Sertifikaciono telo Privredne komore Srbije

Praktična pravila rada
Kvalifikovani elektronski sertifikati

CPS (Certificate Practice Statement)
OID CPS dokumenta (1.3.6.1.4.1. 31266.10.142.1.0)

- verzija 3.0.-

Oktobar 2018.

Sadržaj

Na osnovu člana 45. stav 1. podtačka 2) Statuta Privredne komore Srbije ("Službeni glasnik RS", broj: 45/02, 107/03, 44/05, 29/09, 35/11, 46/11, 103/11, 3/13, 32/13 i 2/14),

Upravnom odboru Privredne komore Srbije, dostavlja se na usvajanje predlog dokumenta

Praktična pravila rada
Kvalifikovani elektronski sertifikati

1. Uvod i pregled osnovnih pretpostavki

Sertifikaciono telo Privredne komore Srbije (u nastavku: PKS CA) izdaje kvalifikovane elektronske sertifikate tako što formira elektronski potpis sertifikata na osnovu svog privatnog ključa i asimetričnog kriptografskog algoritma. U tako formiranom elektronskom sertifikatu, PKS CA se identifikuje kao izdavač kvalifikovanog elektronskog sertifikata u skladu sa Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima. (u daljem tekstu - Zakon).

PKS CA izdaje kvalifikovane elektronske sertifikate korisnika u skladu sa: Preporukom ITU X.509, ITU-T X.520 i dokumentima ETSI EN 319 412-1 „Electronic signatures and infrastructure (ESI) - Certificate profiles- Part 1: Overview and common data structures", IETF RFC 5280 „Internet X.509 Public key infrastructure Certificate and Certificate Revocation List (CRL) Profile", ETSI EN 319 412-2 „Electronic signatures and infrastructure (ESI) - Certificate profiles- Part 2: Certificate Profile for Certificates Issued to Natural Persons", ETSI EN 319 412-3 „Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 3: Certificate profile for certificates issued to legal persons", ETSI EN 319 412-5 „Electronic Signatures and Infrastructures (ESI) – Certificate Profiles – Part 5: QCStatements" zasnovano na dokumentu IETF RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", ETSI EN 319 411-2 „Electronic Signatures and Infrastructures (ESI) – Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Requirements for trust service providers issuing EU qualified certificates" i sa obaveznim sadržajem definisanim u članu 43. Zakona.

1.1 Pregled osnovnih pretpostavki

PKS CA je odgovorno za pružanje kompletnih usluga sertifikacije, koje uključuju sledeće servise, i to:

- Registracija korisnika
- Formiranje asimetričnog para ključeva korisnika za digitalno potpisivanje pomoću SSCD (Secure Signature Creation Device) uređaja kako je Zakonom propisano. SSCD koji se koriste za kreiranje kvalifikovanog elektronskog potpisa mogu biti smart kartica ili usb token.
- Formiranje asimetričnog para ključeva za korisnike koji služe za autentikaciju
- Formiranje kvalifikovanih elektronskih sertifikata
- Distribuciju privatnog ključa i kvalifikovanih elektronskih sertifikata na način propisan zakonom (SSCD)
- Upravljanje procedurom opoziva kvalifikovanih elektronskih sertifikata i
- Obezbeđivanje statusa opozvanosti kvalifikovanih elektronskih sertifikata.

PKS CA obezbeđuje sredstvo za formiranje kvalifikovanog elektronskog potpisa korisnicima (SSCD i pridruženi PIN kod za aktivaciju sredstva, kao i njihovu bezbednu distribuciju do korisnika.

PKS CA utvrđuje Opšta interna pravila pružanja usluge sertifikacije (u daljem tekstu: Opšta pravila) u skladu sa Zakonom koja korisnicima obezbeđuju dovoljno informacija na osnovu kojih se mogu odlučiti o prihvatanju usluga i o obimu usluga. Opšta pravila sertifikacije PKS CA ugrađuju se u dokumenta:

1. **Politika sertifikacije (Certificate Policy);**
2. **Praktična pravila pružanja usluge Sertifikacije (CPS – Certification Practice Statement) (u daljem tekstu: Praktična pravila ili CPS) – ovaj dokument.**

Politika sertifikacije i Praktična pravila su javni dokumenti.

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.

Opšta pravila funkcionisanja PKS CA su 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".

PKS CA 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 i odobrava ih odgovorno lice PKS CA.
Posebna pravila sadrže detaljne odredbe o:

- Sistemu fizičke kontrole pristupa u pojedine prostorije sertifikacionog tela;
- Sistemu logičke kontrole pristupa računarskim resursima sertifikacionog tela;
- Sistemu za čuvanje privatnog ključa sertifikacionog tela
- Sistemu distribuirane odgovornosti pri aktivaciji privatnog ključa sertifikacionog tela;
- Postupcima i radnjama u vanrednim situacijama (požari, poplave, zemljotresi, druge vremenske nepogode, zlonamerni upadi u prostorije ili informacioni sistem sertifikacionog tela).
- Poverljive uloge/dužnosti u PKS CA;
- Procedure backup-a

PKS CA će biti evidentirano i akreditovano od strane Nadležnog organa za poslove akreditacije i supervizije PKI (Public Key Infrastructure) sistema u Srbiji (Ministarstvo trgovine, turizma i telekomunikacija) i biće predmet periodične supervizije u cilju osiguravanja saglasnosti sa zahtevima Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima.

1.2 Ime dokumenta i identifikacija

Ovaj dokument predstavlja Praktična pravila rada PKS CA (u daljem tekstu CPS – Certificate Practice Statement).

PKS CA PKI infrastruktura je odgovorna za izdavanje sledećih vrsta sertifikata:

- Root CA;
- Intermediate CA;
- Kvalifikovani sertifikati za:
  - Fizička lica – građani (pojedinci) ili zakonski zastupnici pravnih lica uključujući i nerezidente,
  - Zaposlene PKS i regionalnih komora u svojstu ovlašćenog lica.

U okviru Praktičnih pravila rada PKS CA definišu se konkretni detalji oko implementacije i procedura rada PKS CA.

Identifikacioni podaci PKS CA su:
PKS CA
Privredna Komora Srbije
Resavska 13-15
11000 Beograd
Srbija

Jedinstveno ime (Dname – issuer):
OU=PKS CA
O=Privredna komora Srbije
C=RS

Ovaj dokument ima jedinstvenu oznaku (OID – Object Identifier):
CPS (Certificate Practice Statement) OID CPS (1.3.6.1.4.1. 31266.10.142.1.0)

1.3 Učesnici u PKI sistemu PKS

U ovom poglavlju su date osnovne informacije o učesnicima u okviru PKI sistema PKS.

1.3.1 PKS CA

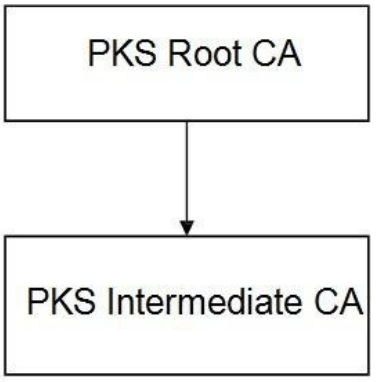
Sertifikaciono telo je organizacija koja izdaje elektronske sertifikate. PKS CA je sertifikaciono telo (CA). PKS CA je odgovorna za publikaciju ovih praktičnih pravila rada u cilju podrške izdavanju elektronskih sertifikata. U tom smislu, ovaj CPS kao i pridruženi dokument Politika

sertifikacija (CP), predstavljaju odgovarajuće politike i pravila koja se primenjuju pri izdavanju PKS CA kvalifikovanih elektronskih sertifikata.

U cilju objavljivanja trećim stranama informacija koje se odnose na opozvane sertifikate, neophodno je da se izvrši odgovarajuća publikacija liste opozvanih sertifikata (CRL – Certificate Revocation List). PKS CA periodično objavljuje takvu listu u skladu sa uslovima definisanim u ovom dokumentu.

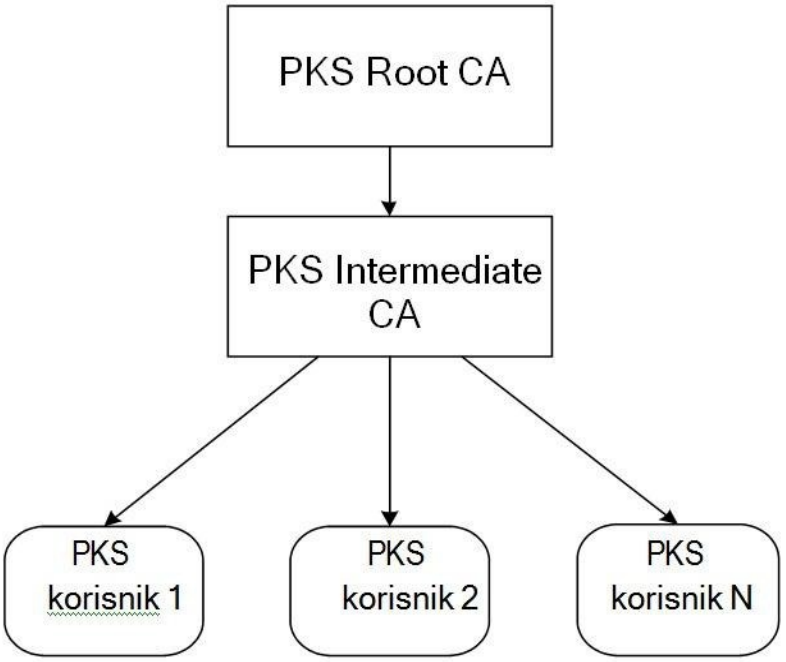
PKS CA predstavlja hijerarhijsku PKI strukturu za izdavanje elektronskih sertifikata za interne i eksterne korisnike. U pomenutoj arhitekturi (slika 1), postoji:

- PKS Root CA – centralno samopotpisano sertifikaciono telo koje izdaje sertifikate intermediate CA telima i potpisuje CRL listu na root nivou.
- Intermediate CA – sertifikaciono telo koje izdaje kvalifikovane elektronske sertifikate. Ovo CA izdaje i CRL listu za sertifikate izdate u svom domenu.



Slika 1: Hijerarhijska struktura PKS PKI sistema

Sertifikat PKS Root CA je samopotpisani sertifikat. PKS Intermediate CA sertifikat je potpisan od strane PKS Root CA tela. Sertifikati PKS korisnika su digitalno potpisani privatnim ključem PKS Intermediate CA tela, Slika 2.



Slika 2: Realizacija hijerarhijske strukture PKS CA sistema

Sertifikati PKS korisnika se generišu na osnovu validnog zahteva za izdavanjem sertifikata koji se formira na osnovu podataka o PKS korisniku koji se uzimaju u procesu registracije korisnika. Korisnički sertifikati mogu biti namenjeni za autentikaciju korisnika i za kreiranje kvalifikovanog elektronskog potpisa.

Sva navedena sertifikaciona tela se nalaze i upravljaju na centralnoj lokaciji PKS, a u okviru Direktorata za informacione tehnologije PKS.

Obaveze PKS CA

PKS CA garantuje da će sprovoditi sve procedure definisane u ovim CPS. PKS CA koristi korisnički ugovor, CP i CPS u cilju sprovođenja legalnih uslova korišćenja PKS CA sertifikata od strane korisnika i trećih strana.

Učesnici od interesa za ove CPS u čitavoj PKS CA PKI infrastrukturi koji imaju odgovarajuće obaveze uključuju CA, RA, korisnike, treće strane i druge učesnike.

Do nivoa specificiranog u odgovarajućim poglavljima CP i ovim CPS, PKS CA se obavezuje na:

- Punu saglasnost sa CP i ovim CPS, kao i svim odgovarajućim dodacima u trenutku kada se publikuju.
- Regularno i periodično ažuriranje dokumenata CP i ovih CPS, kao i njihovo javno publikovanje,
- Objavljivanje kontakt detalja sertifikacionog autoriteta,
- Obezbeđivanje usluga sertifikacije u skladu sa Zakonom, Pravilnikom i ostalim normativnim aktima,
- Obezbeđivanje infrastrukture i sertifikacionih usluga, uključujući uspostavu i održavanje PKS CA repozitorijuma i odgovarajućeg web sajta u cilju pružanja sertifikacionih usluga.
- Obezbeđivanje sigurnih mehanizama koji uključuju mehanizam generisanja ključeva, zaštite ključeva, kao i procedure deljenja tajni u skladu sa svojom sopstvenom PK infrastrukturom.
- Obezbeđivanje promptnog obaveštavanja u slučaju kompromitacije sopstvenog privatnog ključa.
- Obezbeđivanje i validaciju aplikacionih procedura za različite tipove sertifikata koje su javno raspoložive.
- Izdavanje kvalifikovanih elektronskih sertifikata u skladu sa CP i ovim CPS, kao i ispunjavanje sopstvenih preuzetih obaveza.
- Obaveštavanje korisnika da su sertifikati generisani za njih, kao i o načinu kako korisnici mogu da preuzmu sertifikate.
- Obaveštavanje aplikanta ukoliko PKS CA nije sposobno da izvrši validaciju korisničke aplikacije za dobijanje sertifikata u skladu sa CP i ovim CPS.
- Nakon prijema validnog zahteva od strane RA koje radi u okviru PKS CA mreže promptno izdaje sertifikat u skladu sa CP i ovim CPS.
- Opoziv sertifikata koji su izdati u skladu sa CP i ovim CPS nakon prijema validnog zahteva za opoziv sertifikata od strane autorizovanog lica koje može da zahteva opoziv.
- Objavljivanje izdatih sertifikata u skladu sa uslovima definisanim u CP i ovim CPS.
- Obezbeđivanje podrške korisnicima i trećim stranama kao što je opisano u CP i ovim CPS.
- Obnavljanje sertifikata korisnika u skladu sa CP i ovim CPS.
- Regularno i periodično objavljivanje liste opozvanih sertifikata, CRL liste, u skladu sa CP i ovim CPS koja je uvek dostupna svim zainteresovanim stranama,
- Obaveštavanje trećih strana o statusu sertifikata putem publikovanja CRL lista na PKS CA online repozitorijumu.
- Dostavljanja kopije CP i ovim CPS, kao i ostalih primenjivih dokumenata po zahtevu neke od strana.

PKS CA potvrđuje da, osim gore navedenih, nema drugih obaveza po ovom CPS dokumentu.

Odgovornosti PKS CA

- PKS CA je odgovorno za izvršavanje gore navedenih obaveza u obimu koji određuje zakonska regulativa Republike Srbije.
- PKS CA nije odgovorno za zaštitu privatnih ključeva korisnika namenjenih za kreiranje digitalnog potpisa nakon uručenja SSCD korisniku.
- PKS CA nije odgovorno za neodgovarajuću proveru validnosti sertifikata od strane koja se pouzdaje u sertifikat izdat od strane PKS CA.
- PKS CA nije odgovorno za moguću zloupotrebu sertifikata koja je nastala usled neispunjavanja obaveza korisnika ili treće strane koja se pouzdaje u sertifikat izdat od strane PKS CA.
- PKS CA nije odgovorno za neizvršavanje svojih obaveza koje je posledica bilo kog problema Nadležnog organa za poslove akreditacije i supervizije PKI sistema u Srbiji ili nekog drugog javnog autoriteta.
- PKS CA nije odgovorno za neizvršavanje svojih obaveza koje su posledica vanredne situacije ili više sile.

1.3.2 Registraciona tela PKS CA

Zahtevi za izdavanjem sertifikata se prikupljaju u samoj centrali PKS, koje igraju ulogu Registracionih autoriteta (RA – Registration Authority). Drugim rečima, PKS CA pristupa svojim korisnicima putem mreže registracionih tela (centralno RA i mreža RA). Ova registraciona tela mogu biti:

- PKS CA na centralnoj lokaciji, kao centralno RA,
- Regionalne komore kao RA za potrebe korisnika PKS, fizička i pravna lica.
- RA tela interaktivno komuniciraju i sa korisnicima i sa PKS CA u cilju isporuke sertifikacionih usluga krajnjim korisnicima. U tom smislu, registraciona tela PKS CA:
- Prihvataju, analiziraju, potvrđuju ili odbijaju registraciju odgovarajućih korisničkih zahteva za sertifikatima (aplikacije za sertifikate).
- Registruju korisnike za korišćenje PKS CA sertifikacionih usluga
- Sprovode sve korake u proceduri identifikacije korisnika što je definisano važećim zakonskim dokumentima i Opštim pravilima rada PKS CA
- Koriste službene i overene dokumente u cilju provere korisnikove aplikacije.
- Nakon potvrde aplikacije korisnika, dostavljaju sve neophodne informacije do PKS CA u cilju izdavanja sertifikata.
- Iniciraju proces generisanja sertifikata korisnika.
- Iniciraju proces opoziva, suspenzije i aktivacije sertifikata od strane PKS CA.

Registraciona tela PKS CA deluju lokalno u okviru njihovog sopstvenog konteksta geografskog ili poslovnog partnerstva koje je potvrđeno i autorizovano od strane PKS CA. PKS CA registraciona tela deluju u skladu sa praksom, procedurama i osnovnim dokumentima rada PKS CA.

Ne postoji ograničenje na broj registracionih tela koja mogu biti pridružena PKS CA PKI infrastrukturi.

PKS CA obezbeđuje registracionim telima u svojoj infrastrukturi neophodnu tehnologiju i know-how, kao i odgovarajuću obuku, u cilju postizanja visokog nivoa obučenosti u skladu sa PKS CA funkcionalnim zahtevima.

PKS RA obaveze

Sumarno, PKS RA se obavezuje na:

- Prijem aplikacija za izdavanje PKS CA sertifikata u skladu sa CP i ovim CPS.
- Izvršavanje svih aktivnosti na verifikaciji i proveri autentičnosti aplikanata u skladu sa opisom PKS CA procedura, CP i ovim CPS (Provera identiteta osobe koja je podnela zahtev, kao i njenih ovlašćenja).
- Dostavljanje zahteva aplikanata do PKS CA (zahtev za izdavanjem sertifikata), u skladu sa procedurama koje su opisane Politikom sertifikacije (CP) i ovim Praktičnim pravilima rada (CPS) PKS CA.
- Zapisivanje svih aktivnosti u žurnalu događaja.
- Prijem, verifikaciju i prosleđivanje ka PKS CA svih zahteva za opozivom, suspenzijom i aktivacijom PKS CA izdatih sertifikata u skladu sa PKS CA procedurama, CP i ovim CPS.

PKS RA je odgovorno za izvršavanje gore navedenih obaveza.

1.3.3 Korisnici

Korisnici predstavljaju korisnike usluga Sertifikacionog tela PKS CA. Za kvalifikovane sertifikate to su fizička lica i ovlašćena fizička lica u okviru pravnog lica.

Korisnici su strane koje:

- Apliciraju za dobijanje sertifikata
- Identifikovani su kao vlasnici sertifikata u samom sertifikatu,
- Poseduju privatni ključ generisan i čuvan na SSCD uređaju koji matematički, putem asimetričnog kriptografskog algoritma, odgovara javnom ključu koji je naveden u korisnikovom sertifikatu.
- Obaveze korisnika kvalifikovanih elektronskih sertifikata:

Sem ako nije drugačije definisano u CP i ovim CPS, korisnici sertifikacionih usluga PKS CA su odgovorni za:

- Posedovanje odgovarajućih znanja i, ako je neophodno, pohađanje odgovarajuće obuke za korišćenje elektronskih sertifikata i sertifikacionih usluga.
- Poštovanje Politike sertifikacije (CP) i Praktičnih pravila rada (CPS) publikovanih od strane PKS CA.
- Obezbeđivanje korektnih i preciznih informacija u njihovoj komunikaciji sa PKS RA i/ili PKS CA.
- Upoznavanje, razumevanje i saglasnost sa svim stavovima i uslovima u CP i ovim CPS, kao i drugim dokumentima koji su objavljeni na PKS CA repozitorijumu.
- Uzdržavanje od narušavanja integriteta i proizvođenja neispravnim sertifikata izdatog od strane PKS CA.
- Korišćenje PKS CA sertifikata samo za legalne i autorizovane svrhe u skladu sa CP i ovim CPS, kao i važećim zakonskim dokumentima.
- Obaveštavanje PKS CA ili PKS RA o bilo kojim promenama informacija koje su ranije dostavljene.
- Prekid korišćenja PKS CA izdatog sertifikata ukoliko je bilo koja informacija u sertifikatu postala nevalidna.
- Prekid korišćenja PKS CA izdatog sertifikata ukoliko sam sertifikat postane nevalidan.
- Odstranjivanje serverskog sertifikata koji je nevalidan iz bilo koje aplikacije i/ili bilo kog uređaja gde je bio instaliran.
- Korišćenje samo jednog sertifikata za elektronski potpis u datom trenutku.
- Uzdržanje od korišćenja svog privatnog ključa koji odgovara javnom ključu koji je sertifikovan od strane PKS CA, u izdatom sertifikatu, pod istim imenom za potrebe izdavanja drugih sertifikata.
- Razumno korišćenje PKS CA izdatog sertifikata pod različitim okolnostima.
- Sprečavanje kompromitacije, gubljenja, objavljivanja, modifikacije ili bilo kog drugog neautorizovanog korišćenja svog privatnog ključa.
- Korišćenje bezbednih uređaja i proizvoda koji obezbeđuju odgovarajuću
- zaštitu privatnih ključeva
- Za bilo koje aktivnosti i propuste partnera ili agenata u smislu generisanja, zadržavanja, odlaganja, ili uništavanja bilo kog privatnog ključa.
- Uzdržavanje od dostavljanja do PKS CA, ili bilo kog PKS CA direktorijuma, bilo kakvog materijala koji sadrži stavove koji ugrožavaju bilo koji zakon ili bilo koje pravo bilo koje strane.
- Zahtevanje opoziva sertifikata u slučaju događaja koji materijalno utiče na integritet izdatog sertifikata od strane PKS CA.
- Prijavljivanje svake moguće zloupotrebe svog privatnog ključa i zahtevanje da se sertifikat opozove u tom slučaju.

1.3.4 Treće strane

Treće strane su entiteti, kao na primer fizička lica (pojedinci) i/ili pravna lica (kompanije), koja prihvataju sertifikate i verifikuju elektronski potpis određenih elektronskih dokumenata koja su potpisana od strane korisnika PKS CA, kao i koja vrše validaciju sertifikata izdatih od strane PKS CA. Verifikacija digitalnog potpisa se vrši na bazi javnog ključa koji se nalazi u korisnikovom sertifikatu.

U cilju provere validnosti primenjenog elektronskog sertifikata, treće strane moraju uvek da provere status datog sertifikata korišćenjem CRL liste koju izdaje PKS CA pre nego što prihvate informacije koje su navedene u sertifikatu.

Obaveze trećih strana

Strana koja se oslanja na PKS CA izdati sertifikat obavezna je da:

- Poseduje odgovarajuća znanja o korišćenju elektronskih sertifikata i drugih tehnologija vezanih za usluge sertifikacije.
- Upozna se sa Politikom sertifikacije (CP) i ovim Praktičnim pravilima rada (CPS) u vezi navedenih uslova koji važe za treće strane.
- Poštuje i sprovodi odredbe iz CP i ovih CPS.
- Verifikuje PKS CA izdati sertifikat primenom: provere validnosti sertifikata, provere CA koje je izdalo sertifikat, provere elektronskog potpisa sertifikata i provere statusa datog sertifikata u važećoj CRL listi (PKS CA CRL) a u skladu sa procedurom validacije sertifikata i kompletnog lanca sertifikata.
- Proveri kompletnost podataka u sertifikatu izdatom od strane PKS CA, kao i da proveri da li dati sertifikat služi odgovarajućoj oblasti primene koja je navedena u sertifikatu.
- Veruje u PKS CA izdati sertifikat samo ukoliko se sve informacije koje se odnose na takav sertifikat mogu verifikovati da su korektne i ažurne.
- Razumno osloni i pouzda na PKS CA izdati sertifikat u skladu sa odgovarajućim okolnostima.

1.3.5 Drugi učesnici

Obaveze vezane za repozitorijum koji održava PKS CA

Strane u komunikaciji (uključujući korisnike i treće strane) koje pristupaju PKS CA repozitorijumu i web sajtu PKS CA u potpunosti su saglasne sa odredbama CP i ovih CPS, kao i sa bilo kojim drugim uslovima korišćenja koje je PKS CA moglo učiniti dostupnim.

Strane u komunikaciji demonstriraju prihvatanje uslova korišćenja navedenih u CP i ovim CPS dostavljanjem upita vezanih za status elektronskih sertifikata ili bilo kojim drugim načinom koji pokazuje korišćenje ili oslanjanje na obezbeđene informacije ili usluge.

PKS CA repozitorijum uključuje, obezbeđuje ili sadrži:

- Javnu dostupnost svih svojih sertifikata (root CA i intermediate CA sertifikati).
- Javnu dostupnost važeće liste opozvanih sertifikata (CRL).
- Informacije publikovane na PKS CA web sajtu (CP, CPS, itd.).
- Bilo koje druge usluge koje PKS CA može reklamirati ili obezbediti putem svog web sajta.

PKS CA čini sve u svojoj moći u cilju osiguranja da strane koje pristupaju njegovom repozitorijumu dobijaju pouzdane, ažurne i tačne informacije. PKS CA, međutim, ne može prihvatiti bilo kakvu odgovornost koja je van ograničenja definisanih u CP i ovim CPS.

1.4 Korišćenje sertifikata izdatih od strane PKS CA

U ovom poglavlju je dat akcenat na prihvatljivom korišćenju kvalifikovanih elektronskih sertifikata izdatih od strane PKS CA.

1.4.1 Prihvatljivo korišćenje sertifikata

PKS CA sertifikati se u opštem slučaju mogu koristiti za većinu transakcija elektronskog poslovanja i elektronske trgovine koje se baziraju na upotrebi kvalifikovanih elektronskih sertifikata.

U takve transakcije spadaju:

- Transakcije elektronskog poslovanja pravnih lica – kompanija kako između kompanije i PKS tako i između samih kompanija,
- Transakcije elektronskog poslovanja građana – fizičkih lica i PKS,
- Elektronska pošta,
- Elektronski ugovori,
- Pristup bezbednim web sajtovima (SSL autentikacija) i drugim on-line sadržajima,
- Elektronsko potpisivanje dokumenata u elektronskom obliku,
- Proveru kvalifikovanog elektronskog potpisa,
- Šifrovanje i dešifrovanje dokumenata u elektronskom obliku, itd.

1.4.2 Zabranjeno korišćenje sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

1.5 Administracija Praktičnih pravila rada PKS CA

U ovom poglavlju su opisane aktivnosti u vezi administracije ovih Praktičnih pravila rada (CPS) PKS CA.

1.5.1 Organizacija administriranja Praktičnih pravila rada

PKS CA je odgovorno za propisnu administraciju ovih CPS, i to u smislu periodičnog pregleda i ažuriranja, kao i vanrednih promena odgovarajućih odredbi koje proističu iz eventualnih promena u zakonskoj regulativi ili tehničkim karakteristikama primenjenih kriptografskih algoritama i dužina ključeva.

1.5.2 Kontakt osoba

Osoba u PKS CA, odgovorna za ova Praktična pravila rada (CPS) je:

mr Dušan Berdić
Privredna Komora Srbije
Resavska 13-15
11000 Beograd, Srbija
Tel.: 011 3304 545
Fax: 011 3304 556
Email: dusan.berdic@pks.rs

1.5.3 Osoba koja određuje pogodnost CPS dokumenta

Osoba u PKS CA, odgovorna da su ova Praktična pravila rada (CPS) u saglasnosti sa Politikom sertifikacije (CP), koja je takođe publikovana od strane PKS CA, je:

mr Dušan Berdić
Privredna Komora Srbije
Resavska 13-15
11000 Beograd, Srbija
Tel.: 011 3304 545
Fax: 011 3304 556
Email: dusan.berdic@pks.rs

1.5.4 Procedura odobravanja CPS dokumenta

Dokument Praktična pravila rada (CPS) PKS CA se redovno periodično pregleda i po potrebi ažurira. Internom procedurom se definiše period pregleda ove CPS, a koji ne može biti ređi od jednom u toku kalendarske godine.

Prema datoj internoj proceduri, CPS se može evaluirati i po potrebi ažurirati i češće nego jednom godišnje ukoliko se steknu uslovi za to. Takvi uslovi se odnose, između ostalog na vanredne promene u zakonskoj regulativi ili odgovarajuća saznanja o kritičnim slabostima primenjenih kriptografskih algoritama i dužina kriptografskih ključeva.

1.6 Definicije i skraćenice

U ovom dokumentu pojedini izrazi imaju sledeće značenje:
Aktivacioni podaci – Podaci, koji nisu ključevi, koji su zahtevani u cilju rada kriptografskih modula i koji moraju biti zaštićeni (kao na primer PIN, passphrase, ili manuelno razmenjivanje ključeva).

CA sertifikat – Sertifikat za dato CA izdat (digitalno potpisan) od strane drugog CA ili samopotpisan (ukoliko se radi o root CA).

Politika sertifikacije – Imenovan skup pravila koji indicira primenljivost sertifikata na određeno okruženje i/ili na klasu aplikacija sa zajedničkim bezbednosnim zahtevima.

Lanac (put) sertifikata – Uređena sekvenca sertifikata koja se, zajedno sa javnim ključem inicijalnog objekta u lancu (putu), procesira u cilju provere istog u poslednjem objektu na putu.

Certificate Practice Statement (CPS) – Javna Praktična pravila i procedure koje sertifikaciono telo primenjuje u proceduri izdavanja sertifikata.

Sertifikaciono telo – izdavač sertifikata (issuing CA) – U kontekstu određenog sertifikata, sertifikaciono telo – izdavač sertifikata je ono CA koje je izdalo (digitalno potpisalo) sertifikat.

Kvalifikator politike – Informacija koja zavisi od politike sertifikacije i koja je pridružena identifikatoru politike sertifikacije u okviru X.509 sertifikata. Može da uključi i URL na kome se nalazi publikovan CPS datog sertifikacionog tela.

Registraciono telo (RA) – Entitet koji je odgovoran za identifikaciju i autentikaciju korisnika/vlasnika sertifikata, kao i kreiranje zahteva za izdavanje sertifikata, ali koji ne izdaje i ne

potpisuje sertifikat (tj. RA vrši odgovarajuće poslove (identifikaciju korisnika) i u tom smislu je delegirano od CA). Često se i termin LRA (Local Registration Authority) koristi u istom kontekstu.

Treća strana – Primalac sertifikata koji proverava dati sertifikat i/ili proverava digitalni potpis dobijenog elektronskog
dokumenta primenom javnog ključa potpisnika iz sertifikata. Takođe, treća strana proverava validnost sertifikata u istom procesu. Treća strana može biti takođe korisnik sertifikata izdatog od strane istog sertifikacionog tela ali i ne mora.

Elektronski dokument – dokument u elektronskom obliku koji se koristi u pravnim poslovima i drugim pravnim radnjama, kao i u upravnom, sudskom i drugom postupku pred državnim organom.

Elektronski potpis – skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika.

Kvalifikovani elektronski potpis – Elektronski potpis koji se kreira primenom sredstva za kreiranje kvalifikovanog elektronskog potpisa (SSCD – Secure Signature Creation Device) i koji se proverava putem kvalifikovanog elektronskog sertifikata potpisnika. Ovaj potpis je pravno ekvivalentan svojeručnom potpisu po Zakonu o elektronskom potpisu.

Potpisnik – lice koje poseduje sredstva za elektronsko potpisivanje i vrši
elektronsko potpisivanje u svoje ime ili u ime pravnog ili fizičkog lica.

Podaci za formiranje elektronskog potpisa – jedinstveni podaci, kao što su kodovi ili privatni kriptografski ključevi, koje potpisnik koristi za izradu elektronskog potpisa;

Sredstva za formiranje elektronskog potpisa – odgovarajuća tehnička sredstva (softver i hardver) koja se koriste za formiranje elektronskog potpisa, uz korišćenje podataka za formiranje elektronskog potpisa.

Sredstva za formiranje kvalifikovanog elektronskog potpisa – sredstva za formiranje elektronskog potpisa koja ispunjavaju dodatne uslove utvrđene Zakonom o elektronskom potpisu.

Podaci za proveru elektronskog potpisa – podaci, kao što su kodovi ili javni kriptografski ključevi, koji se koriste za proveru i overu elektronskog potpisa.

Sredstva za proveru elektronskog potpisa – odgovarajuća tehnička sredstva (softver i hardver) koja služe za proveru elektronskog potpisa, uz korišćenje podataka za proveru elektronskog potpisa.

Elektronski sertifikat – elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika.

Kvalifikovani elektronski sertifikat – elektronski sertifikat koji je izdat od strane sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata i sadrži podatke predviđene Zakonom o elektronskom potpisu.

Korisnik – pravno lice, preduzetnik, državni organ, organ teritorijalne autonomije, organ lokalne samouprave ili fizičko lice kome se izdaje elektronski sertifikat.

Sertifikaciono telo - pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama Zakona o elektronskom potpisu.

Akreditacija – Formalna deklaracija od strane potvrdnog autoriteta da izvesne funkcije/entiteti zadovoljavaju specifične formalne zahteve.

Aplikacija za sertifikat – Zahtev poslat od strane korisnika koji zahteva sertifikat (aplikant) ka Sertifikacionom telu u cilju izdavanja elektronskog sertifikata.

Arhiva – Specifična baza podataka za čuvanje zapisa za određeni period vremena u cilju bezbednosti, backup-a ili audit-a.

Autentikacija – proces utvrđivanja identiteta pojedinca ili organizacije. U kontekstu PKI sistema, autentikacija se odnosi na dva procesa:

- Utvrđivanje da dato ime pojedinca ili organizacije odgovara realnom identitetu pojedinca ili organizacije
- Utvrđivanje da je pojedinac ili organizacija koji se prijavljuje za određeni servis pod datim imenom u stvari baš taj (pod tim imenom) pojedinac ili organizacija.

Identifikacija – procedura bezbednog logičkog predstavljanja korisnika, tj. utvrđivanja njegovog elektronskog identiteta, odgovarajućoj aplikaciji ili servisu.

Autorizacija – procedura utvrđivanja prava koje neki autentikovani korisnik ima za korišćenje odgovarajuće aplikacije ili servisa.

Ekstenzije u sertifikatu – Dodatna polja u sertifikatu, pored osnovnih, koja daju bliže informacije o vlasniku (korisniku) i izdavaču (CA) sertifikata.

Hijerarhija sertifikata – Sekvenca sertifikata bazirana na nivoima koja ima jedan root CA sertifikat i subordinate/intermediate entitete, kao što su sertifikati drugih CA i korisnici.

Upravljanje sertifikatima – Aktivnosti pridružene upravljanju sertifikatima uključuju čuvanje, isporuku, objavljivanje i opoziv sertifikata.

Lista opozvanih sertifikata (CRL – Certificate Revocation List) – Lista izdata i elektronski potpisana od strane CA koja uključuje serijske brojeve opozvanih sertifikata, kao i vreme i razlog opoziva. Takva lista se mora koristiti od strane trećih strana uvek kada treba proveriti validnost sertifikata i/ili verifikaciju elektronskog potpisa.

Serijski broj sertifikata – Sekvencijalni broj koji jedinstveno identifikuje sertifikat u domenu datog CA.

Zahtev za dobijanje sertifikata (CSR – Sertificate Service Request) – Standardna forma (po PKCS#10 preporuci) koja se koristi za slanje zahteva za dobijanjem sertifikata.

Sertifikacija – Proces izdavanja elektronskog sertifikata.

Asimetrični par ključeva (key pair) – Privatni ključ i javni ključ, kao matematički par koji se koriste za potrebe rada asimetričnog kriptografskog algoritma, kao što je na primer RSA algoritam.

Privatni ključ – Matematički podatak koji se koristi kao ključ za kreiranje elektronskog potpisa i za raspakivanje digitalne envelope - dešifrovanje simetričnog ključa kojim je šifrovan dokument za datog korisnika primenom asimetričnog kriptografskog algoritma.

Javni ključ – Matematički podatak koji može biti javno objavljen (najčešće se objavljuje u formi X.509v3 elektronskog sertifikata) i koji se koristi za verifikaciju

elektronskog potpisa, kreiranog pomoću odgovarajućeg privatnog ključa koji je matematički par sa datim javnim ključem, kao i za šifrovanje podataka za korisnika koji poseduje odgovarajući privatni ključ.
Šifrovanje – transformacija koja, primenom odgovarajućeg kriptografskog algoritma i odgovarajućeg kriptografskog ključa, pretvara originalnu informaciju u oblik koji u kojem sadržaj informacije postaje nedostupan neovlašćenim licima (šifrat).

Dešifrovanje – transformacija kojom se iz šifrata dobija originalna informacija primenom odgovarajućeg kriptografskog algoritma i odgovarajućeg kriptografskog ključa.

Kriptografija – nauka o zaštiti tajnosti informacija.

Kriptografski algoritmi – algoritmi po kojima se vrši transformacija originalne informacije u šifrovanu informaciju (šifrat) i obratno, iz šifrata u originalnu infomaciju, korišćenjem odgovarajućeg kriptografskog ključa.

Kriptografski ključ – tajna i slučajna informacija odgovarajuće dužine u bitovima (na primer 128 ili 256 bita) koja se koristi u kriptografskim algoritmima, u procedurama šifrovanja i dešifrovanja.

Simetrični kriptografski algoritmi – kriptografski algoritmi koji se koriste za realizaciju šifrovanja u cilju zaštite tajnosti informacija. Algoritmi se nazivaju simetričnim zato što se isti kriptografski ključ koristi za šifrovanje i za dešifrovanje.

Asimetrični kriptografski algoritmi – kriptografski algoritmi koji se koriste za realizaciju tehnologije digitalnog potpisa (kojom se obezbeđuje: autentičnost, integritet i neporecivost transakcija) i digitalne envelope (kojom se obezbeđuje čuvanje simetričnog ključa u šifrovanom obliku). Algoritmi se nazivaju asimetričnim zato što se različiti kriptografski ključevi koriste za šifrovanje i za dešifrovanje. Asimetrični kriptografski algoritam koristi par ključeva, javni i privatni.

Hash algoritmi – jednosmerni kriptografski algoritmi pomoću kojih se vrši kriptografska transformacija informacije proizvoljne veličine u hash vrednost fiksne veličine (160, 224, 256, 374, 512 bitova (ili više)).

Identifikator objekta (Object identifier) – Sekvenca brojčanih komponenti koja može biti pridružena nekom registrovanom objektu i koja ima karakteristiku da je jedinstvena u svim identifikatorima objekata u okviru specifičnog domena.

Opoziv sertifikata – Permanentno ukidanje validnosti datog sertifikata i njegovo smeštanje na CRL listu.

Deljena tajna – Deo kriptografske tajne koja je podeljena na unapred definisan broj fizičkih tokena, kao na primer smart kartica.

Smart kartica – Hardverski token koji sadrži čip na kome može da se izvrše odgovarajuće kriptografske funkcije, kao što su: elektronski potpis, šifrovanje, generisanje para asimetričnih ključeva, itd.

Korisnički ugovor – Ugovor između korisnika i CA u cilju obezbeđenja sertifikacionih usluga.

Skraćenice koje se koriste u ovom dokumentu:

CA – Certification Authority

RA – Registration Authority

PKS – Privredna Komora Srbije PKI – Public Key Infrastructure OID – Object IDentifier

TSA – Time Stamping Authority

CRL – Certificate Revocation List CSR – Certificate Service Request CDP – CRL Distribution Point

AIA – Authority Information Access

AKI – Authority Key Identifier SKI – Subject Key Identifier RFC – Request For Comments

ETSI – European Telecommunication Standardization Institute

CP – Certificate Policy

CPS – Certificate Practise Statement

URL – Uniform Resource Locator

2. Odgovornosti za publikovanje i repozitorijume

Ovo poglavlje se odnosi na neke aspekte publikovanja informacija, kao i na lokacije gde se te informacije publikuju, u okviru PKS CA.

2.1 Repozitorijumi

PKS CA publikuje informacije u vezi elektronskih sertifikata koje izdaje na on- line repozitorijumima koji mogu biti na web serveru ili LDAP serveru. PKS CA zadržava pravo da

publikuje statusne informacije o sertifikatima i na repozitorijumu neke treće strane ukoliko je to pogodno.

PKS CA ima on-line repozitorijum dokumenata u kojima se objavljuju informacije o politikama, pravilima i procedurama rada, uključujući CP i CPS. PKS CA zadržava pravo da učini raspoloživim i publikuje informacije u vezi sopstvenih politika i procedura rada putem bilo kog pogodnog načina.

2.2 Publikovanje informacija o sertifikatima

PKS CA publikuje informacije o sertifikatima na prethodno pomenutim repozitorijumima, i to:

- Sertifikate PKS CA (Root i intermediate CA sertifikate),
- Osnovne dokumente rada PKS CA (CP, ova CPS; standardne forme aplikacija za dobijanje sertifikata, standardne korisničke ugovore, itd.).

Iz razloga njihove osetljvosti i poslovne tajne, PKS CA neće publikovati interna pravila rada koja se odnose na izvesne podkomponente i elemente koji uključuju izvesne bezbednosne kontrole, procedure koje se odnose na upravljanje ključevima, distribuiranu odgovornost, bezbednost registraciona tela, root signing proceduru i sve ostale bezbednosno osetljive procedure.

2.3 Vreme i frekvencija publikovanja

PKS CA publikuje informacije o statusu opozvanosti izdatih digitalnih sertifikata (CRL liste) periodično i to u tačno određenim intervalima, kako je to naznačeno i precizirano u ovom CPS dokumentu.

2.4 Kontrole pristupa repozitorijumima

Sve informacije objavljene u online repozitorijumu PKS CA su dostupne preko Interneta svim zainteresovanim stranama, bez ograničenja.

PKS CA održava potpuno raspoloživim pristup do svog javnog repozitorijuma trećim stranama sa svrhom:

- Dobavljanja CA sertifikata PKS CA,

- Dobavljanja CRL liste PKS CA u cilju validacije sertifikata izdatog od strane PKS CA,

PKS CA može ograničiti ili zabraniti pristup određenim uslugama, kao što su publikovanje statusnih informacija o bazama podataka treće strane, određenim privatnim direktorijumima, itd.

Iako je pristup PKS CA repozitorijumu i direktorijumima besplatan, PKS CA zadržava pravo da naplaćuje određena specifična korišćenja svojih servisa.

3. Identifikacija i autentikacija korisnika

PKS CA održava dokumentovana praktična pravila (ovaj dokument) i procedure u cilju autentikacije identiteta i/ili drugih atributa aplikanata/krajnjih korisnika koji zahtevaju izdavanje sertifikata od strane PKS CA, a što se izvršava pre izdavanja sertifikata.

PKS CA autentikuje zahteve strana koje žele da opozovu sertifikate u skladu sa CP i ovim CPS.

PKS CA održava odgovarajuće procedure u cilju određivanja praktičnih pravila za dodeljivanje imena, uključujući i prepoznavanje "trademark" prava u izvesnim imenima.

3.1 Nazivi

3.1.1 Tipovi imena

U cilju identifikacije korisnika, PKS CA sprovodi odgovarajuća pravila dodeljivanja imena i identifikacije koja uključuje tipove imena pridruženih subjektu.

3.1.2 Potreba da imena budu sa realnim značenjem

Kada aplicira za dobijanje sertifikata od strane PKS CA, ime aplikanta mora biti u potpunosti realno, i sa odgovarajućim značenjem, sem ako to nije eksplicintno dozvoljeno u relevantnom opisu procedure u okviru PKS CA, kao i u ovom dokumentu. PKS CA izdaje sertifikate aplikantima koji dostavljaju dokumentovane aplikacije koje sadrže ime koje se može verifikovati.

3.1.3 Anonimnost korisnika

PKS CA ne izdaje anonimne sertifikate korisnicima.

3.1.4 Pravila za interpretaciju različitih formi imena

Ovo poglavlje nije primenljivo u okviru ovih CPS.

3.1.5 Jedinstvenost imena

Imena pridružena korisnicima sertifikata izdatih od strane PKS CA su jedinstvena u domenu PKS CA.

3.1.6 Prepoznavanje, autentikacija i uloga robnih marki („trademarks“)

PKS CA ne prihvata “trademark” oznake, loga ili druge grafičke ili tekstualne materijale koji su zaštićeni od kopiranja a predloženi su za uključenje u sertifikate koje izdaje PKS CA.

3.2 Inicijalna provera identiteta

U cilju realizacije procedure identifikacije i autentikacije za inicijalnu korisnikovu registraciju PKS CA sprovodi sledeće korake:

3.2.1 Autentikacija identiteta organizacije

Zahtevi PKS CA u smislu identifikacije i autentikacije organizacija koje su aplicirale za PKS CA sertifikate, uključuju ali nisu ograničene na konsultovanje određenih baza podataka treće strane koje jednoznačno identifikuju organizacij ili proverom dokumenata o udruživanju date organizacije.

U cilju identifikacije i autentikacije organizacije koja je ovlastila svog predstavnika za apliciranje za kvalifikovani sertifikat, PKS CA može primeniti korake koji uključuju ali nisu ograničeni na:

- Provera dokumenata pojedinca, ovlašćenog predstavnika date organizacije, kao što su identifikacione kartice, pasoš, u skladu sa važećim zakonom.
- Utvrđivanje identiteta organizacije koja se bazira na dostavljenoj dokumentaciji.
- Zahtev je da se pojedinac fizički pojavi u PKS RA u odgovarajućoj fazi pre nego što se sertifikat izda.

- Primenu dodatnih zahteva za organizaciju aplikanta kao što su elektronski potpisani autorizacioni dokumenti (ovlašćenja) ili neka druga identifikaciona oznaka organizacije, uz poštovanje uslova navedenog u prethodnom stavu.

3.2.2 Autentikacija identiteta pojedinca

U cilju identifikacije i autentikacije individualnog korisnika koji aplicira za dobijanje PKS CA sertifikata, PKS CA može primeniti korake koji uključuju ali nisu ograničeni na:

- Provera dokumenata kao što su identifikacione kartice, pasoš, vozačka dozvola, u skladu sa važećim zakonom.
- Utvrđivanje identiteta datog pojedinca koja se bazira na proveri ličnih identifikacionih dokumenata.
- Zahtev je da se pojedinac fizički pojavi u PKS RA u odgovarajućoj fazi pre nego što se sertifikat izda.

3.2.3 Informacije korisnika koje se ne verifikuju

Ovo poglavlje nije primenljivo u okviru ovih CPS.

3.2.4 Validacija autoriteta

Kada PKS CA uključuje informaciju koja indicira određeni autoritet koji treba da se saglasi, kao što su specifična prava, ovlašćenja, ili dozvole uključujući dozvolu da realizuje odgovarajuće aktivnosti u ime date organizacije, PKS CA može zahtevati posebnu, elektronski potpisanuo ovlašćenje od strane date organizacije - autoriteta.

3.2.5 Kriterijumi za interoperabilnost

Ovo poglavlje nije primenljivo u okviru ovih CPS.

3.3 Identifikacija i autentikacija zahteva za obnavljanje ključeva

Ovo poglavlje nije primenljivo u okviru ovih CPS.

3.3.1 Identifikacija i autentikacija za rutinsko obnavljanje ključeva

Ovo poglavlje nije primenljivo u okviru ovih CPS.

3.3.2 Identifikacija i autentikacija za obnavljanje ključeva nakon opoziva

Ovo poglavlje nije primenljivo u okviru ovih CPS.

3.4 Identifikacija i autentikacija zahteva za opoziv sertifikata

U cilju sprovođenja procedura identifikacije i autentikacije zahteva za opozivm sertifikata za odgovarajuće tipove subjekata (RA, korisnici ili drugi učesnici), zahtevi se upućuju odgovarajućem PKS RA do samog PKS CA. PKS RA sprovodi takve zahteve do PKS CA u cilju realizacije procedure opoziva sertifikata.

Primeri bezbednog dostavljanja zahteva za opozivom mogu biti digitalno potpisani zahtevi od strane samih korisnika koji žele da im se opozove sertifikat (ukoliko je takva mogućnost dozvoljena u okviru CPS) ili od strane RA ili CA ovlašćenih službenika.

4. Operativni zahtevi u vezi životnog ciklusa sertifikata

Za sve korisnike ili druge učesnike postoji stalna obaveza da informišu PKS CA o svim promenama u informacijama koje su objavljene u sertifikatu za čitav perod operativnog rada takvog sertifikata. Određene druge obaveze se takođe mogu dodatno primeniti.

4.1 Aplikacija za dobijanje sertifikata

4.1.1 Ko može da dostavi aplikaciju za izdavanje sertifikata?

Zahtev za izdavanje sertifikata od strane PKS CA može da podnese svako ko ispunjava sledeće uslove:

- Korisnik mora biti prihvatljiv krajnji korisnik PKS kako to definiše politika sertifikacije i ovaj CPS dokument.
- Zahtev koji predaje korisnik mora da u sebi sadrži sve neophodne podatke, uključujući dovoljno podataka da korisnik može da bude identifikovan na jedinstven način.

4.1.2 Proces dostavljanja zahteva za izdavanjem sertifikata (enrollment) i odgovornosti

Korisnici sprovode enrolment proces (proces identifikacije, autentikacije i registracije) sa PKS RA koji zahteva:

- Prihvatanje pravila izdavanja i korišćenja kvalifikovanog elektronskog sertifikata.
- Popunjavanje aplikacione forme.
- Prihvatanje korisničkog ugovora.

Aplikanti za dobijanje sertifikata imaju odgovornost da dostave pouzdane i tačne informacije u svojim aplikacijama za dobijanje sertifikata.

Registraciju korisnika PKS CA vrše Registracioni autoriteti. RA mogu biti i druga pravna lica sa kojima su posebnim ugovorima regulisani odnosi, prava i obaveze. Operateri registracionog autoriteta (RAO) vrše proveru podataka o korisniku:

- Ime,
- Prezime,
- JMBG,
- Naziv organizacije (privrednog subjekta) koju korisnik predstavlja,
- Matični broj firme,
- Sedište organizacije (naziv grada),
- Poštanski broj grada,
- Adresu organizacije (ulica i broj) i
- E-mail adresu korisnika u navedenoj organizaciji.

Ovim podacima mogu biti pridruženi i drugi podaci ukoliko je to posebnim popisima drugačije određeno.

4.2 Procesiranje aplikacije za dobijanje sertifikata

4.2.1 Izvršavanje funkcije identifikacije i autentikacije korisnika

Nakon registracije datog korisnika i prijema aplikacije, PKS CA ili PKS RA vrše definisanu identifikacionu i autentikacionu proceduru u cilju validacije aplikacije za izdavanje sertifikata.

4.2.2 Potvrđivanje ili odbijanje aplikacije za dobijanje s kvalifikovanog sertifikata korisnika

Nakon validacije aplikacije korisnika za izdavanje kvalifikovanog sertifikata, PKS CA ili PKS RA potvrđuju ili odbijaju aplikaciju za izdavanje kvalifikovanog sertifikata ukoliko zakonski uslovi nisu ispunjeni.

Nakon dostavljanja aplikacije za izdavanje, PKS RA potvrđuje ili odbija dostavljene zahteve. Drugim rečima, nakon potvrđivanja dostavljenih informacija u aplikaciji za izdavanje sertifikata, PKS RA potvrđuje ili odbija aplikaciju za izdavanje kvalifikovanog sertifikata.

Nakon potvrđivanja aplikacije za izdavanje kvalifikovanog sertifikata, PKS RA šalje zahtev za izdavanje sertifikata do PKS CA.

4.2.3 Potrebno vreme za procesiranje aplikacije korisnika

PKS CA mora da izvrši sve identifikacione aktivnosti i procesira aplikaciju za izdavanje kvalifikovanog sertifikata u okviru vremenskog perioda od sedam (10) radnih dana od dobijanja validnog zahteva.

4.3 Izdavanje sertifikata

4.3.1 Aktivnosti CA tokom procesa izdavanja kvalifikovanog sertifikata

Nakon dostave validnog zahteva korisnika za izdavanjem kvalifikovanog sertifikata, PKS CA sprovodi proces izdavanja odgovarajućeg kvalifikovanog sertifikata koji se sastoji od sledećih aktivnosti:

- Procedura verifikacije RA službenika od strane CA na dostavljenom zahtevu za izdavanje kvalifikovanog sertifikata,
- Procedura generisanja kvalifikovanog sertifikata od strane CA.

Da bi kvalifikovani sertifikat bio izdat neophodno je da budu ispunjeni sledeći uslovi:

- Korisnik koji je podneo zahtev za izdavanje kvalifikovanog sertifikata pozitivno je identifikovan i njegov identitet je potvrđen.
- Podaci koje je naveo u prijavi su istiniti.
- Korisnik ne poseduje validan kvalifikovani sertifikat za koji se prijavio.

U okviru PKS CA, generišu se dva asimetrična para ključeva za korisnike, i to:

- Asimetrični par ključeva i sertifikat za autentikaciju korisnika i digitalnu envelopu (šifrovanje asimetričnim kriptografskim algoritmom) – generiše se u okviru PKS CA gde se i programira na smart karticu.
- Asimetrični par ključeva i kvalifikovani sertifikat korisnika za kvalifikovani elektronski potpis – generiše se na SSCD uređaju (smart kartici) u PKS CA.

4.3.2 Obaveštenje korisnika od strane CA o izdatom sertifikatu

Sertifikat za šifrovanje i kvalifikovani sertifikat se generišu u okviru PKS CA i upisuju na SSCD koji se uručuje lično korisniku.

Ako se desi da zahtev bude odbijen, korisnik će biti informisan o razlozima odbijanja koji su definisani Zakonom.

4.4 Prihvatanje sertifikata

4.4.1 Sprovođenje procesa prihvatanja sertifikata

Izdati sertifikat od strane PKS CA se smatra prihvaćenim od strane korisnika ukoliko se ispuni bilo koji od dole navedenih uslova:

- Korišćenje standardne on-line forme uz odgovarajući elektronski potpis korisnika gde je to moguće primeniti,
- Korišćenje sertifikata prvi put uz odgovarajući elektronski potpis korisnika, Deset (10) dana nakon preuzimanja ukoliko korisnik ne javi da postoje bilo kakvi problemi u izdatom sertifikatu.

Bilo koja primedba na prihvatanje izdatog sertifikata mora biti eksplicitno dostavljena do PKS CA, kao sertifikacionom telu – izdavaocu. Potvrda odbijanja koja uključuje sva eventualna polja u sertifikatu koja sadrže pogrešne informacije mora takođe biti dostavljena.

4.4.2 Objavljivanje sertifikata od strane CA

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.4.3 Obaveštenje drugih entiteta o izdatom sertifikatu

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.5 Korišćenje sertifikata i asimetričnog para ključa

U ovom poglavlju se definišu odgovornosti koje se odnose na korišćenje asimetričnog para ključeva i sertifikata.

4.5.1 Korišćenje privatnog ključa i sertifikata od strane korisnika

Odgovornosti korisnika – korisnik se obavezuje da će koristiti privatni ključ i izgenerisani sertifikat od strane PKS CA samo u predviđenim aplikacijama, kao i u skladu sa definisanim načinom korišćenja ključa u samom sertifikatu (Key Usage i Enhanced Key Usage ekstenzije), osim ako to nije posebnim propisima drugačije određeno.

Korišćenje privatnog ključa i sertifikata predstavlja deo korisnikovog ugovora sa CA. U tom smislu, korisnik može koristiti svoj privatni ključ samo nakon prihvatanja odgovarajućeg sertifikata.

Takođe, korisnik mora prestati da koristi svoj privatni ključ nakon isticanja perioda validnosti ili opoziva izdatog sertifikata.

4.5.2 Korišćenje javnog ključa i sertifikata od strane trećih strana

Odgovornost treće strane – treća strana je obavezna da prihvata izdate sertifikate PKS CA sa predviđenim načinom korišćenja sertifikata definisanim u samom sertifikatu. Treća strana je obavezna da propisno i uspešno primenjuje operaciju javnog ključa koji ekstrahuje iz izdatog sertifikata i odgovorna je da sprovodi proveru statusa datog sertifikata korišćenjem metoda koji je definisan u CP i u ovom CPS dokumentu PKS CA.

4.6 Obnavljanje sertifikata

4.6.1 Uslovi za obnavljanje sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.6.2 Ko može zahtevati obnavljanje sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.6.3 Procesiranje zahteva za obnavljanjem sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.6.4 Obaveštenje korisnika da mu je izdat obnovljeni sertifikat

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.6.5 Sprovođenje procesa prihvatanja obnovljenog sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.6.6 Objavljivanje obnovljenog sertifikata od strane CA

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.6.7 Obaveštenje drugih entiteta od strane CA o obnovi datog sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.7 Generisanje novog para ključeva i sertifikata korisnika

4.7.1 Uslovi za generisanje novog para ključeva i sertifikata

Uslovi za generisanje novog para ključeva korisnika su:

- Sertifikat datog korisnika je istekao ili
- Sertifikat datog korisnika je opozvan, a korisnik ima pravo da naknadno zatraži dobijanje novog sertifikata.

4.7.2 Ko može zahtevati novi sertifikat sa novim javnim ključem

Svi korisnici PKS CA koji ispunjavaju uslove iz tačke 4.7.1.

4.7.3 Procesiranje zahteva za novim parom ključeva i sertifikatom

Korisnici kojima je sertifikat istekao, ukoliko žele da dobiju novi sertifikat, moraju da podnesu zahtev za izdavanje novog sertifikata koji je isti kao i svaki novi zahtev za dobijanje sertifikata. U tom slučaju, uvek se generiše novi par asimetričnih ključeva.

Takođe, ukoliko je sertifikat korisnika opozvan, a razlog za opoziv je kompromitacija ključa, korisnik može dobiti novi sertifikat samo na osnovu generisanog novog para asimetričnih ključeva i putem procedure koja je identična dostavljanju prvobitnog zahteva za izdavanje novog sertifikata.

Nakon dostavljanja zahteva za izdavanjem novog sertifikata, dalja procedura je u potpunosti identična kao i procedura za dobijanje prvog sertifikata.

4.7.4 Obaveštenje korisnika da mu je izdat novi sertifikat

Ova procedure je identična proceduri izdavanja prvog sertifikata.

4.7.5 Sprovođenje procesa prihvatanja novog sertifikata

Ova procedure je identična proceduri prihvatanja prvog sertifikata.

4.7.6 Objavljivanje novog sertifikata od strane CA

Ova procedure je identična proceduri objavljivanja prvog sertifikata.

4.7.7 Obaveštenje drugih entiteta od strane CA o izdavanju novog sertifikata

Ova procedure je identična proceduri obaveštenja drugih entiteta o izdavanju prvog sertifikata od strane CA.

4.8 Modifikacije sertifikata korisnika

4.8.1 Uslovi za modifikaciju sertifikata korisnika

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.8.2 Ko može zahtevati modifikaciju sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.8.3 Procesiranje zahteva za modifikacijom sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.8.4 Obaveštenje korisnika da mu je izdat novi modifikovani sertifikat

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.8.5 Sprovođenje procesa prihvatanja novog modifikovanog sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.8.6 Objavljivanje novog modifikovanog sertifikata od strane CA

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.8.7 Obaveštenje drugih entiteta od strane CA o izdavanju novog modifikovanog sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.9 Opoziv i suspenzija sertifikata

4.9.1 Uslovi za opoziv sertifikata korisnika

Nakon odgovarajućeg zahteva od strane PKS RA ili samog korisnika, PKS CA vrši opoziv izdatog elektronskog sertifikata u slučaju:

- Gubitka, krađe, modifikacije, neautorizovanog objavljivanja ili neke druge kompromitacije privatnog ključa korisnika sertifikata.
- Ako je subjekt sertifikata narušio materijalne obaveze koje su definisane u CP ili u ovom CPS dokumentu.
- Ako izvršenje odgovarajućih obaveza lica koja su navedena u CP i u ovim CPS kasni ili je sprečeno usled prirodne katastrofe, računarskog ili komunikacionog otkaza, ili usled drugog uzroka koji izlazi van kontrole datog lica.
- Ako se desila promena određenih informacija koja se sadrže u sertifikatu datog lica.
- Ako korisnik zahteva opoziv iz njemu ličnih razloga.

4.9.2 Ko može zahtevati opoziv sertifikata

Opoziv sertifikata datog korisnika može zahtevati sam korisnik, zakonski zastupnik pravnog lica u slučaju ako se radi o sertifikatima izdatim fizičkim licima koja zastupaju pravna lica ili ovlašćeni službenik PKS RA ili PKS CA. Drugim rečima, zahtev za opozivom sertifikata može da podnese vlasnik sertifikata, nakon propisne autentikacije, ili odgovarajući službenik PKS CA ili PKS RA uz dokaz da je ispunjen jedan od uslova za opoziv sertifikata, naveden u članu 4.9.1.

4.9.3 Procedura zahteva za opozivom sertifikata

Ako se desi neki od gore pomenutih događaja, korisnik ili neki drugi ovlašćeni predstavnik pravnog lica mora što pre da popuni Zahtev za opoziv.Zahtev za opozivom je poseban formular koji mora biti elektronski potpisan. Pomenuti kontakt može biti on-line ili putem nekih drugih kanala komunikacije. PKS CA opoziva sertifikat promptno nakon verifikacije identiteta strane koja je zahtevala opoziv (službenik PKS RA ili PKS CA, sam korisnik ili neki drugi ovlašćeni predstavnik pravnog lica) i potvrdom da je zahtev podnet u skladu sa procedurom zahtevanom u CP, kao i u ovom CPS dokumentu. Verifikacija identiteta može biti izvršena na osnovu informacionih elemenata koji su sadržani u identifikacionim podacima koje je korisnik dostavio do PKS RA ili PKS CA. Nakon ispunjenja pomenutih uslova, PKS CA izvršava aktivnost u cilju opoziva sertifikata.

Konkretno u PKS CA, operaciju opoziva korisničkih sertifikata vrši RAO. Ona podrazumeva sledeće akcije:

1. Upis serijskog broja sertifikata korisnika u listu opozvanih sertifikata i razloga opoziva (Privilege withdrawn).
2. Promenu stanja sertifikata korisnika u LDAP-u na Opozvan.

4.9.4 Grace period zahteva za opozivom sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.9.5 Vreme za koje CA mora da procesira zahtev za opozivm sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.9.6 Zahtevi za treće strane u vezi provere statusa sertifikata

Treće strane moraju koristiti on-line resurse koje PKS CA čini raspoloživim putem repozitorijuma u cilju provere statusa sertifikata na koje oni žele da se oslone.

Treće strane moraju biti u saglasnosti sa PKS CA politikom sertifikacije a posebno sa obavezama trećih strana publikovanim u CP ili ovom CPS dokumentu.

4.9.7 Frekvencija izdavanja CRL liste

Lista opozvanih sertifikata (CRL – Certificate Revocation List) PKS CA se ažurira na svaka 24 sata.

4.9.8 Maksimalno kašnjenje u izdavanju CRL liste

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.9.9 Raspoloživost procedure online provere statusa sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.9.10 Zahtevi online provere statusa sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.9.11 Raspoloživost drugih formi objavljivanja statusa sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.9.12 Specijalni zahtevi u odnosu na kompromitaciju privatnog ključa

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.9.13 Uslovi za suspenziju sertifikata

Suspenzija sertifikata se može izvršiti ukoliko je korisnik prekršio odgovarajuća pravila korišćenja sertifikata što za sobom povlači privremenu suspenziju rada ili korisnik ide na duže odsustvo i zna da neće koristiti sertifikat i svoj privatni ključ.

Sertifikat se suspenduje u sledećim situacijama:

- Ako suspenziju sertifikata zahteva vlasnik sertifikata, zakonskizastupnik pravnog lica ako je sertifikat izdat fizičkim licima koja zastupaju pravno lice, ili odgovarajući službenik PKS CA ili PKS RA;
- Ako suspenziju sertifikata zahteva nadležni organ za zaštitu podataka ili neki drugi viši organ koji ima opravdane sumnje da sertifikat sadrži neispravne podatke ili da se privatni ključ koji odgovara javnom ključu iz sertifikata može koristiti bez saglasnosti vlasnika;
- Ako suspenziju sertifikata zahteva sud, tužilac ili institucije koje vrše kriminalnu istragu da bi sprečili dalje zločine

4.9.14 Ko može zahtevati suspenziju sertifikata

Suspenziju sertifikata datog korisnika može zahtevati sam korisnik, zakonski zastupnik pravnog lica ako je sertifikat izdat fizičkim licima koja zastupaju pravno lice, ovlašćeni službenik PKS RA, PKS CA, sud, tužilac ili institucije koje vrše kriminalnu istragu.

4.9.15 Procedura zahteva za suspenzijom sertifikata

Zahtev za suspenzijom sertifikata može biti dostavljen od strane korisnika ili PKS RA. Zahtev se u ovom slučaju dostavlja u obliku odgovarajućeg dokumenta, potpisanim digitalno, od strane korisnika ili PKS RA.
Operacija suspenzije sertifikata je identična opozivu s tim što je razlog opoziva drugačiji (Certificate Hold) dok se stanje sertifikata na LDAP-u postavlja na Suspendovan.

4.9.16 Ograničenje perioda suspenzije sertifikata

Suspenzija sertifikata traje onoliko dugo koliko traju i uslovi zbog kojih je suspenzija i zahtevana. Kada ovi uslovi prestanu da važe, korisnik može zahtevati reaktivaciju svog sertifikata.

PKS CA publikuje serijske brojeve svih opozvanih i suspendovanih sertifikata u svojoj CRL listi.

Za vreme suspenzije, ili nakon opoziva sertifikata, period operativnog rada datog sertifikata se istovremeno smatra završenim.

Sertifikat se aktivira u sledećim situacijama:

- Ako aktiviranje sertifikata zahteva vlasnik sertifikata ili odgovarajući službenik PKS CA ili PKS RA na osnovu čijeg zahteva je izvršena suspenzija.
- Ako aktiviranje sertifikata zahteva nadležni organ za zaštitu podataka ili neki drugi viši organ na osnovu čijeg zahteva je izvršena suspenzija.
- Ako aktiviranje sertifikata zahteva sud, tužilac ili institucija na osnovu čijeg zahteva je izvršena suspenzija.

Operaciju aktiviranja sertifikata iz stanja suspendovan vrši RAO. Ona podrazumeva sledeće akcije:

1. Brisanje serijskog broja sertifikata korisnika iz liste opozvanih sertifikata.
2. Promenu stanja sertifikata korisnika u LDAP-u i brisanje sertifikata iz CRL.

4.10 Servisi provere statusa sertifikata

4.10.1 Operativne karakteristike

PKS CA publikuje sve opozvane i suspendovane sertifikate u svojoj CRL listi. Lista opozvanih sertifikata (CRL – Certificate Revocation List) PKS CA se ažurira na svaka 24 sata.

4.10.2 Raspoloživost servisa

Treće strane moraju koristiti on-line resurse koje PKS CA čini raspoloživim putem repozitorijuma u cilju provere statusa sertifikata na koje oni žele da se oslone.

4.10.3 Opciona obeležja

Ovo poglavlje nije primenljivo u okviru ovih CPS.

4.11 Prestanak korišćenja sertifikata

Nakon prestanka korišćenja sertifikata izdatog od strane PKS CA, dati sertifikat mora biti opozvan.

Prestanak korišćenja sertifikata može biti iz sledećih razloga:

- Korisnik želi da prekine korišćenje sertifikacionih servisa PKS CA.
- PKS CA je prestalo sa pružanjem usluga sertifikacije.

4.12 Čuvanje i rekonstrukcija privatnog ključa korisnika

4.12.1 Politika i praksa čuvanja i rekonstrukcije privatnog ključa

PKS CA obezbeđuje uslove za generisanje višestrukih parova asimetričnih ključeva za korisnike. Pri tome,jedan par ključeva se generiše u okviru CA i služi za autentikaciju korisnika i za šifrovanje dokumenata putem procedure digitalne envelope za datog korisnika.U cilju omogućavanja dešifrovanja dokumenata šifrovanih za datog korisnika u incidentnim slučajevima, kao i za eventualne službene potrebe, neophodno je da se dati privatni ključ čuva na bezbedan način na nekom arhivnom server u okviru CA. U vezi toga definišu se i odgovarajuće procedure za bezbedno čuvanje privatnog ključa, za postupak aktiviranja datog privatnog ključa, kao i definicije u kojim sve slučajevima privatni ključ određenog korisnika može biti rekonstruisan iz arhivnog servera. Napominjemo još jednom da se ovde radi o privatnom ključu koji isključivo služi za dešifrovanje digitalne envelope. Privatni ključ korisnika kojim se vrši digitalni potpis ne sme biti nigde čuvan, niti generisan, izuzev na SSCD uređaju korisnika.

4.12.2 Enkapsulacija sesijskog ključa i politika i praksa za rekonstrukciju

Ovo poglavlje nije primenljivo u okviru ovih CPS.

5. Upravne, operativne i fizičke bezbednosne kontrole

Ovo poglavlje opisuje sve one bezbednosne kontrole koje ne spadaju direktno u tehničke kontrole a koje se koriste od strane PKS CA kao podrška u cilju realizacije funkcija generisanja ključeva, autentikacije subjekata, izdavanja sertifikata, opoziva sertifikata, auditinga i arhiviranja.

Ove ne-tehničke bezbednosne kontrole su kritične za poverenje u sertifikate izdate od strane PKS CA pošto nedostatak bezbednosti može kompromitovati operativni rad CA rezultujući na primer u kreiranju sertifikata i CRL sa pogrešnim informacijama ili kompromitacijom privatnog ključa CA.

5.1 Fizičke bezbednosne kontrole

PKS CA implementira odgovarajuće mehanizme fizičke kontrole u svojim prostorijama.

5.1.1 Lokacija i konstrukcija sajta

PKS CA se nalazi u prostorijama Privredne komore Srbije u Beogradu.

PKS CA bezbedne prostorije su locirane u prostoru koji odgovara potrebama izvršenja operacija visoke bezbednosti. Postoje označene zone sa fizičkom kontrolom pristupa i zaključane kancelarije sa odgovarajućim sefovima.

5.1.2 Fizički pristup

Pristup prostorijama PKS CA je omogućen samo ovlašćenom osoblju koje poseduje smart kartice iz sistema PKS.

Fizički pristup je ograničen implementacijom odgovarajućih mehanizama kontrole pristupa iz jedne u drugu zonu bezbednosti, kao i u zonu visoke bezbednosti. U tom smislu, CA operacije su locirane u okviru bezbedne računarske sobe koja je podržana fizičkim nadgledanjem, i bezbednosnim alarmima, a obezbeđena je i podrška da prelazak iz zone u zonu može biti izveden samo korišćenjem tokena (beskontaktnih kartica), kao i listi kontrole pristupa.

5.1.3 Električno napajanje i klimatizacija

Sva oprema PKS CA je priključena na jedinice za neprekidno napajanje. Temperatura i vlažnost vazduha se u prostorijama održava u okviru unapred specificiranih intervala pomoću klima uređaja.

Napajanje i ventilacija se izvršavaju sa redundansom visokog nivoa.

5.1.4 Izloženost poplavama i vremenskim nepogodama

Unutar prostorija PKS CA nema vodovodnih instalacija. Prozori zadovoljavaju najmodernije standard.

Prostorije PKS CA su zaštićene od poplava.

5.1.5 Prevencija i zaštita od požara

Prevencija i zaštita od požara su implementirane.

Prostorije PKS CA su opremljene detektorima dima i sistemom za gašenje požara.

5.1.6 Medijumi za čuvanje podataka

Medijumi se čuvaju na bezbedan način. Backup medijumi se takođe čuvaju na odvojenoj lokaciji koja je fizički obezbeđena i zaštićena od požara i poplava.

5.1.7 Odlaganje smeća

Iznošenje smeća se takođe kontroliše.

Papirni otpad se propušta kroz mašine za sečenje papirnog otpada. Elektronski medijumi se pre odlaganja moraju fizički/mehanički uništiti.

5.1.8 Odlaganje rezervnih kopija

Ovo poglavlje nije primenljivo u okviru ovih CPS.

5.2 Proceduralne kontrole

PKS CA sprovodi kadrovsku i upravnu praksu koja obezbeđuje razumnu sigurnost u poverljivost i kompetenciju zaposlenih, kao i zadovoljavajuće performance u vezi sa njihovim dužnostima u domenu tehnologija koje se odnose na elektronski potpis i PKI sisteme.

Svaki zaposleni PKS CA potpisuje izjavu da će se pridržavati pravne regulative u vezi zaštite podataka, kao i da će zadovoljiti sve postavljene zahteve u vezi sa poverljivošću.

5.2.1 Poverljive uloge

Svi zaposleni u PKS CA koji izvršavaju operacije povezane sa upravljanjem ključevima, kao i bilo koje druge operacije koje materijalno utiču na takve operacije, smatraju se dužnostima na poverljivim pozicijama. Poverljive uloge/dužnosti u PKS CA, između ostalih, su:

- Administrator bezbednosti,
- Sistem administratori,
- Sistem operater i
- Sistem evidentičar

PKS CA sprovodi inicijalno istraživanje svih zaposlenih koji su kandidati za poverljive uloge u cilju razumnog pokušaja sticanja uvida u njihovu poverljivost i kompetencije.

5.2.2 Broj osoba koje se zahtevaju po svakom zadatku

Tamo gde se zahteva dualna kontrola, potrebno je da najmanje dva poverljiva zaposlena PKS CA iskažu njihova podeljena znanja u cilju omogućavanja izvršenja tekućih operacija. Drugim rečima, u okviru PKS CA, nijednu osetljivu operaciju ne može izvršiti samo jedan zaposleni.

5.2.3 Identifikacija i autentikacija za svaku ulogu

Svaka uloga/dužnost definiše odgovarajuće zahteve u pogledu identifikacije i autentikacije korisnika. Lista uloga i dužnosti je definisana internim pravilom PKS CA.

5.2.4 Uloge koje zahtevaju razdvajanje dužnosti

U okviru internog pravila PKS CA definisano je koje uloge/dužnosti mogu biti kombinovane od strane jednog zaposlenog, a koje to ne smeju.

5.3 Kadrovske bezbednosne kontrole

5.3.1 Kvalifikacija i iskustvo

PKS CA izvršava neophodne aktivnosti u cilju provere zahtevane biografije, kvalifikacija, kao i neophodnog iskustva u cilju realizacije u okviru konteksta kompetencije specifičnog posla. Zaposleni u PKS CA ne smeju biti zakonski kažnjavani.

Takve provere biografije tipično uključuju:

- Kriminalne osude za ozbiljne zločine,
- Pogrešne prezentacije informacija od strane kandidata,
- Odgovarajuće reference.

Za rad u PKS CA su neophodni stručnjaci koji su tehnološki i profesionalno kompetentni i koji imaju potrebna znanja iz kriptografije, digitalnog potpisa, PKI sistema, smart kartica, HSM-ova, itd.

5.3.2 Procedura provere biografije

PKS CA realizuje relevantne provere eventualnih zaposlenih na bazi statusnih izveštaja koji su izdati od strane kompetentnih autoriteta, izjava trećih strana ili izjava samih potencijalnih zaposlenih.

5.3.3 Zahtevi za obučenošću

PKS CA obezbeđuje obuku za svoje zaposlene u cilju realizacije funkcija poslovanja CA i RA.

5.3.4 Frekvencija i zahtevi za ponovnu obuku

Periodično ažuriranje obuke može takođe biti izvršeno u cilju uspostave kontinuiteta i ažurnosti znanja zaposlenih, kao i odgovarajućih procedura.

5.3.5 Frekvencija i sekvenca rotacije poslova

Ovo poglavlje nije primenljivo u okviru ovih CPS.

5.3.6 Kaznene mere za neovlašćenje aktivnosti

PKS CA ima odgovarajuće mere za kažnjavanje zaposlenih za neovlašćene aktivnosti, neovlašćeno korišćenje autoriteta, kao i neovlašćeno korišćenje sistema u cilju sprovođenja sankcija za određeno neposlovno i rizično ponašanje, a koje može biti različito u zavisnosti od različitih okolnosti.

5.3.7 Dokumentacija koja se dostavlja zaposlenima

PKS CA čini dostupnom svu dokumentaciju zaposlenima koja se odnosi na PKS CA za potrebe inicijalne obuke, doobuke ili za druge svrhe.

5.4 Procedure bezbednosnih provera logova/auditing

Procedure audit logovanja uključuju logovanje događaja i auditing sistema, i implementirane su za svrhu održavanja bezbednog okruženja. U tom smislu, PKS CA implementira kontrole navedene u narednom tekstu.

5.4.1 Tipovi zabeleženih događaja

PKS CA zapisuje događaje koji uključuju ali nisu ograničeni na operacije vezane za životni ciklus sertifikata, pokušaje pristupa sistemu, kao i zahteve dostavljene sistemu.

5.4.2 Frekvencija procesiranja logova

PKS CA čuva audit logove u realnom vremenu, koji se kasnije procesiraju i arhiviraju na godišnjem nivou.

5.4.3 Period čuvanja audit logova

PKS CA procesira i arhivira audit logove na godišnjem nivou.

5.4.4 Zaštita audit logova

Audit logovi se samo mogu videti od strane autorizovanog osoblja – sistem auditori. Postupak zaštite je definisan u Internom pravilu PKS CA.

5.4.5 Procedure back-up-a audit logova

PKS CA implementira procedure backup-a audit logova.

5.4.6 Sistem sakupljanja audit logova

PKS CA sakuplja i čuva audit logove u realnom vremenu.

5.4.7 Obaveštenje subjekta koji je prouzrokovao događaj

U slučaju alarma ili incidentnog događaja, obaveštava se administrator mreže PKS CA.

Subjekat koji je prouzrokovao određeni audit događaj se ne obaveštava o samoj audit aktivnosti.

5.4.8 Ocena ranjivosti sistema

PKS CA realizuje procenu ranjivosti sistema na svakih 6 meseci.

5.5 Arhiviranje zapisa/logova

Zahtevi za čuvanjem zapisa se primenjuju kako na PKS CA tako i na PKS RA. Opšte politike čuvanja zapisa PKS CA uključuju odredbe navedene u nastavku teksta.

5.5.1 Tipovi arhiviranih zapisa

PKS CA na bezbedan način čuva zapise o PKS CA izdatim elektronskih sertifikata, auditing podacima i informacije o aplikacijama za izdavanje sertifikata.

5.5.2 Period čuvanja arhive

PKS CA čuva na bezbedan način pomenute zapise o PKS CA kvalifikovanim elektronskim sertifikatima za period koji je definisan zakonom.

5.5.3 Zaštita arhive

Uslovi za zaštitu arhive uključuju:

- Zapise koje samo sistem auditori (zaposleni kojima su pridružene dužnosti čuvanja podataka) mogu da vide i arhiviraju.
- Zaštitu u odnosu na modifikaciju arhive, kao što je čuvanje podataka na medijumu na koga se može upisati samo jednom.
- Zaštitu u odnosu na brisanje arhive.
- Zaštitu u odnosu na kvarenje karakteristika medijuma vremenom na kojima se arhiva čuva, kao na primer realizacija zahteva da se podaci periodično migriraju na sveže medijume.

5.5.4 Procedura back-up-a arhive

PKS CA sprovodi odgovarajuću proceduru back-up-a arhive.

PKS CA realizuje zahteve za procedurom čuvanja barem dve odvojene kopije arhive koje su pod kontrolom dve različite osobe.

5.5.5 Zahtevi za timestamping zapisa

Ovo poglavlje nije primenljivo u okviru ovih CPS.

5.5.6 Sistem sakupljanja zapisa

PKS CA sprovodi odgovarajući sistem sakupljanja zapisa/logova koji se arhiviraju.

5.5.7 Procedure za dobijanje i verifikaciju informacija iz arhive

U okviru PKS CA, definisanie su procedure u cilju dobijanja i verifikacije arhivskih informacija.

U cilju dobijanja i verifikacije arhivskih informacija, PKS CA i PKS RA održavaju zapise pod jasnom hijerarhijskom kontrolom i sa jasnim opisom posla. PKS CA čuva zapise u elektronskoj ili papirnoj formi.

PKS CA može zahtevati od svojih RA, korisnika ili njihovih agenata da dostave odgovarajuća dokumenta u cilju podrške ovog zahteva. Ovi zapisi mogu biti čuvani u elektronskoj, papirnoj i u bilo kojoj drugoj formi za koju PKS CA smatra da je odgovarajuća.

PKS CA može da izmeni način čuvanja zapisa ako je to eventualno potrebno da bude u saglasnosti sa odgovarajućom akreditacionom i supervizionom šemom koju sprovodi Nadležni organ za akreditaciju i superviziju PKI sistema u Srbiji.

5.6 Izmena ključeva

U slučaju isteka ili opoziva sertifikata sertifikacionog tela u skladu sa uslovima definisanim u ovom dokumentu PKS CA vrši generisanje novog para ključeva seritifikacionog tela I vrši distribuiranje sertifikata CA svim korisnicima i zainteresovanim stranama, kao i u slučaju prvog generisanog sertifikata CA.

5.7 Kompromitacija i oporavak u slučaju katastrofe

5.7.1 Procedure za postupanje u incidentnim i kompromitujućim situacijama

U Posebnim internim pravilima rada, PKS CA dokumentuje procedure koje treba izvršiti pri rešavanju incidenata, kao i izveštavanja u vezi sa eventualnom kompromitacijom ključeva CA.

5.7.2 Računarski resursi, softver ili podaci koji su oštećen

PKS CA takođe dokumentuje procedure oporavka koje se koriste ukoliko su računarski resursi, softver, i/ili podaci neispravni ili se sumnja da su neispravni.

5.7.3 Procedure koje se sprovode kod kompromitacije privatnog ključa korisnika

PKS CA teži da ponovo uspostavi bezbedno okruženje u koracima koji uključuju, ali nisu ograničeni samo na, opoziv neispravnih, ili se sumnja da su neispravni, sertiifkata odgovarajućih entiteta. Nakon toga, PKS CA može ponovo izdati novi sertifikat datom entitetu.

5.7.4 Mogućnosti kontinuiteta poslovanja nakon katastrofe

Plan kontinualnog poslovanja se implementira da osigura nastavak poslovanja nakon prirodne ili druge katastrofe.

5.8 Završetak rada CA ili RA

Pre nego što prekine svoje aktivnosti pružanja sertifikacionih usluga, PKS CA:

- Obezbeđuje svojim korisnicima koji imaju validne sertifikate obaveštenje o nameri da prestane sa pružanjem sertifikacione usluge, tj. da prestane da izvršava aktivnosti u svojstvu CA.
- Povlači sve sertifikate koji su još uvek validni (tj. one koji nisu opozvani ili im je istekao rok važnosti) nakon obaveštenja, a bez neophodne saglasnosti korisnika.
- Blagovremeno obaveštava o opozivu sertifikata sve korisnike na koje se to odnosi.
- Čini razumne mere u cilju zaštite zapisa koje čuva u skladu sa CP i ovim CPS.
- Ukoliko je to moguće, obezbeđuje odgovarajuće mere obezbeđenja sukcesije u smislu ponovnog izdavana sertifikata od strane drugog CA koje je sukcesor – nastavljač izdavanja sertifikata datog CA – i koje poštuje iste CP i CPS dokumente.

6. Tehničke bezbednosne kontrole

Ovo poglavlje definiše tehničke bezbednosne mere koje primenjuje PKS CA u cilju zaštite kriptografskih ključeva i aktivacionih podataka (kao na primer PIN - ovi, lozinke, itd.). Bezbednosno upravljanje ključevima je kritično u cilju osiguranja da su svi ključevi i aktivacioni podaci zaštićeni i da se koriste isključivo od strane autorizovanih zaposlenih.

Takođe, definisane su i druge tehničke bezbednosne kontrole koje se koriste od strane CA da se bezbedno izvršavaju funkcije generisanja ključeva, autentikacije korisnika, registracije korisnika, izdavanja sertifikata, opoziva sertifikata, auditinga i arhiviranja. Tehničke kontrole uključuju životni ciklus bezbednosnih kontrola kao i operativne bezbednosne kontrole.

U ovom poglavlju se takođe definišu tehničke bezbednosne kontrole nad repozitorijumima, registracionim telima, korisnicima i drugim učesnicima.

6.1 Generisanje i instalacija asimetričnog para ključeva

6.1.1 Generisanje asimetričnog para ključeva

PKS CA bezbedno generiše i štiti svoje sopstvene privatne ključeve, korišćenjem bezbednih i pouzdanih sistema, i primenjuje neophodne preventivne mere u cilju sprečavanja kompromitacije ili neautorizovanog korišćenja. PKS CA implementira i dokumentuje procedure generisanja ključeva u skladu sa CP i ovim CPS. PKS CA primenjuje javne, internacionalne i Evropske standarde u vezi bezbednih i pouzdanih sistema. PKS CA generiše sledeće asimetrične parove ključeva:

- Za potrebe Root CA – asimetrični par ključeva se generiše na hardverskom bezbednosnom modulu (HSM – Hardware Security Module).
- Za potrebe Intermediate CA – asimetrični par ključeva se generiše na hardverskom bezbednosnom modulu (HSM – Hardware Security Module).
- Za potrebe korisnika – digitalna envelopa – ovaj asimetrični par ključeva se generiše u softveru PKS CA i privatni ključ, zajedno sa sertifikatom, se upisuju na smart karticu korisnika.
- Za potrebe korisnika – digitalni potpis – ovaj asimetrični par ključeva se generiše na SSCD uređaju korisnika i nikada ga ne napušta .

PKS CA koristi bezbedan proces generisanja svog root privatnog ključa u skladu sa dokumentovanom procedurom. PKS CA distribuira deljene tajne za svoje privatne ključeve. PKS CA

je vlasnik privatnih ključeva i poseduje autoritet da prenese odgovarajuće deljene tajne na autorizovane nosioce deljenih tajni.

Privatni root ključ PKS CA se koristi za elektronsko potpisivanje PKS CA sertifikata (pre svega za izdavanje intermediate CA sertifikata), liste opozvanih sertifikata. Druge svrhe korišćenja privatnog ključa root PKS CA su zabranjene.

6.1.2 Isporuka privatnog ključa korisniku

PKS CA isporučuje dva privatna ključa korisniku na smart kartici.

6.1.3 Dostava javnog ključa do izdavaoca sertifikata

Javni ključ korisnika, kao deo asimetričnog para ključeva, se dostavlja do PKS CA kroz personalizacioni softver u okviru samog PKS CA (prilikom personalizacije smart kartica), i to u obliku zahteva za izdavanje sertifikata u PKCS#10 formatu. Ovo se odnosi na oba para ključeva korisnika.

Dostavljanje zahteva za izdavanje sertifikata krajnjeg korisnika u PKCS#10 formatu vrši operater registracionog autoriteta (RAO) koji pre slanja zahteva vrši proveru identiteta podnosioca zahteva i istinitost podataka iz pripremljenog zahteva.

6.1.4 Dostava javnog ključa izdavaoca sertifikata trećim stranama

PKS CA dostavlja svoje javne ključeve Root i Intermediate CA, u obliku X.509 v3 sertifikata putem svog online repozitorijuma kome mogu da pristupaju svi korisnici i treće strane.

6.1.5 Dužine ključeva

Za potrebe svog root privatnog ključa i odgovarajuće potpisivanje, PKS Root CA koristi SHA-256/RSA kombinaciju hash i asimetričnog algoritma sa dužinom ključa od 4096 bita i peridom validnosti od 20 godina sa periodom izdavanja sertifikata od 10 godina.

Za svoje intermediate/operativne/online CA privatne ključeve i odgovarajući algoritam za elektronsko potpisivanje, PKS CA koristi SHA-256/RSA kombinaciju hash i asimetričnog algoritma sa dužinom ključa od 3072 bita, kao i period validnosti od 10 godina sa periodom izdavanja sertifikata od 5 godina.

PKS CA zadržava pravo na izmenu gore navedenih kombinacija algoritama i dužina ključeva ukoliko se u kriptografskoj teoriji i praksi pokažu slabosti navedenih algoritama i svetska kriptografska javnost preporuči pouzdanije algoritme, kao i u slučajevima definisanja novih standarda za hash i asimetrične algoritme.

6.1.6 Generisanje kriptografskih parametara i provera kvaliteta

Kriptografski parametri, tj. asimetrični parovi ključeva se generišu pomoću hardverskih generator slučajnih brojeva koji su realizovani na kriptografskim hardverskim uređajima, i to:

- HSM – za ključeve CA
- SSCD uređaj - za ključeve korisnika za potrebe kvalifikovanog elektronskog potpisa

Kvalitet načina generisanja pomenutih kriptografskih parametara isključivo zavisi od kvaliteta hardverskog generatora slučajnih brojeva na HSM-ovima i smart karticama korišćenim u PKS CA.

6.1.7 Moguće „Key Usage" opcije

U elektronskim sertifikatima (root i intermediate CA sertifikati) i kvalifikovanim elektronskim sertifikatima (korisnilki sertifikati) izdatim od strane PKS CA koriste se sledeće vrednosti u ekstenziji „Key Usage“:

Root CA sertifikat:

- Certificate Signing, Off-Line CRL Signing, CRL Signing

Intermediate CA sertifikat:

- Certificate Signing, Off-Line CRL Signing, CRL Signing

Sertifikat za autentikaciju korisnika i digitalnu envelopu:

- Key Encipherment

Kvalifikovani sertifikat za kvalifikovani elektronski potpis korisnika:

- Digital Signature, Non-Repudiation

6.2 Zaštita privatnog ključa i kontrola kriptografskog hardverskog modula

PKS CA koristi odgovarajuće kriptografske uređaje u cilju realizacije zadataka upravljanja i zaštite ključeva PKS CA. Pomenuti kriptografski uređaji su poznati pod imenom Hardverski bezbednosni moduli (HSM - Hardware Security Modules).

6.2.1 Standardi i kontrole kriptografskog hardverskog modula

Generisanje privatnog ključa PKS CA (root i intermediate CA) se vrši u okviru bezbednog kriptografskog uređaja koji zadovoljava odgovarajuće zahteve u skladu sa međunarodnim standardom FIPS 140-2 L3. Ispunjenje ovog standarda garantuje, između ostalog, da je bilo koji pokušaj narušavanja integriteta uređaja ili kriptografske memorije istovremeno detektovan.

HSM uređaji ne smeju da napuštaju PKS CA prostorije izuzev retkih prilika unapred definisanih premeštanja i preseljenja. PKS CA čuva zapise u vezi

U slučaju da odgovarajući HSM zahteva održavanje ili popravku, koja se ne može izvršiti u okviru PKS CA prostorija, oni se onda bezbedno prenose do njihovog proizvođača uz poštovanje svih neophodnih bezbednosnih mera, detaljno opisanih u CPS dokumentu.

6.2.2 K od n distribucija odgovornosti kontrole privatnog ključa

Generisanje privatnog ključa PKS CA zahteva kontrolu od više od jednog, na odgovarajući način autorizovanog, zaposlenog koji ima poverljive pozicije i dužnosti u okviru PKS CA. Autorizacija procedure generisanja ključeva se mora izvršiti od strane više od jednog člana upravne strukture PKS CA.

Procedura deljenja tajni PKS CA koristi višestruke autorizovane nosioce u cilju da zaštiti i poboljša poverljivost privatnih ključeva i obezbedi odgovarajuću proceduru oporavka ključa.

Privatni ključ PKS CA se koristi pod uslovima definisanim u okviru k=3 od n=3 kontrole od strane više zaposlenih sa poverljivim ulogama.

Pre nego što nosilac deljene tajne prihvati deljenu tajnu on mora lično da se upozna sa kreiranjem, ponovnim kreiranjem i distribucijom tajne na njegovog sledećeg člana lanca poverljivosti.

PKS CA čuva pisane zapise u vezi distribucije deljene tajne.

PKS CA dokumentuje sopstvenu distribuciju deljenih tajni za aktivaciju svog privatnog ključa i ima mogućnost da izmeni način distribucije u slučaju da staraoci/nosioci tokena zahtevaju da budu zamenjeni u njihovim rolama.

6.2.3 Bezbedno čuvanje privatnog ključa

PKS CA koristi bezbedni kriptografski uređaj da čuva svoje privatne ključeve u skladu sa zahtevima iskazanim u standardu FIPS 140-2 L3.

Procedura čuvanja privatnog ključa PKS CA zahteva višestruke kontrole od strane, na odgovarajući način autorizovanog, osoblja sa poverljivim rolama. Autorizacija procedure čuvanja ključeva i autorizacija odgovarajućeg osoblja mora biti izvršena od strane više od jednog člana upravne structure.

Hardverski i softverski mehanizmi koji štite privatne ključeve CA su dokumentovani u Posebnim internim pravilima rada.

6.2.4 Back-up privatnog ključa

PKS CA privatni ključ se backup-uje u skladu sa procedurom definisanom u internim pravilima rada PKS CA. U proceduri backup-a, koriste se procedure backup-a ključa koje su podržane od strane datog HSM uređaja.

Kopije privatnog ključa PKS CA se čuvaju na eksternoj memoriji (flash memorija, CD,…) na sigurnom mestu u šifrovanom obliku.

6.2.5 Arhiviranje privatnog ključa

Backup-ovan privatni ključ PKS CA se arhivira prema proceduri opisanoj u internim pravilima rada PKS CA.

6.2.6 Transfer privatnog ključa na hardverski kriptografski modul

Procedura bezbednog eksportovanja privatnog ključa PKS CA u cilju backup- a, kao i procedura bezbednog importa arhiviranog privatnog ključa na HSM su opisane u posebnim internim pravilima rada PKS CA:

6.2.7 Čuvanje privatnog ključa na hardverskom kriptografskom modulu

Kada se privatni ključ PKS CA nalazi i koristi na HSM uređaju, on se čuva u šifrovanom obliku u memoriji HSM uređaja.

6.2.8 Metoda aktivacije privatnog ključa

Nosioci deljenih tajni (staraoci) PKS CA imaju zadatak da aktiviraju i deaktiviraju privatni ključ. Privatni ključ je tada aktivan u definisanom periodu vremena.

Svakom korišćenju privatnog ključa PKS CA prethodi unošenje tajnog podatka od strane operatera.

6.2.9 Metoda deaktiviranja privatnog ključa

Nosioci deljenih tajni (staraoci) PKS CA imaju zadatak da aktiviraju i deaktiviraju privatni ključ. Privatni ključ je tada aktivan u definisanom periodu vremena.

6.2.10 Metoda uništenja privatnog ključa

Privatni ključ PKS CA se ne obnavlja.

Privatni ključ PKS CA će biti uništen na kraju svog životnog ciklusa.

PKS CA privatni ključevi se uništavaju na kraju njihovog životnog veka u cilju garancije da oni neće nikada biti ponovo aktivirani i korišćeni.

Nakon generisanja novog asimetričnog para ključeva i novog sertifikata PKS CA, prethodni privatni ključ se briše iz HSM-a, a backup kopije se čuvaju na CD medijumu se fizički uništavaju na odgovarajućem uređaju.

Pri tome se kreira odgovarajući zapisnik koji se arhivira.

6.2.11 Rangiranje kriptografskih hardverskih modula

Ovo poglavlje nije primenljivo u okviru ovih CPS.

6.3 Drugi aspekti upravljanja parom ključeva

6.3.1 Arhiviranje javnog ključa

PKS CA arhivira svoj sopstveni javni ključ.

6.3.2 Periodi validnosti sertifikata i privatnog ključa

PKS CA izdaje korisničke sertifikate za periodom korišćenja kao što je naznačeno u samim sertifikatima.

Vreme validnosti privatnog ključa PKS Root CA je 10 godina, dok je sam PKS Root CA sertifikat validan 20 godina.

Vreme validnosti privatnog ključa PKS Intermediate CA je 5 godina – dok je sam PKS Intermediate CA sertifikat validan 10 godina.

6.4 Aktivacioni podaci

6.4.1 Generisanje i instalacija aktivacionih podataka

PKS CA bezbedno procesira aktivacione podatke pridružene privatnim ključevima CA, kao i svim drugim privatnim ključevima u datom PKI sistemu (intermediate CA, RA, korisnici).

6.4.2 Drugi aspekti u vezi aktivacionih podataka

Ovo poglavlje nije primenljivo u okviru ovih CPS.

6.5 Bezbednosne kontrole računara

6.5.1 Specifični zahtevi za bezbednost računara

PKS CA implementira specifične bezbednosne kontrole nad računarima koji se koriste u okviru datog PKI Sistema.

Računari koji se koriste u okviru PKS CA čuvaju se unutar specijalne prostorije koja je fizički obezbeđena. Pristup preko računarske mreže se štiti pomoću specijalnih aplikativnih firewall uređaja - kripto komunikacionih servera. Neautorizovan pristup računarima PKS CA nije dozvoljen. PKS CA sistem mogu startovati samo dve ili više ovlašćenih osoba.

6.5.2 Rangiranje bezbednosti računara

Ovo poglavlje nije primenljivo u okviru ovih CPS.

6.6 Mrežne bezbednosne kontrole

PKS CA održava i primenjuje visok nivo sistema mrežne bezbednosti, uključujući primenu firewall uređaja i intrusion detection/prevention sistema.

6.7 Vremenski pečat

Ovo poglavlje nije primenljivo u okviru ovih CPS.

7. Profili sertifikata i CRL lista

Ovo poglavlje specificira formate sertifikata i CRL lista koje izdaje PKS CA.

7.1 Profili sertifikata

PKS CA izdaje sledeće vrste sertifikata:

- Root CA
- Intermediate CA;
- Kvalifikovane sertifikate za:
- Ovlašćena fizička lica u okviru pravnih lica,
- Zaposlene u PKS i u regionalnim privrednim komorama
- Fizička lica

PKS CA publikuje u okviru ovog CPS dokumenta profile sertifikata koje koristi za sve tipove sertifikata koje izdaje.

7.1.1 Broj verzije

PKS CA izdaje sertifikate u formatu X.509v3 tako da su svi sertifikati verzije 3.

7.1.2 Objektni identifikatori algoritama

PKS CA u sertifikatima koje izdaje koristi kombinaciju algoritama:

- SHA512RSA sa OID-om: 1.3.6.1.4.1. 31266.10.142.1.0

Međutim, PKS CA PKI sistem podržava implementaciju bilo kojih kombinacija hash i asimetričnog kriptografskog algoritma.

7.1.3 Forme imena

Za potrebe profila kvalifikovanog sertifikata ovlašćenog korisnika u okviru date organizacije – pravnog lica eksternog korisnika PKS (na primer korisnika – ovlašćeno lice u okviru pravnog lica), obavezno je uneti sledeće podatke:

- Ime i prezime ovlašćenog fizičkog lica za dato pravno lice
- Naziv i matični broj organizacije u kojoj radi fizičko lice
- JMBG ovlašćenog korisnika – fizičkog lica (Legal ID), osim ako posebnim propisima nije drugačije određeno.

7.1.4 Ograničenja imena

Ograničenja koja se odnose na imena korisnika u kvalifikovanim elektronskim sertifikatima proističu iz odgovarajućeg i važećeg podzakonskog akta Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja. U nastavku su navedena pomenuta ograničenja.

- Polje „subject" kvalifikovanog elektronskog sertifikata mora da ima atribut „CommonName".
- Atribut „CommonName" treba da je upisano puno ime i prezime potpisnika i jedinstveni identifikator potpisnika unutar sertifikacionog tela. Po pravilniku o uslovima koje moraju da ispunjavaju kvaklifikovani elektronski sertifikati: Atribut „CommonName" ne sme da se završava sa 13 ili više uzastopnih numeričkih karaktera, niti da se završsva crticom iza koje slede dva slovna karaktera i niz numeričkih. Za atribut „commonName" treba koristiti UTF8String kodiranje, tako da sva slova iz imena i prezimena budu verno predstavljena odgovarajućim karakterima.
- Sertifikaciono telo je dužno da korisniku jasno stavi do znanja da li će sertifikat sadržati JMBG.
- Sertifikati koji se koriste u opštenju organa, opštenju organa i stranaka, dostavljanju i izradi odluke organa u elektronskom obliku u upravnom, sudskom i drugom postupku pred državnim organom, treba da sadrže JMBG. Sertifikate koji sadrže JMBG ili lični broj sertifikaciono telo ne sme učiniti javno dostupnim.

- Izuzeto od stava 2 ovog člana sertifikati koji ne sadrže JMBG mogu se koristiti za potpisivanje Statisičkih izveštaja u skladu sa članom 35 stav 6 Zakona o računovodstvu ("Službeni glasnikRS", broj 62/13) i potpisivanje finansijskih izveštaja i ratećih izjava u skladu sa članom 33 stav 6 tog zakona, ukoliko je potpisnik stranac u smislu Zakona o strancima ("Službeni glasnik RS", broj 97/08).

7.1.5 Objektni identifikator politike sertifikacije

U ovom poglavlju je definisana OID struktura za potrebe Politika sertifikacije i CPS-a koja se koristi pri izdavanju sertifikata u okviru PKI sistema PKS.

Format strukture OID-a je sledeći: 1.3.6.1.4.1. 31266.10.142.1.0

Broj 1.3.6.1.4.1 predstavlja opšti prefiks za private-enterprize broj sa sajta:

http://www.iana.org/assignments/smi-numbers,

31266 je Private Enterprize Number (PEN) dodeljen Privrednoj Komori Srbije. Slova iza PEN-a imaju sledeća predložena značenja:

a. Tip dokumenta

- Certificate Policy
- CPS
- neki drugi tip dokumenta

b. Tip sertifikata

- Kvalifikovani ITU-T X.509 elektronski sertifikati

c. Verzija dokumenta

- Oznaka verzije dokumenta

7.1.6 Korišćenje „Policy Constraints" ekstenzije

Ovo poglavlje nije primenljivo u okviru ovih CPS.

7.1.7 Sintaksa i semantika „Policy Qualifier"-sa

Ovo poglavlje nije primenljivo u okviru ovih CPS.

7.1.8 Semantika procesiranja kritične ekstenzije „Certificate Policies“

U sertifikatima izdatim od strane PKS CA, neophodno je da ekstenzija „Certificate Policies“ ima sledeće vrednosti:

- Odgovarajući OID politike sertifikacije po kojoj se izdaje dati sertifikat
- Internet lokaciju (URL) na kojoj se nalazi ovaj CPS dokument radi preuzimanja.

7.2 Profil CRL liste

U skladu sa IETF PKIX RFC 2459, PKS CA podržava izdavanje CRL lista koje su u saglasnosti sa sledećim uslovima:

- Brojevi verzija su podržani za CRL liste,
- CRL i CRL ekstenzije su popunjene i njihova kritičnost je posebno naznačena

Profil PKS CA CRL (Certificate Revocation List) liste je prikazan u sledećoj tabeli:

<table>
<tr><td>Version</td><td colspan="3">[Version 2]</td></tr>
<tr><td>Issuer Name</td><td colspan="3">CN=PKS CA Class1 – Kvalifikovani sertifikati
OU=PKS CA
O=Privredna komora Srbije
C=RS</td></tr>
<tr><td>This Update</td><td colspan="3">[Date of Issuance]</td></tr>
<tr><td>Next Update</td><td colspan="3">[Date of Issuance + 24 hours]</td></tr>
<tr><td>Signature Algorithm identifier</td><td colspan="3">Sha512RSA</td></tr>
<tr><td>Authority Key identifier</td><td colspan="3"></td></tr>
<tr><td>CRL Number</td><td colspan="3">Redni broj CRL liste</td></tr>
<tr><td rowspan="3">Revoked sertificates</td><td colspan="3">CRL Entries</td></tr>
<tr><td>Sertificate Serial Number</td><td>Date and Time of Revocation</td><td>CRL Reason Code</td></tr>
<tr><td>[Sertificate Serial Number]</td><td>[Date and Time of Revocation]</td><td>[CRL Reason Code]</td></tr>
</table>

7.2.1 Broj verzije

PKS CA generiše i objavljuje CRL liste verzije 2 (X.509v2).

7.2.2 CRL i CRL entry ekstenzije

CRL lista koja se izdaje od strane PKS CA ima sledeće ekstenzije:

- AKI (Authority Key Identifier)
- CRL Number – redni broj CRL liste

CRL entry ekstenzije su:

- Serijski broj opozvanog sertifikata
- Datum i vreme opoziva
- Kod razloga opoziva

7.3 OCSP profil

Ovo poglavlje nije primenljivo u okviru ovih CPS.

7.3.1 Broj verzije

Ovo poglavlje nije primenljivo u okviru ovih CPS.

7.3.2 OCSP ekstenzije

Ovo poglavlje nije primenljivo u okviru ovih CPS.

8. Provera saglasnosti i druga ocenjivanja

8.1 Frekvencija ili uslovi ocenjivanja

PKS CA prihvata periodičnu audit/proveru saglasnosti svojih politika sertifikacije, uključujući ovaj CPS dokument, što uključuje i periodičnu superviziju od strane Nadležnog organa za poslove akreditacije i supervizije PKI sistema u Republici Srbiji.

Rad PKSCA ke takođe u saglasnosti sa najvažnijim međunarodnim i Evropskim standardima u ovoj okbasti, kao i sa Evropskom uredbom (EU) br. 910/2014 Evropskog parlamenta i veća od 23.07.2014.godine.

U domenu izdavanja kvalifikovanih elektronskih serifikata, PKS CA radi u okviru ograničenja definisanim u okviru Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, kao i odgovarajućim podzakonskim aktima.

PKS CA prihvata pod određenim uslovima i proveru/auditing internih procedura i pravila rada koja nisu javno dostupna. PKS CA evaluira rezultate ovakvih provera pre nego što ih implementira.

8.2 Identitet/kvalifikacije procenjivača

Akreditaciju i superviziju rada PKS CA vrši nadležna komisija formirana od strane nadležnog organa za poslove akreditacije i supervizije Republike Srbije.

PKS CA sprovodi takođe redovne interne audit-e usklađenosti poslovanja sa CP, kao i sa ovim CPS dokumentom. Interni audit sprovode odgovarajući zaposleni PKS sa datim zaduženjima.

Nakon akreditacije PKS CA za izdavanje kvalifikovanih elektronskih sertifikata u Srbiji, Nadležni organ za poslove akreditacije i supervizije PKI sistema (Ministarstvo trgovine, turizma i telekomunikacija) vrši obaveznu superviziju PKS CA redovno, i to barem jednom godišnje.

8.3 Odnos ocenjivača prema ocenjivanom entitetu

Ovo poglavlje nije primenljivo u okviru ovih CPS

8.4 Teme pokrivene u procesu ocenjivanja

U procesu ocenjivanja rada PKS CA, bilo eksternog od strane Nadležnog organa ili internog od strane internih auditora, vrši se provera saglasnosti operativnog rada PKS CA sa politkama sertifikacije (CP) i ovim praktičnim pravilima rada (CPS), kao i sa internim pravilima rada.

8.5 Aktivnosti preduzete kao rezultat utvrđenih nedostataka

PKS CA treba da uskladi svoj operativni rad u skladu sa eventualnim nalazima eksternog ili internog auditinga.

8.6 Komunikacija rezultata

Rezultati eksternog ili internog auditing-a su raspoloživi svim korisnicima i trećim strana i javno se publikuju na veb sajtu PKS CA.

9. Drugi poslovni i pravni aspekti

9.1 Cene

9.1.1 Cene izdavanja ili obnove sertifikata

Objavljivanje cena sertifikata i drugih sertifikacionih usluga se vrši putem web sajta PKS CA, partnera PKS CA (treća lica) ili putem odgovarajućeg ugovora tamo gde je to primenljivo.

9.1.2 Cena pristupa sertifikatima

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.1.3 Cena pristupa informacijama o statusu sertifikata

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.1.4 Cene za druge servise

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.1.5 Politika povraćaja novca

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.2 Finansijska odgovornost

9.2.1 Pokrivanje osiguranja

PKS CA obezbeđuje osiguranje za pokrivanje svih odgovornosti opisanih u CP i ovim CPS i to iskazuje u okviru svog ograničenog garancijskog plana koji predstavlja deo CPS.

Sertifikaciono telo PKS CA poseduje odgovarajuće osiguranje za bilo koju štetu koju mogu da pretrpe treća lica a za koju je odgovorno sertifikaciono telo.

Sertifikaciono telo PKS CA garantuje za vrednost pojedinačnog pravnog posla vezanog za kvalifikovani elektronski sertifikat pravnog lica u visini polise osiguranja koje je u skladu sa zakonom.

PKS CA ne prihvata nikakvu drugu odgovornost koja izlazi iz pokrivanja definisanog pomenutim ograničenim garancijskim planom

9.2.2 Druga dobra

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.2.3 Osiguranje ili garancijsko pokrivanje za krajnje korisnike

Korisnik je dužan da obešteti PKS CA u odnosu na bilo koje aktivnosti ili propuste u odgovornosti, bilo koje gubitke ili štetu, kao i za bilo kakve troškove bilo koje vrste, uključujući razumne naknade advokata, koje bi PKS CA mogao da ima kao rezultat:

- Bilo kog lažnog ili pogrešno prezentovanog podatka dostavljenog od strane korisnika ili njihovih agenata.
- Bilo kog propusta korisnika da dostavi materijalnu činjenicu da je pogrešna prezentacija ili propust učinjen iz nemarnosti ili sa namerom da se prevari PKS CA, ili bilo koje lice koje prima i odnosi se prema dobijenom sertifikatu.
- Neobezbeđivanja odgovarajuće zaštite korisnikovog privatnog ključa, nekorišćenja bezbednog sistema kako je zahtevano, ili neizvršenja odgovarajućih preventivnih mera neophodnih da se spreči kompromitacija, gubitak, objavljivanje, modifikacija ili neautorizovano korišćenje korisnikovog privatnog ključa, ili napada na integritet PKS CA Root privatnog ključa.
- Kršenja bilo kojih zakona koji su primenljivi, uključujući one koji se odnose na zaštitu intelektualnih prava, viruse, pristup računarskim sistemima, itd.

9.3 Poverljivost poslovnih informacija

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.3.1 Opseg poverljivih informacija

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.3.2 Informacije koje nisu u opsegu poverljivih informacija

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.3.3 Odgovornost za zaštitu poverljivih informacija

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.4 Privatnost i zaštita personalnih informacija

9.4.1 Plan privatnosti

PKS CA se pridržava pravila zaštite privatnosti personalnih podataka i pravila poverljivosti kako je propisano u ovom CPS dokumentu, kao i u odgovarajućim zakonskim dokumentima.

9.4.2 Informacije koje se tretiraju kao privatne

PKS CA tretira privatnim sve informacije koje se odnose na korisnike sertifikata.

9.4.3 Informacije koje se ne smatraju privatnim

PKS CA ne smatra privatnim samo one informacije korisnika za koje je sam korisnik dao saglasnost da se mogu publikovati. Najčešće se to odnosi samo na podatke koji se sadrže u izdatim elektronskim sertifikatima.

9.4.4 Odgovornost za zaštitu privatnih informacija

PKS CA je odogovorno za zaštitu privatnosti korisnikovih informacija.

9.4.5 Obaveštenje i saglasnost za korišćenje privatnih informacija

PKS CA definiše uslove u vezi objavljivanja privatnih informacija za koje dati korisnik treba da da saglasnost i ti su uslovi objavljeni u ugovoru koji se potpisuje sa korisnikom.

9.4.6 Otkrivanje informacija shodno pravnim i administrativnim procesima

PKS CA ne objavljuje, niti se zahteva da objavljuje, bilo koju poverljivu informaciju bez autentikovanog i potvrđenog zahteva od strane:

- Same strane za koju se takva informacija i čuva,
- Odgovarajućeg suda.

PKS CA može naplatiti odgovarajuću administrativnu cenu za procesiranje ovakvih objavljivanja.

Strane u komunikaciji koje zahtevaju i dobijaju poverljive informacije imaju dozvolu za to na osnovu pretpostavke da će oni te informacije koristiti za zahtevane svrhe, da će ih osigurati od kompromitacije, i da će se uzdržavati od njihovog korišćenja i objavljivanja trećim stranama.

9.4.7 Druge okolnosti za otkrivanje informacija

PKS CA i njegovi partneri mogu učiniti raspoloživom specifičnu politiku privatnosti u cilju zaštite personalnih podataka aplikanta koji zahteva izdavanje sertifikata od strane PKS CA ili njegovog partnera putem njihovih web sajtova i/ili CP ili CPS dokumenata.

9.5 Prava intelektualnog vlasništva

PKS CA poseduje i zadržava sva prava intelektualnog vlasništva pridružena njegovim bazama podataka, veb sajtovima, elektronskim sertifikatima koje izdaje, kao i bilo kojim drugim publikacijama koje na bilo koji način pripadaju ili potiču od strane PKS CA, uključujući CP i ove CPS.

9.6 Predstavljanje i garancije

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.6.1 CA predstavljanje i garancije

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.6.2 RA predstavljanje i garancije

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.6.3 Korisničko predstavljanje i garancije

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.6.4 Predstavljanje i garancije trećih strana

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.6.5 Predstavljanje i garancije drugih učesnika

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.7 Nepriznavanje garancije

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.8 Ograničenja odgovornosti

PKS CA ne prihvata bilo kakvu drugu odgovornost osim one koja je eksplicitno definisana u CP i u ovom CPS dokumentu.

Ni u kom slučaju (izuzev zloupotrebe ili namere) PKS CA nije odgovorno za:

- Bilo kakav gubitak profita.
- Bilo kakav gubitak podataka.
- Bilo koju indirektnu ili slučajnu štetu koja je prouzrokovana ili je vezana za korišćenje, isporuku, licencu, performanse sertifikata ili elektronskih potpisa.
- Bilo koju transakciju ili uslugu ponuđenu ili u okviru obuhvata ovih CPS.
- Bilo koju drugu štetu izuzev onih koje potiču od opravdanog oslanjanja na verifikovane informacije koje se nalaze u izdatom sertifikatu.
- Bilo koju odgovornost koja se pojavila u slučaju greške u verifikovanim informacijama koja je rezultat greške, zloupotrebe ili namere aplikanta.

9.9 Odštete

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.10 Period važnosti i kraj validnosti ovih CPS

Sertifikaciono telo PKS CA zadržava pravo da izmeni politiku sertifikacije (CP) i ova praktična pravila rada (CPS), kao i da nadogradi infrastrukturu bez prethodnog obaveštavanja vlasnika kvalifikovanog elektronskog sertifikata.

Važeći sertifikati tako ostaju važeći do isteka njihove validnosti i za njih još uvek važi onaj CPS dokument koji je važio u vreme njihovog izdavanja. Za sve sertifikate izdate nakon početka validnosti novog CPS dokumenta, važi novi.

Ovaj CPS dokument stupa na snagu onoga dana kada je odobren i objavljen od strane sertifikacionog tela PKS CA.

9.10.1 Važnost

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.10.2 Kraj validnosti

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.10.3 Efekat završetka i ponovnog rada

Prilikom objavljivanja novog CPS, svi kvalifikovani elektronski sertifikati izdati nakon tog datuma procesiraju se prema novom CPS dokumentu.

Novi CPS dokument ne utiče na validnost kvalifikovanih elektronskih sertifikata koji su bili izdati prema prethodnim CPS dokumentima. Takvi kvalifikovani elektronski sertifikati ostaju važeći do isteka validnosti, pri čemu se, gde god je to moguće, procesiraju i-ili tretiraju prema novom CPS dokumentu.

9.11 Pojedinačna obaveštenja i komunikacija sa učesnicima

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.12 Ispravke

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.12.1 Procedure za ispravku

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.12.2 Mehanizam i period obaveštavanja

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.12.3 Uslovi promene objektnog identifikatora (OID)

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.13 Procedure rešavanja sporova

PKS CA se referiše na arbitražu u cilju rešavanja svih sporova koji se odnose na CP i ove CPS. Ako se spor ne reši u okviru deset (10) dana nakon inicijalnog obaveštenja shodno pravilima CP i ove CPS, strane u sporu dostavljaju spor na arbitražu. Arbitraža se sastoji od 3 arbitra, svaka strana predlaže po jednog, dok trećeg predlažu zajedno obe strane u sporu. Mesto za arbitražu je Beograd, Srbija, a arbitri određuju sve troškove arbitraže.

Za sve sporove koji se odnose na tehnologiju, kao i sporove koji se odnose na same CP i CPS dokumente, strane u sporu prihvataju arbitražno telo koje će biti izabrano od strane vlade Srbije.

9.14 Zakon koji se poštuje

Ovaj CPS dokument je izdata u potpunosti u skladu sa odgovarajućom zakonskom regulativom države Srbije, i to pre svega sa Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima. Sve pravne stvari koje se odnose na PKS CA i/ili koji se odnose na sertifikate izdate od strane PKS CA će biti procesuirane od strane odgovarajućeg suda u Srbiji.

9.15 Saglasnost sa primenljivim zakonima

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.16 Razne odredbe

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.16.1 Kompletan ugovor

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.16.2 Dodeljivanje

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.16.3 Ozbiljnost

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.16.4 Sprovođenje pravnog postupka

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.16.5 Viša sila

Ovo poglavlje nije primenljivo u okviru ovih CPS.

9.17 Druge odredbe

Ovo poglavlje nije primenljivo u okviru ovih CPS

10. Istorija dokumenta

Verzija	Datum	Opis	Autor
3.0	22.10.2018.	Radna verzija	Tanja Grujović
3.0	23.10.2018	Radna verzija	Dušan Berdić

PRIVREDNA KOMORA SRBIJE

Direktor Direktorata za

informacione tehnologije

Nebojša Garić

02.01-Broj:
22. oktobar 2018 godine
B e o g r a d