PRAVILNIK
O BLIŽIM USLOVIMA ZA IZDAVANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

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

Član 1

Ovim pravilnikom propisuju se bliži uslovi za izdavanje kvalifikovanih elektronskih sertifikata i način provere njihove ispunjenosti.

I USLOVI KOJE SERTIFIKACIONO TELO TREBA DA ISPUNI ZA IZDAVANJE KVALIFIKOVANIH SERTIFIKATA

Sposobnost za pouzdano obavljanje usluga izdavanja kvalifikovanih elektronskih sertifikata

Član 2

Izdavanje kvalifikovanih elektronskih sertifikata mora biti u skladu sa odgovarajućim međunarodnim standardima i preporukama, odnosno drugim standardima, dokumentima i preporukama koje se odnose na izdavanje kvalifikovanih elektronskih sertifikata, utvrđenim ovim pravilnikom.

Član 3

Sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata (u daljem tekstu: sertifikaciono telo) izdaje kvalifikovane elektronske sertifikate tako što formira kvalifikovani elektronski potpis sertifikata na osnovu svog privatnog ključa i asimetričnog kriptografskog algoritma u skladu sa pravilnikom o tehničko-tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i uslovima i kriterijumima koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa.

Sertifikaciono telo izdaje kvalifikovane elektronske sertifikate 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*" i sa obaveznim sadržajem definisanim u članu 17. Zakona o elektronskom potpisu (u daljem tekstu: Zakon).

Član 4

Sertifikaciono telo dužno je da obezbedi kompletne usluge sertifikacije koje uključuju sledeće servise, i to:

1. Registraciju korisnika;
2. Formiranje kvalifikovanih elektronskih sertifikata;

3. Distribuciju kvalifikovanih elektronskih sertifikata korisnicima;
4. Upravljanje životnim vekom (obnavljanje, suspenzija, opoziv) kvalifikovanih elektronskih sertifikata;
5. Obezbeđivanje pouzdanog i javno dostupnog servisa za proveru statusa opozvanosti kvalifikovanih elektronskih sertifikata.

Sertifikaciono telo može, pored servisa iz stava 1. ovog člana, da obezbedi i formiranje asimetričnog para ključeva za korisnike, kao i distribuciju privatnog ključa i sertifikata korisniku na bezbedan način, ukoliko je to propisano u Politici sertifikacije datog sertifikacionog tela.

Član 5

Sertifikaciono telo, pre početka rada, utvrđuje Opšta interna pravila pružanja usluge sertifikacije (u daljem tekstu: Opšta pravila) koja korisnicima obezbeđuju dovoljno informacija na osnovu kojih se mogu odlučiti o prihvatanju usluga i o obimu usluga.

Opšta pravila Sertifikacionog tela ugrađuju se u dokumentima:
1. Politika sertifikacije (*Certificate Policy*);
2. Praktična pravila pružanja usluge Sertifikacije (*Certification Practices Statement*) (u daljem tekstu: Praktična pravila).

Politika sertifikacije i Praktična pravila jesu javni dokumenti.

Član 6

Politika sertifikacije definiše predmet rada sertifikacionog tela, dok Praktična pravila definišu procese i način njihovog korišćenja pri formiranju i upravljanju kvalifikovanim elektronskim sertifikatima. Politika sertifikacije definiše zahteve poslovanja sertifikacionog tela, dok Praktična pravila definišu operativne procedure u cilju ispunjenja tih zahteva. Praktična pravila definišu način na koji sertifikaciono telo ispunjava tehničke, organizacione i proceduralne zahteve poslovanja koji su identifikovani u Politici sertifikacije.

Politika sertifikacije je manje specifičan i detaljan dokument u odnosu na Praktična pravila koja predstavljaju mnogo detaljniji opis načina poslovanja, kao i poslovne i operativne procedure koje sertifikaciono telo primenjuje u izdavanju i upravljanju kvalifikovanim elektronskim sertifikatima.

Politika sertifikacije se definiše nezavisno od specifičnog operativnog okruženja sertifikacionog tela, dok Praktična pravila daju detaljan opis organizacione strukture, operativnih procedura, kao i fizičko i računarsko okruženje sertifikacionog tela.

Član 7

Opšta pravila funkcionisanja sertifikacionog tela treba da budu u skladu sa dokumentima RFC 3647 "Internet X.509 *Public Key Infrastructure. Certificate Policy and Certification Practices Framework*" i ETSI TS 101 456 "*Policy Requirements for Certification Authorities Issuing Qualified Certificates*".

Član 8

Sadržaj dokumenata Politika sertifikacije i Praktična pravila, obuhvata:

1. Opšte odredbe o radu sertifikacionog tela:
    - Pojam sertifikacionog tela,
    - Sertifikacione usluge,
    - Obuhvat dokumenta Politika sertifikacije,
    - Obuhvat dokumenta Praktična pravila pružanja usluge sertifikacije,
    - korisnike usluga sertifikacije;
2. Uvodne odredbe o Politici izdavanja kvalifikovanih elektronskih sertifikata;
3. Obaveze i odgovornosti:
    - Obaveze sertifikacionog tela,
    - Obaveze korisnika,
    - Odgovornost sertifikacionog tela,
    - Odgovornost korisnika;
4. Funkcionalne zahteve za rad sertifikacionog tela:
    - Operativne procedure rada sertifikacionog tela,
    - Procedure upravljanja životnim ciklusom kriptografskih ključeva:
        - Generisanje ključa sertifikacionog tela,
        - Procedure čuvanja i formiranja rezervnih kopija ključeva sertifikacionog tela,
        - Distribuciju javnog ključa sertifikacionog tela,
        - Korišćenje ključa sertifikacionog tela,
        - Kraj životnog ciklusa ključa sertifikacionog tela,
        - Upravljanje životnim ciklusom kriptografskog hardvera koji se koristi za generisanje kvalifikovanih sertifikata,
        - Upravljanje ključevima korisnika za identifikaciju i digitalnu envelopu,
        - Proceduru pripreme sredstava za formiranje kvalifikovanog elektronskog potpisa;
    - Procedure upravljanja životnim ciklusom sertifikata:
        - Metode registracije korisnika,
        - Izdavanje sertifikata,
        - Distribucija sertifikata,
        - Obnavljanje sertifikata,
        - Suspenzija sertifikata,
        - Opoziv sertifikata,
        - Način publikacije liste opozvanih sertifikata;
    - Upravljanje operativnim radom sertifikacionog tela:
        - Upravljanje u skladu sa bezbednosnim principima,
        - Upravljanje i klasifikacija najvažnijih informacija i podataka u okviru sertifikacionog tela,
        - Kadrovski resursi,
        - Sistem fizičke bezbednosti i bezbednosti okruženja,
        - Upravljanje radom sertifikacionog tela,
        - Upravljanje sistemom kontrole pristupa,
        - Upotreba i održavanje bezbednih kriptografskih sistema,
        - Upravljanje procedurama kontinualnog poslovanja u incidentnim situacijama,
        - Prestanak rada sertifikacionog tela,
        - Usaglašenost rada sa kriterijumima za rad sertifikacionih tela koja izdaju kvalifikovane elektronske sertifikate u skladu sa Zakonom i ovim pravilnikom,
        - Formiranje i čuvanje dokumentacije koja se odnosi na kvalifikovane elektronske sertifikate;
5. Organizacija rada sertifikacionog tela.

Član 9

Sertifikaciono telo demonstrira sposobnost za obezbeđivanje usluga izdavanja kvalifikovanih elektronskih sertifikata, tako što mora:

1. Imati Praktična pravila, i u njima definisane procedure, u kojima se specificira način ispunjenja svih zahteva za izdavanjem kvalifikovanih elektronskih sertifikata koji su identifikovani u Politici sertifikacije;
2. Učiniti raspoloživim Praktična pravila svim korisnicima i drugim zainteresovanim stranama;
3. Objaviti svim korisnicima i potencijalnim zainteresovanim stranama uslove korišćenja kvalifikovanih elektronskih sertifikata;
4. Imati upravnu strukturu najvišeg nivoa koja će imati konačnu autorizaciju i odgovornost za objavljivanje Praktičnih pravila sertifikacionog tela;
5. Imati upravnu strukturu operativnog nivoa u sertifikacionom telu koja je odgovorna za ispravnu primenu Praktičnih pravila;
6. Definisati proces periodične analize i održavanja Praktičnih pravila;
7. Imati odobrene, od strane upravne strukture najvišeg nivoa, sve izmene u Praktičnim pravilima, tj. nove verzije Praktičnih pravila, u skladu sa tačkom 4. ovog stava i, nakon odobravanja, odmah javno objavljene u skladu sa tačkom 2. ovog stava.

Član 10

Sertifikaciono telo utvrđuje i Posebna interna pravila rada sertifikacionog tela i zaštite sistema sertifikacije (u daljem tekstu: Posebna pravila) u kojima su sadržani i detaljno opisani postupci i mere koji se primenjuju prilikom izdavanja i rukovanja kvalifikovanim elektronskim sertifikatima.

Posebna pravila su privatni dokument i predstavljaju poslovnu tajnu sertifikacionog tela.

Član 11

Posebna pravila sadrže detaljne odredbe o:

1. Sistemu fizičke kontrole pristupa u pojedine prostorije sertifikacionog tela;
2. Sistemu logičke kontrole pristupa računarskim resursima sertifikacionog tela;
3. Sistemu za čuvanje privatnog ključa sertifikacionog tela;
4. Sistemu distribuirane odgovornosti pri aktivaciji privatnog ključa sertifikacionog tela;
5. Postupcima i radnjama u vanrednim situacijama (požari, poplave, zemljotresi, druge vremenske nepogode, zlonamerni upadi u prostorije ili informacioni sistem sertifikacionog tela).

Član 12

Sertifikaciono telo obezbeđuje pouzdanu organizaciju rada, a naročito:

1. Pravila i operativne procedure koje nisu diskriminatorske;
2. Dostupnost svojih servisa svim korisnicima čije su aktivnosti u skladu sa objavljenim Opštim pravilima;
3. Poslovanje u svojstvu pravnog lica u skladu sa odgovarajućim domaćim propisima;

4. Sistem kvaliteta i sistem bezbednog upravljanja kvalifikovanim elektronskim sertifikatima u skladu sa uslugama sertifikacije koje pruža;
5. Osiguranje od odgovornosti za štetu koja može da proistekne u vršenju njegovih aktivnosti u skladu sa Politikom sertifikacije;
6. Finansijsku stabilnost i dovoljne resurse koji se zahtevaju u pružanju usluga sertifikacije u skladu sa Politikom sertifikacije;
7. Dovoljan broj stalno zaposlenih na poslovima sertifikacije sa neophodnim obrazovanjem, nivoom obučenosti, tehničkim znanjima i iskustvom;
8. Efikasno postupanje u rešavanju žalbi i sporova sa korisnicima ili drugim zainteresovanim stranama u vezi pružanja usluga sertifikacije;
9. Nezavisnost delova sertifikacionog tela uključenih u poslove generisanja kvalifikovanih elektronskih sertifikata od drugih spoljnih organizacija u sferi pružanja usluga sertifikacije. Posebno upravna struktura sertifikacionog tela, kao i zaposleni sa bezbednosnim funkcijama, moraju biti zaštićeni od bilo kakvih finansijskih i drugih pritisaka koji mogu uticati na poverenje u usluge sertifikacije koje pruža sertifikaciono telo;
10. propisno dokumentovanu strukturu delova sertifikacionog tela povezanih sa generisanjem kvalifikovanih elektronskih sertifikata radi obezbeđivanja nepristrasnosti u pružanju usluga sertifikacije, u skladu sa Opštim i Posebnim pravilima.

Član 13

Sertifikaciono telo je dužno da obezbedi najniži iznos osiguranja od rizika odgovornosti za moguću štetu nastalu vršenjem usluga izdavanja elektronskih sertifikata tako da:

1. Osigurana suma na koju mora biti ugovoreno osiguranje po jednom štetnom događaju ne može iznositi manje od 20.000 evra u dinarskoj protivvrednosti, podrazumevajući pritom kao štetni događaj pojedinačnu štetu nastalu upotrebom jednog kvalifikovanog sertifikata u jednom aktu u pravnom prometu;
2. Ukupna osigurana suma na koju mora biti ugovoreno osiguranje od odgovornosti sertifikacionog tela kumulativno na godišnjem nivou, po svim štetnim događajima, ne može biti niža od 1.000.000 evra u dinarskoj protivvrednosti.

Član 14

Sertifikaciono telo obezbeđuje da u slučaju katastrofa operativni rad bude obnovljen što je moguće pre a u skladu sa Opštim i Posebnim pravilima.

U slučaju kompromitacije svog asimetričnog privatnog ključa, sertifikaciono telo:

1. Prestaje sa izdavanjem kvalifikovanih elektronskih sertifikata;
2. Informiše sve korisnike i druge zainteresovane strane o kompromitaciji privatnog ključa;
3. Javno objavljuje informacije o tome da izdati kvalifikovani elektronski sertifikati, kao i informacije o statusu opozvanosti kvalifikovanih elektronskih sertifikata, više nisu važeće;
4. Vrši opoziv svih izdatih kvalifikovanih elektronskih sertifikata odmah a najkasnije u roku od 24 časa u skladu sa Zakonom.

Bezbedno i ažurno vođenje registra izdatih i opozvanih sertifikata

Član 15

Sertifikaciono telo vodi ažurnu, tačnu i bezbednu evidenciju izdatih kvalifikovanih elektronskih sertifikata koja može biti javno dostupna, osim u slučajevima kada vlasnik sertifikata izričito zahteva da njegovi podaci ne budu javno dostupni, ili kada sertifikat nosi JMBG ili lični broj, a u skladu sa članom 28. tačka 6. Zakona.

Sertifikaciono telo vodi ažurnu i bezbednu evidenciju nevažećih (opozvanih i suspendovanih) kvalifikovanih elektronskih sertifikata i mora za svaki sertifikat koji je izdalo, informaciju o njegovoj validnosti učiniti javno dostupnom.

Tačnost i validnost evidencija iz st. 1. i 2. ovog člana, sertifikaciono telo garantuje svojim kvalifikovanim elektronskim potpisom.

Obezbeđivanje tačnog vremena izdavanja i opoziva sertifikata

Član 16

Za pouzdano određivanje vremena izdavanja i opoziva kvalifikovanih elektronskih sertifikata, sertifikaciono telo mora obezbediti izvor tačnog vremena koji je sinhronizovan sa izvorom referentnog vremena koji odredi Ministarstvo i objavljuje na veb strani Ministarstva.

Tačno vreme izdavanja kvalifikovanog elektronskog sertifikata sertifikaciono telo ugrađuje u izdati kvalifikovani elektronski sertifikat.

Tačno vreme izdavanja i opoziva kvalifikovanih elektronskih sertifikata sertifikaciono telo čuva u evidenciji izdatih i opozvanih sertifikata iz člana 15. ovog pravilnika.

Procedure registracije korisnika

Član 17

Sertifikaciono telo vrši registraciju korisnika, odnosno pouzdanu identifikaciju i autentikaciju korisnika kojima izdaje kvalifikovane elektronske sertifikate, u skladu sa članom 28. tačka 2. Zakona.

Postupke registracije iz stava 1. ovog člana vrši ovlašćeni službenik sertifikacionog tela ili registracionog tela na udaljenoj registracionoj lokaciji koje uspostavlja sertifikaciono telo za potrebe registracije korisnika.

Registraciono telo, u smislu ovog pravilnika, jeste organizaciona jedinica sertifikacionog tela ili ovlašćena jedinica od strane sertifikacionog tela za vršenje poslova registracije korisnika.

Član 18

Sertifikaciono telo dužno je da u postupku registracije korisnika, u skladu sa članom 17. ovog pravilnika, obezbedi da:

1. Se korisnik identifikuje kao fizičko lice sa specifičnim atributima koji mogu označavati organizacionu jedinicu ili ulogu u organizaciji gde je zaposlen;
2. Pre uspostavljanja ugovornog odnosa sa korisnikom, javno informiše korisnika na jasnom i razumljivom jeziku o svim relevantnim uslovima korišćenja kvalifikovanih elektronskih sertifikata;
3. Se verifikuje identitet korisnika u skladu sa važećim propisima. Pod skupom podataka koji jedinstveno identifikuje potpisnika u skladu sa članom 17. tačka 3. Zakona podrazumevaju se identifikacioni podaci koji su sadržani u identifikacionim dokumentima;
4. Za pouzdanu proveru identiteta korisnika u postupku registracije, zahteva fizičko prisustvo korisnika u sertifikacionom telu ili u registracionom telu;
5. Ako je potrebno, verifikuje i bilo koji specifični atribut korisnika kome se izdaje kvalifikovani elektronski sertifikat;
6. Ukoliko se radi o fizičkom licu kao individualnom korisniku, identitet korisnika mora da bude proveren na osnovu zakonom propisanog ličnog identifikacionog dokumenta;
7. Ukoliko se radi o korisniku koji se identifikuje kao pripadnik pravnog lica ili neke organizacije, dokaz njegovog identiteta mora da sadrži sledeće elemente, i to:
    - Zakonom propisani lični identifikacioni dokument,
    - Pravno valjane podatke o registraciji pravnog lica ili organizacije,
    - Dokaz da je korisnik ovlašćen od strane tog pravnog lica ili organizacije za dobijanje kvalifikovanog elektronskog sertifikata;
8. Informacije sadržane u kvalifikovanom elektronskom sertifikatu budu pouzdane i tačne;
9. Korisnik mora dostaviti tačne i pouzdane informacije o fizičkoj adresi, ili drugim atributima, koji opisuju kako se korisnik može kontaktirati;
10. Čuva sve informacije korišćene za verifikaciju identiteta korisnika i dokumentaciju korišćenu za identifikaciju, kao i bilo koja ograničenja njene važnosti;
11. Sa korisnikom zaključi ugovor koji treba, naročito, da sadrži:
    - Obaveze korisnika,
    - Obavezu korisnika da koristi sredstvo za formiranje kvalifikovanog elektronskog potpisa koje obezbeđuje sertifikaciono telo, ako je to u skladu sa Opštim pravilima,
    - Obavezu sertifikacionog tela da čuva podatke korišćene u registraciji korisnika i sve informacije o životnom ciklusu izdatog kvalifikovanog elektronskog sertifikata korisnika. Prosleđivanje ovih informacija trećim stranama je pod uslovima definisanim Politikom sertifikacije,
    - Uslove za publikaciju sertifikata,
    - Potvrdu da su informacije sadržane u sertifikatu korektne;
12. Ugovor iz tačke 11) ovog stava čuva u roku iz člana 31. Zakona;
13. Ako asimetrični par ključeva korisnika nije generisan od strane sertifikacionog tela, proces generisanja zahteva za kvalifikovanim elektronskim sertifikatom u potpunosti obezbeđuje da korisnik poseduje asimetrični privatni ključ koji je matematički, na bazi asimetričnog kriptografskog algoritma, povezan sa javnim ključem koji je prezentiran za sertifikaciju. U tom slučaju korisnik mora obezbediti da se asimetrični par ključeva generiše isključivo u sredstvu za formiranje kvalifikovanog elektronskog potpisa;
14. Se poštuju odredbe važećih propisa kojima se uređuje zaštita podataka o ličnosti.

Kadrovski resursi i upravljanje operativnim radom sertifikacionog tela

Član 19

Sertifikaciono telo obezbeđuje strukturu stalno zaposlenih u skladu sa zahtevima za pouzdano i bezbedno funkcionisanje sertifikacionog tela koje izdaje kvalifikovane elektronske sertifikate na osnovu Zakona i ovog pravilnika.

Član 20

Sertifikaciono telo obezbeđuje neophodne kadrovske resurse, i sa njima povezane preduslove, a naročito da:

1. Zaposleni u sertifikacionom telu moraju da poseduju ekspertsko znanje, iskustvo i neophodnu kvalifikaciju za usluge koje sertifikaciono telo nudi, kao i za odgovarajuće poslovne funkcije, i to:
    - Najmanje 4 zaposlenih sa višom ili visokom školskom spremom iz oblasti informaciono-komunikacionih tehnologija i radnim iskustvom od najmanje 3 godine u oblasti održavanja i bezbednosti informacionih sistema i položen najmanje jedan od ispita: *CompTIA Security+*, ISC2 CISSP ili SANS GSEC,
    - Najmanje 2 od zaposlenih iz prethodne tačke treba da ima visoku školsku spremu i 5 godina radnog iskustva u oblasti informacionih sistema i položen ISC2 CISSP ispit ili SANS GSEC ispite u oblasti bezbednosti informacionih sistema;
2. Uloge i funkcije bezbednosti, utvrđene u Opštim pravilima, moraju biti dokumentovane i detaljno specificirane sa opisima svakog radnog mesta u sertifikacionom telu. Poslovne funkcije od najvišeg nivoa poverljivosti, od kojih najviše zavisi bezbednost funkcionisanja sertifikacionog tela, moraju biti posebno i jasno identifikovane;
3. Zaposleni u sertifikacionom telu (stalni i privremeni) moraju imati opise poslova definisane sa stanovišta razdvajanja dužnosti i privilegija. Opisi poslova moraju razlikovati opšte poslove i specifične funkcije sertifikacionog tela. Preporučuje se da opisi poslova uključe i definicije zahteva za specifičnim veštinama i iskustvom koja se traže od zaposlenih;
4. Zaposleni u upravnoj strukturi sertifikacionog tela moraju da poseduju ekspertizu u tehnologiji elektronskog potpisa, da su dobro upoznati sa bezbednosnim procedurama za zaposlene i sa odgovornostima u domenu bezbednosti, kao i da imaju odgovarajuća iskustva u primeni bezbednih informacionih sistema i proceni rizika;
5. Svi zaposleni u sertifikacionom telu sa bezbednosnim funkcijama ne smeju imati sukobe interesa koji mogu uticati na nepristrasnost rada sertifikacionog tela;
6. Bezbednosne funkcije u sertifikacionom telu uključuju sledeće odgovornosti, i to za:
    - Glavnog administratora bezbednosti - sveukupnu odgovornost za administriranje i implementaciju bezbednosnih funkcija i procedura, kao i upravljanje aktivnostima na dodatnom unapređenju poslova generisanja, opoziva i suspenzije kvalifikovanih elektronskih sertifikata,
    - Sistem administratore - autorizovanu odgovornost za instalaciju, konfigurisanje i održavanje bezbednih sistema sertifikacionog tela za registraciju korisnika, generisanje kvalifikovanih elektronskih sertifikata, obezbeđenje sredstava za formiranje kvalifikovanog

elektronskog potpisa za korisnike i upravljanje opozivom kvalifikovanih elektronskih sertifikata,
   - Sistem operatore - odgovornost za rad bezbednih sistema sertifikacionog tela u tekućem radu na dnevnom nivou i autorizovanu odgovornost za implementaciju sistema za formiranje rezervnih kopija i procedure oporavka,
   - Sistem evidentičare - autorizovanu odgovornost za pregledanje i održavanje arhiva i log fajlova bezbednih sistema sertifikacionog tela;
7. Zaposlenima u sertifikacionom telu moraju biti formalno dodeljene bezbednosne funkcije od strane više upravne strukture nadležne za bezbednost;
8. Sertifikaciono telo ne sme dodeliti bezbednosne ni upravne funkcije osobama koje su osuđivane ili koje su na bilo koji način kažnjavane u odnosu na njihovu podobnost za rad na odgovornim funkcijama. Zaposleni ne smeju imati pristup bezbednosnim funkcijama pre završetka neophodnih provera.

Korišćenje pouzdanih i bezbednih kriptografskih sistema

Član 21

Sertifikaciono telo mora da koristi bezbedne sisteme i proizvode koji su zaštićeni od neovlašćenih modifikacija.

Član 22

Sertifikaciono telo pre početka obavljanja usluga sertifikacije, kao i periodično, tokom operativnog rada, vrši analizu rizika kojom identifikuje kritične servise koji zahtevaju korišćenje bezbednih sistema i visoke nivoe sigurnosti.

Član 23

Sertifikaciono telo obezbeđuje bezbedno i korektno funkcionisanje svojih sistema, sa minimalnim rizikom od kvarova, a naročito:

1. Zaštićen integritet sistema sertifikacionog tela, kao i informacija, od virusa, malicioznog i neautorizovanog softvera;
2. Minimalnu štetu usled mogućih incidenata korišćenjem procedura izveštavanja i odgovarajućih odgovora. Sertifikaciono telo mora da reaguje brzo i koordinirano u cilju odgovora na bezbednosne incidente i da ograniči uticaj bezbednosnih upada;
3. Bezbedno korišćenje memorijskih medijuma u skladu sa unapred specificiranim šemama klasifikacije informacija. Mediji koji sadrže bezbednosno osetljive podatke moraju biti bezbedno arhivirani ukoliko nisu u operativnom radu;
4. Uspostavljene i implementirane procedure za sve bezbedne i administrativne funkcije - role koje imaju uticaj na pružanje usluga sertifikacije. Svaki zaposleni iz upravne strukture sertifikacionog tela je odgovoran za planiranje i efektivnu implementaciju Opštih pravila;
5. Stalni nadzor tekućih i budućih potreba za kapacitetom sistema sertifikacionog tela radi obezbeđenja adekvatne procesne snage i memorijskih kapaciteta.

Član 24

Sertifikaciono telo obezbeđuje da su njegovi asimetrični ključevi generisani u strogo kontrolisanim i bezbednim uslovima, a naročito da se:

1. Generisanje asimetričnih ključeva vrši u fizički zaštićenom okruženju od strane i uz minimalan broj autorizovanih zaposlenih (najmanje dva zaposlena lica) za izvršavanje ove funkcije a prema zahtevima i procedurama definisanim u Praktičnim pravilima;
2. Generisanje asimetričnih ključeva vrši u sredstvu koje:
   - Zadovoljava zahteve iz standarda FIPS PUB 140-2 nivo 3 i viši ili
   - CEN *Workshop Agreement* (CWA) 14169: "*Secure Signature-Creation Device* (EAL 4+)" ili
   - Zadovoljava zahteve 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. Generisanje ključeva vrši korišćenjem algoritma verifikovanog za svrhu generisanja kvalifikovanih elektronskih sertifikata od strane Ministarstva;
4. Da rezervne kopije privatnih ključeva za formiranje kvalifikovanog elektronskog potpisa kvalifikovanih elektronskih sertifikata imaju isti ili viši nivo bezbednosnih kontrola u odnosu na ključeve koji se operativno koriste;
5. Obezbedi da su izdati kvalifikovani elektronski sertifikati potpisani kvalifikovanim elektronskim potpisom sertifikacionog tela.

Član 25

Sertifikaciono telo obezbeđuje zaštitu tajnosti i integritet asimetričnih privatnih ključeva, a naročito:

1. Čuvanje i korišćenje privatnog ključa za formiranje kvalifikovanog elektronskog potpisa u bezbednom kriptografskom uređaju koji:
   - Zadovoljava zahteve iz standarda FIPS PUB 140-2 nivo 3 i viši ili
   - CEN *Workshop Agreement* (CWA) 14169: "*Secure Signature-Creation Device* (EAL 4+)" ili
   - Zadovoljava zahteve 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)";
2. Da su delovi za aktivaciju privatnog ključa sertifikacionog tela, kada se nalaze izvan kriptografskog uređaja šifrovani korišćenjem simetričnog algoritma i dužine ključa, verifikovanih za te potrebe od strane Ministarstva, i koji omogućavaju pouzdanu odbranu od kriptoanalitičkih napada;
3. Čuvanje delova za aktivaciju privatnog ključa, uz obezbeđenje rezervnih kopija tih delova, i aktivacija samo od strane onih zaposlenih koji imaju bezbednosne funkcije, uz korišćenje najmanje dvostruke kontrole u fizički obezbeđenom okruženju. Broj zaposlenih u sertifikacionom telu koji su autorizovani da izvršavaju ove funkcije mora biti minimalan i mora da zadovolji zahteve i procedure definisane u Opštim i Posebnim pravilima rada sertifikacionog tela;
4. Da se merama logičke kontrole pristupa onemogući neovlašćeno aktiviranje kriptografskog uređaja sa privatnim ključem sertifikacionog tela.

Član 26

Sertifikaciono telo obezbeđuje da njegov asimetrični javni ključ koji služi za verifikaciju kvalifikovanog elektronskog potpisa kvalifikovanih elektronskih sertifikata bude raspoloživ svim korisnicima i drugim zainteresovanim stranama na način kojim se obezbeđuje autentičnost i integritet javnog ključa.

Član 27

Sertifikaciono telo mora svoj asimetrični javni ključ i lokaciju liste opozvanih sertifikata distribuirati korisnicima i drugim zainteresovanim stranama na siguran način u obliku kvalifikovanog elektronskog sertifikata, odnosno liste opozvanih sertifikata.

Član 28

Sertifikaciono telo koristi svoj asimetrični privatni ključ u skladu sa Opštim i Posebnim pravilima, a naročito obezbeđuje:

1. Da se koristi isključivo za formiranje kvalifikovanog elektronskog potpisa kvalifikovanih elektronskih sertifikata, kao i kvalifikovanog elektronskog potpisa liste opozvanih sertifikata;
2. Da se koristi samo u okviru fizički zaštićenih prostorija sertifikacionog tela.

Član 29

Sertifikaciono telo obezbeđuje da se njegovi asimetrični privatni ključevi ne koriste nakon isteka njihovog životnog ciklusa, u skladu sa Opštim i Posebnim pravilima.

Privatni ključevi, iz stava 1. ovog člana, moraju biti uništeni na način kojim se obezbeđuje da se ne mogu rekonstruisati.

Član 30

Sertifikaciono telo osigurava bezbednost kriptografskih uređaja koji se koriste za generisanje i čuvanje ključeva i formiranje kvalifikovanog elektronskog potpisa tokom životnog ciklusa uređaja, u skladu sa Posebnim pravilima, a naročito da:

1. Kriptografski uređaj nije kompromitovan tokom transporta;
2. Kriptografski uređaj nije kompromitovan za vreme čuvanja u sertifikacionom telu;
   Pprocedure instalacije aktivacije, kreiranja rezervnih kopija i rekonstrukcije asimetričnog privatnog ključa u kriptografskom uređaju vrši samo uz istovremenu kontrolu najmanje dva zaposlena sa bezbednosnim funkcijama;
3. Kriptografski uređaj funkcioniše korektno;
   Obezbedi da se privatni ključevi sertifikacionog tela koji su čuvani u kriptografskom uređaju unište nakon kraja životnog ciklusa ključeva ili uređaja.

Obezbeđenje zaštite od falsifikovanja sertifikata i tajnosti generisanih ključeva

Član 31

Sertifikaciono telo mora osigurati bezbedan proces generisanja kvalifikovanih elektronskih sertifikata radi obezbeđenja njihove autentičnosti i integriteta.

Član 32

Sertifikaciono telo obezbeđuje:

1. Da se kvalifikovani elektronski sertifikati generišu u skladu sa formatom definisanim u dokumentima ETSI TS 101 862, RFC 3739, RFC 3280 i ETSI TS 102 280;
2. Da je procedura generisanja kvalifikovanog elektronskog sertifikata bezbedno povezana sa odgovarajućim procedurama registracije korisnika, obnavljanja sertifikata uz zadržavanje postojećeg ili generisanje novog asimetričnog para ključeva:
3. U slučaju da sertifikaciono telo generiše korisnikove ključeve:
    - Da je procedura generisanja kvalifikovanog elektronskog sertifikata bezbedno povezana sa procedurom generisanja asimetričnog para ključeva od strane sertifikacionog tela,
    - Da je privatni ključ, odnosno sredstvo za formiranje kvalifikovanog elektronskog potpisa, bezbedno dostavljeno do registrovanog korisnika, a da se aktivacioni kod sredstva za formiranje kvalifikovanog elektronskog potpisa ovlašćenom licu dostavi na bezbedan način drugim putem;
4. Jedinstvenost dodeljenog imena korisniku u okviru domena sertifikacionog tela (za vreme radnog veka sertifikacionog tela mora se obezbediti da korisničko ime koje se dodeli u postupku generisanja sertifikata ne može nikada da se pridruži drugom korisniku);
5. Tajnost i integritet registracionih podataka, i to posebno u slučajevima razmene podataka sa korisnikom ili u slučaju razmene informacija između distribuiranih komponenti sertifikacionog tela;
6. Verifikaciju registracionih podataka korisnika koje autentikovani službenik registracionog tela dostavlja sertifikacionom telu.

Član 33

Sertifikaciono telo obezbeđuje da zahtevi za obnavljanje kvalifikovanih elektronskih sertifikata i/ili zahtevi za izdavanje kvalifikovanih elektronskih sertifikata korisnicima kojima su prethodni sertifikati bili opozvani, budu kompletni, tačni i autorizovani.

Član 34

U zahtevu za obnavljanjem sertifikata, sertifikaciono telo mora uneti ažurirane informacije o korisniku i sve druge izmene koje su prethodno verifikovane na isti način kao i u postupku registracije korisnika, u skladu sa čl. 17. i 18. ovog pravilnika.

Sertifikaciono telo će izdati novi kvalifikovani elektronski sertifikat koristeći prethodno sertifikovani javni ključ korisnika samo ako je njegova kriptografska bezbednost još uvek dovoljna za predviđeni novi životni ciklus sertifikata i ako ne postoje indikacije da je korisnikov privatni ključ kompromitovan.

Odgovornost i osiguranje

Član 35

Sertifikaciono telo je odgovorno da su svi sertifikacioni servisi navedeni u Politici sertifikacije konzistentni i implementirani u skladu sa Praktičnim pravilima.

Član 36

Pružanje usluga sertifikacije reguliše se posebnim ugovorom između sertifikacionog tela i korisnika, u skladu sa članom 18. stav 1. tačka 11) ovog pravilnika.

Ugovor iz stava 1. ovog člana mora da utvrdi obaveze korisnika, a naročito da:

1. Dostavi tačne i kompletne informacije sertifikacionom telu u skladu sa procedurom registracije definisanom u Politici sertifikacije;
2. Isključivo koristi svoj asimetrični privatni ključ za formiranje kvalifikovanog elektronskog potpisa u skladu sa ugovorom;
3. Onemogući neovlašćen pristup svom privatnom ključu;
4. Ukoliko sam generiše asimetrični par ključeva:
    - Za generisanje koristi algoritam verifikovan od strane Ministarstva i usaglašen za potrebe formiranja kvalifikovanog elektronskog potpisa,
    - Koristi propisanu dužinu ključa i propisani algoritam za formiranje kvalifikovanog elektronskog potpisa u skladu sa Pravilnikom o tehničko-tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijumima koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa,
    - Obezbedi da jedino on poseduje svoj privatni ključ;
5. Koristi kvalifikovani elektronski sertifikat samo uz kvalifikovani elektronski potpis koji je formiran sredstvima za formiranje kvalifikovanog elektronskog potpisa;
6. Ukoliko zahteva kvalifikovani elektronski sertifikat od sertifikacionog tela koje ispunjava uslove iz člana 18. Zakona i ovog pravilnika, generiše par ključeva za formiranje i proveru kvalifikovanog elektronskog potpisa u sredstvu za formiranje kvalifikovanog elektronskog potpisa koje je u potpunosti pod njegovom kontrolom;
7. Odmah obavesti sertifikaciono telo ako pre isteka važnosti sertifikata koji je naznačen u samom sertifikatu:
    - Korisnikov privatni ključ se izgubi, ukrade ili nastupi osnovana sumnja da je kompromitovan,
    - Prestane kontrola nad korišćenjem korisnikovog privatnog ključa iz razloga kompromitacije aktivacionih podataka (PIN kod ili lozinka) za sredstvo za formiranje kvalifikovanog elektronskog potpisa ili drugih razloga,
    - Ustanovi netačnost ili izmena sadržaja kvalifikovanog elektronskog sertifikata;
8. Prekine korišćenje svog privatnog ključa ukoliko postoji osnovana sumnja u kompromitaciju ključa ili kontrolu nad aktivacionim podacima za sredstvo za formiranje kvalifikovanog elektronskog potpisa.

Član 37

Zainteresovane strane koje koriste kvalifikovane elektronske sertifikate imaju obavezu da:

1. Provere važnost i ispravnost statusa suspenzije ili opoziva kvalifikovanog elektronskog sertifikata korišćenjem statusnih informacija koje je odgovarajuće sertifikaciono telo javno publikovalo (u zavisnosti od Opštih pravila i primenjenih mehanizama za publikovanje informacija o statusu opoziva kvalifikovanih elektronskih sertifikata postoji mogućnost kašnjenja do jednog dana u ažuriranju statusnih informacija);
2. Uzmu u obzir sva ograničenja u korišćenju kvalifikovanog elektronskog sertifikata koja su naznačena u samom sertifikatu ili publikovana u Opštim pravilima.

Član 38

Sertifikaciono telo obezbeđuje finansijske resurse za osiguranje od rizika i odgovornosti za moguću štetu nastalu vršenjem usluga izdavanja kvalifikovanih elektronskih sertifikata u skladu sa Zakonom i ovim pravilnikom.

Način osiguranja iz stava 1. ovog člana, kao i odgovarajući iznos sredstava, moraju biti jasno navedeni u Opštim pravilima rada.

Čuvanje svih relevantnih informacija

Član 39

Sertifikaciono telo mora da obezbedi čuvanje svih relevantnih informacija koje se tiču kvalifikovanih elektronskih sertifikata u vremenskom periodu definisanom u skladu sa Zakonom i Opštim pravilima, i to posebno u cilju obezbeđenja dokaza o izvršenoj sertifikaciji za pravne svrhe.

Informacije iz stava 1. ovog člana, uključuju podatke o registraciji korisnika i informacije o značajnim događajima vezanim za operativni rad sertifikacionog tela, kao i za upravljanje ključevima i sertifikatima.

Član 40

Sertifikaciono telo obezbeđuje:

1. Tajnost i integritet tekućih i arhiviranih zapisa o kvalifikovanim elektronskim sertifikatima;
2. Kompletno i pouzdano arhiviranje informacija o kvalifikovanim elektronskim sertifikatima u skladu sa objavljenim Opštim pravilima;
3. Da su zapisi u vezi kvalifikovanih elektronskih sertifikata, kao i registracione i druge informacije o korisniku, raspoloživi za potrebe pravnih poslova kao dokaz izvršene sertifikacije;
4. Pouzdano arhiviranje tačnog vremena značajnih događaja u sertifikacionom telu;
5. Da se informacije u vezi kvalifikovanih elektronskih sertifikata čuvaju onoliko vremena koliko je potrebno da se koriste u pravnim poslovima vezanim za elektronske potpise;

6. Evidentiranje svih događaja na način da se ne mogu lako obrisati ili uništiti (izuzev u cilju prenosa na dugotrajne medije za čuvanje) u okviru vremenskog perioda u kome se moraju čuvati;
7. Dokumentovanje specifičnih događaja i podataka koji treba da se evidentiraju;
8. Evidentiranje svih događaja koji se odnose na registraciju korisnika, uključujući i zahteve za obnavljanjem sertifikata, a naročito:
    - Tip identifikacionog dokumenta koji je prezentovan od strane korisnika,
    - Jedinstveni identifikacioni podatak o korisniku preuzet iz identifikacionog dokumenta,
    - Mesto čuvanja kopija aplikativnih i identifikacionih dokumenata, uključujući i potpisan Ugovor sa korisnikom,
    - Specifične elemente iz Ugovora sa korisnikom,
    - Identitet službenika registracionog tela koji je izvršio registraciju korisnika,
    - Podatke o metodi koja je korišćena za validaciju identifikacionih dokumenata,
    - Ime sertifikacionog tela koje je primilo registracione informacije i/ili ime registracionog tela koje je poslalo informacije;
9. Zaštitu privatnosti podataka korisnika;
10. Evidentiranje svih događaja u vezi sa životnim ciklusom ključeva sertifikacionog tela;
11. Evidentiranje svih događaja u vezi sa životnim ciklusom kvalifikovanih elektronskih sertifikata;
12. Evidentiranje svih događaja u vezi sa životnim ciklusom ključeva kojima upravlja sertifikaciono telo, uključujući i korisničke ključeve ako su generisani u sertifikacionom telu;
13. Evidentiranje svih događaja koji se odnose na pripremu sredstava za formiranje kvalifikovanog elektronskog potpisa;
14. Da se svi zahtevi i izveštaji koji se odnose na proceduru opoziva sertifikata evidentiraju, uključujući i sve odgovarajuće aktivnosti.

Član 41

Sertifikaciono telo obezbeđuje minimalnu moguću štetu korisnicima i drugim zainteresovanim stranama u slučaju njegovog prestanka rada i kontinuirano čuvanje podataka koje se zahteva u pravnim procedurama kao dokaz izvršene usluge sertifikacije, a naročito:

1. Pre prestanka pružanja usluga sertifikacije, izvršava sledeće aktivnosti:
    - Informiše sve korisnike i druge zainteresovane strane o prestanku rada,
    - Uništava, ili potpuno onemogućava korišćenje, svojih asimetričnih privatnih ključeva koji su korišćeni za formiranje kvalifikovanog elektronskog potpisa kvalifikovanih elektronskih sertifikata;
2. Obezbeđuje neophodna finansijska sredstva za realizaciju zahteva iz tačke 1) ovog stava;
3. Opštim pravilima definiše proceduru prestanka rada, koja obuhvata:
    - Obaveštavanje zainteresovanih strana,
    - Eventualni prenos obaveza drugim sertifikacionim telima,
    - Proceduru opoziva izdatih kvalifikovanih elektronskih sertifikata kojima nije istekao rok važnosti, i prenos listi opozvanih sertifikata drugom sertifikacionom telu.

Obezbeđivanje bezbednih uslova za korisnike za koje se generišu podaci za formiranje kvalifikovanog elektronskog potpisa

Član 42

Sertifikaciono telo može, uz usluge iz člana 4. ovog pravilnika, a u skladu sa svojim Opštim i Posebnim pravilima, da obezbedi i sredstvo za formiranje kvalifikovanog elektronskog potpisa korisnicima i pridruženu lozinku (ili PIN kod) za aktivaciju sredstva, kao i njihovu bezbednu distribuciju do korisnika.

Član 43

Sertifikaciono telo obezbeđuje da su ključevi korisnika koje ono generiše, generisani bezbedno 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 44

Sertifikaciono telo obezbeđuje da:

1. Se asimetrični par korisničkih ključeva generiše korišćenjem algoritma koji je propisan da zadovolji zahteve koji se primenjuju za kvalifikovane elektronske potpise;
2. Su asimetrični ključevi korisnika propisane dužine i korišćeni u propisanom asimetričnom kriptografskom algoritmu u cilju da se zadovolje propisani zahtevi za implementacijom kvalifikovanog elektronskog potpisa.

Član 45

Ukoliko sertifikaciono telo obezbeđuje sredstva za formiranje kvalifikovanog elektronskog potpisa za korisnike, to čini na bezbedan način a naročito obezbeđuje da:

1. Priprema sredstva za formiranje kvalifikovanog elektronskog potpisa mora biti bezbedno kontrolisana od strane sertifikacionog tela;
2. Sredstva za formiranje kvalifikovanog elektronskog potpisa moraju biti bezbedno čuvana i distribuirana;
3. Deaktiviranje i reaktiviranje sredstava za formiranje kvalifikovanog elektronskog potpisa mora biti bezbedno kontrolisano od strane sertifikacionog tela;
4. Ukoliko sredstva za formiranje kvalifikovanog elektronskog potpisa imaju pridružene aktivacione podatke (PIN kod ili lozinka) isti moraju biti bezbedno pripremljeni i distribuirani odvojeno u odnosu na sredstvo za formiranje kvalifikovanog elektronskog potpisa. Odvojeno slanje može biti obezbeđeno ili dostavom u različito vreme ili na različiti način.

Član 46

Sertifikaciono telo koje izdaje kvalifikovane sertifikate i koje obezbeđuje sredstvo za formiranje kvalifikovanog elektronskog potpisa (SSCD) korisnicima mora da garantuje tajnost identifikacionih podataka (PIN kod, lozinka), nakon što se ugrade u ista.

Lice koga je ovlastilo sertifikaciono telo koje izdaje kvalifikovane sertifikate i koje obezbeđuje korisnicima SSCD i mora iste lično da uruči identifikovanom korisniku i da od korisnika uzme potvrdu uručenja u pisanom obliku sa svojeručnim potpisom ili u elektronskom obliku sa kvalifikovanim elektronskim potpisom datog korisnika. Izdati kvalifikovani sertifikat datom korisniku ne sme da bude sa mogućnošću verifikacije, kao i sa mogućnošću raspoloživosti trećim licima uz dopuštenje korisnika, sve dok korisnik ne potvrdi prijem SSCD uređaja i odgovarajućih identifikacionih podataka.

Sistemi fizičke zaštite uređaja, opreme i podataka i sigurnosna rešenja zaštite od neovlašćenog pristupa

Član 47

Sertifikaciono telo obezbeđuje kontrolu fizičkog pristupa svojim bezbednosno kritičnim resursima, kao i minimizaciju rizika u pristupu svojim ključnim elementima.

Član 48

Sertifikaciono telo obezbeđuje da:

1. Se fizički pristup prostorijama u kojima se obavlja generisanje kvalifikovanih elektronskih sertifikata, priprema sredstava za formiranje kvalifikovanog elektronskog potpisa i upravljanje procedurom opoziva sertifikata, ograniči samo na pouzdano autorizovane osobe;
2. Su implementirane neophodne mere u cilju izbegavanja gubitaka, oštećenja ili kompromitovanja ključnih resursa i eliminisanje mogućnosti prekida poslovnih aktivnosti;
3. Se implementiraju odgovarajuće mere za sprečavanje kompromitovanja ili krađe informacija i/ili uređaja za procesiranje informacija;
4. Su prostorije u kojima se vrši generisanje kvalifikovanih elektronskih sertifikata, priprema sredstava za formiranje kvalifikovanog elektronskog potpisa i upravljanje opozivom, takve da se operativni rad u njima odvija u okruženju koje obezbeđuje fizičku zaštitu sertifikacionih servisa i resursa od kompromitacije prouzrokovane neautorizovanim pristupom sistemu i podacima;
5. Je fizička zaštita uspostavljena kreiranjem jasno definisanih bezbednosnih perimetara (tj. fizičkih barijera) kojima se štite procesi generisanja kvalifikovanih elektronskih sertifikata, obezbeđenja sredstava za formiranje kvalifikovanog elektronskog potpisa i upravljanje opozivom. Bilo koji deo poslovne zgrade koji se deli sa drugim organizacijama mora biti izvan ovih perimetara;
6. Su implementirane odgovarajuće fizičke mere i kontrole bezbednosnog okruženja u cilju zaštite prostorija i sistemskih elemenata sertifikacionog tela;
7. Su implementirane odgovarajuće mere u cilju zaštite uređaja, informacija, memorijskih medija i softvera od otuđivanja sa lokacije bez propisne autorizacije;
8. Se i druge specifične bezbednosne funkcije mogu primeniti u okviru istog bezbednog prostora koji obezbeđuje pristup samo autorizovanim zaposlenim osobama.

Član 49

Sertifikaciono telo obezbeđuje da je pristup sistemu sertifikacije ograničen isključivo na pouzdano autorizovane osobe, a naročito obezbeđuje:

1. Implementaciju kontrola na mrežnom nivou u cilju zaštite interne mreže sertifikacionog tela od eksternih mrežnih domena kojima može pristupiti treća strana, uz zabranu svih protokola i pristupa koji se ne koriste u operativnom radu sertifikacionog tela;
2. Pouzdanu zaštitu osetljivih podataka, koji uključuju i podatke o registraciji korisnika, tokom prolaska kroz delove mreže koji nisu bezbedni;
3. Efikasnu i pouzdanu administraciju korisničkih pristupa (uključujući operatore, administratore i bilo koje specifične korisnike koji imaju direktan pristup sistemu) u cilju održavanja bezbednosti sistema, uključujući i upravljanje nalozima korisnika, evidentiranje i mogućnost modifikacije i zabrane pristupa;
4. Strogo ograničen pristup informacijama i aplikativnim funkcijama sistema u skladu sa Opštim i Posebnim pravilima i politikom kontrole pristupa, identifikovanom u njima, kao i dovoljnu računarsko-bezbednosnu kontrolu u cilju razdvajanja bezbednih funkcija - rola u sistemu koje su identifikovane u Opštim pravilima, uključujući razdvajanje funkcija administratora bezbednosti i operatera, a posebno rad sa korisničkim programima za upravljanje sistemom mora biti posebno ograničeno i strogo kontrolisano;
5. Pouzdanu identifikaciju i autentikaciju zaposlenih u sertifikacionom telu pre korišćenja kritičnih operacija vezanih za procedure upravljanja sertifikatima;
6. Evidentiranje svih aktivnosti zaposlenih u sertifikacionom telu na osnovu odgovarajućih korisničkih naloga i log fajlova, koji su potpisani kvalifikovanim elektronskim potpisom;
7. Pouzdanu zaštitu bezbednosno osetljivih podataka, koji uključuju i registracione podatke korisnika, od neautorizovanog pristupa na osnovu ponovnog korišćenja prethodno obrisanih ili arhiviranih podataka;
8. Da se lokalne mrežne komponente (ruteri i sl.) čuvaju u fizički zaštićenom okruženju i da se njihova konfiguracija periodično kontroliše u cilju ispitivanja usklađenosti sa zahtevima specificiranim u Opštim i Posebnim pravilima;
9. Uređaje za kontinualno monitorisanje i alarmiranje (sistemi za detekciju napada i sistemi za monitorisanje kontrole pristupa i alarma) za pouzdanu detekciju, registraciju i reakciju na bilo kakav neautorizovani i/ili neregularni pokušaj pristupa resursima koja se koriste za pružanje usluga sertifikacije;
10. Da aplikacija za distribuciju sertifikata mora primeniti sistem logičke kontrole pristupa u cilju sprečavanja pokušaja dodavanja ili brisanja odgovarajućih sertifikata i modifikacije drugih pridruženih informacija;
11. Da aplikacija za dobijanje statusa opoziva sertifikata primenjuje sistem logičke kontrole pristupa u cilju sprečavanja pokušaja modifikacije informacija o statusu opoziva sertifikata.

Informacije o uslovima izdavanja i korišćenja sertifikata

Član 50

Sertifikaciono telo obezbeđuje da su sve potrebne informacije o uslovima izdavanja i korišćenja kvalifikovanih elektronskih sertifikata raspoložive korisnicima i drugim zainteresovanim stranama.

Član 51

Sertifikaciono telo obezbeđuje raspoloživost informacija i podataka o svom poslovanju, i to:

1. Opšta pravila sertifikacionog tela koja su trenutno važeća;
2. Ograničenja u korišćenju Opštih pravila;
3. Obaveze korisnika;
4. Informacije o načinu provere važnosti kvalifikovanih elektronskih sertifikata, uključujući i zahteve za proveru statusa opoziva sertifikata;
5. Ograničenja odgovornosti koja uključuju slučajeve za koje sertifikaciono telo prihvata (ili odbija) odgovornost;
6. Vremenski period čuvanja registracionih informacija korisnika;
7. Vremenski period čuvanja log fajlova za evidentiranje;
8. Procedure za rešavanje žalbi i sporova;
9. Pravni sistem koji se primenjuje.

Sertifikaciono telo obezbeđuje da su informacije iz stava 1. ovog člana neprekidno raspoložive korišćenjem jednostavnih vidova komunikacije (Internet i sl.) sa obezbeđenim integritetom tokom vremena, da se mogu prenositi elektronskim putem i da su prikazane na potpuno razumljiv način.

Sistem upravljanja sertifikatima

Član 52

Sertifikaciono telo obezbeđuje uvid u izdate, opozvane i suspendovane kvalifikovane elektronske sertifikate svim korisnicima i drugim zainteresovanim stranama, u skladu sa Zakonom, pri čemu se uvid odnosi samo na status validnosti sertifikata, a ne i na sadržaj samih sertifikata.

Član 53

Sertifikaciono telo obezbeđuje:

1. Da je izdati kvalifikovani elektronski sertifikat raspoloživ korisniku kome je sertifikat izdat;
2. Da su kvalifikovani elektronski sertifikati raspoloživi trećim licima samo u onim slučajevima za koje je dobijen pristanak korisnika i kada sertifikat nema na sebi JMBG ili lični broj, a u skladu sa Opštim pravilima sertifikacionog tela;
3. Raspoloživost informacija o uslovima izdavanja i korišćenja kvalifikovanih elektronskih sertifikata svim zainteresovanim stranama u sistemu i da se primenjeni uslovi mogu lako identifikovati za dati sertifikat;
4. Da su informacije navedene pod tač. 2) i 3) ovog stava raspoložive 24 časa na dan, sedam dana u sedmici. Nakon pada sistema, ili delimičnog gubitka mogućnosti za obezbeđenje servisa, sertifikaciono telo mora da primeni sve raspoložive mere da ovaj informacioni servis bude ponovo aktivan što pre, ali najkasnije do isteka roka predviđenog u Opštim pravilima.

II NAČIN PROVERE ISPUNJENOSTI USLOVA ZA IZDAVANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Član 54

Proveru ispunjenosti uslova za izdavanje kvalifikovanih elektronskih sertifikata (u daljem tekstu: akreditacija) Ministarstvo vrši u postupku razmatranja zahteva sertifikacionog tela za upis u Registar sertifikacionih tela koja izdaju kvalifikovane elektronske sertifikate.

Član 55

Procedura akreditacije obuhvata:

1. Proveru Opštih pravila i Posebnih pravila rada sertifikacionog tela (CP, CPS i interna pravila rada) i njihove usklađenosti sa Zakonom i podzakonskim opštim aktima;
2. Atestiranje i sertifikaciju tehničkih i bezbednosnih komponenata koje koristi sertifikaciono telo za generisanje asimetričnih ključeva i izdavanje kvalifikovanih sertifikata.

Provera ispunjenosti kriterijuma operativnog rada sertifikacionog tela

Član 56

Provera operativnog rada sertifikacionog tela obuhvata:

1. Proceduru registracije korisnika kome se izdaje kvalifikovani elektronski sertifikat;
2. Proceduru pripreme zahteva za izdavanjem kvalifikovanog elektronskog sertifikata u registracionom autoritetu;
3. Proceduru dostavljanja zahteva do sertifikacionog tela;
4. Proceduru generisanja kvalifikovanog elektronskog sertifikata;
5. Korišćenje bezbednih sistema za čuvanje podataka za generisanje kvalifikovanih elektronskih potpisa;
6. Korišćenje bezbednih hardverskih sredstava za formiranje kvalifikovanog elektronskog potpisa (hardverski moduli zaštite (HSM - *Hardware Security Module*));
7. Proceduru dostavljanja kvalifikovanog elektronskog sertifikata, uređaja za generisanje elektronskog potpisa i identifikacionih podataka korisnicima;
8. Proceduru opoziva sertifikata;
9. Proceduru obnavljanja sertifikata;
10. Proceduru suspenzije sertifikata;
11. Način publikacije liste opozvanih i suspendovanih sertifikata;
12. Sisteme fizičke kontrole pristupa u prostorije sertifikacionog tela;
13. Sisteme logičke kontrole pristupa računarskim resursima sertifikacionog tela;
14. Sistem za javno publikovanje osnovnih informacija o pružanju usluga sertifikacije, kao i Opštih pravila rada sertifikacionog tela.

Provera tehničkih i bezbednosnih komponenti koje koristi sertifikaciono telo

Član 57

Provera tehničkih i bezbednosnih komponenti koje koristi sertifikaciono telo obuhvata:

1. Realizaciju sistemskih zahteva bezbednosti;
2. Izdavanje (digitalno potpisivanje) kvalifikovanih elektronskih sertifikata primenom kvalifikovanog elektronskog potpisa;
3. Bezbedno generisanje ključeva sertifikacionog tela.

Član 58

Operativni rad sertifikacionog tela mora da bude usklađen standardom CEN *Workshop Agreement* 14167-1 (*March* 2003) "*Security Requirements for Trustworthy Systems Managing Sertificates for Electronic Signatures - Part 1: System Security Requirements*".

Član 59

Stupanjem na snagu ovog pravilnika prestaje da važi Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata ("Službeni glasnik RS", br. 48/05, 82/05 i 116/05).

Član 60

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