Praktična pravila rada

za pružanje kvalifikovane usluge izdavanja kvalifikovanog elektronskog vremenskog žiga

OID CPS dokumenta (1.3.6.1.4.1.31266.10.1.7)

- verzija 2.0.-

SADRŽAJ

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

Praktična pravila rada za pružanje kvalifikovane usluge izdavanja kvalifikovanog elektronskog vremenskog žiga

1. UVOD

Sertifikaciono telo Privredne komore Srbije (u nastavku: PKSCA) kao registrovani pružalac usluga od poverenja, pruža kvalifikovanu uslugu izdavanja kvalifikovanog elektronskog vremenskog žiga u skladu sa Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju (Sl. glasnik RS, br. 94/2017; u daljem tekstu - Zakon) i odgovarajućim podzakonskim aktima.

PKSCA pruža kvalifikovanu uslugu izdavanja kvalifikovanog elektronskog vremenskog žiga (u daljem tekstu: usluga izdavanja kvalifikovanog elektronskog vremenskog žiga) u skladu sa zahtevima iz evropskog standarda ETSI EN 319 421 "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" (u daljem tekstu: ETSI EN 319 421), uključujući i zahteve iz drugih standarda na koje pomenuti standard direktno ili indirektno upućuje, odgovarajućim međunarodnim standardima i preporukama, odnosno drugim standardima, dokumentima i preporukama koje se odnose na pružanje usluge kvalifikovanog vremenskog žiga utvrđene Pravilnikom o bližim uslovima za kvalifikovane elektronske vremenske žigove (Službeni glasnik RS, broj 59/2019).

Usluga izdavanja kvalifikovanih elektronskih vremenskih žigova je deo PKI produkcije Sertifikacionog tela PKS, a kvalifikovani elektronski vremenski žigovi koje izdaje mogu se koristiti zajedno sa kvalifikovanim sertifikatima koje izdaje PKSCA.

1.1. Pregled

PKSCA ustanovljava Praktična pravila pružanja kvalifikovane usluge izdavanja kvalifikovanog elektronskog vremenskog žiga (u daljem tekstu: Praktična pravila) u skladu sa Zakonom i Politikom pružanja kvalifikovanih usluga od poverenja PKSCA (u daljem tekstu: CP). Praktična pravila obezbeđuju korisnicima dovoljno informacija na osnovu kojih mogu odlučiti o prihvatanju usluge i o obimu usluge.

Politika pružanja kvalifikovanih usluga od poverenja PKSCA i Praktična pravila rada za pružanje kvalifikovane usluge izdavanja kvalifikovanog elektronskog vremenskog žiga su javni dokumenti.

Praktična pravila rada za pružanje usluge izdavanja kvalifikovanog elektronskog vremenskog žiga definišu pravila i operativne procedure, tj. način na koji pružalac usluge kvalifikovanog vremenskog žiga ispunjava tehničke, organizacione i proceduralne zahteve poslovanja koji su određeni u CP dokumentu.

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

Tehnologija primenjena u usluzi izdavanja vremenskih žigova se zasniva na kriptografiji javnog ključa, X.509 sertifikatima i pouzdanim servisima tačnog vremena.

Sadržaj ovih Praktičnih pravila usklađen je sa sledećim evropskim standardima i tehničkim specifikacijama:

- ETSI EN 319 401 V2.2.0 (2017-08) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers,
- ETSI EN 319 421 V1.0.0 (2015-06) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps,
- ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
- ETSI TS 119 312 V1.2.1 (2017-05) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

Svrha ovih Praktičnih pravila je definisanje i uređivanje pravila i načela prema kojima će postupati PKSCA, korisnici usluge izdavanja kvalifikovanih elektronskih vremenskih žigova (u daljem tekstu: korisnici) i pouzdajuće strane.

Odredbe Praktičnih pravila proističu iz Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju Republike Srbije, Uredbe EU br. 910/2014, kao i standarda i preporuka na koje upućuju pomenuti dokumenti.

Kvalifikovani elektronski vremenski žigovi izdati prema ovim Praktičnim pravilima usklađeni su sa zahtevima standarda ETSI EN 319 421 V1.0.0 (2015-06) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

Identifikaciona oznaka (OID) pružanja usluge kvalifikovanog elektronskog vremenskog žiga izdatog po ovim Praktičnim pravilima je OID: 1.3.6.1.4.1.31266.10.2.3.1.0.4.1 PKSCA kao pružalac usluga izdavanja kvalifikovanih elektronskih vremenskih žigova uključuje OID usluge u sve kvalikovane vremenske žigove koje izdaje.

Struktura ovog dokumenta je zasnovana na standardu IETF RFC 3647 - Internet X.509 Public Key Infrastructure; Certificate Policy and Certification Practices Framework.

1.2. Naziv dokumenta i identifikacija

Praktična pravila definišu konkretne detalje implementacije, pravila i procedure rada PKSCA usluge za izdavanje kvalifikovanih vremenskih žigova (u daljem tekstu PKSCA QTSA).

Ovaj dokument se identifikuje na sledeći način:

- **Naziv:** Praktična pravila rada za pružanje kvalifikovane usluge izdavanja kvalifikovanog elektronskog vremenskog žiga
- **Verzija:** 2.0
- **OID:** 1.3.6.1.4.1.31266.10.1.7
- **Internet adresa na kojoj je dokument objavljen:** http://v3.pksca.rs

Identifikacioni podaci PKSCA su:

PKSCA
Privredna Komora Srbije
Resavska 13-15
11000 Beograd
Srbija

1.3. Učesnici u PKI sistemu

1.3.1. Pružalac usluge izdavanja kvalifikovanih elektronskih vremenskih žigova

PKSCA, kao pružalac kvalifikovanih usluga od poverenja, pruža uslugu izdavanja kvalifikovanih elektronskih vremenskih žigova (PKSCA QTSA).

1.3.1.1. PKS CA Root

Sertifikaciono telo PKS je generisalo samopotpisani PKS CA Root sertifikat, kao i CA sertifikat za njemu podređeno CA telo PKS CA TSA. PKS CA Root ne izdaje sertifikate korisnicima.

Podaci o PKSCA Root CA sertifikatu su dati u dokumentu “Pregled profila sertifikata PKSCA”.

PKSCA Root CA sertifikat dostupan je na internet adresi: http://v3.pksca.rs/certs/PKSCARoot.cer.

1.3.1.2. PKS CA TSA

PKS CA TSA izdaje sertifikate jedinici za izdavanje kvalifikovanog vremeskog žiga (u daljem tekstu: TSU – *Time Stamp Unit*) i sopstvenom OCSP servisu.

Podaci o PKSCA TSA i TSU sertifikatu dati su u dokumentu "Pregled profila sertifikata PKSCA".

PKSCA TSA sertifikat dostupan je na internet adresi: http://v3.pksca.rs/certs/PKSCATSA.cer.

1.3.2. Registraciona tela

Poslovi registracije korisnika za uslugu izdavanja kvalifikovaih elektronskih vremenskih žigova 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 vrše operateri registracionih tela. Poslovima registracije u PKSCA RA mreži upravlja centralni PKSCA RA koji je i centralna komunikaciona tačka PKSCA RA mreže.

PKSCA može odrediti i drugi odgovarajući način registracije korisnika.

1.3.3. Korisnici

Korisnici PKS QTSA servisa 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.

1.3.4. Pouzdajuće strane

Pouzdajuće 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.

1.3.5. Ostali učesnici

Nije primenljivo.

1.4. Upotreba vremenskih žigova

1.4.1. Dozvoljena upotreba vremenskih žigova

Kvalifikovani elektronski vremenski žigovi izdati od strane PKSCA QTSA mogu se koristiti za bilo koju primenu koja zahteva dokazivanje postojanja podataka u elektronskom obliku u vremenu navedenom u izdatom vremenskom žigu. Kvalifikovani elektronski vremenski žigovi koje izdaje PKSCA QTSA koriste se i za očuvanje dugotrajnosti drugih usluga od poverenja.

1.4.2. Zabranjena upotreba vremenskih žigova

Nije dozvoljena upotreba kvalifikovanih elektronskih vremenskih žigova za podatke, odnosno elektronske zapise čiji je sadržaj u suprotnosti sa Ustavom Republike Srbije, drugim zakonskim propisima ili moralnim normama društva.

1.5. Administracija Praktičnih pravila rada

1.5.1. Organizacija odgovorna za održavanje dokumenta Praktična pravila

PKSCA je odgovorno za izradu i održavanje dokumenta Praktičnih pravila rada za pružanje kvalifikovanih usluga izdavanja kvalifikovanog elektronskog vremenskog žiga.

Izmene sadržaja dokumenta Praktična pravila obavljaju se na osnovu internih predloga i zahteva za usklađivanjem sa zakonskom regulativom i odgovarajućim standardima.

1.5.2. Kontakt osoba

Osoba u PKSCA koja je odgovorna za dokument Praktična pravila je:

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

1.5.3. Osoba koja određuje usaglašenost Praktičnih pravila

Osoba u PKSCA koja je odgovorna da su ova Praktična pravila usaglašena sa Politikom pružanja kvalifikovanih usluga od poverenja PKSCA, je:

mr Dušan Berdić
Privredna Komora Srbije
Resavska 13-15

11000 Beograd, Srbija
Tel.: 011 3304 545
Fax: 011 3304 556
Email: dusan.berdic@pks.rs

1.5.4. Procedura odobravanja Praktičnih pravila

Dokument Praktična pravila se periodično kontroliše i po potrebi ažurira. Internim pravilima se definiše period kontrole ovog dokumenta, koji ne može biti duži od jedne kalendarske godine.

Praktična pravila se mogu analizirati 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 dužine kriptografskih ključeva.

1.6. Definicije i skraćenice

1.6.1. Definicije

U ovom dokumentu se koriste definicije navedene u dokumentu „Politika pružanja kvalifikovanih usluga od poverenja sertifikacionog tela Privredne komore Srbije". Pored toga, uvode se i dodatne definicije:

Elektronski vremenski žig - je zvanično vreme pridruženo podacima u elektronskom obliku kojim se potvrđuje da su ti podaci postojali u tom vremenskom trenutku.

Kvalifikovani elektronski vremenski žig - je elektronski vremenski žig koji ispunjava uslove propisane Zakonom za kvalifikovani elektronski vremenski žig.

Pružalac usluga od poverenja – je pravno lice ili fizičko u svojstvu registrovanog subjekta koje pruža jednu ili više usluga od poverenja.

Pružalac kvalifikovane usluge od poverenja – je pravnolice ili fizičko lice u svojstvu registrovanog subjekta koje pruža jednu ili više kvalifikovanih usluga od poverenja.

Vremenski žig – sinonim za elektronski vremenski žig

Autoritet za izdavanje vremenskih žigova (Time Stamp Authority – TSA) - Pravno ili fizičko lice koje pruža uslugu izdavanja elektronskog vremenskog žiga – sistem za izdavanje vremenskih žigova – skup informaciono-tehnoloških proizvoda i komponenti namenjen da podrži pružanje usluge izdavanja vremenskih žigova.

Jedinica za formiranje vremenskih žigova (Time Stamp Unit – TSU) – Tehnička celina u okviru sistema za izdavanje vremenskih žigova koju čine odgovarajuće hardverske i softverske komponente i koristi se za formiranje kvalifikovanih vremenskih žigova, pri čemu jedna

jedinica za formiranje vremenskih žigova koristi jedan asimetrični privatni ključ za potpisivanje odnosno pečatiranje vremenskih žigova.

UTC - Koordinirano univerzalno vreme - Merenje vremena na bazi sekunde, kako je to definisano prema ITU-R (International Telecommunications Radio Commitłee) preporuci (ITU-R Recommendation TF.460-5).

1.6.2. Skraćenice

U ovom dokumentu koriste se skraćenice navedene u dokumentu „Politika pružanja kvalifikovanih usluga od poverenja sertifikacionog tela Privredne komore Srbije". Pored toga, uvode se i dodatne skraćenice:

TSA (Time-Stamping Authority)	Pravno ili fizičko lice koje izdaje elektronske vremenske pečate
TSU (Time-Stamping Unit)	Jedinica za izradu zapisa vremenskog pečata
UTC (Coordinated Universal Time)	Koordinirano univerzalno vreme
NTP (Network Time Protocol)	Mrežni vremenski protokol

2. ODGOVORNOST ZA PUBLIKOVANJE I REPOZITORIJUM

2.1. Identifikacija tela koje vodi repozitorijum

PKS je odgovorna za publikovanje informacija u vezi pružanja kvalifikovanih usluga od poverenja i elektronskih sertifikata koje izdaje na online repozitorijumu. U okviru PKS, PKSCA je odgovorno za funkcionisanje repozitoriuma, kao i za objavljivanje dokumenata i informacija na repozitorijumu. PKS zadržava pravo da publikuje pomenute informacije i na repozitorijumu neke treće strane ukoliko je to pogodno.

PKSCA održava online repozitorijum dokumenata u kojima se objavljuju informacije o politikama, praktičnim pravilima i procedurama rada.

Sve podatke i dokumentaciju koja se odnosi na pružanje kvalifikovanih usluga od poverenja PKS CA objavljuje na svojoj internet stranici: http://v3.pksca.rs. Internet stranica je javno dostupna 24 sata na dan, 7 dana u nedelji.

Sertifikaciono telo PKS objavljuje sve relevantne informacije iz oblasti svog rada na zvaničnoj internet stranici: http://v3.pksca.rs.

PKSCA ne publikuje interna pravila rada, kao ni bilo koju vrstu poverljivih dokumenata.

2.2. Objavljivanje informacija o izdavanju vremenskih žigova

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

- aktuelna Politika pružanja kvalifikovanih usluga od poverenja PKSCA,
- aktuelna Praktična pravila pružanja usluga izdavanja kvalifikovanog elektronskog vremenskog žiga,
- ranije verzije Praktičnih pravila
- uslovi pružanja usluga izdavanja elektronskih vremenskih žigova
- sertifikat TSU koji PKSCA QTSA koristi pri potpisivanju vremenskih žigova,
- cenovnik usluga izdavanja vremenskih žigova,
- obrazac zahteva za pristupanje PKSCA QTSA servisu,
- aktuelne lokacije PKSCA RA tela,
- korisnička uputstva,
- obaveštenja korisnicima vezane za pružanje usluga izdavanja vremenskih žigova,
- ostale informacije vezane za rad PKSCA QTSA.

Javno objavljeni sadržaj PKSCA repozitorijuma dostupan je na internet adresi: http://v3.pksca.rs/.

2.3. Vreme ili učestalost objavljivanja

PKSCA analizira i ažurira Praktična pravila za pružanje kvalifikovane usluge izdavanja kvalifikovanih elektronskih vremenskih žigova na godišnjem nivou ili prema ukazanoj potrebi. Ažurirana Praktična pravila se, nakon odobrenja, objavljuju na repozitorijumu iz tačke 2.2. ovog dokumenta.

Drugi PKSCA dokumenti i ostale relevantne informacije objavljuju se prema potrebi, nakon odobrenja.

2.4. Kontrole pristupa repozitoriumu

Informacije objavljene na PKSCA repozitoriumu su javno dostupne i pristup njima se ne naplaćuje.

PKSCA uspostavlja kontrole pristupa repozitorijumu u cilju sprečavanja neautorizovanog dodavanja, izmene ili brisanja informacija, kao i zaštite njihovog integriteta i autentičnosti.

Pravo dodavanja, izmene ili brisanja informacija na PKSCA repozitoriumu imaju ovlašćena lica PKSCA.

3. IDENTIFIKACIJA I AUTENTIKACIJA KORISNIKA

3.1. Identifikacija Korisnika

PKSCA QTSA pruža uslugu izdavanja kvalifikovanih elektronskih vremenskih žigova samo registrovanim korisnicima.

Ukoliko korisnik već ima važeći digitalni sertifikat izdat od PKSCA ili od pružalaca usluga od poverenja odobrenih od strane PKSCA kojim će pristupati PKSCA servisu za izdavanje kvalifikovanih elektronskih vremenskih žigova, potrebno je da popuni i potpiše zahtev za PKSCA uslugu izdavanja kvalifikovanih elektronskih vremenskih žigova i da je prosledi u PKSCA. Forma zahteva popunjava se na portalu usluga PKS na internet stranici

http://usluge.pks.rs

Ako korisnik nema odgovarajući elektronski sertifikat, potrebno je da uz zahtev za korišćenje usluge izdavanja kvalifikovanog elektronskog vremenskog žiga zatraži i izdavanje PKSCA elektronskog sertifikata kojim će pristupati ili se registrovati na portal usluga PKS.

Nakon registracije, korisnik sklapa ugovor sa PKSCA o korišćenju PKSCA usluge izdavanja kvalifikovanog elektronskog vremenskog žiga.

3.1.1. Inicijalno utvrđivanje identiteta korisnika

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

Provera podataka koji se prikupljaju u postupku registracije korisnika PKSCA se vrši njihovim upoređivanjem sa podacima iz dostavljene dokumentacije, u skladu sa važećom zakonskom regulativom.

Za korisnike koji poseduju kvalifikovani elektronski sertifikat već je sprovedena identifikacija korisnika, te za korišćenje usluge izdavanja kvalifikovanog elektronskog vremenskog žiga ovi korisnici PKSCA usluga dostavljaju samo zahtev.

3.1.2. Način dostave zahteva

Zahtev se može dostaviti na sledeći način:

- elektronskom dostavom zahteva potpisanog elektronskim potpisom uz korišćenje kvalifikovanog sertifikata, preko portala usluga PKS.
- ličnim podnošenjem u PKSCA RA,

3.1.3. Sklapanje ugovora

Ugovor o pružanju usluge izdavanja kvalifikovanog elektronskog vremenskog žiga je ugovor koji, u skladu uslovima pružanja usluge izdavanja kvalifikovanog elektronskog vremenskog žiga, Praktičnim pravilima za pružanje usluge izdavanja kvalifikovanog elektronskog vremenskog žiga i propisima koji uređuju pružanje usluge izdavanja kvalifikovanog elektronskog vremenskog žiga, sklapaju korisnici i PKSCA kao pružalac usluge.

3.2. Identifikacija i autentikacija na PKSCA QTSA servis

Registrovani korisnici pristupaju usluzi izdavanja kvalifikovanog elektronskog vremenskog žiga preko portala usluga PKS, po pravilu uz autentikaciju kvalifikovanim elektronskim sertifikatom.

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

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

URL adrese za autentikaciju na PKSCA QTSA servis, u zavisnosti od načina autentikacije su:

- autentikacija sertifikatom: http://v3.pksca.rs/tsa,
- autentikacija korisničkim imenom i lozinkom: http://v3.pksca.rs/tsa.

Interni korisnici PKSCA pristupaju servisu za izdavanje vremenskih žigova korišćenjem IP adresnog prostora za korisnike sistema PKSCA.

3.3. Sertifikat jedinice za izradu vremenskog žiga

PKSCA objavljuje javni ključ jedinice za izdavanje vremenskog žiga kao sadržaj sertifikata PKSCA QTSA na repozitorijumu iz tačke 2.2. ovih Praktičnih pravila.

Sertifikat za TSU izdaje PKS CA TSA u skladu sa zahtevima standarda ETSI EN 319 411-2 V2.2.0 (2017-08) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates .

Pre početka izdavanja elektronskih vremenskih žigova PKSCA QTSA učitava TSU sertifikat. Prilikom dobijanja TSU sertifikata, PKSCA QTSA proverava da li je PKS CA TSA ispravno potpisao sertifikat.

3.4. Elektronski vremenski žig

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

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

Za svaki elektronski vremenski žig garantuje se:

- da sadrži identifikacionu oznaku pružanja usluge kvalifikovanog elektronskog vremenskog žiga izdatog po ovim Praktičnim pravilima,
- 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 PKS CA TSA ima sedište,
- identifikator za PKS CA TSA,
- identifikator TSU koji je izdao elektronski vremenski žig.

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

Samo jedan privatni PKSCA QTSA ključ je aktivan istovremeno.

PKSCA QTSA usluga izdavanja kvalifikovanog elektronskog vremenskog žiga podržava zahteve za izdavanje elektronskih vremenskih žigova u skladu sa standardom ETSI EN 319 422 i preporukom IETF RFC 3161.

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

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

Korisnik koji od PKSCA QTSA zahteva izdavanje elektronskog 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 da podržava 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 kvalifikovanih elektronskih vremenskih žigova na zahtev za izdavanje elektronskog vremenskog žiga u skladu je sa standardom ETSI EN 319 422 i tačkom 2.4.2. dokumenta IETF RFC 3161.

3.5. Profil vremenskog žiga

Osnovni podaci o profilu kvalifikovanih elektronskih vremenskih žigova koje izdaje PKSCA QTSA servis dati su u Tabeli 1.

Polje	Vrednost
Version	V1, vrednost = “1“
Policy OID	PKSCA OID: 1.3.6.1.4.1.31266.10.2.3.1.0.3.2
messageImprint	Podržani hash algoritam: sha-256 (OID: 2.16.840.1.101.3.4.2.1)
serialNumber	Ceo broj
genTime	UTC Vreme, odstupanje od 1 s
ordering	FALSE
Nonce	Ceo broj
signatureAlgorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)

Tabela 1. - Osnovni podaci o kvalifikovanom elektronskom vremenskog žigu kojeg izdaje PKSCA QTSA

3.6. Tačnost vremena u izdatim elektronskim vremenskim žigovima

PKSCA kao pružalac usluga izdavanja kvalifikovanih elektronskih vremenskih žigova u obavezi je da obezbedi 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 od +/- 1 s.

PKSCA QTSA neće izdavati vremenske žigove se ako se ustanovi da je vreme koje koristi PKSCA QTSA TSU izvan deklarisane tačnosti.

3.7. Sinhronizacija sata sa UTC

PKSCA QTSA obezbeđuje 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.

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 tačno vreme u UTC formatu.

Korisnicima i pouzdajućim stranama se preporučuje 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.

3.8. Provera validnosti vremenskog žiga

Pouzdajuće strana vrše proveru validnosti elektronskog potpisa PKSCA QTSA servisa u elektronskom vremenskom žigu prema zahtevima standarda ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

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 sertifikatom PKSCA QTSA usluge,
- 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 usluge, odnosno PKSCA kao

kvalifikovanog pružalaca usluga.

3.9. Raspoloživost usluge

PKSCA kao pružalac usluge izdavanja kvalifikovanog elektronskog vremenskog žiga garantuje kontinuiranu dostupnost usluge izdavanja elektronskog vremenskog žiga i uslova pružanja usluge.

3.10. Izdavanje nekvalifikovanih elektronskih vremenskih žigova

PKSCA QTSA servis za izdavanje kvalifikovanih elektronskih vremenskih žigova izdaje samo kvalifikovane elektronske vremenske žigove.

3.11. Transportni protokol za uslugu izdavanja elektronskih vremenskih žigova

PKSCA QTSA servis koristi siguran HTTPS protokol (TLS) - uz klijentsku autentikaciju sertifikatom – *two-way* TLS), ili drugim metodom ako je to predviđeno.

4. OPERATIVNI ZAHTEVI TOKOM ŽIVOTNOG CIKLUSA SERTIFIKATA

4.1. Izdavanje sertifikata

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

4.2. Opoziv i suspenzija sertifikata

Opoziv TSU sertifikata sprovodi se u skladu sa niže navedenim tačkama.

Suspenzija TSU sertifikata nije dozvoljena.

4.2.1. Razlozi za opoziv

TSU 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 TSU 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.

4.2.2. Ko može tražiti opoziv

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

4.2.3. Učestalost izdavanja CRL

CRL se objavljuje odmah po opozivu sertifikata, kao i svaka 24 sata od prethodnog izdavanja CRL.

4.2.4. Maksimalno kašnjenje za CRL

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

4.2.5. Zahtevi na *online* proveru statusa opozvanosti sertifikata

PKSCA TSA 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/tsaocsp a upisuje se u ekstenziji *Authority Information Access* svakog sertifikata koje izdaje PKS CA TSA.

4.2.6. Drugi dostupni načini objave opozvanih sertifikata

Nije primenljivo.

4.2.7. Dostupnost usluge

CRL i OCSP servis su dostupni 24 sata na dan, 7 dana u nedelji. U slučaju prestanka rada sistema zbog okolnosti na koje PKSCA ne može da utiče ili uticaja više sile, usluge će biti dostupne u skladu sa planom kontinuiteta poslovanja.

4.3. Kraj korišćenja usluge

Korisnici sklapaju sa PKSCA ugovor o korišćenju usluga izdavanja kvalifikovanih elektronskih vremenskih žigova u kome je precizirano vreme korišćenja usluga. Ugovorne obaveze prestaju istekom, sporazumnim raskidom ili otkazom ugovora.

5. PROVERA SISTEMA, UPRAVLJANJA I RADNIH POSTUPAKA

PKSCA obezbeđuje odgovarajuću zaštitu imovine koja se upotrebljava za pružanje usluge izdavanja kvalifikovanog elektronskog vremenskog žiga 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 kvalifikovanih elektronskih vremenskih žigova, kao i postupci provere tog sistema, upravljanja i radnih postupaka u PKSCA, interne su prirode i njihovi detalji se ne objavljuju javno.

5.1. Mere fizičke zaštite

PKSCA, kao pružalac kvalifikovanih usluga od poverenja, primenjuje mere fizičke zaštite PKSCA QTSA sistema sa ciljem minimizacije rizika vezanih za fizičku bezbednost, u skladu sa poslovnom politikom PKSCA, važećom zakonskom regulativom i međunarodnim preporukama.

5.1.1. Lokacije objekta

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

Bezbedni prostori i podprostori u kojima se nalaze komponente PKSCA QTSA sistema u daljnjem tekstu nazivaju se zajedničkim nazivom PKSCA zaštićeni prostor.

5.1.2. Fizički pristup

Fizički pristup PKSCA QTSA sistemu u PKSCA zaštićenom prostoru ostvaruje se uz kontrolu ulaza ovlašćeih osoba PKSCA, a u skladu s njihovim ulogama i ovlašćenjima, na osnovu internih pravila koja regulišu pristup u zaštićenu zonu.

Osobama koje nemaju ovlašćenje za fizički pristup PKSCA QTSA sistemu, pristup je dozvoljen samo u pratnji i uz neprekidni nadzor ovlašćenih osoba PKSCA i uz njihovu kontrolu, u skladu sa internim pravilima PKSCA.

O svakom pristupu PKSCA QTSA sistemima vodi se evidencija.

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

Fizički pristup podacima registrovanih korisnika koje prikuplja RA mreža imaju samo ovlašćene osobe PKSCA 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 repozitorijum, 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

Lokacije na kojima se nalaze PKSCA QTSA sistem, PKSCA RA sistem i repozitorium su zaštićene 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 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 zaštitom od poplave. Ovi mediji su zaštićeni od oštećenja, krađe i neovlašćeog pristupa.

5.1.7. Odlaganje otpada

Uređaji i mediji koji sadrže poverljive informacije u elektronskom obliku, a koji više nisu u upotrebi, bezbedno 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.

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

5.2. Organizacione mere zaštite

5.2.1. Poverljive uloge

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

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

Poverljive uloge u PKSCA su: glavni administrator bezbednosti, administrator sistema, operater sistema, sistem evidentičar, operater sertifikacionog tela i operater registracionog tela.

5.2.2. Broj osoba potrebnih za obavljanje aktivnosti

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

Pristup i obavljanje poslova u PKSCA zaštićenom prostoru vrše se isključivo uz istovremenu prisutnost najmanje dve osobe sa poverljivim ulogama.

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

5.2.3. 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 omogućen je samo ovlašćenim osobama u skladu sa nivoom poverenja za ulogu koju obavljaju.

5.2.4. Uloge koje zahtevaju razdvajanje (separaciju) dužnosti

Zbog bezbednosnih zahteva u procesu izdavanja kvalifikovanih elektronskih vremenskih žigova sprovodi se razdvajanje sledećih dužnosti:

- osobi kojoj je dodeljena poverljiva uloga glavnog administratora bezbednosti ili operatera registracionog tela ne dodeljuje se poverljiva uloga sistem evidentičara,
- osobi kojoj je dodeljena poverljiva uloga administratora sistema ne dodeljuje se

poverljiva uloga operatera sertifikacionog tela ili opratera registracionog tela.

5.3. Provere nivoa znanja osoblja

5.3.1. Kvalifikacije, radno iskustvo i zahtevi za proverom nivoa znanja osoblja

Kandidati za radna mesta na poslovima PKSCA 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.

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

5.3.2. Procedure provere prikladnosti osoblja

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

5.3.3. Zahtevi za školovanjem

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

5.3.4. Učestalost i uslovi za obnovu znanja

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

Zaposleni u PKSCA sa poverljivim ulogama imaju obavezu usavršavanja svog znanja i permanentnog edukovanja.

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

5.3.5. Kazne za neovlašćene radnje

Nepridržavanje propisanih mera za ovlašćene osobe, prilikom obavljanja poslova u PKSCA, smatra se povredom radne obveze prema Kolektivnom ugovoru i podleže kaznenim merama koje se izriču u disciplinskom postupku.

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

5.3.6. Zahtevi na spoljne saradnike

Za ugovorene spoljne saradnike koji za PKSCA obavljaju deo usluga iz opsega usluge izdavanja kvalifikovanog elektronskog vremenskog žiga važe isti zahtevi pri radu u PKSCA kao i za stalno zaposlene.

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

5.3.7. 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.

5.4. Upravljanje audit logovima

5.4.1. Tipovi događaja koji se zapisuju

Audit logovi 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,
- detekciju ispada iz sinhronizacije sa UTC vremenom,

Audit logovi sadrže i zapise o bezbednosnim događajima u PKSCA, vezanim za 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.

5.4.2. Učestalost obrade audit logova

Pregledanje audit logova PKSCA QTS sistema obavlja sistem evidentičar. Pregledanje audit logova obavlja se redovno, jednom dnevno radnim danima, kao i u slučaju vanrednih situacija.

Postupak pregleda audit logova obuhvata:

- pregled stavki dnevnika zapisa sistema koje su stvorene nakon poslednjeg pregleda,
- po potrebi, pripremu kratkog izveštaja koji sadrži objašnjenja važnih događaja.

5.4.3. Vremenski period čuvanja audit logova

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

5.4.4. Zaštita audit logova

Audit logovi u PKSCA zaštićeni su tokom vremena čuvanja. Zaštita dnevnika zapisa sistema obuhvata zaštitu zapisa od njihovog neovlašćeog čitanja i otkrivanja, kao i očuvanje integriteta zapisa.

Audit logovi su raspoloživi samo ovlašćenim osobama, na zahtev, a posebno u svrhu pružanja dokaza o vremenskom žigu za potrebe sudskih postupaka.

5.4.5. Sistem prikupljanja revizionih zapisa (unutarnji ili vanjski)

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

5.4.6. Obaveštavanje subjekta uzročnika događaja

U slučaju uočavanja zapisa o značajnom događaju u radu PKSCA 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.

5.4.7. Procena rizika

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

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

Svaku novu kritičnu ranjivost PKSCA će razmotriti u roku od 48 sati od momenta otkrivanja i primeniće utvrđene postupke za datu situaciju.

5.5. Arhiviranje zapisa

5.5.1. Tipovi arhiviranih zapisa

PKSCA arhivira niže navedene podatke koji, u zavisnosti od tipa, mogu biti u elektronskom

i/ili papirnom obliku:

- Praktična pravila pružanja usluge izdavanja kvalifikovanog elektronskog vremenskog žiga,
- Pravilnici o postupcima izdavanja kvalifikovanih elektronskih vremenskih žigova,
- Uslovi pružanja usluge 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,
- Audit logovi 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.

5.5.2. 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.

5.5.3. Zaštita arhive

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

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

5.5.4. Postupci izrade sigurnosnih kopija arhive

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

5.5.5. Sistem prikupljanja arhivskih zapisa (unutarnji ili spoljašni)

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

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

5.5.6. 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.

5.6. Promena TSU ključa

PKSCA osigurava da PKSCA QTSA kontinuirano pruža kvalifikovanu uslugu od poverenja sa svojim validnim parom ključeva i pripadajućim TSU sertifikatom. Iz tog razloga PKSCA će pre isteka TSU sertifikata, generisati novi par TSU ključeva. Takođe, PKSCA će generišeti 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 TSA CA izdaje TSU sertifikat.

PKSCA će o promeni javnog TSU ključa i o novom TSU sertifikatu pravovremeno obavestiti korisnike PKSCA QTSA.

Novi 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 Praktičnim 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 se arhiviraju.

5.7. Oporavak od kompromitacije ili nepogode

5.7.1. Postupci u slučaju incidenta ili kompromitacije

Planom kontinuiteta poslovanja za PKSCA regulisani su postupci u slučaju incidenta ili kompromitacije sistema. Ovi planovi obuhvataju postupke za oporavak sistema i uspostavu bezbednosnih uslova za pružanje usluga izdavanja elektronskih vremenskih žigova.

Plan kontinuiteta poslovanja revidira se jednom godišnje.

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

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

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

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

5.7.3. 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 TSA.

U slučaju nedostupnosti signala pouzdanog izvora UTC vremena, distribuiranog iz referentnog UTC etalona, iz bilo kog razloga, PKSCA QTSA će prestati sa izdavanjem elektronskih vremenskih žigova sve do ponovne uspostave sinhronizacije.

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

U slučaju veće kompromitacije rada PKSCA QTSA ili gubitka sinhronizacije, PKSCA će putem internet stranica PKSCA repozitoriuma za sve korisnike i pouzdajuće strane objaviti informacije sa jasnom identifikacijom 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 sledeće korisnike PKSCA QTSA:

- PKSCA RA mrežu,
- Korisnike,
- Pouzdajuće (treće) strane.

Nakon ustanovljavanja i otklanjanja uzroka kompromitacije TSU ključa, PKSCA će, ukoliko je to moguće, preduzeti mere za sprečavanje ponavljanja takvog događaja. PKSCA će generisati novi par TSU ključeva i novi javni TSU ključ će izdati novi TSU sertifikat. Novi TSU sertifikat biće dostupan korisnicima PKSCA QTSA na način na koji je bio dostupan i prethodni TSU sertifikat, a u skladu sa ovim Praktičnim pravilima.

5.7.4. Mogućnost nastavka poslovanja nakon nepogode

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

5.8. Prestanak rada PKSCA QTSA servisa

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

- obavestiti sve korisnike usluge, pouzdajuće strane i organ državne uprave nadležan za ove poslove, najmanje tri mjeseca pre planiranog prestanka pružanja usluga izdavanja elektronskih vremenskih žigova,

- uložiti sav napor da kod drugog kvalifikovanog pružaoca usluga od poverenja osigura nastavak pružanja usluga izdavanja elektronskih vremenskih žigova i 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 kvalifikovanih 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.

6. TEHNIČKE MERE ZAŠTITE

6.1. Generisanje i instalacija para ključeva

6.1.1. Generisanje para TSU ključeva

PKSCA vrši generisanje para TSU ključeva za PKSCA QTSA servis koristeći kriptografske algoritme za generisanje ključeva koji su uskladjeni sa standardom ETSI TS 119 312.

Par TSU ključeva generiše se u HSM modulu koji zadovoljava zahteve iz tačke 6.2.1. ovih Praktičnih pravila.

PKSCA QTSA sistem sa pripadajućim HSM modulom nalazi se tokom i nakon postupka generisanja para TSU ključeva u PKSCA zaštićenom prostoru, a pristup PKSCA QTSA sistemu dopušten je ovlašćenim licima PKSCA sa poverljivim ulogama.

U postupku generisanja para TSU ključeva učestvuju ovlašćena lica sa poverljivim ulogama u PKSCA QTSA.

O sprovedenom generisanju TSU ključeva vodi se zapisnik.

6.1.2. Dostava javnog TSU ključa korisnicima i trećim stranama

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

6.1.3. Dužina kriptografskih ključeva

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

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

6.1.4. Generisanje i provera kvaliteta parametara javnog ključa

Ključevi koje upotrebljava PKSCA QTSA generišu se u skladnu sa odredbama stantarda ETSI TS 119 312.

6.1.5. Namene ključeva

Privatni TSU ključ koristi se samo za elektronsko pečaćenje elektronskih vremenskih žigova.

Sertifikat za PKSCA QTSA u ekstenziji *Key Usage* ima postavljene vrednosti *digitalSignature* i *nonrepudiation,* a u ekstenziji *extKeyUsage* ima postavljenu vrednost *timeStamping.*

6.2. Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

6.2.1. Standardi i tehničke mere zaštite kriptografskog modula

HSM modul kojim TSU obavlja pečaćenje vremenskog žiga zadovoljava zahteve FIPS 140-2, nivo 3.

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

Upravljanje privatnim TSU ključem od strane više osoba je bezbednosna 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 TSU ključu za pečaćenje.

6.2.3. Bezbedno skladištenje privatnog ključa

Skladištenje privatnih TSU ključeva nije dozvoljeno.

6.2.4. Bezbedno kopiranje privatnog ključa

Bezbedno kopiranje privatnih TSU ključeva vrši se uz minimalno dvostruku kontrolu od strane ovlašćenih lica sa poverljivim ulogama u PKSCA, u prostoru najvišeg nivoa bezbednosti u okvru zaštićenog prostora PKSCA. Privatni TSU ključ se, izvan HSM modula, nalazi isključivo u šifrovanom obliku. On se u tom obliku kopira i čuva u prostoru najvišeg nivoa bezbednosti, u okviru zaštićenog prostora PKSCA, na odvojenim lokacijama.

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

6.2.5. Arhiviranje privatnog ključa

Nije dozvoljeno arhiviranje privatnih TSU ključeva.

6.2.6. Prenos privatnog ključa

Privatni TSU ključ je, kada se nalazi izvan HSM modula, kriptografski zaštićen. Šifrovanje privatnog ključa vrši se uz strogo pridržavanje zahteva navedenih u sertifikacionoj dokumentaciji HSM modula, kako bi se obezbedio ekvivalentan nivo zaštite privatnog ključa kao i kada se nalazi u HSM modulu.

Prenos privatnog ključa vrše samo ovlašćene osobe sa poverljivim ulogama u PKSCA, uz dvostruku kontrolu i unutar PKSCA zaštićenog prostora. Privatni TSU ključevi prenose se iz HSM modula isključivo radi izrade bezbednosne kopije.

Ukoliko se privatni TSU ključ prenosi iz jednog HSM modula u drugi, dozvoljeno je njegovo prenošenje samo u HSM sa istim ili višim nivoom bezbednosti u odnosu na HSM iz koga se prenosi.

6.2.7. Čuvanje privatnog ključa u kriptografskom modulu

Privatni TSU ključevi zaštićeni su HSM modulima i mogu se koristiti jedino ako su propisno aktivirani.

Nema ograničenja vezanih za format u kome se privatni ključevi čuvaju u HSM modulima.

6.2.8. Metoda aktivacije privatnog TSU ključa

Aktivacija privatnih TSU ključeva vrši se uz dvosruku kontrolu ovlašćenih osoba sa poverljivim ulogama administratora sistema i glavnog administratora bezbednosti u PKSCA. Svako od pomenutih ovlašćenih lica za aktivaciju HSM-a upotrebljava upravljačku karticu kriptografskog modula i pripadajući tajni PIN.

Kada se jednom aktivira, privatni ključ ostaje aktiviran u neograničenom vremenskom periodu.

6.2.9. Metoda deaktivacije privatnog TSU ključa

Deaktivacija privatnog TSU ključa vrši se na osnovu postupaka i uz zadovoljenje zahteva navedenih u sertifikacionom dokumentu korišćenog HSM modula, pod dvostrukom kontrolom ovlašćenih lica sa poverljivim ulogama administratora sistema i glavnog administratora bezbednosti u PKSCA.

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

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

6.2.10. Metoda uništavanja privatnog TSU ključa

Postupak uništavanja privatnog TSU ključa sprovodi se nakon isteka roka važenja privatnog TSU ključa, usled kompromitacije ili opravdane sumnje u kompromitaciju privatnog TSU ključa, ili zbog prestanka njegovog korišćenja, a sprovode ga ovlašćene osobe sa poverljivim ulogama u PKSCA, uz minimalno dvostruku kontrolu. Postupkom uništavanja privatnog TSU ključa trajno se onesposobljavaju i sve njegove bezbednosne kopije, tako da njihovo korišćenje više nije moguće.

Uništavanje privatnog TSU ključa vrši se u skladu sa PKSCA internim dokumentima i o njemu se vodi zapisnik.

6.2.11. Ocena kriptografskog modula

Ocena HSM modula vrši se sertifikovanjem prema odgovarajućim standardima za kriptografske module, navedenim u tački 6.2.1. ovog dokumenta.

6.3. Ostali vidovi upravljanja parom ključeva

6.3.1. Arhiviranje javnog ključa

Javni ključevi TSU 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 TSU sertifikata koji se arhiviraju u skladu sa tačkama 5.5.2., 5.5.3. i 5.5.4. ovih Praktičnih pravila.

6.3.2. Vremenski period važenja PKSCA QTSA sertifikata i korišćenja para TSU ključeva

TSU sertifikat ima rok važenja od 5 godina.

Period važenja TSU sertifikata nije duži od vremenskog perioda u kojem se korišćeni kriptografski algoritmi i dužine ključeva smatraju bezbednim 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 je 3 meseca.

Privatni TSU ključevi ne upotrebljavaju se nakon isteka roka važenja sertifikata, nakon opoziva sertifikata ili nakon isteka roka važenja privatnog TSU ključa, pa se u tom slučaju zahtevi za izdavanje elektronskog vremenskog žiga odbacuju.

6.3.3. Upravljanje životnim ciklusom kriptografskih modula

PKSCA mora da izvrši proveru i ustanovi da HSM kriptografski moduli nisu modifikovani tokom transporta ili skladištenja.

Instalaciju i aktivaciju HSM kriptografskih modula u PKSCA zaštićenom prostoru vrše ovlašćena lica PKSCA sa poverljivim ulogama koja imaju parvo da izvršavaju operacije upravljanja kriptografskim modulom.

PKSCA kontinuirano proverava i obezbeđuje da HSM kriptografski moduli rade ispravno.

Nakon isteka radnog veka HSM kriptografskog modula, privatni ključevi u HSM kriptografskom modulu se uništavaju.

6.4. Aktivacioni podaci

6.4.1. Generisanje i instalacija aktivacionih podataka

Aktivacioni podaci povezani s privatnim TSU ključem generišu se i instaliraju tokom postupka generisanja odgovarajućeg privatnog ključa.

6.4.2. Zaštita aktivacionih podataka

Aktivacioni podaci povezani s privatnim TSU ključem se nalaze na upravljačkim karticama kriptografskog modula, a zaštićeni su odgovarajućim PIN-ovima. Upravljačke kartice kriptografskog modula se na bezbedan način čuvaju u PKSCA zaštićenom prostoru.

6.5. Upravljanje informacionom bezbednošću

6.5.1. Posebni tehnički zahtevi za informacionu bezbednost

Pristup IT sistemu i aplikacijama u PKSCA imaju isključivo ovlašćena lica nakon autentikacije. Kontrola pristupa operativnim sistemima PKSCA QTSA servera dopušta pristup samo ovlašćenim licima sa poverljivim ulogama u PKSCA.

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

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

PKSCA vrši neprekidno praćenje pristupa sistemu i poseduje alarmni sistem u svrhu detektovanja, evidentiranja i pravovremenog reagovanja na pokušaje nedozvoljenog pristupa resursima sistema.

Na informacionom sistemu PKSCA implementirana je zaštita od malicioznog softvera.

Korišćenje neautorizovanog softvera u PKSCA je zabranjeno.

6.5.2. Ocena informacione bezbednosti

PKSCA ima uspostavljen sistem upravljanja informacionom bezbednošću usklađen sa odredbama Zakona o informacionoj bezbednosti Republike Srbije (Sl. glasnik RS, br. 6/2016, 94/2017 i 77/2019) i podzakonskim aktima koji iz njega proističu. Usklađenost sistema upravljanja informacionononom bezbednošću proverava se periodično od strane nadležnog ministarstva.

6.6. Tehničke bezbednosne mere tokom životnog ciklusa

6.6.1. Bezbednosne mere tokom razvoja sistema

Analiza bezbednosnih zahteva sprovodi se u fazi dizajna i specifikacije bilo kog projekta razvoja PKSCA PKI sistema, kako bi se garantovalo da su bezbednosni mehanizmi ugrađeni u informacione tehnologije u svim PKSCA PKI sistemima.

Ukoliko je planovima razvoja sistema predviđeno učešće eksternog izvođača, PKSCA ugovorom sa dobavljačem dobara ili usluga osigurava bezbednosne principe razvoja sistema.

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 izmenama.

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

6.6.2. Mere za upravljanja bezbednošću

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

U slučaju narušavanja bezbednosti 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 obavestiti telo državne uprave nadležno za nadzor pružalaca kvalifikovanih usluga od poverenja, a, prema potrebi, i druga nadležna tela. Ukoliko se ustanovi da gubitak integriteta može imati negativan uticaj na korisnike usluga od poverenja, PKSCA će o tome bez odlaganja obavestiti sva pravna i fizička lica na koje se narušavanje bezbednosti odnosi.

6.6.3. Bezbednosne mere životnog ciklusa

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

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

PKSCA prati raspoložive kapacitete PKI sistema, procenjuje iskorišćenost postojećih kapaciteta i neophodne kapacitete za buduće potrebe sistema, kako bi se pravovremeno planiralo njihovo proširenje.

6.7. Bezbednosne mere u računarskoj mreži

Bezbednost računarske mreže PKSCA sistema zasnovana je na konceptu segmentranja mreže na mrežne zone različitih nivoa bezbednosti. Mrežne zone su odvojene zaštitnim barijerama koje propuštaju samo neophodan mrežni saobraćaj. Na sve sisteme unutar jedne mrežne zone primenjuju se iste bezbednosne mere.

Pristup mrežnim zonama i komunikacija između zona je ograničena na ovlašćena lica PKSCA 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 neovlašćeog pristupa, uključujući pristup korisnika i trećih strana.

Svi kritični sistemi za pružanje usluga od poverenja smešteni su u PKSCA zaštićenom prostoru.

Mrežne komponente PKSCA sistema se čuvaju u fizički i logički bezbednom okruženju. Usaglašenost njihove konfiguracije se periodično proverava.

6.8. Upotreba vremenskog žiga

Vreme u PKSCA sistemu je usklađeno sa UTC tačnim vremenom. Audit logovi PKSCA QTSA sistema sadrže tačan podatak o datumu i vremenu njihovog nastanka, uz odstupanje manje od +/- 1 s.

7. SADRŽAJ SERTIFIKATA, LISTA OPOZVANIH SERTIFIKATA I OCSP PROFILI

7.1. Profil sertifikata PKSCA QTSA

TSU sertifikat izdaje PKS CA TSA sertifikaciono telo.

Profil TSU sertifikata je usklađen sa standardima EN 319 411-2 i ETSI EN 319 422.

7.1.1. Verzije sertifikata

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

7.1.2. Osnovna polja i ekstenzije sertifikata

Detaljan opis profila PKS CA TSA i TSU sertifikata, sa pripadajućim osnovnim poljima i ekstenzijama, dat je u dokumentu "Pregled profila sertifikata PKSCA" koji se nalazi na internet stranici repozitorijuma iz tačke 2.2. ovog dokumenta.

7.1.3. Identifikator objekta (OID) algoritama

Algoritmi sa pripadajućim OID identifikatorima za TSU sertifikat PKSCA QTSA sistema prikazani su u sledećoj tabeli:

Algoritam	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

Tabela 2. - Algoritmi s pripadajućim OID identifikatorima

7.1.4. Oblici naziva

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

commonName (CN)	PKSCA QTSA + redni broj izdatog sertifikata
organizationName (O)	Privredna komora Srbije
Organizational Unit	PKS CA
countryName (C)	RS

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: 1.3.6.1.4.1.31266.10.2.3.1.0.3.2.

7.1.7. Upotreba ekstenzije *Policy Constraints*

Ekstenzija *Policy Constraints* se ne koristi.

7.1.8. Procesne semantike za kritičnu ekstenziju *Certificate Policies*

Nije primenljivo.

7.2. Profil CRL

Profil CRL u skladu sa preporukom IETF RFC 5280.

7.2.1. Broj(evi) verzije

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

7.2.2. CRL i ekstenzije unosa u CRL

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

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

Ni jedna od ovih ekstenzija nije postavljena kao kritična.

7.3. OCSP profil

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

7.3.1. Broj(evi) verzije

Profil odgovora PKSCA OCSP servisa sukladan je verziji 1 prema IETF RFC 6960.

7.3.2. OCSP ekstenzije

Ekstenzije odgovora PKSCA OCSP servisa prikazane su:

- *Nonce*
- *Extended Revoked Definition.*

Ni jedna od ovih ekstenzija nije postavljena kao kritična.

8. PROVERA USAGLAŠENOSTI

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

Nadzor nad radom pružaoca kvalifikovanih usluga od poverenja u području prikupljanja, upotrebe i zaštite ličnih podataka korisnika sprovode državna i druga tela određena zakonom i drugim propisima koji uređuju zaštitu ličnih podataka.

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

8.1. Učestalost ili okolnosti provere usaglašenosti

Provere usaglašenosti rada PKSCA mogu biti eksterne i interne.

8.1.1. Eksterna provera usaglašenosti

Eksterna provera usaglašenosti sprovodi se najmanje jednom na svaka 24 meseca, u skladu sa zahtevima Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju.

8.1.2. Interna provera usaglašenosti

Interna provera usaglašenosti sprovodi se pre početka pružanja nove kvalifikovane usluge od poverenja i periodično, najmanje jednom u toku kalendarske godine, kao i nakon značajnijih promena u radu PKSCA PKI.

8.2. Identitet/kvalifikacije ocenjivača

Eksternu proveru usaglašenosti sprovodi telo za ocenjivanje usaglašenosti. Osposobljenost tela za ocenjivanje usaglašenosti i osposobljenost pripadajućih ocenjivača garantuje se akreditacijom tela za ocenjivanje usaglašenosti.

Internu proveru usaglašenosti vrše interni ocenjivači, koji raspolažu znanjima i razumevanjem:

- odredbi standarda ETSI EN 319 421,
- PKI oblasti, tehnologije vremenskog žiga, kao i područja informacione bezbednosti,
- zakonske regulative iz područja pružanja usluga od poverenja.

8.3. Odnos ocenivača sa telom koje se ocjenjuje

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

Interni ocenjivači usaglašenosti ne ocenjuju usaglašenost iz sopstvenog delokruga odgovornosti.

8.4. Predmet ocjenjivanja usaglašenosti

Predmet ocenjivanja usaglašenosti su sledeća područja pružanja usluga od poverenja:

- celovitost i tačnost dokumentacije,
- implementacija zahteva za usluge od poverenja,
- organizacioni procesi i procedure,
- tehnički procesi i procedure,
- implementirane mere informacione bezbednosti,
- fizička bezbednost.

Opis predmetnog ocenjivanja usaglašenosti definisan je planom ocenjivanja usaglašenosti.

8.5. Mere u slučaju neusaglašenosti

Ukoliko je u pružanju kvalifikovane usluge od poverenja utvrđena neusaglašenost, PKSCA će preduzeti potrebne korake kako bi se ona otklonila, ako je to moguće - u roku koji je odredilo nadzorno telo.

8.6. Objavljivanje rezultata

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

U slučaju eksterne provere usaglašenosti, PKSCA će dostaviti izvještaj eksternog ocenjivača o proveri usaglašenosti nadzornom telu u roku od tri radna dana od momenta prijema izveštaja.

9. OSTALE POSLOVNE I PRAVNE ODREDBE

9.1. Naknada za usluge

PKSCA, u skladu sa uslovima iz sklopljenog ugovora o pružanju usluge izdavanja kvalifikovanih 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 stranici repozitoriuma iz tačke 2.2. ovih Praktičnih pravila.

PKSCA zadržava pravo izmene cenovnika. Izmene cenovnika objavljuju se na internet stranici repozitoriuma iz tačke 2.2. ovog dokumenta.

9.1.1. Povratak uplaćenih sredstava

PKSCA vrši povratak uplaćenih sredstava u slučaju pogrešne uplate ili preplate.

9.2. 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 dokumentom.

9.2.1. 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, udara vozila, pada ili udara letelice, demonstracija, osiguranje opreme, računarske opreme, elektronskih i komunikacijskih uređaja, instalacija i slično.

9.2.2. Ostala sredstva

Nije primenljivo.

9.3. Poverljivost poslovnih podataka

9.3.1. Opseg poverljivih poslovnih podataka

Poverljivi poslovni podaci su svi podaci, u bilo kom obliku, koje na bilo koji način između sebe razmene učesnici u uspostavi i pružanju usluga izdavanja vremenskih žigova, koji su označeni kao poverljivi, ili određenim stepenom tajnosti, ili koji su po prirodi poverljivi jer bi njihovo neovlašćeno otkrivanje moglo prouzrokovati štetu učesniku.

9.3.2. Podaci koji se ne smatraju poverljivim poslovnim podacima

Poslovni podaci, u bilo kom obliku, koje na bilo koji način između sebe razmene učesnici u uspostavi i pružanju usluga izdavanja elektronskih vremenskih žigova, a koje učesnici ne označe poverljivim, ili određenim 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.

9.3.3. Odgovornost za zaštitu poverljivih poslovnih podataka

Svaki učesnik u pružanju usluge izdavanja vremenskih žigova je dužan da štiti poverljive poslovne podatke iz tačke 9.3.1. ovog dokumenta, bez obzira na način na koji je do njih došao, u skladu sa propisima koji uređuju zaštitu tajnih podataka.

9.4. Zaštita ličnih podataka

PKSCA posvećuje pažnju zaštiti ličnih podataka koje prikuplja, skladišti i upotrebljava u svrhu pružanja usluga od poverenja i sa ličnim podacima postupa u skladu sa Zakonom o zaštiti podataka o ličnosti (Službeni glasnik RS, br. 87/2019) i Uredbom EU 2016/679.

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.

9.4.1. 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 zloupotrebe, 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 sistema za izdavanje kvalifikovanih elektronskih vremenskih žigova, kao i prilikom čuvanja i arhiviranja ličnih podataka korisnika, do njihovog izlučivanja iz arhive i uništavanja.

9.4.2. Poverljivi lični podaci

U postupku registracije korisnika i nakon toga, PKSCA je ovlašćena da prikuplja lične podatke koji su potrebni za pouzdano utvrđivanje identiteta korisnika, kao i druge podatke potrebne za validno pružanje usluga izdavanja kvalifikovanih elektronskih vremenskih žigova. Lični podaci koje prikupi PKSCA, a koji nisu sadržaj sertifikata, koji se ne prikazuju u javnim

evidencijama i/ili registrima vođenim za potrebe pružanja usluge od poverenja su poverljivi lični podaci koje PKSCA štiti na propisani način.

9.4.3. Lični podaci koji nisu poverljivi

Svi prikupljeni lični podaci smatraju se poverljivim.

9.4.4. Odgovornost za zaštitu ličnih podataka

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

9.4.5. Ovlašćenje za korištenje ličnih podataka

PKSCA je ovlašćeno, osim za potrebe ispunjenja zakonskih obveza, odnosno ugovornih obveza po ugovoru o pružanju usluga izdavanja kvalifikovanih elektronskih vremenskih žigova, da koristi ili objavljuje lične podatke samo na osnovu pismene saglasnosti korisnika.

9.4.6. Dostupnost podataka nadležnim telima

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

9.4.7. Ostale okolnosti objave podataka

Nije primenljivo.

9.5. Prava intelektualnog vlasništva

Praktična pravila, kao i druga PKSCA dokumentacija objavljena na internet stranici repozitoriuma iz tačke 2.2. ovog dokumenta, intelektualno je vlasništvo PKSCA.

PKSCA ne polaže pravo intelektualnog vlasništva na softver koji se koristi u PKSCA, a koji je u vlasništvu trećih strana.

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

9.6. Obveze učesnika

9.6.1. Obveze PKSCA

PKSCA se, kao pružalac kvalifikovane usluge izdavanja kvalifikovanih elektronskih vremenskih žigova, obavezuje da:

- sprovodi pružanje usluga izdavanja kvalifikovanih elektronskih vremenskih žigova u skladu sa, Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, Uredbom (EU) br. 910/2014, standardima i preporukama, ovim Praktičnim pravilima, kao i drugim aktima PKSCA vezanim za obavljanje usluga izdavanja elektronskih vremenskih žigova,
- izdaje kvalifikovane elektronske vremenske žigove u skladu sa profilom određenim u tački 3.5. Praktičnih pravila,
- obezbedi tačnost vremena u izdatim kvalifikovanim elektronskim vremenskim žigovima u skladu sa tačkom 3.6. Praktičnih pravila,
- sprovodi potpisivanje kvalifikovanog elektronskog vremenskog žiga na opremi koja zadovoljava zahteve iz tačke 6.2.1. Praktičnih pravila,
- sprovodi zahtevane bezbednosne mere za zaštitu prostora i opreme sistema za izdavanje kvalifikovanih elektronskih vremenskih žigova,
- osigura nesmetan rad i maksimalnu raspoloživost usluga izdavanja kvalifikovanih elektronskih vremenskih žigova u skladu sa najboljom poslovnom praksom,
- objavi akte koji mogu biti javno dostupni na internet stranicama repozitoriuma iz tačke 2.2. ovih Praktičnih pravila,
- obavi usluge izdavanja kvalifikovanih elektronskih vremenskih žigova sa pažnjom dobrog stručnjaka,
- primenjuje u svom poslovanju organizacione i tehničke mere zaštite podataka prikupljenih od korisnika pri ugovaranju korišćenja ove usluge i te podatke čuva kao poslovnu tajnu, a da ih koristiti isključivo za potrebe usluga izdavanja kvalifikovanih elektronskih vremenskih žigova iz opsega ovih Praktičnih pravila i dodatnih usluga od poverenja iz skupa PKSCA usluga od poverenja,
- primenjuje odredbe Zakona o zaštiti ličnih podataka i drugih propisa kojima je uređena zaštita ličnih podataka i tajnost podataka u Republici Srbiji,
- poštuje intelektualno vlasništvo, licencna i druga prava,
- rešava zastoje i greške u radu sistema za izdavanje kvalifikovanih elektronskih vremenskih žigova u najkraćem mogućem roku,
- planira održavanje i dalji razvoj sistema za izdavanje kvalifikovanih elektronskih vremenskih žigova u skladu sa važećim standardima i razvojem tehnologije.

9.6.2. Obaveze RA

Obaveze PKSCA RA mreže su:

- sprovođenje postupka registracije i identifikacije fizičkih i pravnih lica na način propisan ovim dokumentom,
- prosleđivanje celovitih, tačnih i proverenih podataka o korisnicima na dalju obradu u PKSCA QTSA,
- čuvanje, arhiviranje i zaštita podataka i dokumentacije u periodu 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.

9.6.3. Obaveze Korisnika

Korisnik je dužan da:

- prilikom predaje zahteva za korištenje usluga izdavanja kvalifikovanih elektronskih vremenskih žigova u zahtevu navede istinite lične podatke, a o promeni tih podataka odmah obavesti PKSCA,
- validira elektronski potpis PKSCA QTSA servisa na primljenom elektronskom vremenskom žigu i proveri važenje TSU sertifikata,
- čuva privatni ključ i pripadajuće aktivacione podatke koji se odnose na način kojim pristupa usluzi izdavanja elektronskih vremenskih žigova,
- za korišćenje usluge izdavanja vremenskog žiga plati naknadu PKSCA u skladu sa cenovnikom usluga iz tačke 9.1. ovih Praktičnih pravila.

Korisnik se obvezuje da neće zahtevati izdavanje kvalifikovanog elektronskog vremenskog žiga za one podatke, odnosno elektronske zapise čiji je sadržaj u suprotnosti sa Ustavom Republike Srbije, propisima ili moralnim normama društva.

Korisnik se, takođe, obvezuje da prati i upoznaje se sa objavljenim izmenama i/ili dopunama ovih Praktičnih pravila, na internet stranicama PKSCA repozitorijuma iz tačke 2.2. ovih Praktičnih pravila.

9.6.4. Obaveze trećih strana

Pre pouzdanja u kvalifikovani elektronski vremenski žig treća strana mora da:

- obaviti validaciju potpisa kvalifikovanog elektronskog vremenskog žiga,
- proveriti opozvanost TSIU sertifikata, na važećoj listi opozvanih sertifikata (CRL), ili korišćenjem online PKSCA OCSP servisa.

U slučaju provere elektronskog vremenskog žiga nakon isteka vremena važenja TSU 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 kriptografski algoritam za pečaćenje, kao i dužina TSU ključa kojima je pečaćen kvalifikovani elektronski vremenski žig, još uvek smatraju bezbednim.

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

9.7. Odgovornosti učesnika

9.7.1. Odgovornosti PKSCA

PKSCA kao pružalac kvalifikovanih 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 kvalifikovanih elektronskih vremenskih žigova, što uključuje postupke koje se odnose na izdavanje kvalifikovanih elektronskih vremenskih žigova, nadzor sistema i sigurnosne kontrole, budu u skladu sa odredbama ovih Praktičnih pravila.

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

9.7.2. Odgovornosti Korisnika

Korisnik je odgovoran za:

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

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

9.7.3. Odgovornosti trećih strana

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

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

9.8. Odricanje od odgovornosti

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

PKSCA nije odgovorna za:

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

9.9. Ograničenja odgovornosti

Ukupna finansijska odgovornost PKSCA za kvalifikovane elektronske 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.

9.10. Naknada štete

Svaki učesnik odgovara oštećenom za štetu koju je počinio zbog nepoštovanja 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 kvalifikovani elektronski vremenski žig bez provere njegove validnosti ili ga koristi protivno svrhama određenim u ovim Praktičnim pravilima.

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

9.11. Trajanje i prestanak važenja

9.11.1. 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.

9.11.2. 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.

9.11.3. Posledice prestanka važenja i nastavak delovanja

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

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

9.12. Individualna obaveštenja i komunikacija sa učesnicima

Individualna komunikacija sa učesnicima primarno se provodi preko PKSCA on line Helpdesk aplikacije na adresi: http://helpdesk.pksca.rs

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

Kontaktni podaci za dostavu dopisa prema PKSCA	
Poštanska adresa:	Privredna komora Srbije Sertifikaciono telo Resavska 13 -15 11000 Beograd Srbija
E-mail:	pksca@pks.rs

9.13. Izmene i dopune

9.13.1. Procedure izmena i dopuna

Ova Praktična pravila PKSCA revidira po potrebi, a najmanje jednom u 12 meseci.

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

Svi učesnici mogu na kontakt 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 kontakt podaci osobe koja je poslala predlog izmene. PKSCA može prihvatiti, prilagoditi ili odbiti predložene ismene, nakon razmatranja istih.

9.13.2. Mehanizmi obaveštavanja i vremenski periodi

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

Nove verzije Praktičnih pravila sa izmijenjenim 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 ili novog dokumenta Praktičnih pravila naznačeni su na njegovoj naslovnoj strani kao i na internet stranicama na kojima je objavljen.

9.13.3. Okolnosti pod kojima se mora mijenjati 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.

9.14. 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 nadležnim sudom u Beogradu.

9.15. Važeći propisi

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

9.16. Usklađenost sa važećim propisima

Ova Praktična pravila i pružanje usluga izdavanja kvalifikovanih elektronskih vremenskih žigova obuhvaćenih ovim Praktičnim pravilima, usklađeni su sa propisima iz tačke 9.15.

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

9.17. Ostale odredbe

Usluga izdavanja kvalifikovanih elektronskih vremenskih žigova i proizvodi za krajnjeg korisnika koji se koriste pri pružanju ove usluge, gde je to moguće, dostupni su osobama sa invaliditetom.

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

Korisnici se, pre sklapanja ugovora o pružanju usluga izdavanja kvalifikovanih elektronskih vremenskih žigova, 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.

10. Istorija dokumenta

Verzija	Datum	Opis	Autor
1.0	20.04.2021.	Radna verzija	Dušan Berdić
2.0	07.06.2021.	Radna verzija	Jelena Radić

11.Odobrenje dokumenata

Ime i prezime	Radno mesto	Potpis	Datum
Dušan Berdić	Rukovodilac CA		07.06.2021.

PRIVREDNA KOMORA SRBIJE

mr Dušan Berdić

Sertifikaciono telo