**Praktična pravila rada**

**za pružanje usluge kvalifikovanog vremenskog žiga**

CPS (Certificate Practice Statement)

 OID CPS dokumenta (1.3.6.1.4.1.31266.10.1.3)

 - verzija 2.1.-

 Januar, 2020.

Sadržaj

[1. Uvod i pregled osnovnih pretpostavki 8](#_Toc30252141)

[1.1. Pregled osnovnih pretpostavki 8](#_Toc30252142)

[1.2. Ime dokumenta i identifikacija 10](#_Toc30252143)

[1.3. Korisnici usluga PKSCA QTSA 10](#_Toc30252144)

[1.3.1. Pružalac usluga izdavanja kvalifikovanih elektronskih vremenskih žigova 10](#_Toc30252145)

[1.3.2. Korisnici 11](#_Toc30252146)

[1.3.3. Registraciona tela 11](#_Toc30252147)

[1.3.4. Treće strane 12](#_Toc30252148)

[1.4. Upotreba vremenskih žigova 12](#_Toc30252149)

[1.4.2. Zabrane upotrebe vremenskih žigova 12](#_Toc30252150)

[1.5. Administracija Praktičnih pravila rada PKS CA 12](#_Toc30252151)

[1.5.1. Organizacija odgovorna za održavanje dokumenta Praktična pravila 12](#_Toc30252152)

[1.5.2. Kontakt osoba 12](#_Toc30252153)

[1.4.3 Osoba koja određuje pogodnost CPS dokumenta 13](#_Toc30252154)

[1.4.4 Procedura odobravanja CPS dokumenta 13](#_Toc30252155)

[2. OBJAVE I ODGOVORNOSTI ZA REPOZITORIUM 13](#_Toc30252156)

[2.1. Identifikacija tela koje vodi repozitorium 13](#_Toc30252157)

[2.2. Objava informacija o izdavanju vremenskih žigova 14](#_Toc30252158)

[2.3. Vreme ili učestalost objavljivanja 14](#_Toc30252159)

[2.4. Kontrole pristupa repozitoriumu 14](#_Toc30252160)

[3. IDENTIFIKACIJA KORISNIKA I IZDAVANJE ELEKTRONSKIH VREMENSKIH ŽIGOVA 15](#_Toc30252161)

[3.1. Identifikacija Korisnika 15](#_Toc30252162)

[3.1.1. Inicijalno utvrđivanje identiteta Korisnika 15](#_Toc30252163)

[3.1.2. Način dostave zahteva 15](#_Toc30252164)

[3.1.3. Sklapanje ugovora 15](#_Toc30252165)

[3.2. Identifikacija i autentikacija na PKSCA QTSA servis 16](#_Toc30252166)

[3.3. Sertifikat modula za izradu vremenskog žiga 16](#_Toc30252167)

[3.4. Elektronski vremenski žig 16](#_Toc30252168)

[3.4.1. Zahtev za izdavanje vremenskog žiga (*Time-Stamp Request*) 17](#_Toc30252169)

[3.4.2. Odgovor servisa za izdavanje elektronskih vremenskih žigova (*Time-Stamp Response*) 17](#_Toc30252170)

[3.5. Profil vremenskog žiga 17](#_Toc30252171)

[3.6. Tačnost vremena u izdatim elektronskim vremenskim žigovima 18](#_Toc30252172)

[3.7. Sinhronizacija sata sa UTC 18](#_Toc30252173)

[3.7.1. Letnje računanje vremena 18](#_Toc30252174)

[3.8. Provera validnosti vremenskog žiga 18](#_Toc30252175)

[3.9. Raspoloživost usluge 19](#_Toc30252176)

[3.10. Izdavanje nekvalifikovanih elektronskih vremenskih žigova 19](#_Toc30252177)

[3.11. Transportni protokol za uslugu izdavanja elektronskih vremenskih žigova 19](#_Toc30252178)

[4. OPERATIVNI ZAHTEVI ZA ŽIVOTNI CIKLUS SERTIFIKATA ZA PKSCA QTSA 20](#_Toc30252179)

[4.1. Izdavanje sertifikata 20](#_Toc30252180)

[4.2. Opoziv i suspenzija sertifikata 20](#_Toc30252181)

[4.2.1. Razlozi za opoziv 20](#_Toc30252182)

[4.2.2. Ko može tražiti opoziv 20](#_Toc30252183)

[4.2.3. Učestalost izdavanja CRL 20](#_Toc30252184)

[4.2.4. Maksimalno kašnjenje za CRL 20](#_Toc30252185)

[4.2.5. Zahtevi na *online* proveru statusa opozvanosti sertifikata 21](#_Toc30252186)

[4.2.6. Drugi dostupni načini objave opozvanih sertifikata 21](#_Toc30252187)

[5. PROVERA SISTEMA, UPRAVLJANJA I RADNIH POSTUPAKA 22](#_Toc30252188)

[5.1. Mere fizičke zaštite 22](#_Toc30252189)

[5.1.1. Lokacija objekta i konstrukcija 22](#_Toc30252190)

[5.1.2. Fizički pristup 22](#_Toc30252191)

[5.1.3. Sistemi za napajanje i klimatizaciju 40](#_Toc30252192)

[5.1.4. Opasnost od poplave 40](#_Toc30252193)

[5.1.5. Protivpožarna zaštita 40](#_Toc30252194)

[5.1.6. Čuvanje medija 40](#_Toc30252195)

[5.1.7. Zbrinjavanje otpada 40](#_Toc30252196)

[5.2. Organizacione mere zaštite 41](#_Toc30252197)

[5.2.1. Poverljive uloge 41](#_Toc30252198)

[5.2.2. Broj osoba potrebnih za obavljanje aktivnosti 41](#_Toc30252199)

[5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu 41](#_Toc30252200)

[5.2.4. Uloge koje zahtevaju odvajanje (separaciju) dužnosti 42](#_Toc30252201)

[5.3. Provere nivoa znanja osoblja 42](#_Toc30252202)

[5.3.1. Kvalifikacije, radno iskustvo i zahtevi za proverom nivoa znanja osoblja 42](#_Toc30252203)

[5.3.2. Procedure provere prikladnosti osoblja 42](#_Toc30252204)

[5.3.3. Zahtevi za školovanjem 42](#_Toc30252205)

[5.3.4. Učestalost i uslovi za obnovu znanja 42](#_Toc30252206)

[5.3.5. Kazne za neovlašćene radnje 43](#_Toc30252207)

[5.3.6. Zahtevi na spoljne saradnike 43](#_Toc30252208)

[5.3.7. Dokumentacija koja je dostupna zaposlenima 43](#_Toc30252209)

[5.4. Postupci upravljanja revizionim zapisima 43](#_Toc30252210)

[5.4.1. Tipovi događaja koji se zapisuju 43](#_Toc30252211)

[5.4.2. Učestalost obrade revizionih zapisa 44](#_Toc30252212)

[5.4.3. Vremenski period čuvanja revizionih zapisa 44](#_Toc30252213)

[5.4.4. Zaštita revizionih zapisa 44](#_Toc30252214)

[5.4.5. Sistem prikupljanja revizionih zapisa (unutrašnji ili spoljni) 44](#_Toc30252215)

[5.4.6. Obaveštavanje subjekta uzročnika događaja 44](#_Toc30252216)

[5.4.7. Procena rizika 45](#_Toc30252217)

[5.5. Arhiviranje zapisa 45](#_Toc30252218)

[5.5.1. Tipovi arhiviranih zapisa 45](#_Toc30252219)

[5.5.2. Vremenski period arhiviranja 45](#_Toc30252220)

[5.5.3. Zaštita arhive 45](#_Toc30252221)

[5.5.4. Postupci izrade sigurnosnih kopija arhive 46](#_Toc30252222)

[5.5.5. Sistem prikupljanja arhivskih zapisa (unutrašnji ili spoljni) 46](#_Toc30252223)

[5.5.6. Postupci dobijanja i provere arhiviranih zapisa 46](#_Toc30252224)

[5.6. Promena TSU ključa 46](#_Toc30252225)

[5.7. Oporavak od kompromitacije ili nepogode 47](#_Toc30252226)

[5.7.1. Postupci u slučaju incidenta ili kompromitacije 47](#_Toc30252227)

[5.7.2. Postupci u slučaju oštećenja u računarskim resursima, programima i/ili podacima 47](#_Toc30252228)

[5.7.3. Postupci u slučaju kompromitovanja privatnog ključa ili ispada iz sinhronizacije sa UTC vremenom 47](#_Toc30252229)

[5.7.4. Mogućnost nastavka poslovanja nakon nepogode 48](#_Toc30252230)

[5.8. Prestanak rada PKSCA QTSA servisa 48](#_Toc30252231)

[6. TEHNIČKE MERE ZAŠTITE 49](#_Toc30252232)

[6.1. Generisanje i instalacija para ključeva 49](#_Toc30252233)

[6.1.1. Generisanje para TSU ključeva 49](#_Toc30252234)

[6.1.2. Dostava javnog TSU ključa korisnicima i trećim stranama 49](#_Toc30252235)

[6.1.3. Dužina kriptografskih ključeva 49](#_Toc30252236)

[6.1.4. Generisanje i provera kvalitete parametara javnog ključa 50](#_Toc30252237)

[6.1.5. Namene ključeva 50](#_Toc30252238)

[6.2. Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom 50](#_Toc30252239)

[6.2.1. Standardi i tehničke mere zaštite kriptografskog modula 50](#_Toc30252240)

[6.2.2. Upravljanje privatnim TSU ključem od strane više osoba (n od m) 50](#_Toc30252241)

[6.2.3. Sigurno skladištenje privatnog ključa 50](#_Toc30252242)

[6.2.4. Sigurnosno kopiranje privatnog ključa 50](#_Toc30252243)

[6.2.5. Arhiviranje privatnog ključa 51](#_Toc30252244)

[6.2.6. Prenos privatnog ključa 51](#_Toc30252245)

[6.2.7. Čuvanje privatnog ključa u kriptografskom modulu 51](#_Toc30252246)

[6.2.8. Metoda aktivacije privatnog TSU ključa 51](#_Toc30252247)

[6.2.9. Metoda deaktivacije privatnog TSU ključa 51](#_Toc30252248)

[6.2.10. Metoda uništavanja privatnog TSU ključa 52](#_Toc30252249)

[6.2.11. Ocena kriptografskog modula 52](#_Toc30252250)

[6.3. Ostali vidovi upravljanja parom ključeva 52](#_Toc30252251)

[6.3.1. Arhiviranje javnog ključa 52](#_Toc30252252)

[6.3.2. Vremenski period važenja PKSCA QTSA sertifikata i korišćenja para TSU ključeva 52](#_Toc30252253)

[6.3.3. Upravljanje životnim ciklusom kriptografskih modula 53](#_Toc30252254)

[6.4. Aktivacioni podaci 53](#_Toc30252255)

[6.4.1. Generisanje i instalacija aktivacionih podataka 53](#_Toc30252256)

[6.4.2. Zaštita aktivacionih podataka 53](#_Toc30252257)

[6.5. Upravljanje informacionom bezbednošću 54](#_Toc30252258)

[6.5.1. Posebni tehnički zahtevi na informacionu bezbednost 54](#_Toc30252259)

[6.6. Tehničke kontrole životnog ciklusa 54](#_Toc30252260)

[6.6.1. Kontrole daljeg razvoja sistema 54](#_Toc30252261)

[6.6.2. Kontrole upravljanja bezbednošću 55](#_Toc30252262)

[6.6.3. Sigurnosne kontrole životnog ciklusa 55](#_Toc30252263)

[6.7. Provera mrežne bezbednosti 55](#_Toc30252264)

[6.8. Upotreba vremenskog žiga 55](#_Toc30252265)

[7. SADRŽAJ SERTIFIKATA, LISTA OPOZVANIH SERTIFIKATA I OCSP PROFILI 56](#_Toc30252266)

[7.1. Profil sertifikata PKSCA QTSA 56](#_Toc30252267)

[7.1.1. Broj(evi) verzije 56](#_Toc30252268)

[7.1.2. Ekstenzije sertifikata 56](#_Toc30252269)

[7.1.3. Identifikator objekta (OID) algoritama 56](#_Toc30252270)

[7.1.4. Oblici naziva 56](#_Toc30252271)

[7.1.5. Ograničenja u nazivima 57](#_Toc30252272)

[7.1.6. Identifikator objekta (OID) Praktičnih pravila TSU sertifikata 57](#_Toc30252273)

[7.1.7. Upotreba ekstenzije *Policy Constraints* 57](#_Toc30252274)

[7.1.8. Procesne semantike za kritičnu ekstenziju *Certificate Policies* 57](#_Toc30252275)

[7.2. Profil CRL 57](#_Toc30252276)

[7.2.1. Broj(evi) verzije 57](#_Toc30252277)

[7.2.2. CRL i ekstenzije unosa u CRL 57](#_Toc30252278)

[7.3. OCSP profil 58](#_Toc30252279)

[7.3.1. Broj(evi) verzije 58](#_Toc30252280)

[7.3.2. OCSP ekstenzije 58](#_Toc30252281)

[8. PROVERA USKLAĐENOSTI 59](#_Toc30252282)

[8.1. Učestalost ili okolnosti provere usklađenosti 59](#_Toc30252283)

[8.1.1. Eksterna provera usklađenosti 59](#_Toc30252284)

[8.1.2. Interna provera usklađenosti 59](#_Toc30252285)

[8.2. Identitet/kvalifikacije ocenitelja 59](#_Toc30252286)

[8.3. Odnos ocenjivača sa telom koje se ocenjuje 60](#_Toc30252287)

[9. OSTALE POSLOVNE I PRAVNE ODREDBE 60](#_Toc30252288)

[9.1. Naknada za usluge 60](#_Toc30252289)

[9.1.1. Povraćaj uplaćenih sredstava 60](#_Toc30252290)

[9.2. Finansijska odgovornost 60](#_Toc30252291)

[9.2.1. Pokrivenost osiguranjem 60](#_Toc30252292)

[9.2.2. Druga sredstva 61](#_Toc30252293)

[9.3. Poverljivost poslovnih podataka 61](#_Toc30252294)

[9.3.1. Opseg poverljivih poslovnih podataka 61](#_Toc30252295)

[9.3.2. Podaci koji se ne smatraju poverljivim poslovnim podacima 61](#_Toc30252296)

[9.3.3. Odgovornost za zaštitu poverljivih poslovnih podataka 61](#_Toc30252297)

[9.4. Zaštita ličnih podataka 61](#_Toc30252298)

[9.4.1. Plan zaštite ličnih podataka 62](#_Toc30252299)

[9.4.2. Poverljivi lični podaci 62](#_Toc30252300)

[9.4.3. Lični podaci koji nisu poverljivi 62](#_Toc30252301)

[9.4.4. Odgovornost za zaštitu ličnih podataka 62](#_Toc30252302)

[9.4.5. Ovlašćenje za korišćenje ličnih podataka 62](#_Toc30252303)

[9.4.6. Dostupnost podataka merodavnim telima 63](#_Toc30252304)

[9.4.7. Ostale okolnosti objave podataka 63](#_Toc30252305)

[9.5. Prava intelektualnog vlasništva 63](#_Toc30252306)

[9.6. Obaveze učesnika 63](#_Toc30252307)

[9.6.1. Obaveze PKSCA 63](#_Toc30252308)

[9.6.2. Obaveze RA 64](#_Toc30252309)

[9.6.3. Obaveze Korisnika 64](#_Toc30252310)

[9.6.4. Obaveze trećih strana 65](#_Toc30252311)

[9.7. Odgovornosti učesnika 65](#_Toc30252312)

[9.7.1. Odgovornosti PKSCA 65](#_Toc30252313)

[9.7.2. Odgovornosti Korisnika 66](#_Toc30252314)

[9.7.3. Odgovornosti trećih strana 66](#_Toc30252315)

[9.8. Odricanje od odgovornosti 67](#_Toc30252316)

[9.9. Ograničenja odgovornosti 67](#_Toc30252317)

[9.10. Naknada štete 67](#_Toc30252318)

[9.11. Trajanje i prestanak važenja 67](#_Toc30252319)

[9.11.1. Trajanje 67](#_Toc30252320)

[9.11.2. Prestanak važenja 68](#_Toc30252321)

[9.11.3. Posledice prestanka važenja i nastavak delovanja 68](#_Toc30252322)

[9.12. Individualna obaveštenja i komunikacija sa učesnicima 68](#_Toc30252323)

[9.13. Izmene i dopune 68](#_Toc30252324)

[9.13.1. Procedure izmena i dopuna 68](#_Toc30252325)

[9.13.2. Mehanizmi obaveštavanja i vremenski periodi 69](#_Toc30252326)

[9.13.3. Okolnosti pod kojima se mora menjati OID 69](#_Toc30252327)

[9.14. Postupak rešavanja sporova 69](#_Toc30252328)

[9.15. Važeći propisi 70](#_Toc30252329)

[9.16. Usklađenost sa primenjivim propisima 70](#_Toc30252330)

[9.17. Ostale odredbe 70](#_Toc30252331)

[8.4. Predmeti ocenjivanja usklađenosti 71](#_Toc30252332)

[8.5. Mere u slučaju neusklađenosti 71](#_Toc30252333)

[8.6. Saopštavanje rezultata 71](#_Toc30252334)

[10. Istorija dokumenta 72](#_Toc30252335)

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**

**usluge izdavanja kvalifikovanog vremenskog žiga**

# Uvod i pregled osnovnih pretpostavki

Sertifikaciono telo Privredne komore Srbije (u nastavku: PKS CA) kao registrovani pružalac usluga od poverenja, vrši uslugu kvalifikovanog vremenskog žiga 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 uslugu vremenskog žiga obavlja saglasno zahtevima iz standarda ETSI TS 119 441 "Electronic Signatures and Infrastructures (ESI), Policy requirements for TSP providing signature validation services" (u daljem tekstu ETSI TS 119 441) koji se odnose na uslugu vremenskog žiga, uključujući zahteve iz drugih standarda na koje se iz tog standarda direktno i indirektno upućuje, odgovarajućim međunarodnom standardima i preporukama, odnosno drugim standardima, dokumentima i preporukama koje se odnose na pružanje usluge kvalifikovanog vremenskog žiga utvrđene Pravilnikom o validaciji kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata (Službeni glasnik RS, broj 43. od 19. juna 2019.godine.)

Usluga izdavanja kvalifikovanih elektroinskih vremenskih žigova (u daljem tekstu PKSCA QTSA) je deo PKI produkcije Sertifikacionog tela PKS, a kvalifikovani elektronski vremenski žigovi koje izdaje mogu se koristiti zajedno sa kvalifikovanim sertifikatima koje izdaje PKSCA

## Pregled osnovnih pretpostavki

PKS CA utvrđuje Praktična pravila pružanja usluge kvalifikovanog elektronskog vremenskog žiga (u daljem tekstu: Praktična pravila) u skladu sa Zakonom koja korisnicima obezbeđuju dovoljno informacija na osnovu kojih se mogu odlučiti o prihvatanju usluge i o obimu usluge.

Politika sertifikacije i Praktična pravila rada su javni dokumenti.

Praktična pravila za pružanje usluge kvalifikovanog vremenskog žiga (u daljem tekstu: praktična pravila) definišu operativne procedure u cilju ispunjenja tih zahteva, tj. način na koji pružalac usluge kvalifikovanog vremenskog žiga ispunjava tehničke, organizacione i proceduralne zahteve poslovanja koji su određeni u politici vremenskog žiga.

Politika sertifikacije je manje specifičan i detaljan dokument i definiše se nezavisno od specifičnog operativnog okruženja sertifikacionog tela u odnosu na Praktična pravila koja predstavljaju mnogo detaljniji opis načina poslovanja, kao i poslovne i operativne procedure koje sertifikaciono telo primenjuje.

PKS CA utvrđuje i posebna interna pravila rada sertifikacionog tela i zaštite sistema usluga od poverenja (u daljem tekstu: Posebna pravila) u kojima su sadržani i detaljno opisani postupci i mere koji se primenjuju prilikom izdavanja i rukovanja kvalifikovanim uslugama od poverenja. Posebna pravila su privatni dokument i predstavljaju poslovnu tajnu sertifikacionog tela i odobrava ih odgovorno lice PKS CA.

Ovaj dokument Praktična pravila pružanja usluga izdavanja kvalifikovanih elektronskih vremenskih žigova (engl.: *Qualified Time-Stamp Policy*, QTP) sadrži pravila za pružanje usluga izdavanja kvalifikovanih elektronskih vremenskih žigova.

Primenjena tehnologija vremenskih žigova zasniva se na kriptografiji javnog ključa, X.509 sertifikatima i pouzdanim servisima tačnog vremena.

Sadržaj ovih Praktičnih pravila usklađen je sa standardima:

* + - ETSI EN 319 401,
		- ETSI EN 319 421,
		- ETSI EN 319 422,
		- ETSI TS 119 312.

Svrha ovih Praktičnih pravila je definisanje i uređivanje pravila i načela prema kojima trebaju postupati PKSCA QTSA, korisnici usluge izdavanja kvalifikovanih elektronskih vremenskih žigova (u daljem tekstu: Korisnici) i treće strane kao korisnici usluga od poverenja.

Za tumačenje odredaba ovih Praktičnih pravila merodavne su odredbe Uredbe (EU) br. 910/2014, Zakona o elektronskoj identifikaciji, elektronskom dokumentu i uslugama od poverenja u elektronskom poslovanju Republike Srbije, kao i standarda i preporuka na koje isti upućuju.

Kvalifikovani elektronski vremenski žigovi izdati prema ovim Opštim pravilima usklađeni su sa zahtevima standarda ETSI EN 319 421.

PKSCA kao pružalac usluga izdavanja kvalifikovanih elektronskih vremenskih žigova uključuje svoj vlastiti OID u vremenske žigove koje izdaje. U kvalifikovanim elektronskim vremenskim žigovima PKSCA nalazi se identifikator ovih Praktičnih pravila pružanja usluga izdavanja kvalifikovanih elektronskih vremenskih žigova (QTP OID: 1.3.6.1.4.1.31266.10.1.3).

Pružanje usluge izdavanja kvalifikovanih elektronskih vremenskih žigova usklađeno je sa ETSI EN 319 421 BTSP (*Best practices Time-Stamp Policy*): Praktična pravila najbolje prakse za vremenske žigove, OID: 0.4.0.2023.1.1.

Struktura ovog dokumenta urađena je na osnovu standarda IETF RFC 3647.

## Ime dokumenta i identifikacija

Ovaj dokument predstavlja Praktična pravila rada PKS CA usluge vremenskog žiga (u daljem tekstu praktična pravila).

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 (1.3.6.1.4.1.31266.10.1.3)**

## Korisnici usluga PKSCA QTSA

### 1.3.1. Pružalac usluga izdavanja kvalifikovanih elektronskih vremenskih žigova

PKSCA preko servisa PKS QTSA pruža uslugu izdavanja kvalifikovanih elektronskih vremenskih žigova (u daljem tekstu: usluga izdavanja vremenskih žigova).

#### 1.3.1.1 PKSCA Root CA

Sertifikaciono telo PKS je generisalo samopotpisani PKSCA Root CA sertifikat, kao i CA sertifikat za njemu subordinantni Intermediate PKSCACLOUD. PKSCA Root CA ne izdaje sertifikate korisnicima.

Osnovni podaci o PKSCA Root CA sertifikatu dati su u Tabeli 1.:

|  |  |  |
| --- | --- | --- |
| **Polje** | **Atribut** | **Vrijednost** |
| Issuer | commonName | PKSCA Root CA |
| organizationName | Privredna komora Srbije |
| countryName | SR |
| Validity | notBefore | *Vreme izdavanja sertifikata* |
| notAfter | *Vreme izdavanja sertifikata + 20 godina* |
| Subject | commonName | PKSCA Root CA |
| organizationName | Privredna komora Srbije |
| countryName | SR |
| SHA-1 *fingerprint*:  |
| SHA-256 *fingerprint*: |

***Tabela 1. Osnovni podaci o PKSCA Root CA sertifikatu***

PKSCA Root CA sertifikat dostupan je na sledećoj internet adresi: <http://v3.pksca.rs/>

####  PKSCA CLOUD sertifikati za TSU

PKSCA CLOUD izdaje sertifikate za TSU.

Osnovni podaci o PKSCA CLOUD sertifikatu za TSU dati su u Tabeli 2.:

|  |  |  |
| --- | --- | --- |
| **Polje** | **Atribut** | **Vrednost** |
| Issuer | commonName | PKSCA Root CA |
| organizationName | PKS |
| countryName | RS |
| Validity | notBefore | *Vreme izdavanja sertifikata* |
| notAfter | *Vreme izdavanja sertifikata + 10 godina* |
| Subject | commonName | PKSCA Cloud |
| organizationName | PKS |
| countryName | RS |
| SHA-1 *fingerprint*:  |
| SHA-256 *fingerprint*:  |

***Tabela 2. Osnovni podaci o*** PKSCA Cloud ***sertifikatu***

PKSCA Cloud sertifikat dostupan je na sledećoj internet adresi: <http://v3.pksca.rs/>

### 1.3.2. Korisnici

Korisnici servisa PKS QTSA su fizička lica - građani ili Pravna lica koji sa PKSCA ugovaraju korišćenje usluga izdavanja vremenskih žigova.

Korisnici servisa PKSCA za izdavanje kvalifikovanih elektronskih vremenskih žigova su i interni korisnici PKS.

### 1.3.3. Registraciona tela

Poslovi registracije Korisnika za PKSCA QTSA obavljaju se u registracionim telima Sertifikacionog tela PKS. PKSCA ima organizovanu mrežu registracionih tela (u daljem tekstu: PKSCA RA mreža) koja obavlja poslove registracije Korisnika za PKS QTSA.

PKSCA RA mrežu čini mreža regionalnih registracionih kancelarija (u daljem tekstu: PKSCA RRA) u poslovnoj mreži Privredne komore Srbije, kao i centralni PKSCA RA. Registraciju Korisnika u PKSCA RA mreži sprovodi PKSCA RRA, kao centralni PKSCA RA. U PKSCA RRA registraciju sprovode operateri registracionih tela. Poslovima registracije u PKSCA RA mreži upravlja centralni PKSCA RA koji je središnja komunikaciona tačka PKSCA RA mreže.

PKSCA može odrediti i drugi odgovarajući način registracije Korisnika.

### Treće strane

Treće strane su fizička ili pravna lica koji su korisnici kvalifikovanih elektronskih vremenskih žigova i deluju na osnovu razumnog poverenja u vremenske žigove koje izdaje PKSCA QTSA.

## Upotreba vremenskih žigova

* + 1. **Primerena upotreba vremenskih žigova**

Kvalifikovani vremenski žigovi koje izdaje servis PKSCA QTSA mogu se koristiti za bilo koju primenu koja zahteva dokazivanje postojanja podataka u elektronskom obliku u vremenu koje je navedeno u izdatom vremenskom žigu. Kvalifikovani vremenski žigovi koje izdaje PKSCA QTSA koriste se i za očuvanje dugotrajnosti elektronski potpisanih i pečatiranih dokumenata.

## Zabrane upotrebe vremenskih žigova

Nije dozvoljena upotreba kvalifikovanih vremenskih žigova za one podatke, odnosno elektronske zapise čiji je sadržaj protivan Ustavu Republike Srbije, propisima ili moralu društva.

## Administracija Praktičnih pravila rada PKS CA

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

### Organizacija odgovorna za održavanje dokumenta Praktična pravila

Za izradu i održavanje ovog dokumenta Praktičnih pravila odgovorno je Sertifikacionmo telo PKS.

Ovlašćene osobe iz organizacijskih jedinica PKS koje učestvuju u izradi, održavanju, implementaciji i odobravanju pravila i postupaka u PKSCA PKI koja se primenjuju u pružanju usluga od poverenja, u daljnjem tekstu nazivaju se zajedničkim nazivom PKSCA PMA.

Promene sadržaja ovog dokumenta Praktičnih pravila obavljaju se na temelju internih predloga i zahteva za usklađivanjem sa zakonskom regulativom i merodavnim standardima.

### 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

### 1.4.3 Osoba koja određuje pogodnost CPS dokumenta

Osoba u PKS CA, odgovorna da su ova Praktična pravila rada (CPS) u saglasnosti sa Politikom vremenskog žiga (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

### 1.4.4 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.

# OBJAVE I ODGOVORNOSTI ZA REPOZITORIUM

## Identifikacija tela koje vodi repozitorium

PKSCA PKI repozitorium vodi PKSCA kao kvalifikovani pružalac usluga poverenja. PKSCA je odgovorno za rad PKSCA PKI repozitoriuma, kao i za objavu dokumenata i informacija na repozitoriumu.

PKSCA osigurava dostupnost repozitoriuma na internet stranicama, uz raspoloživost 24 sata na dan, 7 dana u nedelji.

## Objava informacija o izdavanju vremenskih žigova

Na PKSCA PKI repozitoriumu javno su objavljeni dokumenti i informacije o pružanju usluga izdavanja vremenskih žigova:

* aktuelna politika sertifikacije pružanja usluga od poverenja,
* aktuelni Pravilnik o postupcima pružanja usluga izdavanja kvalifikovanih vremenskih žigova,
* ranije verzije praktičnih pravila pružanja usluga izdavanja kvalifikovanih vremenskih žigova
* uslovi pružanja usluga izdavanja elektronskih vremenskih žigova
* sertifikat TSU kojeg PKSCA QTSA servis koristi pri potpisivanju vremenskih žigova,
* cenovnik usluga izdavanja vremenskih žigova,
* obrazac zahteva za pristupanje PKSCA Servisu vremenskog žigosanja,
* informacije o sertifikatu za potpis vremenskog žiga,
* aktuelne lokacije PKSCA RA/LRA tela,
* Korisnička uputstva,
* obaveštenja korisnicima vezane za pružanje usluga izdavanja vremenskih žigova,
* ostale informacije vezane za rad PKSCA QTSA.

Javno objavljeni sadržaj PKSCA QTSA repozitoriuma, koji je sastavni deo PKSCA PKI repozitoriuma, dostupan je na internet adresi:

<http://v3.pksca.rs/>

U PKSCA PKI repozitoriumu ne objavljuju se poverljivi podaci.

## Vreme ili učestalost objavljivanja

PKSCA na godišnjem nivou i prema potrebi održava i ažurira Praktična pravila pružanja usluga izdavanja kvalifikovanih elektronskih vremenskih žigova, a zatim ih, nakon odobrenja, objavljuje. Drugi PKSCA PKI dokumenti i ostale relevantne informacije objavljuju se prema potrebi, nakon odobrenja.

## Kontrole pristupa repozitoriumu

Dokumenti i informacije objavljene na PKSCA PKI repozitoriumu su besplatne i javno dostupne.

PKSCA na repozitoriumu ima uspostavljene kontrole pristupa u cilju sprečavanja neautorizovanog dodavanja, promene ili brisanja informacija, kao i zaštite njihove celovitosti i autentičnosti.

Pravo dodavanja, promene ili brisanja informacija na PKSCA PKI repozitoriumu imaju ovlašćene osobe PKSCA.

# IDENTIFIKACIJA KORISNIKA I IZDAVANJE ELEKTRONSKIH VREMENSKIH ŽIGOVA

## Identifikacija Korisnika

PKSCA QTSA pruža uslugu izdavanja kvalifikovanih elektronskih vremenskih žigova (u daljem tekstu: elektronski vremenski žig) samo registrovanim korisnicima.

Ako korisnik već ima važeći digitalni sertifikat izdat od PKSCA ili od pružalaca usluga od poverenja koje PKSCA odobri i kojim će pristupati PKSCA servisu za izdavanje elektronskih vremenskih žigova treba popuniti i potpisati zahtev za PKSCA uslugu izdavanja elektronskih vremenskih žigova, pa je proslediti u PKSCA. Forma zahteva popunjava se u okviru portala usluga PKS na internet stranicama

<http://usluge.pks.rs>

Nakon registracije korisnik sa PKSCA sklapa ugovor o korišćenju PKSCA usluge izdavanja elektronskih vremenskih žigova.

## Inicijalno utvrđivanje identiteta Korisnika

PKSCA prikuplja lične podatke fizičkih lica i podatke pravnih lica isključivo za potrebe registracije u cilju izdavanja elektronskih vremenskih žigova.

Proveru podataka koji se prikupljaju u postupku registracije korisnika PKSCA sprovodi njihovim poređenjem sa podacima iz dostavljene dokumentacije, kao i, ukoliko je primenjivo, korišćenjem komunikacionih kanala u skladu sa važećom zakonskom regulativom.

Za korisnike kvalifikovanih elektronskih sertifikata već je sprovedena identifikacija korisnika, pa za korišćenje usluge izdavanja elektronskih vremenskih žigova Korisnici u PKSCA dostavljaju samo zahtev.

## Način dostave zahteva

Pristupnica se može dostaviti na sledeći način:

* + - * lično podnošenje u PKSCA LRA,
			* elektronskom dostavom zahteva potpisanog naprednim elektronskim potpisom uz korišćenje kvalifikovanog sertifikata, preko portala usluga PKS.

## Sklapanje ugovora

Ugovor o pružanju usluga izdavanja elektronskih vremenskih žigova je ugovor koji u skladu sa uslovima o pružanju usluge izdavanja kvalifikovanih elektronskih vremenskih žigova, praktičnim pravilima pružanja usluga izdavanja kvalifikovanih elektronskih vremenskih žigova i propisima koji uređuju pružanje usluge izdavanja elektronskih vremenskih žigova, sklapaju korisnici i PKSCA kao pružalac usluge.

## Identifikacija i autentikacija na PKSCA QTSA servis

Registrovani Korisnici pristupaju usluzi izdavanja elektronskih vremenskih žigova na način predviđen kroz portal usluga PKS.

Registrovani korisnici mogu pristupiti usluzi izdavanja elektronskih vremenskih žigova i uz autentikaciju sertifikatom izdatim od drugih pružalaca usluga od poverenja koje PKSCA prihvati.

PKSCA može korisnicima odobriti i drugi odgovarajući način autentikacije korisnika (npr. korisničko ime i lozinka).

URL adresa za autentikaciju na PKSCA QTSA servis je:

* + - * autentikacija korisničkim imenom i lozinkom: v3.pksca.rs/tsa.

PKSCA interni korisnici pristupaju servisu za izdavanje vremenskih žigova korišćenjem IP adresnog područja za korisnike sistema PKSCA.

## Sertifikat modula za izradu vremenskog žiga

PKSCA QTSA javno objavljuje javni ključ modula za izradu vremenskog žiga (TSU) kao sadržaj sertifikata PKSCA QTSA na repozitoriumu iz tačke 2.2. ovih Praktičnih pravila.

Sertifikat za TSU izdaje PKSCA CLOUD CA u skladu sa zahtevima standarda ETSI EN 319 411-2.

Pre početka izdavanja elektronskih vremenskih žigova PKSCA QTSA učitava svoj sertifikat za TSU. Pri dobijanju sopstvenog TSU sertifikata PKSCA QTSA proverava da li jei PKSCA CLOUD ispravno potpisao TSU sertifikat.

## Elektronski vremenski žig

Elektronski vremenski žigovi potpisuju se RSA privatnim ključem PKSCA QTSA servisa, dužine 2048 bitova uz korišćenje kriptografskih algoritama SHA-256 i RSA.

PKSCA QTSA osigurava da se elektronski vremenski žigovi izdaju na siguran način i sa tačnom oznakom vremena.

Za svaki elektronski vremenski žig osigurava se:

* + - da sadrži OID ovih Praktičnih pravila po kom je izdat,
		- da ima jedinstveni identifikator,
		- da se vreme korišćeno u TSU može povezati sa stvarnim vremenom dostavljenim od pouzdanog izvora,
		- da sadrži tačan podatak o vremenu iz TSU u vreme izdavanja elektronskog vremenskog žiga,
		- da sadrži *hash* vrednost elektronskog zapisa za koji se izdaje elektronski vremenski žig,
		- da je potpisan privatnim TSU ključem koji ima isključivu namenu potpisivanja vremenskog žiga,
		- identifikator države u kojoj je PKSCA QTSA ima sedište,
		- identifikator za PKSCA QTSA,
		- identifikator TSU koja je izdala elektronski vremenski žig.

Elektronski vremenski žig izdaje se u skladu sa preporukom ITF RFC 3161 i standarda ETSI EN 319 421 kao i sa profilom usklađenim sa standardom ETSI EN 319 422.

Samo jedan privatni TSU ključ je aktivan istovremeno.

PKSCA QTSA servis za izdavanje elektronskih vremenskih žigova podržava zahteve za izdavanje elektronskih vremenskih žigova u skladu sa standardom ETSI EN 319 422 i preporuci IETF RFC 3161.

### 3.4.1. Zahtev za izdavanje vremenskog žiga (*Time-Stamp Request*)

Zahtev za izdavanje elektronskog vremenskog žiga u skladu je sa standardom ETSI EN 319 422 i tačkom 2.4.2. u dokumentu IETF RFC 3161.

Korisnik koji od PKSCA QTSA zahteva izdavanje vremenskog žiga mora ostvariti autentikovanu konekciju sa komunikacionim serverom PKSCA QTSA sistema. U slučaju neuspele konekcije, transakcija će biti prekinuta, a korisnik će na odgovarajući način biti obavešten o neuspeloj konekciji.

Klijentska aplikacija na strani korisnika koja se koristi za ugradnju vremenskog žiga, treba podržavati protokol za elektronski vremenski žig u skladu sa preporukom IETF RFC 3161.

### 3.4.2. Odgovor servisa za izdavanje elektronskih vremenskih žigova (*Time-Stamp Response*)

Odgovor PKSCA QTSA servisa za izdavanje elektronskih vremenskih žigova na zahtev za izdavanje elektronskog vremenskog žiga u skladu je sa normom ETSI EN 319 422 i tačkom 2.4.2. u dokumentu IETF RFC 3161.

## Profil vremenskog žiga

Osnovni podaci o profilu kvalifikovanih elektronskih vremenskih žigova koje izdaje PKSCA QTSA servis dati su u Tabeli 3.:

|  |  |
| --- | --- |
| **Polje** | **Vrednosti za kvalifikovani elektronski vremenski žig kojeg izdaje PKSCA QTSA** |
| Version | V1, vrednost=“1“ |
| Policy OID | PKSCA OID: 1.3.6.1.4.1.31266.10.2 |
| messageImprint | Podržani hash algoritam: sha-256 (OID: 2.16.840.1.101.3.4.2.1) |
| serialNumber | Ceo broj |
| genTime | UTC Vreme, odstepenet od 1 s |
| ordering | FALSE |
| Nonce | Ceo broj |
| signatureAlgorithm | sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) |

***Tabela 3.: Osnovni podaci o kvalifikovanom elektronskom vremenskog žigu kojeg izdaje PKSCA QTSA***

## Tačnost vremena u izdatim elektronskim vremenskim žigovima

PKSCA kao pružalac usluga izdavanja kvalifikovanih elektronskih vremenskih žigova obavezuje se na tačnost podataka o vremenu ugrađenom u elektronski vremenski žig. Podatak o UTC vremenu koji se ugrađuje u svaki pojedini elektronski vremenski žig ima garantovanu tačnost 1 s.

## Sinhronizacija sata sa UTC

PKSCA QTSA osigurava da je vreme PKSCA QTSA sistema sinhronizovano sa UTC vremenom, u okviru preciznosti propisane u tački 3.6. ovih Praktičnih pravila, a posebno:

* + - periodičnom kalibracijom sata,
		- zaštitom od neautorizovane izmene vremena TSU,
		- detekcijom pomaka ili ispada iz sinhronizacije sa UTC vremenom,
		- uračunavanjem „*leap second*“ događaja.

Primarni izvor pouzdanog UTC vremena u PKSCA QTSA sistemu je modul sinhronizovan sa etalonom u Direkciji za mere i dragocene metale Republike Srbije putem internet veze korišćenjem NTP protokola.

Kao alternativni pouzdani izvor UTC vremena PKSCA QTSA sistem koristi podatak o UTC vremenu dobijen od strane GPS satelitskog signala.

U slučaju ispada primarnog izvora pouzdanog UTC vremena PKSCA QTSA sistem automatski prelazi na alternativni pouzdani izvor UTC vremena.

### 3.7.1. Letnje računanje vremena

PKSCA QTSA servis u izdatim elektronskim vremenskim žigovima upisuje vreme u UTC formatu.

Preporuka je Korisnicima i pouzdajućim stranama da provere na koji način klijentska aplikacija prikazuje vreme u izdatim elektronskim vremenskim žigovima, kao i da obrate pažnju na prikazivanje lokalnog vremena u različitim vremenskim zonama, a naročito u vreme prelaska na letnje računanje vremena.

## Provera validnosti vremenskog žiga

Proveru validnosti elektronskog potpisa PKSCA QTSA servisa u vremenskom žigu pouzdajuće strane sprovode prema zahtevima standarda ETSI EN 319 102-1.

Provera validnosti elektronskog vremenskog žiga obuhvata sledeće provere:

* + - proveru da su podaci za koje je tražen elektronski vremenski žig povezani sa tim elektronskim vremenskim žigom i TSU sertifikatom PKSCA QTSA servisa,
		- validaciju potpisa kojim je potpisan elektronski vremenski žig,
		- proveru da izdati elektronski vremenski žig ispunjava specifične zahteve u pogledu tačnosti, pouzdanosti i odgovornosti PKSCA QTSA servisa, odnosno PKSCA kao kvalifikovanog pružaoca usluga.

## Raspoloživost usluge

PKSCA kao pružalac usluga izdavanja kvalifikovanih elektronskih vremenskih žigova garantuje kontinuiranu dostupnost usluge izdavanja elektronskih vremenskih žigova i uslova pružanja usluge.

## Izdavanje nekvalifikovanih elektronskih vremenskih žigova

TSU jedinice PKSCA QTSA servisa za izdavanje kvalifikovanih elektronskih vremenskih žigova izdaju samo kvalifikovane elektronske vremenske žigove.

## Transportni protokol za uslugu izdavanja elektronskih vremenskih žigova

PKSCA QTSA servis koristi HTTP protokol - uz klijentsku autentikaciju.

# OPERATIVNI ZAHTEVI ZA ŽIVOTNI CIKLUS SERTIFIKATA ZA PKSCA QTSA

## Izdavanje sertifikata

Izdavanje PKSCA QTSA sertifikata obavljaju ovlašćene osobe sa poverljivim ulogama u PKSCA PKI, pod dualnom kontrolom, u PKSCA PKI zazaštićenom prostoru.

## Opoziv i suspenzija sertifikata

Opoziv sertifikata za PKSCA QTSA servis sprovodi se u skladu sa niže navedenim tačkama. Suspenzija sertifikata za PKSCA QTSA servis nije dozvoljena.

### 4.2.1. Razlozi za opoziv

PKSCA QTSA sertifikat opoziva se iz sledećih razloga:

* + - * u slučaju kompromitovanja privatnog ključa ili ako se pojavi osnovana sumnja da je privatni ključ kompromitovan,
			* ako neka od informacija sadržanih u sertifikatu postane netačna,
			* u slučaju trajne nedostupnosti ili gubitka privatnog ključa,
			* u slučaju zabranjene upotrebe privatnog TSU ključa,
			* ako PKSCA proceni da PKSCA QTSA sertifikat svojim tehničkim karakteristikama, profilom ili sadržajem ne pruža adekvatan nivo poverenja pouzdajućim stranama,
			* ako PKSCA QTSA prestaje sa radom, a PKSCA nije u mogućnosti osigurati nastavak pružanja usluga kod drugog kvalifikovanog pružaoca usluga,
			* ako sertifikat nije izdat u skladu sa zahtevom ili odredbama ovih Praktičnih pravila.

## Ko može tražiti opoziv

Zahtev za opoziv PKSCA QTSA sertifikata može podneti ovlašćena osoba u PKSCA QTSA uz odobrenje odgovorne osobe PKSCA QTSA.

## Učestalost izdavanja CRL

CRL se objavljuje jednom u 24 sata, a postoji mogućnost objavljivanja odmah po opozivu sertifikata.

## Maksimalno kašnjenje za CRL

Maksimalno kašnjenje CRL od trenutka njenog izdavanja do trenutka objave u redovnim uslovima iznosi dva minuta.

## Zahtevi na *online* proveru statusa opozvanosti sertifikata

PKSCA CLOUD CA podržava *online* proveru statusa opozvanosti izdatih sertifikata putem PKSCA OCSP servisa čiji je rad usklađen sa preporukom IETF RFC 6960.

Informacija o statusu opozvanosti sertifikata korišćenjem PKSCA OCSP servisa dostupna je u realnom vremenu.

Adresa PKSCA OCSP servisa je http://v3.pksca.rs/cloudocsp, a upisuje se u ekstenziji *Authority Information Access* svakog sertifikata koje izdaje CA navedeni u ovoj tački.

## Drugi dostupni načini objave opozvanih sertifikata

Nema odredbi.

# PROVERA SISTEMA, UPRAVLJANJA I RADNIH POSTUPAKA

PKSCA osigurava primerenu zaštitu imovine koja se upotrebljava za pružanje usluga izdavanja elektronskih vremenskih žigova i u tu svrhu vodi celokupni popis te imovine sa pripadajućom klasifikacijom koja je u skladu sa procenom rizika.

Mere fizičke zaštite, postupci koje PKSCA primenjuje u zaštiti sistema za izdavanje elektronskih vremenskih žigova kao i postupci provere tog sistema, upravljanja i radnih postupaka u PKSCA PKI interne su prirode, pa se njihovi detalji ne objavljuju javno.

## Mere fizičke zaštite

PKSCA kao pružalac usluga izdavanja kvalifikovanih elektronskih sertifikata i kvalifikovanih elektronskih vremenskih žigova primenjuje mere fizičke zaštite PKSCA QTSA sistema sa ciljem minimizacije rizika vezanih uz fizički zaštitu i u skladu sa poslovnom politikom PKSCA, važećom zakonskom regulativom i međunarodnim preporukama.

### 5.1.1. Lokacija objekta i konstrukcija

Produkcioni PKSCA QTSA sistem smešten je u zgradi Privredne komore Srbije, u posebnom zazaštićenom prostoru, izdvojenom za tu namenu, uz primenu više nivoa fizičke i tehničke zaštite koje onemogućuju neovlašćen fizički pristup sistemu i podacima, i time sprečavaju kompromitovanje sistema i usluga. Fizička zaštita postavljena je na konceptu upotrebe sigurnosnih zona, tako da se nivo zaštite povećava svakim prolaskom u sledeću zonu. Fizička zaštita od upada ostvarena je sigurnosnim perimetrima koji razdvajaju zone postavljene oko PKSCA QTSA sistema.

Sigurni prostori i podprostori u kojima se nalaze komponente PKSCA QTSA Sistema u daljem tekstu nazivaju se zajedničkim nazivom PKSCA PKI zaštićeni prostor.

### 5.1.2. Fizički pristup

Fizički pristup PKSCA QTSA sistemu u PKSCA PKI zazaštićenom prostoru i pripadajućim podprostorima unutar tog prostora ostvaruje se uz kontrolu prolaza ovlašćeih osoba PKSCA PKI, a u skladu s njihovim ulogama i ovlašćenjima, a u skladu sa internim pravilom koje reguliše pristupe u zaštićenu zonu.

Osobama koje nemaju ovlašćenje fizičkog pristupa PKSCA QTSA sistemu pristup je dozvoljen samo u pratnji i uz celovremeni nadzor ovlašćenih osoba PKSCA PKI uz njihovu kontrolu, a u skladu sa internim procedurama PKSCA.

O svakom pristupu PKSCA QTSA sistemima vodi se evidencija.

Oprema, informacije, mediji i softver iz PKSCA PKI zaštićenog prostora iznosi se isključivo uz minimalno dualnu kontrolu ovlašćeih osoba u PKSCA PKI kojima su dodeljene odgovarajuće poverljive uloge, i uz prethodno ovlašćenje.

Fizički pristup podacima registrovanih korisnika koje prikuplja RA mreža imaju samo ovlašćeni zaposleni PKSCA PKI i ovlašćeni zaposleni PKSCA RA mreže, koji lične podatke o fizičkim osobama prikupljaju, čuvaju, koriste i brišu u skladu sa odgovarajućim propisima o zaštiti ličnih podataka.

### 5.1.3. Sistemi za napajanje i klimatizaciju

Uređaji i prostor u kom se nalazi PKSCA QTSA sistem, PKSCA RA sistem i repozitorium, kao i sistemi tehničke zaštite, opremljeni su neprekidnim napajanjem električnom energijom i klimatizacijom koja je dimenzionisana na način koji osigurava odgovarajuće radne uslove i u slučaju prekida napajanja.

### 5.1.4. Opasnost od poplave

Lokacija na kojoj se nalazi PKSCA QTSA sistem, PKSCA RA sistem i repozitorium zaštićena je od poplave.

### 5.1.5. Protivpožarna zaštita

PKSCA QTSA sistem, PKSCA RA sistem i repozitorium zaštićeni su sistemom za detekciju požara u skladu sa važećom zakonskom regulativom.

### 5.1.6. Čuvanje medija

Mediji na kojima se nalaze arhivske i sigurnosne kopije PKSCA PKI podataka u elektronskom obliku, kopije sadržaja repozitoriuma, kao i sigurnosne kopije programske opreme čuvaju se na dve odvojene zaštićene lokacije sa uspostavljenom protivpožarnom zaštitom i koje su osigurane od poplave. Ovi mediji zaštićeni su od oštećenja, krađe i neovlašćenog pristupa.

### 5.1.7. Zbrinjavanje otpada

Uređaji i mediji koji sadrže poverljive informacije u elektronskom obliku, a koji više nisu potrebni, sigurnosno se uništavaju tako da poverljive informacije ne mogu više biti čitljive niti obnovljene. Uništavanje ovih uređaja i medija odvija se pod nadzorom ovlašćenih osoba u PKSCA PKI.

Papirnati dokumenti i materijali koji sadrže poverljive informacije sigurnosno se uništavaju pre odlaganja u otpad.

## Organizacione mere zaštite

### Poverljive uloge

Poslovi upravljanja informacionim i komunikacionim sistemom, poslovi upravljanja izdavanjem elektronskih vremenskih žigova, administriranje i implementacije sigurnosnih postupaka, kao i poslovi nadzora delovanja PKSCA PKI obavljaju se unutar odvojenih organizacionih jedinica PKSCA.

Poslovi, obaveze i odgovornosti zaposlenih podeljene su prema odgovarajućim poverljivim ulogama. Poverljive uloge čine osnovu poverenja u PKSCA PKI i dodeljuju se ovlašćenim zaposlenima. Svaka poverljiva uloga je dokumentovana sa jasno definisanim opisom poslova i odgovornostima.

Poverljive uloge uključuju uloge Glavnog administrator bezbednosti, Administratora sistema, Operatera sistema, Sistem evidentičara, Operatera sertifikacionog tela i Operatera registracionog tela.

### Broj osoba potrebnih za obavljanje aktivnosti

Poslove u PKSCA PKI obavljaju isključivo ovlašćene osobe. PKSCA ima stalno zaposlen dovoljan broj stručnih osoba sa znanjem, iskustvom i kvalifikacijama koje su potrebne u PKSCA PKI za pružanje usluga iz opsega ovih Praktičnih pravila.

Pristup i poslovi u PKSCA PKI zaštićenom prostoru sprovode se isključivo uz istovremenu prisutnost dve osobe sa poverljivim ulogama, koje imaju dozvole pristupa tom sistemu.

Za obavljanje pojedinih bezbednosno osetljivih zadataka u PKSCA PKI zaštićenom prostoru, zahteva se učešće propisanog broja osoba sa određenim poverljivim ulogama.

### Identifikacija i potvrđivanje identiteta za svaku ulogu

Identifikacija i potvrda identiteta osobe sprovodi se odgovarajućom metodom autentikacije. Pristup i korišćenje aplikacija i servisa unutar PKSCA PKI omogućen je samo ovlašćenim osobama u skladu sa nivoom poverenja za ulogu koju obavljaju.

### Uloge koje zahtevaju odvajanje (separaciju) dužnosti

Zbog sigurnosnih zahteva izdavanja kvalifikovanih elektronskih vremenskih žigova sprovodi se odvajanje sledećih dužnosti:

* + - * osobi kojoj je dodeljena poverljiva uloga Glavni administrator bezbednosti ili Operater registracionog tela ne dodeljuje se poverljiva uloga Sistem evidentičar,
			* osobi kojoj je dodeljena poverljiva uloga Administrator sistema ne dodeljuje se poverljiva uloga Operater sertifikacionog tela ili Oprater registracionog tela.

## Provere nivoa znanja osoblja

### Kvalifikacije, radno iskustvo i zahtevi za proverom nivoa znanja osoblja

Pre početka rada na poslovima PKSCA PKI kandidati moraju posedovati odgovarajuća stručna znanja, iskustvo, kvalifikacije i edukacije u radu sa kriptografskim tehnologijama, zaštitom informacionih sistema, informacionom bezbednošću, kao i zaštitom ličnih podataka u oblasti sopstvenog delokruga rada, u okviru poslova PKSCA.

Zaposleni koji rade na poslovima PKSCA PKI ne smeju biti u radnom, odnosno poslovnom odnosu sa drugim pružaocima usluga od poverenja.

### Procedure provere prikladnosti osoblja

Pre početka rada na poslovima PKSCA PKI, PKSCA sprovodi odgovarajuće provere kandidata u cilju procene njihove stručnosti, sposobnosti i pouzdanosti u skladu sa potrebama poslova PKSCA PKI.

### Zahtevi za školovanjem

Zaposlenima koji obavljaju poslove u okviru PKSCA PKI osigurava se školovanje i usavršavanje u skladu sa njihovim poverljivim ulogama.

### Učestalost i uslovi za obnovu znanja

Predavanja o informacionoj bezbednosti sprovode se jednom godišnje za sve zaposlenike PKSCA PKI.

Zaposleni u PKSCA PKI sa poverljivim ulogama u PKSCA PKI imaju obavezu sticati i usavršavati svoje znanje.

Obnova znanja zaposlenih PKSCA RA mreže, obzirom na poslove koje obavljaju, sprovodi se redovno, najmanje jednom godišnje.

### Kazne za neovlašćene radnje

Nepridržavanje propisanih mera za ovlašćene osobe, prilikom obavljanja poslova u PKSCA PKI, podleže povredi radne obaveze prema Kolektivnom ugovoru, a eventualne kaznene mere određuju se disciplinskim postupkom.

U slučaju neovlašćenih radnji od strane ugovornih partnera primenjuju se odredbe definisane ugovorom sa ugovornim partnerom.

### Zahtevi na spoljne saradnike

Za ugovorene spoljne saradnike koji za PKSCA obavljaju deo usluga iz opsega usluga izdavanja kvalifikovanih elektronskih vremenskih žigova važe isti zahtevi pri radu u PKSCA kao i za interne zaposlene.

Zahtevi za dobavljače robe i usluga za PKSCA regulisani su internim dokumentima Privredne komore Srbije, kojim je definisan rad sa dobavljačima. Pristup spoljnih saradnika informacionom sistemu u PKSCA odobrava se isključivo na osnovu ugovora isključivo za onaj deo informacionog sistema koja je predmet ugovora i samo za aktivnosti navedene u ugovoru.

### Dokumentacija koja je dostupna zaposlenima

Svakom zaposlenom u PKSCA dostupna je dokumentacija potrebna za obavljanje njegovih radnih zadataka u skladu sa dodeljenom poverljivom ulogom i pripadajućim ovlašćenjima.

## Postupci upravljanja revizionim zapisima

### Tipovi događaja koji se zapisuju

Revizioni zapisi PKSCA QTSA sistema sadrže zapise o događajima vezanim za:

* + - * upravljanje životnim ciklusom TSU ključeva PKSCA QTSA sistema,
			* upravljanje životnim ciklusom TSU sertifikata za PKSCA QTSA sistem,
			* sinhronizaciju TSU sata sa UTC,

Revizioni zapisi sadrže i zapise o bezbednosnim događajima u PKSCA vezanim uz promene bezbednosnih politika, fizičku i tehničku zaštitu PKSCA zaštićenog prostora, pokretanje i zaustavljanje rada sistema, sistemske greške i kvarove hardvera, aktivnosti zaštitnih uređaja i računarske opreme, kao i drugih bitnih elemenata informacionog Sistema za koje je neophodno obezbediti revizioni trag.

### Učestalost obrade revizionih zapisa

Preglede revizionih zapisa PKSCA QTS sistema obavlja Sistem evidentičar. Pregledi revizionih zapisa obavljaju se redovno, jednom dnevno radnim danima, kao i u slučaju vanrednih situacija.

Postupak pregleda revizionih zapisa obuhvata:

* + - * pregled stavki dnevnika zapisa sistema koje su stvorene nakon poslednje revizije,
			* po potrebi, pripremu kratkog izveštaja koji sadrži objašnjenja važnih događaja.

### Vremenski period čuvanja revizionih zapisa

Revizioni zapisi iz tačke 5.4.1. ovih Praktičnih pravila čuvaju se najmanje 10 godina od izdavanja elektronskog vremenskog žiga na koji se zapisi odnose.

### Zaštita revizionih zapisa

Revizioni zapisi u PKSCA zaštićeni su tokom vremena čuvanja. Zaštita dnevnika zapisa sistema obuhvata zaštitu zapisa od njihovog neovlašćenog čitanja i otkrivanja, kao i očuvanje integriteta zapisa.

Tako zaštićeni revizioni zapisi na zahtev su raspoloživi samo ovlašćenim osobama, posebmo u svrhu pružanja dokaza o vremenskom žigu za potrebe sudskih postupaka.

### Sistem prikupljanja revizionih zapisa (unutrašnji ili spoljni)

Zavisno od vrste podataka, revizioni zapisi prikupljaju se automatski ili ih prikuplja ovlašćena osoba. Revizioni zapisi nastali u PKSCA PKI i PKSCA RA mreži prikupljaju se interno.

### Obaveštavanje subjekta uzročnika događaja

U slučaju uočavanja zapisa o značajnom događaju u radu PKSCA PKI koji je povezan sa određenim subjektom, PKSCA zadržava pravo odlučivanja o obaveštavanju subjekta ili korisnika koji je taj događaj uzrokovao, u skladu sa zakonskom regulativom.

### Procena rizika

PKSCA obavlja redovnu procenu rizika informacionog sistema i imovine, procenu ranjivosti za prepoznate javne i privatne adrese, kao i penetraciono testiranje.

Procena rizika informacionog sistema i imovine sprovodi se jednom godišnje. Procena ranjivosti sistema za javne i privatne adrese PKSCA provodi se kvartalno. Penetracioni test sprovodi se jednom godišnje.

Svaku novu kritičnu ranjivost PKSCA će razmotriti u roku od 48 sati od momenta ortkrivanja, i postupiće u skladu sa utvrđenim postupcima za datu situaciju.

## Arhiviranje zapisa

### Tipovi arhiviranih zapisa

PKSCA arhivira niže navedene podatke koji, zavisno od tipa, mogu biti u elektronskom i/ili papirnom obliku:

* + - * Praktična pravila pružanja usluga izdavanja kvalifikovanih elektronskih vremenskih žigova,
			* Pravilnici o postupcima izdavanja kvalifikovanih elektronskih vremenskih žigova,
			* Uslovi pružanja usluga izdavanja kvalifikovanih elektronskih vremenskih žigova,
			* Zahtevi za izdavanje kvalifikovanih elektronskih vremenskih žigova,
			* Ugovor o pružanju usluge izdavanja kvalifikovanih elektronskih vremenskih žigova,
			* Podaci i pripadajuća dokumentacija prikupljena postupkom registracije pravnih i fizičkih lica i poslovnih subjekata,
			* Revizioni zapisi PKSCA QTSA sistema iz tačke 5.4.1. ovih Praktičnih pravila,
			* Drugi interni dokumenti PKSCA.

Svaki zapis koji se arhivira sadrži podatak o vremenu koje se odnosi na taj zapis.

### Vremenski period arhiviranja

Sve arhivirane podatke i dokumentaciju PKSCA čuva najmanje 10 godina od izdavanja vremenskog žiga na koji se ti podaci i dokumentacija odnose.

### Zaštita arhive

Arhivirani podaci i dokumentacija zaštićeni su mehanizmima i postupcima propisanog nivoa sigurnosti koje osiguravaju poverljivost i integritet arhive. Arhiva se štiti od neovlašćenog pregleda, modifikovanja i brisanja podataka.

Tako zaštićeni arhivirani zapisi, na zahtev su raspoloživi samo ovlašćenim osobama, a posebno u svrhu pružanja dokaza o izdatom vremenskom žigu za potrebe sudskih postupaka.

### Postupci izrade sigurnosnih kopija arhive

Sigurnosna kopija arhiviranih podataka u elektronskom obliku izrađuje se u PKSCA zaštićenom prostoru i čuva se na siguran način na drugoj lokaciji.

### Sistem prikupljanja arhivskih zapisa (unutrašnji ili spoljni)

Zapisi za arhiviranje prikupljaju se na način koji zavisi od vrste zapisa.

Zapisi za arhiviranje nastali u PKSCA PKI i PKSCA RA mreži prikupljaju se i arhiviraju interno.

### Postupci dobijanja i provere arhiviranih zapisa

Pristup zapisima iz arhive imaju samo osobe ovlašćene za pristup tim podacima. Verifikacija podataka iz arhive obavlja se proverom njihovog integriteta.

## Promena TSU ključa

PKSCA osigurava da PKSCA QTSA kontinuirano pruža kvalifikovanu uslugu od poverenja sa svojim validnim parom ključeva i pripadajućim TSU sertifikatom za PKSCA QTSA sistem. Iz tog razloga PKSCA će pre isteka TSU sertifikata, generisati novi par TSU ključeva. Takođe, PKSCA će generisati novi par TSU ključeva i u slučaju kada tu promenu zahteva nivo sigurnosti kriptografskog algoritma privatnog TSU ključa u upotrebi. U oba slučaja za novi javni TSU ključ PKSCA RDC CA izdaće TSU sertifikat za PKSCA QTSA servis.

PKSCA će o promeni javnog TSU ključa i o novom TSU sertifikatu za PKSCA QTSA sistem pravovremeno obaveštavati korisnike PKSCA QTSA.

Novi pripadajući javni TSU ključ biće dostupan korisnicima PKSCA QTSA na način na koji je to bio i prethodni javni TSU ključ, a u skladu sa ovim Opštim pravilima.

Nakon generisanja novog para TSU ključeva, elektronski vremenski žigovi potpisivaće se korišćenjem novog privatnog TSU ključa.

Stari javni TSU ključ i stari pripadajući TSU sertifikat za PKSCA QTSA servis se arhiviraju.

## Oporavak od kompromitacije ili nepogode

### Postupci u slučaju incidenta ili kompromitacije

Planom kontinuiteta poslovanja za PKSCA PKI regulisani su postupci u slučaju incidenta ili kompromitacije sistema, a koji obuhvataju postupke za oporavak sistema i uspostavu sigurnosnih uslova za pružanje usluga izdavanja elektronskih vremenskih žigova.

Plan kontinuiteta poslovanja revidira se jednom godišnje.

### Postupci u slučaju oštećenja u računarskim resursima, programima i/ili podacima

PKSCA QTSA sistem zasnovan je na pouzdanim hardverskim i softverskim komponentama, a kritične operacije sistema podržane su redudantnim komponentama.

Funkcionalnost, ispravnost rada i pravovremeno otklanjanje oštećenja komponenti PKSCA QTSA sistema osigurano je kroz ugovore o podršci i održavanju sa dobavljačima hardvera i sofrvera.

Plan kontinuiteta poslovanja za PKSCA PKI reguliše postupke oporavka PKSCA QTSA sistema u slučaju kvarova ili oštećenja opreme i mrežnih resursa, kao i ponovo uspostavljanje funkcionalnosti.

### Postupci u slučaju kompromitovanja privatnog ključa ili ispada iz sinhronizacije sa UTC vremenom

U slučaju kompromitovanja privatnog TSU ključa za PKSCA QTSA sistem pripadajući TSU sertifikat će biti opozvan od strane PKSCA CA.

PKSCA će za sve korisnike i pouzdajuće strane, putem internet stranica PKSCA repozitoriuma objaviti opis kompromitacije ili gubitka kalibracije.

U slučaju veće kompromitacije rada PKSCA QTSA ili gubitka kalibracije PKSCA će putem internet stranica PKSCA repozitoriuma za sve korisnike i pouzdajuće strane objaviti informacije za jasnu identifikaciju izdatih vremenskih žigova koji sadrže neispravne podatke.

PKSCA će o opozivu TSU sertifikata za PKSCA QTSA sistem ili ispada iz sinhronizacije sa UTC vremenom obaveštavati korisnike PKSCA QTSA:

* PKSCA RA mrežu,
* Korisnike,
* Treće strane.

Nakon ustanovljavanja i otklanjanja uzroka koji su prouzrokovali kompromitaciju TSU ključa, PKSCA će, ako je primenjivo, preduzeti mere za sprečavanje ponavljanja takvog događaja.

PKSCA će generisati novi par TSU ključeva. PKSCA CA će za novi javni TSU ključ izdati novi TSU sertifikat za PKSCA QTSA sistem.

Novi TSU sertifikat za PKSCA QTSA sistem biće dostupan korisnicima PKSCA QTSA na način na koji je bio dostupan i prethodni TSU sertifikat, a u skladu sa ovim Opštim pravilima.

### Mogućnost nastavka poslovanja nakon nepogode

U Planu kontinuiteta poslovanja PKSCA PKI određeni su postupci za nastavak poslovanja nakon katastrofe.

## Prestanak rada PKSCA QTSA servisa

O planiranom prestanku pružanja usluga izdavanja elektronskih vremenskih žigova PKSCA će:

* obavestiti sve korisnike usluge, treće strane i centralno telo državne uprave nadležno za ove poslove, najmanje tri meseca pre planiranog prestanka pružanja usluga izdavanja elektronskih vremenskih žigova,
* uložiti sav napor da kod drugog kvalifikovanog pružalaca usluga od poverenja osigura nastavak pružanja usluga izdavanja elektronskih vremenskih žigova, da će tom pružalacu usluga dostaviti svu dokumentaciju prikupljenu u postupku registracije korisnika kao i svu dokumentaciju o izdatim elektronskim vremenskim žigovima,
* uništiti aktuelni privatni ključ TSU i opozvati sve važeće PKSCA QTSA sertifikate.

U slučaju prestanka pružanja usluga izdavanja elektronskih vremenskih žigova PKSCA će arhivirati, zaštititi i čuvati zapise prema odredbama iz ovih Praktičnih pravila, kako bi ti zapisi bili raspoloživi za pružanje dokaza u sudskim, upravnim i drugim postupcima u skladu sa važećim odredbama zakonske regulative, ili će PKSCA sa drugim poslovnim subjektom ugovoriti takvo arhiviranje, zaštitu i čuvanje zapisa.

# TEHNIČKE MERE ZAŠTITE

Ovo poglavlje opisuje mere zaštite koje se preduzimaju u cilju postizanja zahtevanog nivoa sigurnosti kriptografskih ključeva, aktivacionih podataka, kritičnih sigurnosnih parametara, upravljanja ključevima i drugih mera tehničke sigurnosti za PKSCA QTSA i za izdavanje elektronskih vremenskih žigova.

## Generisanje i instalacija para ključeva

### 6.1.1. Generisanje para TSU ključeva

PKSCA provodi generisanje para TSU ključeva za PKSCA QTSA sistem koristeći kriptografske algoritme za generisanje ključeva koji su uskladjeni sa normativnim dokumentom ETSI TS 119 312.

Par TSU ključeva za PKSCA QTSA sistem generiše se u KMS modulu koji zadovoljava zahteve iz tačke 6.2.1. ovih Praktičnih pravila.

PKSCA QTSA sistem sa pripadajućim KMS modulom nalazi se tokom i nakon postupka generisanja para TSU ključeva u PKSCA PKI zaštićenom prostoru iz ovih Praktičnih pravila, a pristup PKSCA QTSA sistemu dopušten je ovlašćenim osobama PKSCA PKI sa poverljivim ulogama.

U postupku generisanja para TSU ključeva za PKSCA QTSA sistem učestvuju ovlašćene osobe sa poverljivim ulogama u PKSCA QTSA.

O sprovedenom generisanju PKSCA QTSA TSU ključeva vodi se zapisnik.

### 6.1.2. Dostava javnog TSU ključa korisnicima i trećim stranama

Javni TSU ključ PKSCA QTSA servisa služi za proveru potpisa vremenskog žiga, a nalazi se u sertifikatu za PKSCA QTSA servis koji je objavljen internet strani http://v3.pksca.rs

### 6.1.3. Dužina kriptografskih ključeva

Dužina kriptografskih TSU ključeva za PKSCA QTSA servis i algoritmi za potpisivanje vremenskog žiga su:

* + - * RSA kriptografski algoritam sa dužinom ključa od 2048 bita,
			* *sha256WithRSA* algoritam.

### 6.1.4. Generisanje i provera kvalitete parametara javnog ključa

Ključevi koje upotrebljava PKSCA QTSA generišu se u skladnu sa normatvnim dokumentom ETSI TS 119 312.

### 6.1.5. Namene ključeva

Privatni TSU ključ za PKSCA QTSA koristi se samo za elektronski potpis elektronskih vremenskih žigova.

Sertifikat za PKSCA QTSA u ekstenziji *Key Usage* ima postavljene vrednosti *digitalSignature* i

*nonRepudiation* te u ekstenziji *extKeyUsage* ima postavljenu vrednost *timeStamping.*

## Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

### Standardi i tehničke mere zaštite kriptografskog modula

HSM modul kojim TSU obavlja potpisivanje vremenskog žiga ima mogućnost podešavanja prema FIPS 140-2, nivo 3.

### Upravljanje privatnim TSU ključem od strane više osoba (n od m)

Upravljanje privatnim TSU ključem od strane više osoba sigurnosna je mera koja zahteva autorizaciju više ovlašćeih osoba za pristup privatnom TSU ključu za potpis vremenskog žiga. Taj mehanizam sprečava jednu osobu da sama pristupi privatnom potpisnom TSU ključu.

### Sigurno skladištenje privatnog ključa

Nije dozvoljeno skladištenje privatnih TSU ključeva za PKSCA QTSA.

### Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje privatnih TSU ključeva PKSCA QTSA sistema provodi se uz dualnu kontrolu ovlašćenih osoba sa poverljivim ulogama u PKSCA QTSA, u prostoru najvišeg nivoa sigurnosti u okviru zaštićenog prostora PKSCA. Privatni TSU ključ koristi se iz KMS modula isključivo u enkriptovanom obliku, pa se u tom obliku kopira i čuva u sigurnom prostoru najvišeg nivoa sigurnosti u okviru zaštićenih prostora PKSCA na odvojenim lokacijama.

Fizički pristup sigurnosnim kopijama privatnih TSU ključeva PKSCA QTSA sistema imaju isključivo ovlašćene osobe sa poverljivim ulogama u PKSCA QTSA.

### Arhiviranje privatnog ključa

Nije dozvoljeno arhiviranje privatnih TSU ključeva.

### Prenos privatnog ključa

Za vreme dok je izvan KMS modula, privatni TSU ključ je zaštićen enkriptovanjem. Enkriptovanje privatnog ključa sprovodi se strogim pridržavanjem zahteva navedenih u sertifikacionoj dokumentaciji HSM modula, tako da se time osigurava jednak nivo sigurnosti zaštite privatnog ključa kao i kad se ključ nalazi u HSM modulu. Prenos privatnog ključa sprovode samo ovlašćene osobe sa poverljivim ulogama u PKSCA QTSA. Privatni TSU ključevi prenose se iz KMS modula isključivo u svrhe izrade sigurnosne kopije.

Kod prenosa privatnog TSU ključa iz jednog KMS modula u drugi KMS privatni ključ se sme prenositi samo u KMS jednakog ili višeg nivoa sigurnosti u odnosu na KMS iz kog se privatni ključ prenosi.

### Čuvanje privatnog ključa u kriptografskom modulu

Privatni TSU ključevi PKSCA QTSA zaštićeni su KMS modulima i mogu se koristiti jedino ako su propisno aktivirani.

Nema ograničenja obzirom na format u kojem se privatni ključevi čuvaju u KMS modulima.

### Metoda aktivacije privatnog TSU ključa

Aktivacija privatnih TSU ključeva za PKSCA QTSA sprovodi se pod dualnom kontrolom ovlašćenih osoba sa poverljivom ulogom Administrator sistema i Glavni administrator bezbednosti u PKSCA QTSA. Svaka od ovih ovlašćenih osoba za aktivaciju KMS-a upotrebljava pripadajući tajni PIN.

Jednom aktiviran, privatni ključ ostaje aktiviran bez vremenskog ograničenja.

### Metoda deaktivacije privatnog TSU ključa

Deaktivacija privatnog TSU ključa PKSCA QTSA sprovodi se prema postupcima i uz zadovoljenje zahteva određenih u sertifikacionom dokumentu upotrebljenog KMS modula, pod dualnom kontrolom ovlašćenih osoba sa poverljivom ulogom Administrator sistema i Glavni administrator bezbednosti u PKSCA QTSA.

Deaktivacija privatnih TSU ključeva sprovodi se kada postoji neposredan zahtev za privremenim obustavljanjem aktivnosti sistema, u slučajevima isteka perioda validnosti privatnog ključa, kao i u slučaju opoziva pripadajućeg sertifikata.

Privatni TSU ključ mora se čuvati u zaštićenom obliku i kad je deaktiviran.

### Metoda uništavanja privatnog TSU ključa

Postupak uništavanja privatnog TSU ključa provodi se nakon isteka perioda važenja privatnog TSU ključa, zbog kompromitiranja ili opravdane sumnje u kompromitovanost privatnog ključa, ili zbog prestanka njegovog korišćenja, a sprovode ga ovlašćene osobe sa poverljivim ulogama u PKSCA QTSA, uz minimalno dualnu kontrolu. Postupkom uništavanja privatnog TSU ključa trajno su onesposobljene i sve sigurnosne kopije tog privatnog ključa, tako da ih više nije moguće upotrebiti.

### Ocena kriptografskog modula

Ocena HSM modula sprovodi se sertifikovanjem prema odgovarajućim normama za kriptografske module.

## Ostali vidovi upravljanja parom ključeva

### Arhiviranje javnog ključa

Javni ključevi PKSCA QTSA arhiviraju se u svrhu pružanja dokaza o izdatim elektronskim vremenskim žigovima u sudskim, upravnim i drugim postupcima.

Javni TSU ključevi PKSCA QTSA sistema sastavni su deo pripadajućih PKSCA QTSA sertifikata koji se arhiviraju u skladu sa ovim Praktičnim pravilima.

### Vremenski period važenja PKSCA QTSA sertifikata i korišćenja para TSU ključeva

PKSCA QTSA sertifikat ima period važenja od 5 godine.

Period važenja PKSCA QTSA sertifikata nije duži od vremenskog perioda u kojem se korišćeni kriptografski algoritmi i dužine ključeva smatraju sigurnim za primenu.

Zbog osiguranja kriptografske zaštite izdatih elektronskih vremenskih žigova period važenja privatnog TSU ključa mora biti manji od vremenskog perioda važenja pripadajućeg sertifikata.

Period važenja privatnog TSU ključa PKSCA QTSA servisa definisan ekstenzijom *Private Key Usage Period* u PKSCA QTSA sertifikatu je 3 meseca.

Privatni TSU ključevi PKSCA QTSA ne upotrebljavaju se nakon isteka roka važenja sertifikata, nakon opoziva sertifikata ili nakon isteka perioda važenja privatnog TSU ključa te se u tom slučaju zahtevi za izdavanjem vremenskog žiga odbacuju.

### Upravljanje životnim ciklusom kriptografskih modula

PKSCA QTSA mora proveriti da HSM kriptografski moduli nisu menjani tokom transporta ili tokom skladištenja.

Instalaciju i aktivaciju HSM kriptografskih modula u PKSCA PKI zaštićenom prostoru sprovodi ovlašćeno osoblje PKSCA QTSA koje ima ovlašćenja za izvršavanje operacija upravljanja kriptografskim modulom.

PKSCA QTSA kontinuirano proverava i osigurava da HSM kriptografski moduli rade ispravno.

Na kraju radnog veka HSM kriptografskog modula, privatni ključevi u HSM kriptografskom modulu se uništavaju.

## Aktivacioni podaci

### Generisanje i instalacija aktivacionih podataka

Aktivacioni podaci povezani s privatnim TSU ključem za PKSCA QTSA generišu se i instaliraju prilikom postupka generisanja pripadajućeg privatnog ključa.

### Zaštita aktivacionih podataka

Aktivacioni podaci povezani s privatnim TSU ključem za PKSCA QTSA podeljeni su na upravljačke kartice kriptografskog modula, a zaštićeni su pripadajućim PIN-ovima te se na siguran način čuvaju u PKSCA PKI zaštićenom prostoru.

## Upravljanje informacionom bezbednošću

### Posebni tehnički zahtevi na informacionu bezbednost

Pristup IT sistemu i aplikacijama u PKSCA PKI imaju isključivo ovlašćene osobe nakon autentikacije. Kontrola pristupa operativnim sistemima PKSCA QTSA servera dopušta pristup samo ovlašćenom osoblju sa poverljivim ulogama u PKSCA QTSA.

PKSCA sprovodi odvajanje dužnosti i odgovornosti za poverljive uloge osoblja u PKSCA QTSA, u skladu sa tačkom 5.2.4. ovog dokumenta.

Identifikacija i potvrđivanje identiteta za svaku poverljivu ulogu u PKSCA QTSA sprovodi se korišćenjem odgovarajućih sredstava za autentikaciju.

PKSCA PKI sistem sprovodi kontinuirano praćenje i poseduje alarmni sistem u svrhu detektovanja, beleženja i pravovremenog reagovanja na pokušaje nedozvoljenog pristupa resursima sistema.

Implementiran je sistema zaštite od zlonamernog koda, a zabranjeno je korišćenja neautorizovanog softvera.

## Tehničke kontrole životnog ciklusa

### Kontrole daljeg razvoja sistema

Pri planovima razvoja sistema u kojima učestvuje eksterni izvođač, PKSCA ugovorom sa dobavljačem usluga osigurava bezbednosne principe razvoja sistema.

Analiza bezbednosnih zahteva sprovodi se u fazi dizajna i specifikacije bilo kog projekta razvoja PKSCA PKI sistema, kako bi se osiguralo da je sigurnost ugrađena u informacione tehnologije u svim PKSCA PKI sistemima.

Softver koji se koristi za pružanje usluge izdavanja elektronskih vremenskih žigova potiče iz pouzdanog izvora. Implementacija softvera u produkciji sprovodi se u skladu sa dokumentovanim postupcima upravljanja promenama.

Plan za upravljanje konfiguracijom PKSCA PKI sistema sadrži jasan prikaz trenutnog stanja, popis dokumentacije nastale u sklopu izrade informacionog sistema, mere za osiguranje kvaliteta, procenu rizika, softverski dizajn, sistemski test i definicije kontrolnih mehanizama.

### Kontrole upravljanja bezbednošću

PKSCA sprovodi proveru svih delova sistema za izdavanje elektronskih vremenskih žigova u odnosu na bezbednost, pouzdanost i kvalitet delovanja, a u skladu sa važećim propisima.

U slučaju povrede sigurnosti PKSCA QTSA sistema ili gubitka njegovog integriteta koji može imati značajan uticaj na pružanje usluge od poverenja ili na zaštitu ličnih podataka, PKSCA će u roku od 24 sata o istome obavati nadležno centralno telo državne uprave kao telo nadležno za nadzor kvalifikovanih pružalaca usluga od poverenja a prema potrebi, i druga nadležna tela. U slučaju da gubitak integriteta može imati negativni uiecaj na korisnike usluga od poverenja, PKSCA će o istome bez odlaganja obaveštavati sva pravna i fizička lica na koje povreda sigurnosti može uticati.

### Sigurnosne kontrole životnog ciklusa

PKSCA sprovodi upravljanje promenama u sistemu, kako bi se promene izvodile iz opravdanog razloga i na kontrolisani i formalizovan način.

Integritet sistema za izdavanje elektronskih vremenskih žigova i informacija štiti se antivirusnom zaštitom i upotrebom autorizovanog softvera.

Sprovodi se praćenje raspoloživih kapaciteta PKSCA PKI Sistema, a procenjuje se iskorišćenost postojećih kapaciteta za buduće potrebe sistema, kako bi se pravovremeno planiralo njihovo proširenje.

## Provera mrežne bezbednosti

Sigurnost računarske mreže PKSCA sistema zasnovana je na konceptu podele mreže na mrežne zone različitih nivoa bezbednosti. Mrežne zone dele se zaštitnim mehanizmima koji propuštaju samo neophodan mrežni promet. Na sve sisteme locirane unutar jedne mrežne zone primenjuju se jednake sigurnosne mere.

Pristup i komunikacija između zona je ograničen na autorizovano osoblje sa poverljivim ulogama neophodnim za pružanje usluge. Nepotrebne komunikacije, nalozi, portovi, protokoli i servisi su eksplicitno zabranjeni ili deaktivirani.

Interna računarska mreža PKSCA zaštićena je od neovlašćenog pristupa, uključujući pristup korisnika i trećih strana.

Svi sistemi kritični za pružanje usluga od poverenja smešteni su u PKSCA zaštićenom prostoru. PKSCA QTSA sistem je sigurnosno podešen i ojačan.

## Upotreba vremenskog žiga

Vreme u PKSCA sistemu usklađeno je sa UTC tačnim vremenom.

# SADRŽAJ SERTIFIKATA, LISTA OPOZVANIH SERTIFIKATA I OCSP PROFILI

## Profil sertifikata PKSCA QTSA

Profil sertifikata za PKSCA QTSA sistem usklađen je sa standardima EN 319 411-2 i ETSI EN 319 422.

Sertifikat za PKSCA QTSA servis izdaje PKSCA sertifikaciono telo (CA): PKSCA CLOUD.

### 7.1.1. Broj(evi) verzije

Sertifikati su u skladu sa verzijom 3 prema X.509 specifikaciji.

### 7.1.2. Ekstenzije sertifikata

Dokument sa opisom profila sertifikata dostupan je na internet stranicama PKSCA QTSA repozitoriuma iz tačke 2.2. ovih Praktičnih pravila.

### 7.1.3. Identifikator objekta (OID) algoritama

Algoritmi sa pripadajućim OID identifikatorima za sertifikat PKSCA QTSA sistema prikazani su u Tabeli 4.

|  |  |
| --- | --- |
| **Algoritam** | **OID** |
| sha256WithRSAEncryption | 1.2.840.113549.1.1.11 |
| rsaEncryption | 1.2.840.113549.1.1.1 |

***Tabela 4. Algoritmi s pripadajućim OID identifikatorima***

### 7.1.4. Oblici naziva

Oblici naziva za polje *Subject* u sertifikatu PKSCA QTSA sistema:

|  |  |
| --- | --- |
| commonName (CN) | Time Stamp server |
| organizationUnit | PKS CA |
| organizationName (O) | Privredna komora Srbije |
| countryName (C) | SR |

### 7.1.5. Ograničenja u nazivima

Ekstenzija *Name Constraints* se ne koristi.

### 7.1.6. Identifikator objekta (OID) Praktičnih pravila TSU sertifikata

Ekstenzija *Certificate Policies* TSU sertifikata sadrži PKSCA OID: 1.3.6.1.4.1.31266.10.2.2

### 7.1.7. Upotreba ekstenzije *Policy Constraints*

Ekstenzija *Policy Constraints* se ne koristi.

### 7.1.8. Procesne semantike za kritičnu ekstenziju *Certificate Policies*

Nema odredbi.

## Profil CRL

Profil CRL u skladu sa preporukom IETF RFC 5280.

### Broj(evi) verzije

CRL su u skladu sa verzijom 2 prema X.509 specifikaciji.

### CRL i ekstenzije unosa u CRL

Ekstenzije CRL koje se koriste u CRL listama i u elementima unosa CRL lista koje izdaje PKSCA CLOUD su:

* + - * *cRLNumber,*
			* *AuthorityKeyIdentifier,*
			* *reasonCode.*

Ni jedna od ovih ekstenzija nije postavljena kao kritična.

## OCSP profil

Profil odgovora PKSCA OCSP servisa usklađen je s preporukom IETF RFC 6960 [15].

### Broj(evi) verzije

Profil odgovora PKSCA OCSP servisa usklađen je sa verzijom 1 prema IETF RFC 6960 [15].

### OCSP ekstenzije

Ekstenzije odgovora PKSCA OCSP servisa prikazane su:

* + - * *Nonce*
			* *Extended Revoked Definition.*

Ni jedna od ovih ekstenzija nije postavljena kao kritična.

# PROVERA USKLAĐENOSTI

Nadzor nad radom PKSCA kao kvalifikovanog pružaoca usluga od poverenja regulisan je Zakonom o elektronskoj identifikaciji, elektronskom dokumentu i uslugama od poverenja u elektronskom poslovanju, a sprovodi ga nadležno ministarstvo.

Nadzor nad radom kvalifikovanog pružaoca usluga od poverenja u području prikupljanja, upotrebe i zaštite ličnih podataka potpisnika mogu sprovoditi državna i druga tela određena zakonom i drugim propisima koji uređuju zaštitu ličnih podataka.

Provera usklađenosti obavlja se u cilju potvrđivanja da PKSCA kao kvalifikovani pružalac usluga od poverenja, koje PKSCA pruža, uključujući uslugu izdavanja kvalifikovanih elektronskih vremenskih žigova, ispunjavaju zahteve utvrđene Uredbom (EU) br. 910/2014, Zakonom o elektronskoj identifikaciji, elektronskom dokumentu i uslugama od poverenja u elektronskom poslovanju i standardima ETSI EN 319 401 i ETSI EN 319 421.

## Učestalost ili okolnosti provere usklađenosti

Provere usklađenosti u radu PKSCA su eksterne provere usklađenosti i interne provere usklađenosti.

### 8.1.1. Eksterna provera usklađenosti

Eksterna provera usklađenosti sprovodi se najmanje svaka 24 meseca, u skladu sa zahtevima Uredbe (EU) br. 910/2014 i standardu ETSI EN 319 403.

### 8.1.2. Interna provera usklađenosti

Interna provera usklađenosti sprovodi se pre početka pružanja nove kvalifikovane usluge od poverenja, periodično najmanje svakih 12 meseci, kao i nakon značajnijih promena u radu PKSCA PKI.

## Identitet/kvalifikacije ocenitelja

Eksternu proveru usklađenosti sprovodi telo za ocenjivanje usklađenosti. Osposobljenost tela za ocenjivanje usklađenosti i osposobljenost pripadajućih ocenjivača osigurana je akreditacijom tela za ocenjivanje usklađenosti prema standardu ETSI EN 319 403.

Internu proveru usklađenosti sprovode interni ocenjivači usklađenosti, koji zajedno raspolažu znanjima i razumevanjem:

* + - * odredbi standarda ETSI EN 319 421,
			* PKI oblasti, tehnologije vremenske overe, kao i područja informacione bezbednosti,
			* zakonske regulative iz područja davanja usluga od poverenja.

## Odnos ocenjivača sa telom koje se ocenjuje

Kontrolno telo za ocenjivanje usklađenosti i pripadajući ocenjivači nezavisni su od PKSCA i usluge ocenjivanja Privredne komore Srbije.

Interni ocenjivači usklađenosti ne ocenjuju usklađenost iz sopstvenog delokruga odgovornosti.

# OSTALE POSLOVNE I PRAVNE ODREDBE

## Naknada za usluge

PKSCA, u skladu sa uslovima iz sklopljenog ugovora o pružanju usluge izdavanja elektronskih vremenskih žigova obaveštava korisnike i pouzdajuće strane o naplati usluge. Ukoliko posebnim ugovorom nije drugačije određeno, usluga se naplaćuje u skladu sa cenovnikom PKSCA. Cenovnik svih usluga koje se naplaćuju objavljen je na internet stranicama repozitoriuma iz tačke 2.2. ovih Praktičnih pravila.

PKSCA zadržava usluge izmene cenovnika. Izmene cenovnika objavljuju se na internet stranicama repozitoriuma iz tačke 2.2. ovih Praktičnih pravila.

### 9.1.1. Povraćaj uplaćenih sredstava

Povraćaj uplaćenih sredstava PKSCA isplaćuje korisnicima u slučaju pogrešne uplate ili preplate.

## Finansijska odgovornost

PKSCA kao pružalac usluga od poverenja poseduje finansijsku stabilnost i raspolaže dovoljnim finansijskim sredstvima koja osiguravaju nesmetano pružanje usluga izdavanja vremenskih žigova u skladu sa ovim Praktičnim pravilima.

### Pokrivenost osiguranjem

PKSCA kao pružalac usluga od poverenja ima osiguran rizik od odgovornosti za štete koje nastanu obavljanjem usluga izdavanja elektronskih vremenskih žigova.

PKSCA dodatno osigurava imovinu polisom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda, poplava, eksplozija, udar vozila, pad ili udar letelice, demonstracija, osiguranje opreme, računarske opreme, elektronskih i komunikacijskih uređaja, instalacija i slično.

### Druga sredstva

Nema odredbi.

## Poverljivost poslovnih podataka

### Opseg poverljivih poslovnih podataka

Poverljivi poslovni podaci su svi podaci, u bilo kojem obliku, koje na bilo koji način između sebe razmene učesnici u vezi sa uspostavom i pružanjem usluga izdavanja vremenskih žigova, a koje učesnici označe poverljivim, ili određenom vrstom ili stepenom tajnosti, ili koji usluga prirodi poverljivi jer bi njihovo neovlašćeno otkrivanje moglo prouzrokovati štetu učesniku.

### Podaci koji se ne smatraju poverljivim poslovnim podacima

Poslovni podaci u bilo kojem obliku koje na bilo koji način između sebe razmene učesnici u vezi sa uspostavom i pružanjem usluga izdavanja elektronskih vremenskih žigova, a koje učesnici ne označe poverljivim, ili određenom vrstom ili stepenom tajnosti, ili koji po svojoj prirodi nisu poverljivi, jer se njihovim neovlašćenim otkrivanjem ne bi mogla prouzrokovati šteta učesniku, su podaci koji se ne smatraju poverljivim poslovnim podacima.

### Odgovornost za zaštitu poverljivih poslovnih podataka

Svaki učesnik obavezan je štititi poverljive poslovne podatke iz tačke 9.3.1. ovih Praktičnih pravila, koje je saznao na bilo koji način, u skladu sa propisima koji uređuju zaštitu podataka prema vrsti podatka, odnosno vrsti i stepenu tajnosti podataka. U protivnom odgovara za nastalu štetu.

## Zaštita ličnih podataka

Sklapanjem ugovora o pružanju usluga izdavanja kvalifikovanih elektronskih vremenskih žigova korisnici su saglasni da PKSCA koristi i obrađuje njihove podatke prikupljene u postupku registracije u skladu sa važećom zakonskom regulativom, kao i da su saglasni da je PKSCA ovlašćena da čuva te podatke u trajanju od najmanje 10 godina.

### Plan zaštite ličnih podataka

PKSCA sprovodi tehničke, kadrovske i organizacione mere zaštite ličnih podataka u skladu sa zakonskom regulativom u svrhu zaštite privatnosti osoba i zaštite podataka od moguće zloupotreba, kao i očuvanja tačnosti, potpunosti i ažurnosti ličnih podataka.

Mere zaštite ličnih podataka primenjuju se prilikom razmene ličnih podataka korisnika između PKSCA RA mreže i usluge za izdavanje elektronskih vremenskih žigova, kao i prilikom čuvanja i arhiviranja ličnih podataka korisnika, do njihovog izlučivanja iz arhive i uništavanja.

### Poverljivi lični podaci

U postupku registracije korisnika i nakon toga, PKSCA je ovlašćena da prikuplja lične podatke koji su potrebni za validno utvrđivanje identiteta korisnika, kao i druge podatke potrebne za validno pružanje usluga izdavanja elektronskih vremenskih žigova. Lični podaci koje prikupi PKSCA i koji nisu sadržaj sertifikata, koji se ne prikazuju u javnim evidencijama i/ili registrima koji se za potrebe davanja sluge od poverenja moraju propisano voditi, su poverljivi lični podaci koje PKSCA propisano štiti.

### Lični podaci koji nisu poverljivi

Svi prikupljeni lični podaci smatraju se poverljivima.

### Odgovornost za zaštitu ličnih podataka

PKSCA je odgovorna za zaštitu ličnih podataka prikupljenih u svrhu pružanja usluga izdavanja elektronskih vremenskih žigova.

### Ovlašćenje za korišćenje ličnih podataka

PKSCA je ovlašćena, osim za potrebe ispunjenja zakonskih obaveza, odnosno ugovornih obaveza po ugovoru o pružanju usluga izdavanja kvalifikovanih elektronskih vremenskih žigova, koristiti ili objavljivati lične podatke samo na osnovu pisane saglasnosti korisnika.

### Dostupnost podataka merodavnim telima

PKSCA neće činiti dostupnima podatke iz tačaka 9.3.1. i 9.4.2. ovih Praktičnih pravila, osim u slučajevima propisanim zakonom ili kada to pisano zahteva merodavni sud, upravno ili neko drugo merodavno državno telo.

### Ostale okolnosti objave podataka

Nema odredbi.

## Prava intelektualnog vlasništva

Ovaj dokument Praktičnih pravila kao i druga PKSCA dokumentacija objavljena na internet stranicama repozitoriuma iz tačke 2.2. ovog dokumenta, intelektualno je vlasništvo PKSCA.

PKSCA ne polaže intelektualno vlasništvo na softver koji se koristi u PKSCA PKI, a koji je u vlasništvu trećih strana.

Privatni TSU ključevi i pripadajući TSU sertifikati za PKSCA QTSA sistem, koji se koriste za potpisivanje elektronskih vremenskih žigova, vlasništvo su PKSCA.

## Obaveze učesnika

### Obaveze PKSCA

PKSCA kao kvalifikovani pružalac usluga izdavanja kvalifikovanih elektronskih vremenskih žigova obavezuje se:

* + - * sprovoditi pružanje usluga izdavanja elektronskih vremenskih žigova u skladu s Uredbom (EU) br. 910/2014, Zakonom o elektronskoj identifikaciji, elektronskom dokumentu i uslugama od poverenja u elektronskom poslovanju, standardima i preporukama, ovim Praktičnim pravilima, kao i drugim aktima PKSCA vezanim za obavljanje usluga izdavanja elektronskih vremenskih žigova,
			* izdavati kvalifikovane elektronske vremenske žigove u skladu sa uslugom određenom u tački
	1. ovih Praktičnih pravila,
		+ - osigurati tačnost vremena u izdatim elektronskim vremenskim žigovima u skladu sa tačkom
	2. ovih Praktičnih pravila,
		+ - sprovoditi potpisivanje vremenskog žiga na opremi koja udovoljava zahtevima iz tačke

6.2.1. ovih Praktičnih pravila,

* + - * sprovoditi zahtevane sigurnosne mere za zaštitu prostora i opreme usluge za izdavanje elektronskih vremenskih žigova,
			* osigurati nesmetan rad i maksimalnu raspoloživost usluga izdavanja elektronskih vremenskih žigova u skladu sa najboljom poslovnom praksom,
			* objaviti akte koji mogu biti javno dostupni na internet stranicama repozitoriuma iz tačke 2.2. ovih Praktičnih pravila,
			* obavljati usluge izdavanja elektronskih vremenskih žigova sa pažnjom dobrog stručnjaka,
			* primenjivati u svom poslovanju organizacione i tehničke mere zaštite podataka prikupljenih od korisnika pri ugovaranju korišćenja ove usluge i podatke čuvati kao poslovnu tajnu, a koristiti ih isključivo za potrebe usluga izdavanja elektronskih vremenskih žigova iz opsega ovih Praktičnih pravila i dodatnih usluga od poverenja iz skupa PKSCA PKI usluga (npr. Izdavanje kvalifikovanih elektronskih sertifikata),
			* primenjivati odredbe Zakona o zaštiti ličnih podataka i drugih propisa kojima je uređena zaštita ličnih podataka i tajnost podataka u Republici Srbiji,
			* poštovati intelektualno vlasništvo, licencna i druga prava,
			* rešavati zastoje i greške u radu usluge za izdavanje elektronskih vremenskih žigova u najkraćem mogućem roku,
			* planirati održavanje i dalji razvoj usluge za izdavanje elektronskih vremenskih žigova u skladu sa važećim normama u razvoju tehnologije.

### Obaveze RA

Obaveze PKSCA RA mreže:

* sprovođenje postupka registracije i identifikacije fizičkih i pravnih lica na način propisan ovim dokumentom,
* prosleđivanje celovitih, tačnih i proverenih podataka o subjektima na dalju obradu u PKSCA QTSA,
* čuvanje, arhiviranje i zaštita podataka i dokumentacije na period od najmanje 10 godina,
* osiguravanje od gubitka ili povrede poverljivosti, integriteta i dostupnosti arhiviranih podataka korisnika, na način propisan ovim dokumentom,
* obaveštavanje podnosioca zahteva za korišćenje usluga izdavanja elektronskih vremenskih žigova o javno objavljenim i dostupnim uslovima pružanja usluge izdavanja kvalifikovanih elektronskih vremenskih žigova.

### Obaveze Korisnika

Korisnik je obavezan:

* prilikom predaje zahteva za korišćenje usluga izdavanja elektronskih vremenskih žigova u zahtevu navesti tačne i istinite lične podatke, a odmah obavestiti PKSCA, kao pružaoca usluga, o svakoj promeni tih podataka,
* validirati elektronski potpis PKSCA QTSA servisa na primljenom vremenskom žigu i proveriti važenje PKSCA QTSA sertifikata,
* čuvati privatni ključ i pripadajuće aktivacione podatke koji se odnose na način kojim pristupa usluzi izdavanja elektronskih vremenskih žigova,
* za korišćenje usluge izdavanja vremenskog žiga plaćati PKSCA naknadu u skladu sa cenovnikom usluga iz tačke 9.1. ovih Praktičnih pravila.

Korisnik se obavezuje da neće zahtevati izdavanje vremenskog žiga za one podatke, odnosno elektronske zapise čiji je sadržaj protivan Ustavu Republike Srbije, propisima ili moralu društva. U protivnom, odgovoran je za svu štetu.

Korisnik je, takođe, obavezan sa pažnjom dobrog domaćina, odnosno privrednika, na vreme pratiti i upoznati se sa objavljenim izmenama i/ili dopunama ovih Praktičnih pravila, na internet stranicama PKSCA QTSA repozitoriuma iz tačke 2.2. ovih Praktičnih pravila.

### Obaveze trećih strana

Pre pouzdanja u elektronski vremenski žig treća strana mora:

* + - * obaviti validaciju potpisa elektronskog vremenskog žiga,
			* proveriti na važećoj listi opozvanih sertifikata (CRL), ili korišćenjem *online* PKSCA OCSP servisa opozvanost PKSCA QTSA sertifikata, čijim je privatnim TSU ključem potpisan elektronski vremenski žig.

U slučaju verifikovanja vremenskog žiga nakon isteka vremena važenja PKSCA QTSA sertifikata, treća strana treba da proveri, na internet stranicama PKSCA QTSA repozitoriuma iz tačke 2.2. ovih Praktičnih pravila, da li je privatni TSU ključ bio kompromitovan i da li se kriptografski *hash* algoritam i potpisni kriptografski algoritam i dužina potpisnog TSU ključa kojima je potpisan elektronski vremenski žig, još uvek smatraju sigurnim.

Treća strana obavezna je da se pridržava odredbi ovih Praktičnih pravila.

## Odgovornosti učesnika

### Odgovornosti PKSCA

PKSCA kao kvalifikovani pružalac usluga izdavanja kvalifikovanih vremenskih žigova ima punu odgovornost za pružanje usluga izdavanja elektronskih vremenskih žigova i za ispunjenje svih zahteva propisanih ovim Praktičnim pravilima.

PKSCA ima odgovornost da svi zahtevi koji se odnose na pružanje usluga izdavanja elektronskih vremenskih žigova, što uključuje postupke koje se odnose na izdavanje elektronskih vremenskih žigova, nadzor usluge i sigurnosne kontrole, budu u skladu sa odredbama ovih Praktičnih pravila.

Ova Praktična pravila sastavni su deo ugovora o pružanju usluga izdavanja elektronskih vremenskih žigova koji sklapaju korisnik i PKSCA kao pružalac usluga izdavanja kvalifikovanih elektronskih vremenskih žigova.

### Odgovornosti Korisnika

Korisnik je odgovoran za:

* + - * sadržaj podataka, odnosno elektronskog zapisa za koji traži izdavanje elektronskog vremenskog žiga,
			* korisničku aplikaciju koju koristi za ugradnju vremenskog žiga, kao i da osigura njenu potpunu interoperabilnost sa PKSCA QTSA sistemom,
			* za štetu koju prouzrokuje otkrivanjem svog privatnog ključa i/ili pripadajućih aktivacionih podataka, koji se odnose na sertifikat kojim pristupa usluzi izdavanja elektronskih vremenskih žigova,
			* potpunost i tačnost, odnosno istinitost svih podataka koje je naveo u zahtevu za korišćenje usluga izdavanja elektronskih vremenskih žigova na temelju kojeg je ugovorio korišćenje usluge,
			* nepravilnosti koje su nastale zbog neispunjavanja obaveza utvrđenih u tački 9.6.2. ovih Praktičnih pravila.

Korisniku koji ne postupa u skladu sa preuzetim obavezama može se privremeno ili trajno uskratiti usluga izdavanja elektronskih vremenskih žigova, tako da može izgubiti sva prava proizašla iz ugovora o pružanju usluga izdavanja elektronskih vremenskih žigova.

### Odgovornosti trećih strana

Treća strana koja se, ne poštujući odredbe iz ovih Praktičnih pravila i protivno utvrđenim obavezama iz tačke 9.6.3. ovih Praktičnih pravila, pouzda u nevažeći elektronski vremenski žig, snosi sama sve rizike nastale kao posledica tog pouzdanja u takav elektronski vremenski žig.

Treća strana snosi sve rizike pouzdanja u elektronski vremenski žig, ako zna ili ima razloga smatrati da postoje činjenice koje mogu prouzrokovati ličnu ili poslovnu štetu prouzrokovanu korišćenjem elektronskog vremenskog žiga.

## Odricanje od odgovornosti

PKSCA nije odgovorna za štete, uključujući i indirektne, štete za slučaj nezgode, štete za slučaj nepogode sa posledicama ili za bilo koji gubitak dobiti, gubitak podataka ili druge indirektne štete koje su proizašle iz veze sa uslugama izdavanja elektronskih vremenskih žigova.

PKSCA nije odgovorna za:

* štete prouzrokovane prevarnom ili nemarnom autentikacijom na PKSCA servis za izdavanje elektronskih vremenskih žigova,
* štete nastale kao rezultat neispravnosti i grešaka u softveru i hardveru korisnika i treće strane.

## Ograničenja odgovornosti

Ukupna finansijska odgovornost PKSCA za vremenske žigove izdate prema ovim Prektičnim pravilima, kao i za transakcije obavljene na osnovu poverenja u tako izdate vremenske žigove iznosi najviše 100.000,00 eura u dinarskoj protivvrednosti.

## Naknada štete

Svaki učesnik odgovara oštećenom za štetu koju je počinio zbog nepoštivanja odredbi ovih Praktičnih pravila i važećih relevantnih propisa.

Korisnik PKSCA usluge izdavanja kvalifikovanih elektronskih vremenskih žigova odgovora oštećenom, odnosno svakom drugom učesniku, ako koristi uslugu na osnovu lažnog predstavljanja prilikom prijave na servis za izdavanje elektronskih vremenskih žigova.

Treća strana odgovora oštećenom, odnosno svakom drugom učesniku, ako se pouzda u izdati elektronski vremenski žig bez provere njegove validnosti ili ga koristi protivno svrhama određenim u ovim Opštim pravilima.

PKSCA je odgovorna osobi koja veruje u izdati elektronski vremenski žig i PKSCA QTSA sertifikat samo ako je ta odgovornost jasno uspostavljena ugovorom, ovim Prektičnim pravilima ili zakonskom regulativom Republike Srbije.

## Trajanje i prestanak važenja

### Trajanje

Ovaj dokument važi do stupanja na snagu novog dokumenta Praktičnih pravila, ili do objave prestanka njegovog važenja. Nova verzija dokumenta ili objava prestanka važenja objavljuje se na internet stranicama repozitoriuma iz tačke 2.2. ovih Praktičnih pravila, sa naznačenim danom stupanja na snagu. Novom dokumentu dodeljuje se nova verzija i novi OID, a u njemu će biti naznačene obavljene izmene.

### Prestanak važenja

PKSCA može za pojedine odredbe važećeg dokumenta Praktičnih pravila izraditi izmene i dopune kao što je to navedeno u tački 9.13. ovih Praktičnih pravila.

### Posledice prestanka važenja i nastavak delovanja

Stupanjem na snagu nove verzije dokumenta Praktičnih pravila na sve vremenske žigove izdate od tog dana primenjuju se odredbe iz tog dokumenta.

Novi dokument Praktičnih pravila ne utiče na važenje elektronskih vremenskih žigova koji su izdati primenom prethodnih dokumenata Praktičnih pravila.

## Individualna obaveštenja i komunikacija sa učesnicima

Individualna komunikacija sa učesnicima primarno se sprovodi preko PKSCA on line Helpdesk aplikacije na adresi:

* + - * <http://helpdesk.pksca.rs>

Individualna obaveštenja i druga službena komunikacija u pisanom obliku sprovodi se korišćenjem sledećih podataka:

|  |
| --- |
| **Kontaktni podaci za dostavu dopisa prema PKSCA** |
| Poštanska adresa: | Privredna komora SrbijeSertifikaciono telo Resavska 13 -1511000 Beograd Srbija |
| *E-mail*: | pksca@pks.rs |

## Izmene i dopune

### Procedure izmena i dopuna

Ova Praktična pravila PKSCA revidira po potrebi.

PKSCA može bez obaveštenja unositi tipografske ispravke, promene podataka, kao i druge manje ispravke koje ne utiču bitno na učesnike.

Svi učesnici mogu na adresu PKSCA iz tačke 1.5. ovih Praktičnih pravila poslati dopis sa predlogom za ispravke grešaka, predlog dopuna ili izmena ovog dokumenta. U dopisu se navode podaci osobe koja je poslala predlog promene. PKSCA može prihvatiti, prilagoditi ili odbiti predložene promene nakon razmatranja istih.

### Mehanizmi obaveštavanja i vremenski periodi

Sve izmene i dopune dokumenta Praktičnih pravila objavljuju se u elektronskom obliku na internet stranicama repozitoriuma iz tačke 2.2. ovih Praktičnih pravila.

Nove verzije Praktičnih pravila sa izmenjenim OID-om Praktičnih pravila objavljuju se u elektronskom obliku na internet stranicama repozitoriuma iz tačke 2.2. ovih Praktičnih pravila.

Datum stupanja na snagu izmena i dopuna, kao i novoobjavljenog dokumenta Praktičnih pravila, objavljeno je na naslovnoj strani odgovarajućeg dokumenta, kao i na internet stranicama na kojima je objavljen.

### Okolnosti pod kojima se mora menjati OID

Veće izmene u dokumentu Praktičnih pravila koje mogu uticati na učesnike zahtevaju i izmenu OID-a Praktičnih pravila. Novi OID za novu verziju dokumenta određuje PKSCA.

## Postupak rešavanja sporova

U slučaju spora ili neslaganja između PKSCA i drugih učesnika povodom radnji i/ili postupaka pružanja usluge izdavanja vremenskih žigova uređene ovim Praktičnim pravilima, isti će se nastojati rešiti sporazumno. Ako sporazumno rešenje spora nije moguće, isti će se rešiti pred merodavnim sudom u Beogradu.

## Važeći propisi

Kvalifikovane usluge poverenja iz opsega ovog dokumenta PKSCA pruža u skladu sa odredbama Zakona o elektronskoj identifikaciji, elektronskom dokumentu i uslugama od poverenja u elektronskom poslovanju, kao i standardima ETSI EN 319 401 i ETSI EN 319 421.

## Usklađenost sa primenjivim propisima

Ova Praktična pravila i pružanje usluga izdavanja kvalifikovanih elektronskih vremenskih žigova koje su obuhvaćene ovim Praktičnim pravilima usklađeni su sa propisima iz tačke 9.15. ovih Praktičnih pravila.

Svi učesnici saglasni su sa primenom postojeće zakonske regulative u tumačenju primenjenih odredbi.

## Ostale odredbe

Gde je to moguće, usluga izdavanja kvalifikovanih elektronskih vremenskih žigova koju pruža PKSCA i proizvodi za krajnjeg korisnika koji se koriste pri pružanju ove usluge, dostupni su osobama sa invaliditetom.

PKSCA javno objavljuje ova Praktična pravila, i uslove pružanja usluga izdavanja elektronskih vremenskih žigova.

Pre sklapanja ugovora o pružanju usluga izdavanja kvalifikovanih elektronskih vremenskih žigova korisnici se informišu o uslovima pružanja usluga izdavanja kvalifikovanih elektronskih vremenskih žigova. Prihvatanje uslova pružanja usluga izdavanja kvalifikovanih elektronskih vremenskih žigova preduslov je za izdavanje kvalifikovanih elektronskih vremenskih žigova.

Pre sklapanja ugovora o obavljanju usluga izdavanja vremenskih žigova korisnici se informišu o uslovima pružanja usluga izdavanja kvalifikovanih elektronskih vremenskih žigova

## Predmeti ocenjivanja usklađenosti

Predmeti ocenjivanja usklađenosti obuhvataju sedeća područja pružanja usluga od poverenja:

* + - * celovitost i tačnost dokumentacije,
			* implementiranost zahteva za usluge od poverenja,
			* organizacione procese i procedure,
			* tehničke procese i procedure,
			* implementirane mere informacione bezbednosti,
			* verodostojne sisteme,
			* fizičku sigurnost predmetnih lokacija.

Opis predmetnog ocenjivanja usklađenosti definisan je planom ocenjivanja usklađenosti.

## Mere u slučaju neusklađenosti

Ako je u pružanju kvalifikovane usluge od poverenja utvrđena neusklađenost, PKSCA će preduzeti potrebne korake kako bi otklonila neusklađenost, ako je primenjivo u roku koji je odredilo nadzorno telo.

## Saopštavanje rezultata

Rezultati interne provere usklađenosti poverljive su prirode i PKSCA ih ne objavljuje javno.

U slučaju eksterne provere usklađenosti, PKSCA će dostaviti izveštaj eksternog ocnjivača o proveri usklađenosti nadzornom telu u roku od tri radna dana od momenta prijema izveštaja.

# Istorija dokumenta

|  |  |  |  |
| --- | --- | --- | --- |
| Verzija | Datum | Opis | Autor |
| 1.0 | 25.10.2019. | Radna verzija | Dušan Berdić |
| 2.0 | 28.12.2019. | Finalna verzija | Dušan Berdić |
| 2.1 | 15.01.2020 | Korekcija grešaka | Ivana Božinović Pavlović |

PRIVREDNA KOMORA SRBIJE

02.01-Broj:

28. decembar 2019 godine

B e o g r a d