,
3) кадровски ресурси,
4) систем физичке безбједности и безбједности окружења,
5) управљање радом овјериоца,
6) управљање системом контроле приступа,
7) употребу и одржавање безбједним криптографских система,
8) управљање процедурама континуалног пословања у инцидентним ситуацијама,
9) престанак рада овјериоца,
10) усаглашеност рада са критеријумима за рад овјерилаца који издају квалификоване потврде у складу са чланом 8. Закона и овим Правилником,
11) формирање и чување документације која се односи на квалификоване потврде.

г) организацију рада овјериоца.

Члан 7.
(Способност за обезбјеђење услуге)

Овјерилац демонстрира способност за обезбјеђење услуге издавања квалификованих потврда, уколико:

а) посједује практична правила, и у њима дефинисане процедуре, у којима се спецификује начин испуњења свих захтјева за издавањем квалификованих потврда који су идентификовани у политици сертификације;
б) доступним практична правила свим корисницима и другим заинтересованим странама;
ц) учини доступним свим корисницима и потенцијалним заинтересованим странама услове коришћења квалификованих потврда;
д) посједује управну структуру највишег нивоа која има коначну ауторизацију и одговорност за објављивање практичних правила овјериоца;
е) посједује управну структуру оперативног нивоа у овјериоцу која је одговорна за исправну примјену практичних правила;
ф) дефинише поступак периодичне анализе и ревизије практичних правила;
г) посједује све измјене практичних правила, јавно објављене и одобрене од стране управне структуре највишег нивоа.

Члан 8.
(Посебна интерна правила)

(1) Овјерилац утврђује и посебна интерна правила рада овјериоца и заштите система сертификације (у даљем тексту: посебна правила) у којима су садржани и детаљно описани поступци и мјере које се примјењују приликом издавања и поступања квалификованим потврдама.
(2) Посебна правила су приватни документ и представљају пословну тајну овјериоца.

Члан 9.
(Посебна правила)

Посебна правила садрже одредбе којим се ближе уређује:

а) систем физичке контроле приступа у поједине просторије овјериоца;
б) систем логичке контроле приступа рачунарским ресурсима овјериоца;
ц) систем чувања приватног кључа овјериоца;
д) систем додијељене одговорности при активацији приватног кључа овјериоца и
е) поступци и радње у ванредним ситуацијама (пожари, поплаве, земљотреси, друге временске непогоде, злонамјерни упади у просторије или информациони систем овјериоца).

Члан 10.
(Организација рада)

Овјерилац обезбјеђује поуздану организацију рада тако што:

а) доноси правила и оперативне процедуре које нису дискриминаторске;
б) чини доступним своје сервисе свим корисницима чије су активности у складу са објављеним општим правилима;
ц) послује као правно лице у складу са прописима;
д) има систем квалитета и систем безбједног управљања квалификованим потврдама у складу са услугама сертификације које пружа;
е) посједује обезбјеђење од одговорности за штету, која може да проистекне у вршењу његових активности у складу са политиком сертификације;
ф) има финансијску стабилност и довољне ресурсе који се захтијевају у пружању услуга сертификације у складу са политиком сертификације;
г) има довољан број стално запослених на пословима сертификације са неопходним образовањем, нивоом обучености, техничким знањима и искуством;
х) ефикасно поступа приликом рјешавања жалби и спорова са корисницима или другим заинтересованим странама у вези пружања услуга сертификације;
и) пружа независност дијелова овјериоца укључених у послове генерисања квалификованих потврда од других спољних организација у сфери пружања услуга сертификације. Посебно управне структуре овјериоца, као и запослених са безбједносним функцијама, морају бити заштићени од било каквих финансијских и других притисака који могу утицати на повјерење у услуге сертификације које пружа овјерилац;
ј) има прописно документирану структуру дијелова овјериоца повезаних са генерисањем квалификованих потврда ради обезбјеђења

непристрасности у пружању услуга сертификације, у складу са општим и посебним правилима.

Члан 11.

(Обезбјеђење од одговорности за штету)

Овјерилац је дужан обезбиједити најнижи износ осигурања од ризика одговорности за штету насталу вршењем услуга издавања електронских потврда, тако да:

а) осигурана сума на коју мора бити уговорено осигурање по једном штетном догађају не може износити мање од 50.000 КМ, подразумијевајући притом као штетни догађај појединачну штету насталу употребом једне квалификоване потврде у једном акту у правном промету;

б) укупна осигурана сума на коју мора бити уговорено осигурање од одговорности овјериоца кумулативно на годишњем нивоу, по свим штетним догађајима, не може бити нижа од 1.500.000,00 КМ.

Члан 12.

(Поступање овјериоца у случају ванредних околности)

Овјерилац обезбјеђује да у случају ванредних околности оперативни рад буде обновљен што је могуће прије а у складу са општим и посебним правилима. У случају компромитовања свог асиметричног приватног кључа, овјерилац:

а) престаје са издавањем квалифицикованих потврда;

б) информише све кориснике и друге заинтересоване стране о компромитовању приватног кључа;

ц) јавно објављује информације о томе да издате квалификоване потврде, као и информације о статусу опозваности квалификованих потврда, више нису важеће;

д) врши опозив свих издатих квалификованих потврда одмах а најкасније у року од 24 сата у складу са чланом 10. Закона о електронском потпису ("Службени гласник БиХ", број 91/06, у даљем тексту: Закон).

Члан 13.

(Евиденција издатих квалификованих потврда)

(1) Овјерилац води ажурну, тачну и сигурну евиденцију издатих квалификованих потврда која може бити јавно доступна, осим у случајевима када власник потврде изричито захтијева да његови подаци не буду јавно доступни.

(2) Овјерилац води ажурну и сигурну евиденцију опозваних и суспендованих квалификованих потврда и мора за сваку потврду коју је издало, информацију о његовој валидности учинити јавно доступном.

(3) За тачност и валидност евиденција из ст. (1) и (2) овог члана гарантује овјерилац, својом квалификованом потврдом.

Члан 14.

(Одређивање времена издавања и опозива)

(1) За одређивање времена издавања и опозива квалификованих потврда, овјерилац обезбјеђује извор тачног времена који је синхронизован са извором референтног времена којег одреди Надзорни орган и објављује на службеној Интернет страници Надзорног органа.

(2) Вријеме издавања квалификоване потврде овјерилац уписује у издату квалификовану потврду.

(3) Вријеме издавања и опозива квалификованих потврда овјерилац чува у евиденцији издатих и опозваних потврда из члана 13. овог Правилника.

ГЛАВА III - Регистрација корисника

Члан 15.

(Регистрација корисника)

(1) Овјерилац врши поуздану идентификацију и аутентикацију корисника у циљу издавања квалификоване потврде, те води регистар потврда.

(2) Поступке регистрације из става (1) овог члана врши овлашћени службеник овјериоца.

Члан 16.

(Обавезе овјериоца у поступку регистрације корисника)

У поступку регистрације корисника, овјерилац је дужан обезбиједити да:

а) се корисник идентификује као физичко лице са специфичним атрибутима који могу означавати организациону јединицу или улогу у организацији гдје је запослен;

б) прије успостављања уговорног односа са корисником, јавно информише корисника на јасан и недвосмислен начин о свим релевантним условима коришћења квалификованих потврда;

ц) се у поступку регистрације, идентитет корисника физичког лица, утврђује непосредним увидом у важећи идентификациони документ у присуству подносиоца захтјева;

д) уколико се ради о кориснику, правном лицу се изврши увид у:

1) извод из судског регистра из којег се може утврдити ко је одговорно лице у правном лицу,

2) акт којим је корисник овлашћен од стране тог правног лица или организације за добијање квалификоване потврде;

е) се у изузетном случају утврђује сваки специфични атрибут корисника коме се издаје квалификована потврда;

ф) информације садржане у квалификованој потврди буду поуздане и тачне;

г) корисник достави тачне и поуздане информације о физичкој адреси, или другим атрибутима, који описују како се корисник може контактирати;

х) се чувају све информације коришћене за верификацију идентитета корисника и документацију коришћену за идентификацију, као и било која ограничења њене важности;

и) се закључи уговор са корисником којим се регулише сљедеће:

1) обавеза корисника да користи средство за формирање безбједног електронског потписа које обезбјеђује овјерилац у складу са општм правилима,

2) обавеза овјериоца да чува податке коришћене у регистрацији корисника и све информације о животном циклусу издате квалификоване потврде корисника.

3) услови под којима се објављује потврда,

4) клаузулу о тачности података садржаних у потврди;

ј) ако асиметрични пар кључева корисника није генерисан од стране овјериоца, процес генерисања захтијева за квалификованом потврдом у потпуности обезбјеђује да корисник посједује приватни кључ који је математички повезан са

јавним кључем који је презентован за сертификацију. У том случају корисник мора обезбиједити да се асиметрични пар кључева генерише искључиво у средству за формирање безбједног електронског потписа;

к) се поштују одредбе важећих прописа којима је уређена област заштите личних података.

ГЛАВА IV - Кадровски ресурси и управљање оперативним радом овјериоца

Члан 17.

(Функционисање овјериоца)

Овјерилац је дужан обезбиједити поуздано, безбједно и несметано обављање послова издавања квалификоване потврде.

Члан 18.

(Људски ресурси)

(1) Овјерилац обезбјеђује да запослени у овјериоцу посједују неопходно потребну квалификацију, искуство и експертско знање, за обављање послова овјериоца, и то:
   а) потребан број запослених са високом школском спремом из области информационо-комуникационих технологија,
   б) радно искуство запослених од најмање 3 године на пословима одржавања и безбједности информационих система,
   ц) положен испит из области безбједности информационих система,
   д) посједовање специфичних вјештина и искуства,
   е) да посједују експертизу у технологији електронског потписа, да су добро упознати са безбједносним процедурама за запослене и са одговорностима у домену безбједности, као и да имају одговарајућа искуства у примјени безбједних информационих система и процјени ризика.

(2) Овјерилац је дужан обезбиједити сљедеће безбједносне функције у овјериоцу за:
   а) главног администратора безбједности - свеукупну одговорност за администрирање и имплементацију безбједносних функција и процедура, као и управљање активностима на додатном унапређењу послова генерисања, опозива и суспензије квалификованих потврда,
   б) систем администраторе - ауторизовану одговорност за инсталацију, конфигурисање и одржавање безбједних система овјериоца за регистрацију корисника, генерисање квалификованих потврда, обезбјеђење средстава за формирање безбједног електронског потписа за кориснике и управљање опозивом квалификованих потврда,
   ц) систем операторе - одговорност за рад безбједних система овјериоца у текућем раду на дневном нивоу и ауторизовану одговорност за имплементацију система за формирање резервних копија и процедуре опоравка,
   д) систем евидентичаре - ауторизовану одговорност за прегледање и одржавање архива и лог фајлова безбједних система овјериоца;

(3) Одговорно лице у овјериоцу, вршиоцима послова из става (2) овог члана, посебним актом утврђује безбједносне функције.

(4) У опису сваког радног мјеста у овјериоцу, улога и степен безбједности утврђене у општим правилима, морају бити јасно и прецизно наведене, са нагласком на степен повјерљивости.

(5) Запослени у овјериоцу који имају одређен степен безбједносне функције не смију бити у сукобу интереса који могу утицати на непристрасност рада овјериоца.

(6) Безбједносне функције не могу се додијелити лицу које је осуђивано за радње које су у вези са пословима које обављају код овјериоца. Приступ безбједносним функцијама обезбјеђује се по окончању прописаних провјера.

ГЛАВА V - Поуздани и безбједни криптографски системи

Члан 19.

(Коришћење безбједних система)

Овјерилац користи безбједне системе и производе који су заштићени од неовлашћених модификација.

Члан 20.

(Анализа ризика)

Овјерилац врши анализу ризика којом идентификује критичне сервисе који захтијевају коришћење безбједних система и високе нивое безбједности:

а) прије почетка обављања услуга сертификације,

б) током оперативног рада по потреби, а најмање сваких шест мјесеци.

Члан 21.

(Безбједно и коректно функционисање система)

Овјерилац обезбјеђује безбједно и коректно функционисање својих система, са минималним ризиком од кварова, а нарочито:

а) заштиту интегритета система овјериоца и информација од вируса, малициозног и неауторизованог софтвера;

б) минималан ризик од штете усљед могућих инцидената коришћењем процедура извјештавања, брзим и координисаним реаговањем на безбједносне инциденте у циљу смањења утицаја безбједносних упада;

ц) безбједно коришћење меморијских медија у складу са унапријед специфікованим шемама класификације информација. Медији који нису у оперативном раду, безбједносно осјетљиве податке морају безбједно архивирани;

д) успоставити и имплементисати процедуре за све безбједне и административне функције које имају утицај на пружање услуга сертификације. Одговорно лице овјериоца је одговорно за планирање и ефикасну имплементацију општих правила;

е) сталним надзором текућих и планираних потреба за капацитетом система овјериоца ради обезбјеђења адекватне процесне снаге и меморијских капацитета.

Члан 22.

(Асиметрични кључеви)

(1) Асиметрични кључеви могу бити јавни и приватни;

(2) Овјерилац обезбјеђује да се његови асиметрични кључеви генеришу у строго контролисаним и безбједним условима, а нарочито да се:
   а) генерисање асиметричних кључева врши у физички заштићеном окружењу од стране и уз минималан број ауторизованих запослених (најмање два запослена лица) за извршавање ове функције а према захтјевима и процедурама дефинисаним у практичним правилима;

b) генерисање асиметричних кључева врши у средству које:
   1) задовољава захтјеве из стандарда FIPS PUB 140-2 ниво 3 и виши или
   2) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)" или
   3) задовољава захтјеве из стандарда 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)";

(3) Резервне копије приватних кључева за формирање безбједног електронског потписа квалификованих потврда имају исти или виши ниво безбједносних контрола у односу на кључеве који се оперативно користе.

(4) Овјерилац обезбјеђује да су издате квалификоване потврде потписане безбједним електронским потписом овјериоца.

Члан 23.

(Заштита тајности и интегритета)

Овјерилац обезбјеђује заштиту тајности и интегритет приватних кључева, а нарочито:

а) чување и коришћење приватног кључа за формирање безбједног електронског потписа у безбједном криптографском уређају који:
   1) задовољава захтјеве из стандарда FIPS PUB 140-2 ниво 3 и виши или
   2) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)" или
   3) задовољава захтјеве из стандарда 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)";

б) да су дијелови за активацију приватног кључа овјериоца, када се налазе изван криптографског уређаја шифровани коришћењем симетричног алгоритма и дужине кључа, и омогућавају поуздану одбрану од криптоаналитичких напада;

ц) чување дијелова за активацију приватног кључа, уз обезбјеђења резервних копија тих дијелова, и активација коју врше запослени који имају безбједносне функције, уз коришћење најмање двоструке контроле у физички обезбијеђеном окружењу;

д) да се мјерама логичке контроле приступа онемогући неовлашћено активирање криптографског уређаја са приватним кључем овјериоца.

Члан 24.

(Верификација безбједног електронског потписа)

Овјерилац обезбјеђује да његов јавни кључ којим се верификује безбједни електронски потпис квалификованих потврда буде расположив свим корисницима и другим заинтересованим странама на начин којим се обезбјеђује аутентичност и интегритет јавног кључа.

Члан 25.

(Јавни кључ)

Овјерилац доставља свој јавни кључ и локацију листе опозваних потврда корисницима и другим заинтересованим странама на безбједан начин у облику квалификоване потврде или листе опозваних потврда.

Члан 26.

(Коришћење приватног кључа)

(1) Овјерилац користи свој приватни кључ у складу са општим и посебним правилима и обезбјеђује:
   а) да се користи искључиво за формирање безбједног електронског потписа квалификованих потврда, као и безбједног електронског потписа листе опозваних потврда;
   б) да се користи само у оквиру физички заштићених просторија овјериоца.

(2) Овјерилац обезбјеђује да се његови приватни кључеви не користе након истека њиховог животног циклуса, у складу са општим и посебним правилима.

(3) Приватни кључеви, из става (2) овог члана, уништавају се на начин којим се обезбјеђује да исти не може бити поново формиран.

Члан 27.

(Безбједност криптографских уређаја)

Овјерилац обезбјеђује безбједност криптографских уређаја који се користе за генерисање и чување кључева и формирање безбједног електронског потписа током животног циклуса уређаја, у складу са посебним правилима, а нарочито да:

а) криптографски уређај није компромитован током транспорта;

б) криптографски уређај није компромитован за вријеме чувања код овјериоца;

ц) процедуре инсталације активације, креирања резервних копија и поновног формирања приватног кључа у криптографском уређају врши се у присуству најмање два запослена којима је додијељена безбједност функција;

д) исправност функционисања криптографског уређаја;

е) да се приватни кључеви овјериоца чувани у криптографском уређају уништавају након краја животног циклуса кључева или уређаја.

ГЛАВА VI - Заштита потврда и тајности генерисаних кључева

Члан 28.

(Процес генерисања квалификованих потврда)

Овјерилац обезбјеђује безбједан процес генерисања квалификованих потврда ради обезбјеђења њихове аутентичности и интегритета.

Члан 29.

(Остале обавезе овјериоца)

Овјерилац обезбјеђује:

а) да се квалификоване потврде генеришу у складу са форматом дефинисаним у документима ETSI TS 101 862, RFC 3739, RFC 3280 i ETSI TS 102 280;

б) да је процедура генерисања квалификоване потврде безбједно повезана са одговарајућим процедурама регистрације корисника, обнављања потврда уз задржавање постојећег или генерисање новог пара кључева;

ц) у случају да овјерилац генерише корисникове кључеве обезбјеђује:

1) да је процедура генерисања квалификоване потврде безбједно повезана са процедуром генерисања асиметричног пара кључева од стране овјериоца,
2) да је приватни кључ, односно средство за формирање безбједног електронског потписа, безбједно достављено до регистрованог корисника, а да се активациони код средства за формирање безбједног електронског потписа овлашћеном лицу достави на безбједан начин другим путем;

д) јединственост додијељеног имена кориснику у оквиру домена овјериоца;
е) тајност и интегритет регистрационих података, и то посебно у случајевима размјене података са корисником или у случају размјене информација између дистрибуираних компоненти овјериоца;
ф) верификацију достављених регистрационих података.

Члан 30.

(Обнављање и издавање нове квалификоване потврду)

Овјерилац обезбјеђује да се на захтјев корисника раније опозвана квалификована потврда обнавља или издаје нова уколико су исти комплетни, тачни и ауторизовани.

Члан 31.

(Захтјеви за обнављање и издавање нове квалификоване потврде)

(1) На захтјев за обнављањем потврда, овјерилац уноси ажуриране информације о кориснику и све друге измјене које су претходно верификоване на исти начин као и у поступку регистрације корисника, у складу са чл. 15. и 16. овог Правилника.
(2) Овјерилац ће издати нову квалификовану потврду користећи претходно сертификовани јавни кључ корисника само ако је његова криптографска безбједност још увијек довољна за предвиђени нови животни циклус потврде и ако не постоје индикације да је корисников приватни кључ компромитован.

ГЛАВА VII - Одговорност и обезбјеђење

Члан 32.

(Одговорност овјериоцу у вези сертификационих сервиса)

Овјерилац је одговоран да су сви сертификациони сервиси наведени у политици сертификовања у складу са практичним правилима.

Члан 33.

(Пружање услуга сертификовања)

(1) Пружање услуга сертификовања регулише се посебним уговором између овјериоца и корисника.
(2) Уговором из става (1) овог члана уређује се сљедеће:
а) обавеза достављања тачних и комплетних информација овјериоцу у складу са процедуром регистрације дефинисаном у политици сертификације;
б) коришћење приватног кључа за формирање безбједног електронског потписа;
ц) начин приступа свом приватном кључу;
д) користи квалификовану потврду само уз безбједан електронски потпис који је формиран средствима за формирање безбједног електронског потписа;
е) уколико захтијева квалификована потврда од овјериоца која испуњава услове из Закона о електронском потпису и овог Правилника, генерише пар кључева за формирање и провјеру безбједног електронског потписа у средству за формирање безбједног електронског потписа које је у потпуности под његовом контролом;
ф) одмах обавјештење овјериоца ако прије истека важности потврде који је назначен у самој потврди:
1) корисников приватни кључ се изгуби, украде или наступи основана сумња да је компромитован,
2) престане контрола над коришћењем корисниковог приватног кључа из разлога компромитовања активационих података (ПИН код или лозинка) за средство за формирање безбједног електронског потписа или других разлога,
3) установи нетачност или измјену садржаја квалификоване потврде;

г) прекине коришћење свог приватног кључа уколико постоји основана сумња у компромитацију кључа или контролу над активационим подацима за средство за формирање безбједног електронског потписа.

Члан 34.

(Обавезе заинтересованих страна)

У случају суспензије или опозива квалификоване потврде, корисник провјерава статусне информације у вези суспензије или опозива потврде које је овјерилац јавно објавио у складу са општм правилима, уважавајући сва ограничења у коришћењу квалификационе потврде која су назначена у самој потврди или објављена у општим правилима.

Члан 35.

(Финансијска способност овјериоца)

(1) Финансијска средства овјериоца потребна за обављање регистроване дјелатности се пријављују и документују Надзорном органу, заједно са пријавом отпочињања дјелатности.
(2) Овјериоци који издају квалифициона потврде или стављају на располагање безбједне електронске поступке израде потписа, морају посједовати основни капитал у износу од најмање 600.000,00 КМ.
(3) Овјериоци који издају квалификоване потврде или стављају на располагање безбједне електронске поступке израде потписа, морају осим тога, истовремено са пријавом отпочињања своје дјелатности, доказати Надзорном органу да су закључили осигурање од одговорности са минималном сумом осигурања од 1.500.000,00 КМ, које покрива најмање три осигуравајућа случаја у години.
(4) Од обавеза из ст. (1) и (2) овог члана су ослобођени овјериоци који су законом успостављени као органи државне управе у Босни и Херцеговини.

ГЛАВА VIII - Чување података

Члан 36.

(Чување података)

(1) Овјерилац обезбјеђује трајно чување свих релевантних података које се тичу квалификованих потврда.
(2) У вези са ставом (1) овог члана, овјерилац обезбјеђује:
а) тајност и интегритет текућих и архивираних записа о квалификованим потврдама;
б) комплетно и поуздано архивирање података о квалификованим потврдама у складу са општм правилима;
ц) да су записи у вези квалификованих потврда, као и регистрационе и друге податке о кориснику,

расположиви за потребе правних послова као доказ извршене сертификације;

д) поуздано архивирање тачног времена значајних догађаја у овјериоцу;

е) да се подаци у вези квалификованих потврда чувају онолико времена колико је потребно да се користе у правним пословима везаним за електронске потписе;

ф) евидентирање свих догађаја на начин да се не могу лако обрисати или уништити (изузев у циљу преноса на дуготрајне медије за чување) у оквиру временског периода у коме се морају чувати;

г) документовање специфичних догађаја и података који треба да се евидентирају;

х) евидентирање свих догађаја који се односе на регистрацију корисника, укључујући и захтјеве за обнављањем потврда, а нарочито:
   1) тип идентификационог документа који је презентован од стране корисника,
   2) јединствени идентификациони податак о кориснику преузет из идентификационог документа,
   3) мјесто чувања копија апликативних и идентификационих докумената, укључујући и потписан Уговор са корисником,
   4) специфичне информације из Уговора са корисником,
   5) идентитет службеника овјериоца који је извршио регистрацију корисника,
   6) податке о методи која је коришћена за провјеру важења идентификационих докумената,

и) име овјериоца које је примило регистрационе информације;

ј) заштиту приватности података корисника и евидентирање свих догађаја у вези са животним циклусом кључева овјериоца;

к) евидентирање свих догађаја у вези са животним циклусом квалификованих потврда и кључева којима управља овјерилац, укључујући и корисничке кључеве ако су генерисани у овјериоцу;

л) евидентирање свих догађаја који се односе на примјену средстава за формирање безбједног електронског потписа;

м) да се сви захтјеви и извјештаји који се односе на процедуру опозива потврда евидентирају, укључујући и све одговарајуће активности.

Члан 37.

(Поступање овјериоца у случају престанка рада)

Овјерилац обезбјеђује да у случају престанка рада корисник претрпи минималну могућу штету тако што ће на прописан начин чувати податке као доказ извршене услуге, а нарочито:

а) прије престанка обављања дјелатности, извршава сљедеће активности:
   1) информиса све кориснике о престанку рада,
   2) уништава, или потпуно онемогућава коришћење, својих приватних кључева који су коришћени за формирање безбједног електронског потписа квалификованих потврда;

б) обезбјеђује неопходна финансијска средства за реализацију захтјева из тачке а) овог става;

ц) општим правилима дефинише процедуру престанка рада, која обухвата:
   1) обавјештавање корисника,
   2) евентуални пренос обавеза другим овјериоцима,
   3) процедуру опозива издатих квалификованих потврда којима није истекао рок важности, и пренос листи опозваних потврда другом овјериоцу.

ГЛАВА IX - Обезбјеђење услова за кориснике за које се генеришу подаци за формирање безбједног електронског потписа

Члан 38.

(Средство за формирање безбједног електронског потписа)

Овјерилац може, уз услуге из члана 4. овог Правилника, а у складу са својим општим и посебним правилима, да обезбиједи средство за формирање безбједног електронског потписа корисницима и придружену лозинку (или ПИН код) за активацију средства, као и њихову безбједну дистрибуцију до корисника.

Члан 39.

(Кључеви корисника)

Овјерилац обезбјеђује да су кључеви корисника које он генерише, генерисани безбједно и да је обезбијеђена тајност приватног кључа корисника све до његове доставе кориснику и да при испоруци само корисник има приступ свом приватном кључу.

Члан 40.

(Асиметрични пар корисничких кључева)

Овјерилац обезбјеђује да:

а) се асиметрични пар корисничких кључева генерише коришћењем алгоритма који је прописан да задовољи захтјеве који се примјењују за безбједне електронске потписе;

б) су асиметрични кључеви корисника прописане дужине и коришћени у прописаном асиметричном криптографском алгоритму у циљу да се задовоље прописани захтјеви за имплементацијом безбједног електронског потписа.

Члан 41.

(Услови безбједности средстава за формирање безбједног електронског потписа)

Уколико овјерилац обезбиједи средства за формирање безбједног електронског потписа за кориснике, то чини на безбједан начин а нарочито обезбјеђује да:

а) пријем средства за формирање безбједног електронског потписа мора бити безбједно контролисан од стране овјериоца;

б) средства за формирање безбједног електронског потписа морају бити безбједно чувана и дистрибуисана;

ц) деактивирање и реактивирање средстава за формирање безбједног електронског потписа мора бити безбједно контролисано од стране овјериоца;

д) уколико средство за формирање безбједног електронског потписа има придружене активационе податке (ПИН код или лозинка) исти мора бити безбједно припремљен и шаљу одвојено у односу на средство за формирање безбједног електронског потписа, у различито вријеме или на различит начин.

Члан 42.

(Тајност идентификационих података)

(1) Овјерилац који издаје квалификоване потврде и који обезбјеђује средство за формирање безбједног електронског потписа (енгл. SSCD: Secure Signature –

Creation Device) корисницима гарантује тајност идентификационих података (ПИН код, лозинка), након што се уграде у иста.

(2) Овлашћено лице овјериоца квалификовану потврду, уз осигурање SSCD корисницима, квалификовану потврду уручује лично кориснику уз својеручни потпис корисника о уручењу исте или исту доставља у електронском облику безбједним електронским потписом датог корисника.

(3) Квалификована потврда из става (1) овог члана се верификује и ставља на располагање трећим лицима тек након потврде пријема SSCD уређаја и одговарајућих идентификационих података, уз допуштење корисника.

ГЛАВА X - Физичка заштита

Члан 43.

(Контрола физичког приступа)

Овјерилац обезбјеђује контролу физичког приступа својим безбједносно критичним ресурсима и минималан ризик у приступу својим кључним елементима система.

Члан 44.

(Мјере које предузима овјерилац)

Овјерилац обезбјеђује да:

а) се физички приступ просторијама у којима се обавља генерисање квалификованих потврда, пријем средстава за формирање безбједног електронског потписа и управљање процедуром опозива потврда, ограничи само на поуздано ауторизована лица;

б) су имплементиране неопходне мјере у циљу избјегавања губитака, оштећења или компромитовања кључних ресурса и елиминисање могућности прекида пословних активности;

ц) се имплементирају одговарајуће мјере за спречавање компромитовања или неовлашћеног преузимања информација и уређаја за процесирање информација;

д) су просторије у којима се врши генерисање квалификованих потврда, пријем средстава за формирање безбједног електронског потписа и управљање опозивом, такве да се оперативни рад у њима одвија у окружењу које обезбјеђује физичку заштиту сертификационих сервиса и ресурса у случају злоупотребе приликом неауторизованог приступа систему и подацима;

е) је физичка заштита успостављена креирањем јасно дефинисаних безбједносних физичких баријера којима се штите процеси генерисања квалификованих потврда, обезбјеђење средстава за формирање безбједног електронског потписа и управљање опозивом;

ф) су имплементиране одговарајуће физичке мјере и контроле безбједносног окружења у циљу заштите просторија и системских елемената овјериоца;

г) су имплементиране одговарајуће мјере у циљу заштите уређаја, информација, меморијских медија и софтвера од отуђивања са локације без прописне ауторизације;

х) се и друге специфичне сигурносне функције могу примијенити у оквиру истог сигурног простора који осигурава приступ само ауторизираним запосленим лицима.

Члан 45.

(Обезбјеђење приступа систему сертификације)

Овјерилац је дужан да приступ систему сертификације ограничи искључиво на ауторизована лица, а нарочито обезбјеђује:

а) имплементацију контрола на мрежном нивоу у циљу заштите интерне мреже овјериоца од екстерних мрежних домена којима може приступити трећа страна, уз забрану свих протокола и приступа који се не користе у оперативном раду овјериоца;

б) поуздану заштиту осјетљивих података, који укључују и податке о регистрацији корисника, током проласка кроз дијелове мреже који нису безбједни;

ц) ефикасну и поуздану администрацију корисничких приступа (укључујући операторе, администраторе и било које специфичне кориснике који имају директан приступ систему) у циљу одржавања безбједних система, укључујући и управљање налозима корисника, евидентирање и могућност модификације и забране приступа;

д) строго ограничен приступ информацијама и апликативним функцијама система у складу са општм и посебним правилима и политиком контроле приступа, идентификованом у њима, као и довољну рачунарско-безбједносну контролу у циљу раздвајања безбједносних функција у систему које су идентификоване у општим правилима, укључујући раздвајање функција администратора безбједности и оператера, а рад са корисничким програмима за управљање системом мора бити посебно ограничен и строго контролисан;

е) поуздану идентификацију и аутентикацију запослених код овјериоца прије коришћења критичних операција везаних за процедуре управљања потврдама;

ф) евидентирање свих активности запослених код овјериоца на основу одговарајућих корисничких налога и лог фајлова, који су потписани безбједним електронским потписом;

г) поуздану заштиту безбједносно осетљивих података, који укључују и регистрационе податке корисника, од неауторизованог приступа претходно обрисаним или архивираним подацима;

х) да се локалне физичке мрежне компоненте чувају у физички заштићеном окружењу и да се њихова конфигурација периодично контролише у циљу испитивања усклађености са захтјевима специфицираним у општим и посебним правилима;

и) стално надзирање и алармирање користећи системе за детекцију напада и надзирање контроле приступа и аларма у циљу поуздане детекције, регистрације и реакције на неауторизован или нерегуларан покушај приступа ресурсима који се користе за пружање услуга сертификације;

ј) да апликација за дистрибуцију потврда примијењује систем логичке контроле приступа у циљу спречавања покушаја додавања или брисања одговарајућих потврда и измјене других придружених информација;

к) да апликација за добијање статуса опозива потврда примјењује систем логичке контроле

приступа у циљу спречавања покушаја измјене информација о статусу опозива потврда.

ГЛАВА XI - Информације о условима издавања и коришћења потврда

Члан 46.

(Расположивост информације)

(1) Овјерилац обезбјеђује да информације о условима издавања и коришћења квалификованих потврда буду расположиве корисницима и другим заинтересованим странама.

(2) Расположивост информација из става (1) овог члана обезбјеђује се коришћењем једноставних видова комуникације (Интернет и сл.) са обезбијеђеним интегритетом током времена, да се могу преносити електронским путем и да су приказане на потпуно разумљив начин.

Члан 47.

(Начин обезбјеђења расположивости информација)

Овјерилац обезбјеђује расположивост информација и података о свом пословању, и то:

а) општа правила овјериоца која су тренутно важећа;
б) ограничења у коришћењу општх правила;
ц) обавезе корисника;
д) информације о начину провјере важности квалификованих потврда, укључујући и захтјеве за провјеру статуса опозива потврда;
е) ограничења одговорности која укључују случајеве за које овјерилац прихвата или одбија одговорност;
ф) временски период чувања регистрационих информација корисника;
г) временски период чувања лог фајлова за евидентирање;
х) процедуру у случају подношења жалби;
и) процедуру у случају спора;

XII - Управљање потврдама

Члан 48.

(Увид у квалификовану потврду)

Овјерилац обезбјеђује увид у статус квалификоване потврде свим корисницима и заинтересованим странама без увида у садржај исте.

Члан 49.

(Расположивост података из квалификоване потврде)

(1) Овјерилац обезбјеђује:
а) да је квалификована потврда расположива кориснику којем је издата;
б) да је квалификована потврда расположива трећим лицима само по одобрењу корисника, а у складу са општим правилима овјериоца;
ц) једноставну идентификацију информација о условима издавања и коришћења квалификованих потврда свим заинтересованим странама у систему;
д) да су информације наведене под тач. б) и ц) овог става расположиве 24 часа на дан, седам дана у седмици;

(2) У случају пада система или дјелимичног губитка могућности за обезбјеђење сервиса, овјерилац је обавезан предузети све расположиве мјере у циљу активирања информационог сервиса, најкасније до истека рока предвиђеног у општим правилима.

ГЛАВА XIII - Провјера испуњености услова за издавање квалификованих потврда

Члан 50.

(Провјера испуњености услова)

Провјеру испуњености услова за издавање квалификованих потврда врши Надзорни орган у поступку разматрања захтјева овјериоца за упис у Регистар овјерилаца.

Члан 51.

(Испуњавање услова)

Провјера испуњености услова за издавање квалификованих потврда обухвата:

а) провјеру општих правила и посебних правила рада овјериоца и њихове усклађености са Законом и подзаконским актима;
б) провјеру атеста и сертификације техничких и безбједносних компонената које користи овјерилац за генерисање јавних и приватних кључева и издавање квалификованих потврда.

Члан 52.

(Провјера оперативног рада овјериоца)

Провјера оперативног рада овјериоца обухвата:

а) процедуру регистрације корисника коме се издаје квалификоване потврда;
б) процедуру пријема захтјева за издавањем квалификоване потврде у регистрационом ауторитету;
ц) процедуру достављања захтјева до овјериоца;
д) процедуру генерисања квалификоване потврде;
е) коришћење безбједносних система за чување података за генерисање квалификованих потврда;
ф) коришћење безбједних хардверских средстава за формирање безбједног електронског потписа (хардверски модели заштите (HSM - Hardware Security Module));
г) процедуру достављања квалификоване потврде, уређаја за генерисање електронског потписа и идентификационих података корисницима;
х) процедуру опозива потврде;
и) процедуру обнављања потврде;
ј) процедуру суспензије потврде;
к) начин објављивања листе опозваних и суспендованих потврда;
л) системе физичке контроле приступа у просторије овјериоца;
м) системе логичке контроле приступа рачунарским ресурсима овјериоца;
н) систем за јавно објављивање основних информација о пружању услуга сертификације, као и општих правила рада овјериоца.

Члан 53.

(Провјера техничких и безбједносних компоненти)

Провјера техничких и безбједносних компоненти које користи овјерилац обухвата:

а) реализацију системских захтјева безбједности;
б) издавање квалификованих потврда примјеном безбједног електронског потписа;
ц) безбједно генерисање кључева овјериоца.

Члан 54.

(Оперативни рад овјериоца)

Оперативни рад овјериоца се обавља у складу са стандардом CEN WorkshopAgreement 14167-1 (March 2003) "Security Requirements for Trustworthy SystemsManaging

Sertificates for Electronic Signatures - Part 1: System Security Requirements".

Član 55.
(Stupanje na snagu)

Ovaj Pravilnik stupa na snagu narednog dana od dana objavljivanja u "Službenom glasniku BiX".

SM broj 14/17	Predsjedavajući
18. januara 2017. godine	Savjeta ministara BiX
Sarajevo	Dr **Denis Zvizdić**, s. r.

Na osnovu člana 17. Zakona o Vijeću ministara Bosne i Hercegovine ("Službeni glasnik BiH", br. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 i 24/08) i člana 26. stav (1) Zakona o elektronskom potpisu ("Službeni glasnik BiH", broj 91/06), na prijedlog ministra komunikacija i prometa Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine na 88. sjednici, održanoj 18. januara 2017. godine, donijelo je

PRAVILNIK
O BLIŽIM UVJETIMA ZA IZDAVANJE KVALIFICIRANIH POTVRDA

POGLAVLJE I - Opće odredbe

Član 1.
(Predmet Pravilnika)

Ovim Pravilnikom propisuju se bliži uvjeti za izdavanje kvalificiranih potvrda i uvjeti koje ovjerilac mora ispunjavati za izdavanje kvalificiranih potvrda.

Član 2.
(Primjena međunarodnih standarda)

(1) Prilikom izdavanja kvalificiranih potvrda primjenjuju se međunarodni standardi i preporuke, kao i drugi odgovarajući standardi, dokumenata i preporuka.
(2) Ovjerilac za izdavanje kvalificiranih potvrda (u daljem tekstu: ovjerilac) izdaje kvalificirane potvrde korisnicima u skladu sa 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 and Certificate Revocation List (CRL) Profile" i ETSI TS 102 280 "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".

POGLAVLJE II - Pouzdano obavljanje usluga izdavanja kvalificiranih potvrda

Član 3.
(Način formiranja sigurnog elektronskog potpisa)

Ovjerilac izdaje kvalificirane potvrde formiranjem sigurnog elektronskog potpisa na osnovu svog privatnog ključa i asimetričnog kriptografskog algoritma, na način propisan Pravilnikom o tehničko-tehnološkim postupcima za formiranje sigurnog elektronskog potpisa i uvjetima i kriterijumima, koje treba da ispune sredstva za formiranje sigurnog elektronskog potpisa.

Član 4.
(Usluge certifikacije)

(1) Ovjerilac je dužan osigurati potpunu uslugu certifikacije koja uključuje slijedeće servise, i to:
   a) registraciju korisnika;
   b) formiranje kvalificiranih potvrda;
   c) distribuciju kvalificiranih potvrda korisnicima;
   d) upravljanje životnim vijekom (obnavljanje, suspenzija, opoziv) kvalificiranih potvrda;
   e) osiguravanje pouzdanog i javno dostupnog servisa za provjeru statusa opozvanosti kvalificiranih potvrda.
(2) Ovjerilac može, pored servisa iz stava (1) ovog člana, da osigura i formiranje asimetričnog para ključeva za korisnike, kao i distribuciju privatnog ključa i potvrde korisniku na siguran način, ukoliko je to propisano u politici certificiranja datog ovjerioca.

Član 5.
(Opći akti ovjerioca)

(1) Ovjerilac, prije početka rada, donosi opća interna pravila pružanja usluge certifikacije (u daljem tekstu: opća pravila) koja korisnicima pružaju dovoljno informacija na osnovu kojih se mogu odlučiti o prihvatanju usluga i o obimu usluga.
(2) Opća pravila funkcioniranja ovjerioca treba da budu u skladu sa dokumentima RFC 3647 "Internet X.509 Public Key Infrastructure. Certificate Policy and CertificationPractices Framework" i ETSI TS 101 456 "Policy Requirements for Certification Authorities Issuing Qualified Certificates".
(3) Na osnovu općih pravila ovjerilac donosi slijedeće opće akte:
   a) Politiku certifikacije (engl.Certificate Policy);
   b) Praktična pravila pružanja usluge certifikacije (engl.Certification Practices Statement) (u daljem tekstu: praktična pravila).

Član 6.
(Politika certifikacije i praktična pravila)

(1) Politika certifikacije i praktična pravila su javni dokumenti.
(2) Politika certifikacije definira predmet rada i zahtjeve poslovanja ovjerioca.
(3) Praktična pravila definiraju procese i način njihovog korištenja pri formiranju i upravljanju kvalificiranim potvrdama, operativne procedure u cilju ispunjenja tih zahtjeva i način na koji ovjerilac ispunjava tehničke, organizacione i proceduralne zahtjeve poslovanja koji su identificirani u politici certifikacije.
(4) Politikom certifikacije i praktičnim pravilima uređuju se slijedeće oblasti:
   a) opće odredbe o radu ovjerioca:
      1) pojam ovjerioca,
      2) certifikacione usluge,
      3) obuhvat dokumenta politika certifikacije,
      4) obuhvat dokumenta praktičnih pravila pružanja usluge certifikacije,
      5) korisničke usluge certifikacije.
   b) uvodne odredbe o politici izdavanja kvalificiranih potvrda;
   c) obaveze i odgovornosti ovjerioca i korisnika;
   d) funkcionalne zahtjeve za rad ovjerioca: operativne procedure rada ovjerioca i procedure upravljanja životnim ciklusom kriptografskih ključeva:
      1) generiranje ključa ovjerioca,
      2) procedure čuvanja i formiranja rezervnih kopija ključeva ovjerioca,
      3) distribuciju javnog ključa ovjerioca,
      4) korištenje ključa ovjerioca,
      5) kraj životnog ciklusa ključa ovjerioca,
      6) upravljanje životnim ciklusom kriptografskog hardvera koji se koristi za generiranje kvalificiranih potvrda,
      7) upravljanje ključevima korisnika za identificiranje,
      8) proceduru primjene sredstava za formiranje sigurnog elektronskog potpisa.
   e) procedure upravljanja životnim ciklusom certifikata:
      1) metode registracije korisnika,

2) izdavanje potvrda,
3) distribuciju potvrda,
4) obnavljanje potvrda,
5) suspenziju potvrda,
6) opoziv potvrda,
7) način publikacije liste opozvanih potvrda;

f) upravljanje operativnim radom ovjerioca:
1) upravljanje u skladu sa sigurnosnim principima,
2) upravljanje i klasifikacija najvažnijih informacija i podacima u okviru ovjerioca,
3) kadrovski resursi,
4) sistem fizičke sigurnosti i sigurnosti okruženja,
5) upravljanje radom ovjerioca,
6) upravljanje sistemom kontrole pristupa,
7) upotrebu i održavanje sigurnim kriptografskih sistema,
8) upravljanje procedurama kontinualnog poslovanja u incidentnim situacijama,
9) prestanak rada ovjerioca,
10) usaglašenost rada sa kriterijumima za rad ovjerilaca koji izdaju kvalificirane potvrde u skladu sa članom 8. Zakona i ovim Pravilnikom,
11) formiranje i čuvanje dokumentacije koja se odnosi na kvalificirane potvrde.

g) organizaciju rada ovjerioca.

Član 7.
(Sposobnost za osiguranje usluge)

Ovjerilac demonstrira sposobnost za osiguranje usluge izdavanja kvalifikovanih potvrda, ukoliko:

a) posjeduje praktična pravila, i u njima definirane procedure, u kojima se specificira način ispunjenja svih zahtjeva za izdavanjem kvalificiranih potvrda koji su identificirani u politici certifikacije;
b) učini dostupnim praktična pravila svim korisnicima i drugim zainteresiranim stranama;
c) učini dostupnim svim korisnicima i potencijalnim zainteresiranim stranama uvjete korištenja kvalificiranih potvrda;
d) posjeduje upravnu strukturu najvišeg nivoa koja ima konačnu autorizaciju i odgovornost za objavljivanje praktičnih pravila ovjerioca;
e) posjeduje upravnu strukturu operativnog nivoa u ovjeriocu koja je odgovorna za ispravnu primjenu praktičnih pravila;
f) definira postupak periodične analize i revizije praktičnih pravila;
g) posjeduje sve izmjene praktičnih pravila, javno objavljene i odobrene od strane upravne strukture najvišeg nivoa.

Član 8.
(Posebna interna pravila)

(1) Ovjerilac utvrđuje i posebna interna pravila rada ovjerioca i zaštite sistema certifikacije (u daljem tekstu: posebna pravila) u kojima su sadržani i detaljno opisani postupci i mjere koje se primjenjuju prilikom izdavanja i postupanja kvalificiranim potvrdama.
(2) Posebna pravila su privatni dokument i predstavljaju poslovnu tajnu ovjerioca.

Član 9.
(Posebna pravila)

Posebna pravila sadrže odredbe kojim se bliže uređuje:

a) sistem fizičke kontrole pristupa u pojedine prostorije ovjerioca;
b) sistem logičke kontrole pristupa računarskim resursima ovjerioca;
c) sistem čuvanja privatnog ključa ovjerioca;
d) sistem dodijeljene odgovornosti pri aktivaciji privatnog ključa ovjerioca i
e) postupci i radnje u vanrednim situacijama (požari, poplave, zemljotresi, druge vremenske nepogode, zlonamjerni upadi u prostorije ili informacioni sistem ovjerioca).

Član 10.
(Organizacija rada)

Ovjerilac osigurava pouzdanu organizaciju rada tako što:

a) donosi pravila i operativne procedure koje nisu diskriminatorske;
b) čini dostupnim svoje servise svim korisnicima čije su aktivnosti u skladu sa objavljenim općim pravilima;
c) posluje kao pravno lice u skladu sa propisima;
d) ima sistem kvaliteta i sistem sigurnog upravljanja kvalificiranim potvrdama u skladu sa uslugama certifikacije koje pruža;
e) posjeduje osiguranje od odgovornosti za štetu, koja može da proistekne u vršenju njegovih aktivnosti u skladu sa politikom certifikacije;
f) ima finansijsku stabilnost i dovoljne resurse koji se zahtijevaju u pružanju usluga certifikacije u skladu sa politikom certifikacije;
g) ima dovoljan broj stalno zaposlenih na poslovima certifikacije sa neophodnim obrazovanjem, nivoom obučenosti, tehničkim znanjima i iskustvom;
h) efikasno postupa prilikom rješavanja žalbi i sporova sa korisnicima ili drugim zainteresiranim stranama u vezi pružanja usluga certifikacije;
i) pruža nezavisnost dijelova ovjerioca uključenih u poslove generiranja kvalificiranih potvrda od drugih vanjskih organizacija u sferi pružanja usluga certifikacije. Posebno upravne strukture ovjerioca, kao i zaposlenih sa sigurnosnim funkcijama, moraju biti zaštićeni od bilo kakvih finansijskih i drugih pritisaka koji mogu utjecati na povjerenje u usluge certifikacije koje pruža ovjerilac;
j) ima propisno dokumentiranu strukturu dijelova ovjerioca povezanih sa generiranjem kvalificiranih potvrda radi osiguranja nepristrasnosti u pružanju usluga certifikacije, u skladu sa općim i posebnim pravilima.

Član 11.
(Osiguranje od odgovornosti za štetu)

Ovjerilac je dužan osigurati najniži iznos osiguranja od rizika odgovornosti za štetu nastalu vršenjem usluga izdavanja elektronskih potvrda, tako da:

a) osigurana suma na koju mora biti ugovoreno osiguranje po jednom štetnom događaju ne može iznositi manje od 50.000 KM, podrazumijevajući pritom kao štetni događaj pojedinačnu štetu nastalu upotrebom jedne kvalificirane potvrde u jednom aktu u pravnom prometu;
b) ukupna osigurana suma na koju mora biti ugovoreno osiguranje od odgovornosti ovjerioca kumulativno na godišnjem nivou, po svim štetnim događajima, ne može biti niža od 1.500.000,00 KM.

Član 12.
(Postupanje ovjerioca u slučaju vanrednih okolnosti)

Ovjerilac osigurava da u slučaju vanrednih okolnosti operativni rad bude obnovljen što je moguće prije a u skladu sa općim i posebnim pravilima. U slučaju kompromitiranja svog asimetričnog privatnog ključa, ovjerilac:

a) prestaje sa izdavanjem kvalificiranih potvrda;

b) informira sve korisnike i druge zainteresirane strane o kompromitiranju privatnog ključa;
c) javno objavljuje informacije o tome da izdate kvalificirane potvrde, kao i informacije o statusu opozvanosti kvalificiranih potvrda, više nisu važeće;
d) vrši opoziv svih izdatih kvalificiranih potvrda odmah a najkasnije u roku od 24 sata u skladu sa članom 10. Zakona o elektronskom potpisu ("Službeni glasnik BiH", broj 91/06, u daljem tekstu: Zakon).

Član 13.
(Evidencija izdatih kvalificiranih potvrda)

(1) Ovjerilac vodi ažurnu, tačnu i sigurnu evidenciju izdatih kvalificiranih potvrda koja može biti javno dostupna, osim u slučajevima kada vlasnik potvrde izričito zahtjeva da njegovi podaci ne budu javno dostupni.
(2) Ovjerilac vodi ažurnu i sigurnu evidenciju opozvanih i suspendiranih kvalificiranih potvrda i mora za svaku potvrdu koju je izdalo, informaciju o njegovoj validnosti učiniti javno dostupnom.
(3) Za tačnost i validnost evidencija iz st. (1) i (2) ovog člana garantira ovjerilac, svojom kvalificiranom potvrdom.

Član 14.
(Određivanje vremena izdavanja i opoziva)

(1) Za određivanje vremena izdavanja i opoziva kvalificiranih potvrda, ovjerilac osigurava izvor tačnog vremena koji je sinhroniziran sa izvorom referentnog vremena kojeg odredi Nadzorni organ i objavljuje na službenoj Internet stranici Nadzornog organa.
(2) Vrijeme izdavanja kvalificirane potvrde ovjerilac upisuje u izdatu kvalificiranu potvrdu.
(3) Vrijeme izdavanja i opoziva kvalificiranih potvrda ovjerilac čuva u evidenciji izdatih i opozvanih potvrda iz člana 13. ovog Pravilnika.

POGLAVLJE III - Registracija korisnika

Član 15.
(Registracija korisnika)

(1) Ovjerilac vrši pouzdanu identifikaciju i autentikaciju korisnika u cilju izdavanja kvalificirane potvrde, te vodi registar potvrda.
(2) Postupke registracije iz stava (1) ovog člana vrši ovlašteni službenik ovjerioca.

Član 16.
(Obaveze ovjerioca u postupku registracije korisnika)

U postupku registracije korisnika, ovjerilac je dužan osigurati da:

a) se korisnik identificira kao fizičko lice sa specifičnim atributima koji mogu označavati organizacionu jedinicu ili ulogu u organizaciji gdje je zaposlen;
b) prije uspostavljanja ugovornog odnosa sa korisnikom, javno informira korisnika na jasan i nedvosmislen način o svim relevantnim uvjetima korištenja kvalificiranih potvrda;
c) se u postupku registracije, identitet korisnika fizičkog lica, utvrđuje neposrednim uvidom u važeći identifikacioni dokument u prisustvu podnosioca zahtjeva;
d) ukoliko se radi o korisniku, pravnom licu se izvrši uvid u:
   1) izvod iz sudskog registra iz kojeg se može utvrditi ko je odgovorno lice u pravnom licu,
   2) akt kojim je korisnik ovlašten od strane tog pravnog lica ili organizacije za dobijanje kvalificirane potvrde;
e) se u izuzetnom slučaju utvrđuje svaki specifični atribut korisnika kome se izdaje kvalificirana potvrda;
f) informacije sadržane u kvalificiranoj potvrdi budu pouzdane i tačne;
g) korisnik dostavi tačne i pouzdane informacije o fizičkoj adresi, ili drugim atributima, koji opisuju kako se korisnik može kontaktirati;
h) se čuvaju sve informacije korištene za verifikaciju identiteta korisnika i dokumentaciju korištenu za identifikaciju, kao i bilo koja ograničenja njene važnosti;
i) se zaključi ugovor sa korisnikom kojim se regulira slijedeće:
   1) obaveza korisnika da koristi sredstvo za formiranje sigurnog elektronskog potpisa koje osigurava ovjerilac u skladu sa općim pravilima,
   2) obaveza ovjerioca da čuva podatke korištene u registraciji korisnika i sve informacije o životnom ciklusu izdate kvalificirane potvrde korisnika.
   3) uvjeti pod kojima se objavljuje potvrda,
   4) klauzulu o tačnosti podataka sadržanih u potvrdi;
j) ako asimetrični par ključeva korisnika nije generiran od strane ovjerioca, proces generiranja zahtijeva za kvalificiranom potvrdom u potpunosti osigurava da korisnik posjeduje privatni ključ koji je matematički povezan sa javnim ključem koji je prezentiran za certifikaciju. U tom slučaju korisnik mora osigura da se asimetrični par ključeva generira isključivo u sredstvu za formiranje sigurnog elektronskog potpisa;
k) se poštuju odredbe važećih propisa kojima je uređena oblast zaštite ličnih podataka.

POGLAVLJE IV - Kadrovski resursi i upravljanje operativnim radom ovjerioca

Član 17.
(Funkcioniranje ovjerioca)

Ovjerilac je dužan osigurati pouzdano, sigurno i nesmetano obavljanje poslova izdavanja kvalificirane potvrde.

Član 18.
(Ljudski resursi)

(1) Ovjerilac osigurava da zaposleni u ovjeriocu posjeduju neophodno potrebnu kvalifikaciju, iskustvo i ekspertsko znanje, za obavljanje poslova ovjerioca, i to:
   a) potreban broj zaposlenih sa visokom školskom spremom iz oblasti informaciono-komunikacionih tehnologija,
   b) radno iskustvo zaposlenih od najmanje 3 godine na poslovima održavanja i sigurnosti informacionih sistema,
   c) položen ispit iz oblasti sigurnosti informacionih sistema,
   d) posjedovanje specifičnih vještina i iskustva,
   e) da posjeduju ekspertizu u tehnologiji elektronskog potpisa, da su dobro upoznati sa sigurnosnim procedurama za zaposlene i sa odgovornostima u domenu sigurnosti, kao i da imaju odgovarajuća iskustva u primjeni sigurnih informacionih sistema i procjeni rizika.
(2) Ovjerilac je dužan osigurati slijedeće sigurnosne funkcije u ovjeriocu za:
   a) glavnog administratora sigurnosti - sveukupnu odgovornost za administriranje i implementaciju sigurnosnih funkcija i procedura, kao i upravljanje aktivnostima na dodatnom unapređenju poslova

generiranja, opoziva i suspenzije kvalificiranih potvrda,

b) sistem administratore - autoriziranu odgovornost za instalaciju, konfiguriranje i održavanje sigurnih sistema ovjerioca za registraciju korisnika, generiranje kvalificiranih potvrda, osiguranje sredstava za formiranje sigurnog elektronskog potpisa za korisnike i upravljanje opozivom kvalificiranih potvrda,

c) sistem operatore - odgovornost za rad sigurnih sistema ovjerioca u tekućem radu na dnevnom nivou i autoriziranu odgovornost za implementaciju sistema za formiranje rezervnih kopija i procedure oporavka,

d) sistem evidentičare - autoriziranu odgovornost za pregledanje i održavanje arhiva i log fajlova sigurnih sistema ovjerioca;

(3) Odgovorno lice u ovjeriocu, vršiteljima poslova iz stava (2) ovog člana, posebnim aktom utvrđuje sigurnosne funkcije.

(4) U opisu svakog radnog mjesta u ovjeriocu, uloga i stepen sigurnosti utvrđene u općim pravilima, moraju biti jasno i precizno navedene, sa naglaskom na stepen povjerljivosti.

(5) Zaposleni u ovjeriocu koji imaju određen stepen sigurnosne funkcije ne smiju biti u sukobu interesa koji mogu utjecati na nepristrasnost rada ovjerioca.

(6) Sigurnosne funkcije ne mogu se dodijeliti licu koje je osuđivano za radnje koje su u vezi sa poslovima koje obavljaju kod ovjerioca. Pristup sigurnosnim funkcijama osigurava se po okončanju propisanih provjera.

POGLAVLJE V - Pouzdani i sigurni kriptografski sistemi

Član 19.

(Korištenje sigurnih sistema)

Ovjerilac koristi sigurne sisteme i proizvode koji su zaštićeni od neovlaštenih modifikacija.

Član 20.

(Analiza rizika)

Ovjerilac vrši analizu rizika kojom identificira kritične servise koji zahtijevaju korištenje sigurnih sistema i visoke nivoe sigurnosti:

a) prije početka obavljanja usluga certifikacije,

b) tokom operativnog rada po potrebi, a najmanje svakih šest mjeseci.

Član 21.

(Sigurno i korektno funkcioniranje sistema)

Ovjerilac osigurava sigurno i korektno funkcioniranje svojih sistema, sa minimalnim rizikom od kvarova, a naročito:

a) zaštitu integriteta sistema ovjerioca i informacija od virusa, malicioznog i neautoriziranog softvera;

b) minimalan rizik od štete uslijed mogućih incidenata korištenjem procedura izvještavanja, brzim i koordiniranim reagiranjem na sigurnosne incidente u cilju smanjenja utjecaja sigurnosnih upada;

c) sigurno korištenje memorijskih medija u skladu sa unaprijed specificiranim šemama klasifikacije informacija. Mediji koji nisu u operativnom radu, sigurnosno osjetljive podatke moraju sigurno arhivirani;

d) uspostaviti i implementirati procedure za sve sigurne i administrativne funkcije koje imaju utjecaj na pružanje usluga certifikacije. Odgovorno lice ovjerioca je odgovorno za planiranje i efikasnu implementaciju općih pravila;

e) stalnim nadzorom tekućih i planiranih potreba za kapacitetom sistema ovjerioca radi osiguranja adekvatne procesne snage i memorijskih kapaciteta.

Član 22.

(Asimetrični ključevi)

(1) Asimetrični ključevi mogu biti javni i privatni;

(2) Ovjerilac osigurava da se njegovi asimetrični ključevi generiraju u strogo kontroliranim i sigurnim uvjetima, a naročito da se:

a) generiranje asimetričnih ključeva vrši u fizički zaštićenom okruženju od strane i uz minimalan broj autoriziranih zaposlenih (najmanje dva zaposlena lica) za izvršavanje ove funkcije a prema zahtjevima i procedurama definiranim u praktičnim pravilima;

b) generiranje asimetričnih ključeva vrši u sredstvu koje:

1) zadovoljava zahtjeve iz standarda FIPS PUB 140-2 nivo 3 i viši ili

2) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)" ili

3) zadovoljava zahtjeve iz standarda 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)";

(3) Rezervne kopije privatnih ključeva za formiranje sigurnog elektronskog potpisa kvalificiranih potvrda imaju isti ili viši nivo sigurnosnih kontrola u odnosu na ključeve koji se operativno koriste.

(4) Ovjerilac osigurava da su izdate kvalificirane potvrde potpisane sigurnim elektronskim potpisom ovjerioca.

Član 23.

(Zaštita tajnosti i integriteta)

Ovjerilac osigurava zaštitu tajnosti i integritet privatnih ključeva, a naročito:

a) čuvanje i korištenje privatnog ključa za formiranje sigurnog elektronskog potpisa u sigurnom kriptografskom uređaju koji:

1) zadovoljava zahtjeve iz standarda FIPS PUB 140-2 nivo 3 i viši ili

2) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)" ili

3) zadovoljava zahtjeve iz standarda 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)";

b) da su dijelovi za aktivaciju privatnog ključa ovjerioca, kada se nalaze izvan kriptografskog uređaja šifrovani korištenjem simetričnog algoritma i dužine ključa, i omogućavaju pouzdanu odbranu od kriptoanalitičkih napada;

c) čuvanje dijelova za aktivaciju privatnog ključa, uz osiguranje rezervnih kopija tih dijelova, i aktivacija koju vrše zaposleni koji imaju sigurnosne funkcije, uz korištenje najmanje dvostruke kontrole u fizički osiguranom okruženju;

d) da se mjerama logičke kontrole pristupa onemogući neovlašteno aktiviranje kriptografskog uređaja sa privatnim ključem ovjerioca.

Član 24.

(Verifikacija sigurnog elektronskog potpisa)

Ovjerilac osigurava da njegov javni ključ kojim se verificira sigurni elektronski potpis kvalificiranih potvrda bude raspoloživ svim korisnicima i drugim zainteresiranim stranama na način kojim se osigurava autentičnost i integritet javnog ključa.

Član 25.

(Javni ključ)

Ovjerilac dostavlja svoj javni ključ i lokaciju liste opozvanih potvrda korisnicima i drugim zainteresiranim stranama na siguran način u obliku kvalificirane potvrde ili liste opozvanih potvrda.

Član 26.

(Korištenje privatnog ključa)

(1) Ovjerilac koristi svoj privatni ključ u skladu sa općim i posebnim pravilima i osigurava:
   a) da se koristi isključivo za formiranje sigurnog elektronskog potpisa kvalificiranih potvrda, kao i sigurnog elektronskog potpisa liste opozvanih potvrda;
   b) da se koristi samo u okviru fizički zaštićenih prostorija ovjerioca.
(2) Ovjerilac osigurava da se njegovi privatni ključevi ne koriste nakon isteka njihovog životnog ciklusa, u skladu sa općim i posebnim pravilima.
(3) Privatni ključevi, iz stava (2) ovog člana, uništavaju se na način kojim se osigurava da isti ne može biti ponovo formiran.

Član 27.

(Sigurnost kriptografskih uređaja)

Ovjerilac osigurava sigurnost kriptografskih uređaja koji se koriste za generiranje i čuvanje ključeva i formiranje sigurnog elektronskog potpisa tokom životnog ciklusa uređaja, u skladu sa posebnim pravilima, a naročito da:
   a) kriptografski uređaj nije kompromitiran tokom transporta;
   b) kriptografski uređaj nije kompromitiran za vrijeme čuvanja kod ovjerioca;
   c) procedure instalacije aktivacije, kreiranja rezervnih kopija i ponovnog formiranja privatnog ključa u kriptografskom uređaju vrši se u prisustvu najmanje dva zaposlena kojima je dodijeljena sigurnosna funkcija;
   d) ispravnost funkcioniranja kriptografskog uređaja;
   e) da se privatni ključevi ovjerioca čuvani u kriptografskom uređaju uništavaju nakon kraja životnog ciklusa ključeva ili uređaja.

POGLAVLJE VI - Zaštita potvrda i tajnosti generiranih ključeva

Član 28.

(Proces generiranja kvalificiranih potvrda)

Ovjerilac osigurava siguran proces generiranja kvalificiranih potvrda radi osiguranja njihove autentičnosti i integriteta.

Član 29.

(Ostale obaveze ovjerioca)

Ovjerilac osigurava:
   a) da se kvalificirane potvrde generiraju u skladu sa formatom definiranim u dokumentima ETSI TS 101 862, RFC 3739, RFC 3280 i ETSI TS 102 280;
   b) da je procedura generiranja kvalificirane potvrde sigurno povezana sa odgovarajućim procedurama registracije korisnika, obnavljanja potvrda uz zadržavanje postojećeg ili generiranje novog para ključeva;
   c) u slučaju da ovjerilac generira korisnikove ključeve osigurava:
      1) da je procedura generiranja kvalificirane potvrde sigurno povezana sa procedurom generiranja asimetričnog para ključeva od strane ovjerioca,
      2) da je privatni ključ, odnosno sredstvo za formiranje sigurnog elektronskog potpisa, sigurno dostavljeno do registriranog korisnika, a da se aktivacioni kod sredstva za formiranje sigurnog elektronskog potpisa ovlaštenom licu dostavi na siguran način drugim putem;
   d) jedinstvenost dodijeljenog imena korisniku u okviru domena ovjerioca;
   e) tajnost i integritet registracionih podataka, i to posebno u slučajevima razmjene podataka sa korisnikom ili u slučaju razmjene informacija između distribuiranih komponenti ovjerioca;
   f) verifikaciju dostavljenih registracionih podataka.

Član 30.

(Obnavljanje i izdavanje nove kvalificirane potvrdu)

Ovjerilac osigurava da se na zahtjev korisnika ranije opozvana kvalificirana potvrda obnavlja ili izdaje nova ukoliko su isti kompletni, tačni i autorizirani.

Član 31.

(Zahtjevi za obnavljanje i izdavanje nove kvalificirane potvrde)

(1) Na zahtjev za obnavljanjem potvrda, ovjerilac unosi ažurirane informacije o korisniku i sve druge izmjene koje su prethodno verificirane na isti način kao i u postupku registracije korisnika, u skladu sa čl. 15. i 16. ovog Pravilnika.
(2) Ovjerilac će izdati novu kvalifikovanu potvrdu koristeći prethodno certificirani javni ključ korisnika samo ako je njegova kriptografska sigurnost još uvijek dovoljna za predviđeni novi životni ciklus potvrde i ako ne postoje indikacije da je korisnikov privatni ključ kompromitiran.

POGLAVLJE VII - Odgovornost i osiguranje

Član 32.

(Odgovornost ovjeriocu u vezi certifikacionih servisa)

Ovjerilac je odgovoran da su svi certifikacioni servisi navedeni u politici certificiranja u skladu sa praktičnim pravilima.

Član 33.

(Pružanje usluga certificiranja)

(1) Pružanje usluga certificiranja regulira se posebnim ugovorom između ovjerioca i korisnika.
(2) Ugovorom iz stava (1) ovog člana uređuje se slijedeće:
   a) obaveza dostave tačnih i kompletnih informacija ovjeriocu u skladu sa procedurom registracije definiranom u politici certifikacije;
   b) korištenje privatnog ključa za formiranje sigurnog elektronskog potpisa;
   c) način pristupa svom privatnom ključu;
   d) koristi kvalifikovanu potvrdu samo uz siguran elektronski potpis koji je formiran sredstvima za formiranje sigurnog elektronskog potpisa;
   e) ukoliko zahtijeva kvalificirana potvrda od ovjerioca koja ispunjava uvjete iz Zakona o elektronskom potpisu i ovog Pravilnika, generira par ključeva za formiranje i provjeru sigurnog elektronskog potpisa u sredstvu za formiranje sigurnog elektronskog potpisa koje je u potpunosti pod njegovom kontrolom;
   f) odmah obavještenje ovjerioca ako prije isteka važnosti potvrde koji je naznačen u samoj potvrdi:

1) korisnikov privatni ključ se izgubi, ukrade ili nastupi osnovana sumnja da je kompromitiran,
2) prestane kontrola nad korištenjem korisnikovog privatnog ključa iz razloga kompromitiranja aktivacionih podataka (PIN kod ili lozinka) za sredstvo za formiranje sigurnog elektronskog potpisa ili drugih razloga,
3) ustanovi netačnost ili izmjenu sadržaja kvalificirane potvrde;

g) prekine korištenje svog privatnog ključa ukoliko postoji osnovana sumnja u kompromitaciju ključa ili kontrolu nad aktivacionim podacima za sredstvo za formiranje sigurnog elektronskog potpisa.

Član 34.

(Obaveze zainteresiranih strana)

U slučaju suspenzije ili opoziva kvalificirane potvrde, korisnik provjerava statusne informacije u vezi suspenzije ili opoziva potvrde koje je ovjerilac javno objavio u skladu sa općim pravilima, uvažavajući sva ograničenja u korištenju kvalifikacijske potvrde koja su naznačena u samoj potvrdi ili objavljena u općim pravilima.

Član 35.

(Finansijska sposobnost ovjerioca)

(1) Finansijska sredstva ovjerioca potrebna za obavljanje registrirane djelatnosti se prijavljuju i dokumentiraju Nadzornom organu, zajedno sa prijavom otpočinjanja djelatnosti.
(2) Ovjerioci koji izdaju kvalificione potvrde ili stavljaju na raspolaganje sigurne elektronske postupke izrade potpisa, moraju posjedovati osnovni kapital u iznosu od najmanje 600.000,00 KM.
(3) Ovjerioci koji izdaju kvalificirane potvrde ili stavljaju na raspolaganje sigurne elektronske postupke izrade potpisa, moraju osim toga, istovremeno sa prijavom otpočinjanja svoje djelatnosti, dokazati Nadzornom organu da su zaključili osiguranje od odgovornosti sa minimalnom sumom osiguranja od 1.500.000,00 KM, koje pokriva najmanje tri osiguravajuća slučaja u godini.
(4) Od obaveza iz st. (1) i (2) ovog člana su oslobođeni ovjerioci koji su zakonom uspostavljeni kao organi državne uprave u Bosni i Hercegovini.

POGLAVLJE VIII - Čuvanje podataka

Član 36.

(Čuvanje podataka)

(1) Ovjerilac osigurava trajno čuvanje svih relevantnih podataka koje se tiču kvalificiranih potvrda.
(2) U vezi sa stavom (1) ovog člana, ovjerilac osigurava:
a) tajnost i integritet tekućih i arhiviranih zapisa o kvalificiranim potvrdama;
b) kompletno i pouzdano arhiviranje podataka o kvalificiranim potvrdama u skladu sa općim pravilima;
c) da su zapisi u vezi kvalificiranih potvrda, kao i registracione i druge podatke o korisniku, raspoloživi za potrebe pravnih poslova kao dokaz izvršene certifikacije;
d) pouzdano arhiviranje tačnog vremena značajnih događaja u ovjeriocu;
e) da se podaci u vezi kvalificiranih potvrda čuvaju onoliko vremena koliko je potrebno da se koriste u pravnim poslovima vezanim za elektronske potpise;
f) evidentiranje svih događaja na način da se ne mogu lako obrisati ili uništiti (izuzev u cilju prijenosa na dugotrajne medije za čuvanje) u okviru vremenskog perioda u kome se moraju čuvati;
g) dokumentiranje specifičnih događaja i podataka koji treba da se evidentiraju;
h) evidentiranje svih događaja koji se odnose na registraciju korisnika, uključujući i zahtjeve za obnavljanjem potvrda, a naročito:
1) tip identifikacionog dokumenta koji je prezentiran od strane korisnika,
2) jedinstveni identifikacioni podatak o korisniku preuzet iz identifikacionog dokumenta,
3) mjesto čuvanja kopija aplikativnih i identifikacionih dokumenata, uključujući i potpisan Ugovor sa korisnikom,
4) specifične informacije iz Ugovora sa korisnikom,
5) identitet službenika ovjerioca koji je izvršio registraciju korisnika,
6) podatke o metodi koja je korištena za provjeru važenja identifikacionih dokumenata,
i) ime ovjerioca koje je primilo registracione informacije;
j) zaštitu privatnosti podataka korisnika i evidentiranje svih događaja u vezi sa životnim ciklusom ključeva ovjerioca;
k) evidentiranje svih događaja u vezi sa životnim ciklusom kvalificiranih potvrda i ključeva kojima upravlja ovjerilac, uključujući i korisničke ključeve ako su generirani u ovjeriocu;
l) evidentiranje svih događaja koji se odnose na primjenu sredstava za formiranje sigurnog elektronskog potpisa;
m) da se svi zahtjevi i izvještaji koji se odnose na proceduru opoziva potvrda evidentiraju, uključujući i sve odgovarajuće aktivnosti.

Član 37.

(Postupanje ovjerioca u slučaju prestanka rada)

Ovjerilac osigurava da u slučaju prestanka rada korisnik pretrpi minimalnu moguću štetu tako što će na propisan način čuvati podatake kao dokaz izvršene usluge, a naročito:

a) prije prestanka obavljanja djelatnosti, izvršava slijedeće aktivnosti:
1) informira sve korisnike o prestanku rada,
2) uništava, ili potpuno onemogućava korištenje, svojih privatnih ključeva koji su korišteni za formiranje sigurnog elektronskog potpisa kvalificiranih potvrda;
b) osigurava neophodna finansijska sredstva za realizaciju zahtjeva iz tačke a) ovog stava;
c) općim pravilima definira proceduru prestanka rada, koja obuhvata:
1) obavještavanje korisnika,
2) eventualni prijenos obaveza drugim ovjeriocima,
3) proceduru opoziva izdatih kvalificiranih potvrda kojima nije istekao rok važnosti, i prijenos listi opozvanih potvrda drugom ovjeriocu.

POGLAVLJE IX - Osiguranje uvjeta za korisnike za koje se generiraju podaci za formiranje sigurnog elektronskog potpisa

Član 38.

(Sredstvo za formiranje sigurnog elektronskog potpisa)

Ovjerilac može, uz usluge iz člana 4. ovog Pravilnika, a u skladu sa svojim općim i posebnim pravilima, da osigura i sredstvo za formiranje sigurnog elektronskog potpisa korisnicima i pridruženu lozinku (ili PIN kod) za aktivaciju sredstva, kao i njihovu sigurnu distribuciju do korisnika.

Član 39.
(Ključevi korisnika)

Ovjerilac osigurava da su ključevi korisnika koje on generira, generirani sigurno i da je osigurana tajnost privatnog ključa korisnika sve do njegove dostave korisniku i da pri isporuci samo korisnik ima pristup svom privatnom ključu.

Član 40.
(Asimetrični par korisničkih ključeva)

Ovjerilac osigurava da:

a) se asimetrični par korisničkih ključeva generira korištenjem algoritma koji je propisan da zadovolji zahtjeve koji se primjenjuju za sigurne elektronske potpise;
b) su asimetrični ključevi korisnika propisane dužine i korišteni u propisanom asimetričnom kriptografskom algoritmu u cilju da se zadovolje propisani zahtjevi za implementacijom sigurnog elektronskog potpisa.

Član 41.
(Uvjeti sigurnosti sredstava za formiranje sigurnog elektronskog potpisa)

Ukoliko ovjerilac osigura sredstva za formiranje sigurnog elektronskog potpisa za korisnike, to čini na siguran način a naročito osigurava da:

a) prijem sredstva za formiranje sigurnog elektronskog potpisa mora biti sigurno kontroliran od strane ovjerioca;
b) sredstva za formiranje sigurnog elektronskog potpisa moraju biti sigurno čuvana i distribuirana;
c) deaktiviranje i reaktiviranje sredstava za formiranje sigurnog elektronskog potpisa mora biti sigurno kontrolirano od strane ovjerioca;
d) ukoliko sredstvo za formiranje sigurnog elektronskog potpisa ima pridružene aktivacione podatke (PIN kod ili lozinka) isti mora biti sigurno pripremljen i šalju odvojeno u odnosu na sredstvo za formiranje sigurnog elektronskog potpisa, u različito vrijeme ili na različit način.

Član 42.
(Tajnost identifikacionih podataka)

(1) Ovjerilac koji izdaje kvalificirane potvrde i koji osigurava sredstvo za formiranje sigurnog elektronskog potpisa (engl. SSCD: Secure Signature - Creation Device) korisnicima garantira tajnost identifikacionih podataka (PIN kod, lozinka), nakon što se ugrade u ista.
(2) Ovlašteno lice ovjerioca kvalificiranu potvrdu, uz osiguranje SSCD korisnicima, kvalificiranu potvrdu uručuje lično korisniku uz svojeručni potpis korisnika o uručenju iste ili istu dostavlja u elektronskom obliku sigurnim elektronskim potpisom datog korisnika.
(3) Kvalificirana potvrda iz stava (1) ovog člana se verificira i stavlja na raspolaganje trećim licima tek nakon potvrde prijema SSCD uređaja i odgovarajućih identifikacionih podataka, uz dopuštenje korisnika.

POGLAVLJE X - Fizička zaštita

Član 43.
(Kontrola fizičkog pristupa)

Ovjerilac osigurava kontrolu fizičkog pristupa svojim sigurnosno kritičnim resursima i minimalan rizik u pristupu svojim ključnim elementima sistema.

Član 44.
(Mjere koje preduzima ovjerilac)

Ovjerilac osigurava da:

a) se fizički pristup prostorijama u kojima se obavlja generiranje kvalificiranih potvrda, prijem sredstava za formiranje sigurnog elektronskog potpisa i upravljanje procedurom opoziva potvrda, ograniči samo na pouzdano autorizirana lica;
b) su implementirane neophodne mjere u cilju izbjegavanja gubitaka, oštećenja ili kompromitiranja ključnih resursa i elimininiranje mogućnosti prekida poslovnih aktivnosti;
c) se implementiraju odgovarajuće mjere za sprječavanje kompromitiranja ili neovlaštenog preuzimanja informacija i uređaja za procesiranje informacija;
d) su prostorije u kojima se vrši generiranje kvalificiranih potvrda, prijem sredstava za formiranje sigurnog elektronskog potpisa i upravljanje opozivom, takve da se operativni rad u njima odvija u okruženju koje osigurava fizičku zaštitu certifikacionih servisa i resursa u slučaju zloupotrebe prilikom neautoriziranog pristupa sistemu i podacima;
e) je fizička zaštita uspostavljena kreiranjem jasno definiranih sigurnosnih fizičkih barijera kojima se štite procesi generiranja kvalificiranih potvrda, osiguranje sredstava za formiranje sigurnog elektronskog potpisa i upravljanje opozivom;
f) su implementirane odgovarajuće fizičke mjere i kontrole sigurnosnog okruženja u cilju zaštite prostorija i sistemskih elemenata ovjerioca;
g) su implementirane odgovarajuće mjere u cilju zaštite uređaja, informacija, memorijskih medija i softvera od otuđivanja sa lokacije bez propisne autorizacije;
h) se i druge specifične sigurnosne funkcije mogu primijeniti u okviru istog sigurnog prostora koji osigurava pristup samo autoriziranim zaposlenim licima.

Član 45.
(Osiguranje pristupa sistemu certifikacije)

Ovjerilac je dužan da pristup sistemu certifikacije ograniči isključivo na autorizirana lica, a naročito osigurava:

a) implementaciju kontrola na mrežnom nivou u cilju zaštite interne mreže ovjerioca od eksternih mrežnih domena kojima može pristupiti treća strana, uz zabranu svih protokola i pristupa koji se ne koriste u operativnom radu ovjerioca;
b) pouzdanu zaštitu osjetljivih podataka, koji uključuju i podatke o registraciji korisnika, tokom prolaska kroz dijelove mreže koji nisu sigurni;
c) efikasnu i pouzdanu administraciju korisničkih pristupa (uključujući operatore, administratore i bilo koje specifične korisnike koji imaju direktan pristup sistemu) u cilju održavanja sigurnosti sistema, uključujući i upravljanje nalozima korisnika, evidentiranje i mogućnost modifikacije i zabrane pristupa;
d) strogo ograničen pristup informacijama i aplikativnim funkcijama sistema u skladu sa općim i posebnim pravilima i politikom kontrole pristupa, identificiranom u njima, kao i dovoljnu računarsko-sigurnosnu kontrolu u cilju razdvajanja sigurnosnih funkcija u sistemu koje su identificirane u općim pravilima, uključujući razdvajanje funkcija administratora sigurnosti i operatera, a rad sa korisničkim programima za upravljanje sistemom mora biti posebno ograničen i strogo kontroliran;
e) pouzdanu identifikaciju i autentikaciju zaposlenih kod ovjerioca prije korištenja kritičnih operacija vezanih za procedure upravljanja potvrdama;
f) evidentiranje svih aktivnosti zaposlenih kod ovjerioca na osnovu odgovarajućih korisničkih naloga i log

fajlova, koji su potpisani sigurnim elektronskim potpisom;

g) pouzdanu zaštitu sigurnosno osetljivih podataka, koji uključuju i registracione podatke korisnika, od neautoriziranog pristupa prethodno obrisanim ili arhiviranim podacima;
h) da se lokalne fizičke mrežne komponente čuvaju u fizički zaštićenom okruženju i da se njihova konfiguracija periodično kontrolira u cilju ispitivanja usklađenosti sa zahtjevima specificiranim u općim i posebnim pravilima;
i) stalno nadziranje i alarmiranje koristeći sisteme za detekciju napada i nadziranje kontrole pristupa i alarma u cilju pouzdane detekcije, registracije i reakcije na neautoriziran ili neregularan pokušaj pristupa resursima koji se koriste za pružanje usluga certifikacije;
j) da aplikacija za distribuciju potvrda primijenjuje sistem logičke kontrole pristupa u cilju sprječavanja pokušaja dodavanja ili brisanja odgovarajućih potvrda i izmjene drugih pridruženih informacija;
k) da aplikacija za dobijanje statusa opoziva potvrda primjenjuje sistem logičke kontrole pristupa u cilju sprječavanja pokušaja izmjene informacija o statusu opoziva potvrda.

POGLAVLJE XI - Informacije o uvjetima izdavanja i korištenja potvrda

Član 46.

(Raspoloživost informacije)

(1) Ovjerilac osigurava da informacije o uvjetima izdavanja i korištenja kvalificiranih potvrda budu raspoložive korisnicima i drugim zainteresiranim stranama.
(2) Raspoloživost informacija iz stava (1) ovog člana osigurava se korištenjem jednostavnih vidova komunikacije (Internet i sl.) sa osiguranim integritetom tokom vremena, da se mogu prenositi elektronskim putem i da su prikazane na potpuno razumljiv način.

Član 47.

(Način osiguranja raspoloživosti informacija)

Ovjerilac osigurava raspoloživost informacija i podataka o svom poslovanju, i to:

a) opća pravila ovjerioca koja su trenutno važeća;
b) ograničenja u korištenju općih pravila;
c) obaveze korisnika;
d) informacije o načinu provjere važnosti kvalificiranih potvrda, uključujući i zahtjeve za provjeru statusa opoziva potvrda;
e) ograničenja odgovornosti koja uključuju slučajeve za koje ovjerilac prihvata ili odbija odgovornost;
f) vremenski period čuvanja registracionih informacija korisnika;
g) vremenski period čuvanja log fajlova za evidentiranje;
h) proceduru u slučaju podnošenja žalbi;
i) proceduru u slučaju spora;

XII - Upravljanje potvrdama

Član 48.

(Uvid u kvalificiranu potvrdu)

Ovjerilac osigurava uvid u status kvalificirane potvrde svim korisnicima i zainteresiranim stranama bez uvida u sadržaj iste.

Član 49.

(Raspoloživost podataka iz kvalificirane potvrde)

(1) Ovjerilac osigurava:
a) da je kvalificirana potvrda raspoloživa korisniku kojem je izdata;
b) da je kvalificirana potvrda raspoloživa trećim licima samo po odobrenju korisnika, a u skladu sa općim pravilima ovjerioca;
c) jednostavnu identifikaciju informacija o uvjetima izdavanja i korištenja kvalificiranih potvrda svim zainteresiranim stranama u sistemu;
d) da su informacije navedene pod tač. b) i c) ovog stava raspoložive 24 časa na dan, sedam dana u sedmici;

(2) U slučaju pada sistema ili djelimičnog gubitka mogućnosti za osiguranje servisa, ovjerilac je obavezan preduzeti sve raspoložive mjere u cilju aktiviranja informacionog servisa, najkasnije do isteka roka predviđenog u općim pravilima.

POGLAVLJE XIII - Provjera ispunjenosti uvjeta za izdavanje kvalificiranih potvrda

Član 50.

(Provjera ispunjenosti uvjeta)

Provjeru ispunjenosti uvjeta za izdavanje kvalificiranih potvrda vrši Nadzorni organ u postupku razmatranja zahtjeva ovjerioca za upis u Registar ovjerilaca.

Član 51.

(Ispunjavanje uvjeta)

Provjera ispunjenosti uvjeta za izdavanje kvalificiranih potvrda obuhvata:

a) provjeru općih pravila i posebnih pravila rada ovjerioca i njihove usklađenosti sa Zakonom i podzakonskim aktima;
b) provjeru atesta i certifikacije tehničkih i sigurnosnih komponenata koje koristi ovjerilac za generiranje javnih i privatnih ključeva i izdavanje kvalificiranih potvrda.

Član 52.

(Provjera operativnog rada ovjerioca)

Provjera operativnog rada ovjerioca obuhvata:

a) proceduru registracije korisnika kome se izdaje kvalificirana potvrda;
b) proceduru prijema zahtjeva za izdavanjem kvalificirane potvrde u registracionom autoritetu;
c) proceduru dostavljanja zahtjeva do ovjerioca;
d) proceduru generiranja kvalificirane potvrde;
e) korištenje sigurnih sistema za čuvanje podataka za generiranje kvalificiranih potvrda;
f) korištenje sigurnih hardverskih sredstava za formiranje sigurnog elektronskog potpisa (hardverski moduli zaštite (HSM - Hardware Security Module));
g) proceduru dostavljanja kvalifikovane potvrde, uređaja za generiranje elektronskog potpisa i identifikacionih podataka korisnicima;
h) proceduru opoziva potvrde;
i) proceduru obnavljanja potvrde;
j) proceduru suspenzije potvrde;
k) način objavljivanja liste opozvanih i suspendiranih potvrda;
l) sisteme fizičke kontrole pristupa u prostorije ovjerioca;
m) sisteme logičke kontrole pristupa računarskim resursima ovjerioca;
n) sistem za javno objavljivanje osnovnih informacija o pružanju usluga certifikacije, kao i općih pravila rada ovjerioca.

Član 53.

(Provjera tehničkih i sigurnosnih komponenti)

Provjera tehničkih i sigurnosnih komponenti koje koristi ovjerilac obuhvata:

a) realizaciju sistemskih zahtjeva sigurnosti;

b) izdavanje kvalificiranih potvrda primjenom sigurnog elektronskog potpisa;
c) sigurno generiranje ključeva ovjerioca.

Član 54.
(Operativni rad ovjerioca)

Operativni rad ovjerioca se obavlja u skladu sa standardom CEN WorkshopAgreement 14167-1 (March 2003) "Security Requirements for Trustworthy SystemsManaging Sertificates for Electronic Signatures - Part 1: System Security Requirements".

Član 55.
(Stupanje na snagu)

Ovaj Pravilnik stupa na snagu narednog dana od dana objave u "Službenom glasniku BiH".

VM broj 14//17
18. januara 2017. godine
Sarajevo

Predsjedavajući
Vijeća ministara BiH
Dr. **Denis Zvizdić**, s. r.

DRŽAVNA REGULATORNA KOMISIJA ZA ELEKTRIČNU ENERGIJU - DERK

216

Na temelju članka 4.2 i 4.7 Zakona o prijenosu, regulatoru i operatoru sustava električne energije u Bosni i Hercegovini ("Službeni glasnik BiH", br. 7/02, 13/03, 76/09 i 1/11), članka 51. Poslovnika o radu Državne regulatorne komisije za električnu energiju ("Službeni glasnik BiH", broj 2/05), članka 78. Pravilnika o javnim raspravama ("Službeni glasnik BiH", broj 38/05) i članka 35. Pravilnika o priključku ("Službeni glasnik BiH", br. 95/08, 79/10 i 60/12), na sjednici Državne regulatorne komisije za električnu energiju, održanoj 26. siječnja 2017. godine, donijeta je

ODLUKA
O RJEŠAVANJU SPORA

1. Javnom poduzeću Elektroprivreda Hrvatske zajednice Herceg Bosne, d.d. Mostar nalaže se da Elektroprijenosu Bosne i Hercegovine, a.d. Banja Luka plati iznos od 3.510.000,00 KM sa uključenim porezom na dodanu vrijednost, na ime fiksnog dijela naknade za priključak Hidroelektrane Mostarsko blato na prijenosnu mrežu.
2. Ova odluka stupa na snagu danom donošenja, a izreka odluke bit će objavljena u "Službenom glasniku BiH" i službenim glasilima entiteta.

Broj 03-14-2-191-17/16
26. siječnja 2017. godine
Tuzla

Predsjedatelj Komisije
Suad Zeljković, v. r.

На основу члана 4.2 и 4.7 Закона о преносу, регулатору и оператору система електричне енергије у Босни и Херцеговини ("Службени гласник БиХ", бр. 7/02, 13/03, 76/09 и 1/11), члана 51. Пословника о раду Државне регулаторне комисије за електричну енергију ("Службени гласник БиХ", број 2/05), члана 78. Правилника о јавним расправама ("Службени гласник БиХ", број 38/05) и члана 35. Правилника о прикључку ("Службени гласник БиХ", бр. 95/08, 79/10 и 60/12), на сједници Државне регулаторне комисије за електричну енергију, одржаној 26. јануара 2017. године, донијета је

ОДЛУКА
О РЈЕШАВАЊУ СПОРА

1. Јавном предузећу Електропривреда Хрватске заједнице Херцег Босне, д.д. Мостар налаже се да Електропреносу Босне и Херцеговине, а.д. Бања Лука плати износ од 3.510.000,00 КМ са укљученим порезом на додату вриједност, на име фиксног дијела накнаде за прикључак Хидроелектране Мостарско блато на преносну мрежу.
2. Ова одлука ступа на снагу даном доношења, а диспозитив одлуке биће објављен у "Службеном гласнику БиХ" и службеним гласилима ентитета.

Број 03-14-2-191-17/16
26. јануара 2017. године
Тузла

Предсједавајући Комисије
Суад Зељковић, с. р.

Na osnovu člana 4.2 i 4.7 Zakona o prijenosu, regulatoru i operatoru sistema električne energije u Bosni i Hercegovini ("Službeni glasnik BiH", br. 7/02, 13/03, 76/09 i 1/11), člana 51. Poslovnika o radu Državne regulatorne komisije za električnu energiju ("Službeni glasnik BiH", broj 2/05), člana 78. Pravilnika o javnim raspravama ("Službeni glasnik BiH", broj 38/05) i člana 35. Pravilnika o priključku ("Službeni glasnik BiH", br. 95/08, 79/10 i 60/12), na sjednici Državne regulatorne komisije za električnu energiju, održanoj 26. januara 2017. godine, donijeta je

ODLUKA
O RJEŠAVANJU SPORA

1. Javnom preduzeću Elektroprivreda Hrvatske zajednice Herceg Bosne, d.d. Mostar nalaže se da Elektroprijenosu Bosne i Hercegovine, a.d. Banja Luka plati iznos od 3.510.000,00 KM sa uključenim porezom na dodatu vrijednost, na ime fiksnog dijela naknade za priključak Hidroelektrane Mostarsko blato na prijenosnu mrežu.
2. Ova odluka stupa na snagu danom donošenja, a izreka odluke bit će objavljena u "Službenom glasniku BiH" i službenim glasilima entiteta.

Broj 03-14-2-191-17/16
26. januara 2017. godine
Tuzla

Predsjedavajući Komisije
Suad Zeljković, s. r.

KONKURENCIJSKO VIJEĆE BOSNE I HERCEGOVINE

217

Konkurencijsko vijeće Bosne i Hercegovine na temelju članka 25. stavak (1) točka e), članka 42. stavak (1) točka d), a u svezi sa čl. 12., 14., 16. i 18. Zakona o konkurenciji ("Službeni glasnik BiH", br. 48/05, 76/07 i 80/09), rješavajući po Prijavi koncentracije gospodarskog subjekta ORBICO d.o.o. za trgovinu Zagreb, Koturaška cesta 69, Zagreb, Republika Hrvatska, podnesenoj putem Odvjetničkog društva dmb legal d.o.o., Kralja Tvrtka 6, 71 000 Sarajevo, Bosna i Hercegovina na 136. (stotinutridesetšestoj) sjednici održanoj dana 21.12.2016. godine, donio je

RJEŠENJE

1. Ocjenjuje se dopuštenom koncentracija na tržištu trgovine na veliko parfemima i kozmetikom na teritoriju Bosne i Hercegovine, koja će nastati stjecanjem kontrole gospodarskog subjekta ORBICO d.o.o. za trgovinu Zagreb nad gospodarskim subjektom EVERET INTERNATIONAL međunarodna trgovinska družba d.o.o. Ljubljana.
2. Ovo Rješenje o koncentraciji se upisuje u Registar koncentracija.
3. Ovo Rješenje je konačno i bit će objavljeno u "Službenom glasniku BiH", službenim glasnicima entiteta i Brčko distrikta Bosne i Hercegovine.