**Praktična pravila rada**

**za pružanje usluge izdavanja kvalifikovanog elektronskog sertifikata za elektronski potpis u oblaku i kvalifikovanog elektronskog sertifikata za elektronski pečat u oblaku**

CPS (Certificate Practice Statement)

OID CPS dokumenta (1.3.6.1.4.1.31266.10.1.2)

- verzija 2.0.-

Decembar 2019.

Contents

[1. Uvod i pregled osnovnih pretpostavki 8](#_Toc23412909)

[1.1. Pregled osnovnih pretpostavki 8](#_Toc23412910)

[1.2. Ime dokumenta i identifikacija 10](#_Toc23412911)

[1.3. Korisnici usluga PKSCA QTSA 10](#_Toc23412912)

[1.3.1. Pružalac usluga izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata 10](#_Toc23412913)

[1.3.2. Korisnici 12](#_Toc23412914)

[1.3.3. Registraciona tela 12](#_Toc23412915)

[1.4. Upotreba kvalifikovanog elektronskog sertifikata 13](#_Toc23412916)

[1.4.2. Zabrane upotrebe kvalifikovanog elektronskog sertifikata 13](#_Toc23412917)

[1.5. Administracija Praktičnih pravila rada PKS CA 13](#_Toc23412918)

[1.5.1. Organizacija odgovorna za održavanje dokumenta Praktična pravila 13](#_Toc23412919)

[1.5.2. Kontakt osoba 13](#_Toc23412920)

[1.4.3 Osoba koja određuje pogodnost CPS dokumenta 14](#_Toc23412921)

[1.4.4 Procedura odobravanja CPS dokumenta 14](#_Toc23412922)

[2. OBJAVE I ODGOVORNOSTI ZA REPOZITORIUM 14](#_Toc23412923)

[2.1. Identifikacija tela koje vodi repozitorium 14](#_Toc23412924)

[2.2. Objava informacija o izdavanju kvalifikovanog elektronskog sertifikata 15](#_Toc23412925)

[2.3. Vreme ili učestalost objavljivanja 15](#_Toc23412926)

[2.4. Kontrole pristupa repozitoriumu 15](#_Toc23412927)

[3. IDENTIFIKACIJA KORISNIKA I IZDAVANJE KVALIFIKOVANOG ELEKTRONSKOG SERTIFIKATA 16](#_Toc23412928)

[3.1. Identifikacija Korisnika 16](#_Toc23412929)

[3.1.1. Inicijalno utvrđivanje identiteta Korisnika 16](#_Toc23412930)

[3.1.2. Način dostave zahteva 16](#_Toc23412931)

[3.1.3. Sklapanje ugovora 16](#_Toc23412932)

[3.2. Identifikacija i autentikacija na PKSCA QTSA servis 17](#_Toc23412933)

[3.3. Sertifikat modula za izradu vremenskog žiga 17](#_Toc23412934)

[3.4. Elektronski vremenski žig 17](#_Toc23412935)

[3.4.1. Zahtev za izdavanje vremenskog žiga (*Time-Stamp Request*) 18](#_Toc23412936)

[3.4.2. Odgovor servisa za izdavanje kvalifikovanog elektronskog sertifikata (*Time-Stamp Response*) 18](#_Toc23412937)

[3.5. Profil vremenskog žiga 18](#_Toc23412938)

[3.6. Tačnost vremena u izdatim elektronskim vremenskim žigovima 19](#_Toc23412939)

[3.7. Sinhronizacija sata sa UTC 19](#_Toc23412940)

[3.7.1. Letnje računanje vremena 19](#_Toc23412941)

[3.8. Provera validnosti vremenskog žiga 19](#_Toc23412942)

[3.9. Raspoloživost usluge 20](#_Toc23412943)

[3.10. Izdavanje nekvalifikovanih kvalifikovanog elektronskog sertifikata 20](#_Toc23412944)

[3.11. Transportni protokol za uslugu izdavanja kvalifikovanog elektronskog sertifikata 20](#_Toc23412945)

[4. OPERATIVNI ZAHTEVI ZA ŽIVOTNI CIKLUS SERTIFIKATA ZA PKSCA QTSA 21](#_Toc23412946)

[4.1. Izdavanje sertifikata 21](#_Toc23412947)

[4.2. Opoziv i suspenzija sertifikata 21](#_Toc23412948)

[4.2.1. Razlozi za opoziv 21](#_Toc23412949)

[4.2.2. Ko može tražiti opoziv 21](#_Toc23412950)

[4.2.3. Učestalost izdavanja CRL 21](#_Toc23412951)

[4.2.4. Maksimalno kašnjenje za CRL 21](#_Toc23412952)

[4.2.5. Zahtevi na *online* proveru statusa opozvanosti sertifikata 22](#_Toc23412953)

[4.2.6. Drugi dostupni načini objave opozvanih sertifikata 22](#_Toc23412954)

[5. PROVERA SISTEMA, UPRAVLJANJA I RADNIH POSTUPAKA 23](#_Toc23412955)

[5.1. Mere fizičke zaštite 23](#_Toc23412956)

[5.1.1. Lokacija objekta i konstrukcija 23](#_Toc23412957)

[5.1.2. Fizički pristup 23](#_Toc23412958)

[5.1.3. Sistemi za napajanje i klimatizaciju 24](#_Toc23412959)

[5.1.4. Opasnost od poplave 24](#_Toc23412960)

[5.1.5. Protivpožarna zaštita 24](#_Toc23412961)

[5.1.6. Čuvanje medija 24](#_Toc23412962)

[5.1.7. Zbrinjavanje otpada 24](#_Toc23412963)

[5.2. Organizacione mere zaštite 25](#_Toc23412964)

[5.2.1. Poverljive uloge 25](#_Toc23412965)

[5.2.2. Broj osoba potrebnih za obavljanje aktivnosti 25](#_Toc23412966)

[5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu 25](#_Toc23412967)

[5.2.4. Uloge koje zahtevaju odvajanje (separaciju) dužnosti 26](#_Toc23412968)

[5.3. Provere nivoa znanja osoblja 26](#_Toc23412969)

[5.3.1. Kvalifikacije, radno iskustvo i zahtevi za proverom nivoa znanja osoblja 26](#_Toc23412970)

[5.3.2. Procedure provere prikladnosti osoblja 26](#_Toc23412971)

[5.3.3. Zahtevi za školovanjem 26](#_Toc23412972)

[5.3.4. Učestalost i uslovi za obnovu znanja 26](#_Toc23412973)

[5.3.5. Kazne za neovlašćee radnje 27](#_Toc23412974)

[5.3.6. Zahtevi na spoljne saradnike 27](#_Toc23412975)

[5.3.7. Dokumentacija koja je dostupna zaposlenima 27](#_Toc23412976)

[5.4. Postupci upravljanja revizionim zapisima 27](#_Toc23412977)

[5.4.1. Tipovi događaja koji se zapisuju 27](#_Toc23412978)

[5.4.2. Učestalost obrade revizionih zapisa 28](#_Toc23412979)

[5.4.3. Vremenski period čuvanja revizionih zapisa 28](#_Toc23412980)

[5.4.4. Zaštita revizionih zapisa 28](#_Toc23412981)

[5.4.5. Sistem prikupljanja revizionih zapisa (unutarnji ili vanjski) 28](#_Toc23412982)

[5.4.6. Obavještavanje subjekta uzročnika događaja 40](#_Toc23412983)

[5.4.7. Procena rizika 40](#_Toc23412984)

[5.5. Arhiviranje zapisa 40](#_Toc23412985)

[5.5.1. Tipovi arhiviranih zapisa 40](#_Toc23412986)

[5.5.2. Vremenski period arhiviranja 40](#_Toc23412987)

[5.5.3. Zaštita arhive 41](#_Toc23412988)

[5.5.4. Postupci izrade sigurnosnih kopija arhive 41](#_Toc23412989)

[5.5.5. Sistem prikupljanja arhivskih zapisa (unutarnji ili spoljašni) 41](#_Toc23412990)

[5.5.6. Postupci dobijanja i provere arhiviranih zapisa 41](#_Toc23412991)

[5.6. Promena TSU ključa 41](#_Toc23412992)

[5.7. Oporavak od kompromitacije ili nepogode 42](#_Toc23412993)

[5.7.1. Postupci u slučaju incidenta ili kompromitacije 42](#_Toc23412994)

[5.7.2. Postupci u slučaju oštećenja u računarskim resursima, programima i/ili podacima 42](#_Toc23412995)

[5.7.3. Postupci u slučaju kompromitovanja privatnog ključa ili ispada iz sinhronizacije sa UTC vremenom 42](#_Toc23412996)

[5.7.4. Mogućnost nastavka poslovanja nakon nepogode 43](#_Toc23412997)

[5.8. Prestanak rada PKSCA QTSA servisa 43](#_Toc23412998)

[6. TEHNIČKE MERE ZAŠTITE 45](#_Toc23412999)

[6.1. Generišenje i instalacija para ključeva 45](#_Toc23413000)

[6.1.1. Generišenje para TSU ključeva 45](#_Toc23413001)

[6.1.2. Dostava javnog TSU ključa korisnicima i trećim stranama 45](#_Toc23413002)

[6.1.3. Dužina kriptografskih ključeva 45](#_Toc23413003)

[6.1.4. Generišenje i provera kvalitete parametara javnog ključa 45](#_Toc23413004)

[6.1.5. Namene ključeva 46](#_Toc23413005)

[6.2. Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom 46](#_Toc23413006)

[6.2.1. Standardi i tehničke mere zaštite kriptografskog modula 46](#_Toc23413007)

[6.2.2. Upravljanje privatnim TSU ključem od strane više osoba (n od m) 46](#_Toc23413008)

[6.2.3. Sigurno skladištenje privatnog ključa 46](#_Toc23413009)

[6.2.4. Sigurnosno kopiranje privatnog ključa 46](#_Toc23413010)

[6.2.5. Arhiviranje privatnog ključa 47](#_Toc23413011)

[6.2.6. Prenos privatnog ključa 47](#_Toc23413012)

[6.2.7. Čuvanje privatnog ključa u kriptografskom modulu 47](#_Toc23413013)

[6.2.8. Metoda aktivacije privatnog TSU ključa 47](#_Toc23413014)

[6.2.9. Metoda deaktivacije privatnog TSU ključa 47](#_Toc23413015)

[6.2.10. Metoda uništavanja privatnog TSU ključa 48](#_Toc23413016)

[6.2.11. Ocena kriptografskog modula 48](#_Toc23413017)

[6.3. Ostali vidovi upravljanja parom ključeva 48](#_Toc23413018)

[6.3.1. Arhiviranje javnog ključa 48](#_Toc23413019)

[6.3.2. Vremenski period važenja PKSCA QTSA sertifikata i korištenja para TSU ključeva 48](#_Toc23413020)

[6.3.3. Upravljanje životnim ciklusom kriptografskih modula 49](#_Toc23413021)

[6.4. Aktivacioni podaci 49](#_Toc23413022)

[6.4.1. Generišenje i instalacija aktivacionih podataka 49](#_Toc23413023)

[6.4.2. Zaštita aktivacionih podataka 49](#_Toc23413024)

[6.5. Upravljanje informacionom bezbednošću 49](#_Toc23413025)

[6.5.1. Posebni tehnički zahtevi na informacionu bezbednost 50](#_Toc23413026)

[6.6. Tehničke kontrole životnog ciklusa 50](#_Toc23413027)

[6.6.1. Kontrole daljeg razvoja sistema 50](#_Toc23413028)

[6.6.2. Kontrole upravljanja bezbednošću 50](#_Toc23413029)

[6.6.3. Sigurnosne kontrole životnog ciklusa 51](#_Toc23413030)

[6.7. Provera mrežne bezbednosti 51](#_Toc23413031)

[6.8. Upotreba vremenskog žiga 51](#_Toc23413032)

[7. SADRŽAJ SERTIFIKATA, LISTA OPOZVANIH SERTIFIKATA I OCSP PROFILI 52](#_Toc23413033)

[7.1. Profil sertifikata PKSCA QTSA 52](#_Toc23413034)

[7.1.1. Broj(evi) verzije 52](#_Toc23413035)

[7.1.2. Ekstenzije sertifikata 52](#_Toc23413036)

[7.1.3. Identifikator objekta (OID) algoritama 52](#_Toc23413037)

[7.1.4. Oblici naziva 52](#_Toc23413038)

[7.1.5. Ograničenja u nazivima 53](#_Toc23413039)

[7.1.6. Identifikator objekta (OID) Praktičnih pravila TSU sertifikata 53](#_Toc23413040)

[7.1.7. Upotreba ekstenzije *Policy Constraints* 53](#_Toc23413041)

[7.1.8. Procesne semantike za kritičnu ekstenziju *Certificate Policies* 53](#_Toc23413042)

[7.2. Profil CRL 53](#_Toc23413043)

[7.2.1. Broj(evi) verzije 53](#_Toc23413044)

[7.2.2. CRL i ekstenzije unosa u CRL 53](#_Toc23413045)

[7.3. OCSP profil 54](#_Toc23413046)

[7.3.1. Broj(evi) verzije 54](#_Toc23413047)

[7.3.2. OCSP ekstenzije 54](#_Toc23413048)

[8. PROVERA USKLJAĐENOSTI 55](#_Toc23413049)

[8.1. Učestalost ili okolnosti provere uskljađenosti 55](#_Toc23413050)

[8.1.1. Eksterna provera uskljađenosti 55](#_Toc23413051)

[8.1.2. Interna provera uskljađenosti 55](#_Toc23413052)

[8.2. Identitet/kvalifikacije ocjenitelja 55](#_Toc23413053)

[8.3. Odnos ocenivača sa telom koje se ocjenjuje 56](#_Toc23413054)

[9. OSTALE POSLOVNE I PRAVNE ODREDBE 56](#_Toc23413055)

[9.1. Naknada za usluge 56](#_Toc23413056)

[9.1.1. Povraćaj uplaćenih sredstava 56](#_Toc23413057)

[9.2. Finansijska odgovornost 56](#_Toc23413058)

[9.2.1. Pokrivenost osiguranjem 56](#_Toc23413059)

[9.2.2. Druga sredstva 57](#_Toc23413060)

[9.3. Poverljivost poslovnih podataka 57](#_Toc23413061)

[9.3.1. Opseg poverljivih poslovnih podataka 57](#_Toc23413062)

[9.3.2. Podaci koji se ne smatraju poverljivim poslovnim podacima 57](#_Toc23413063)

[9.3.3. Odgovornost za zaštitu poverljivih poslovnih podataka 57](#_Toc23413064)

[9.4. Zaštita ličnih podataka 57](#_Toc23413065)

[9.4.1. Plan zaštite ličnih podataka 58](#_Toc23413066)

[9.4.2. Poverljivi lični podaci 58](#_Toc23413067)

[9.4.3. Lični podaci koji nisu poverljivi 58](#_Toc23413068)

[9.4.4. Odgovornost za zaštitu ličnih podataka 58](#_Toc23413069)

[9.4.5. Ovlašćenje za korištenje ličnih podataka 58](#_Toc23413070)

[9.4.6. Dostupnost podataka merodavnim telima 58](#_Toc23413071)

[9.4.7. Ostale okolnosti objave podataka 59](#_Toc23413072)

[9.5. Prava intelektualnog vlasništva 59](#_Toc23413073)

[9.6. Obveze učesnika 59](#_Toc23413074)

[9.6.1. Obveze PKSCA 59](#_Toc23413075)

[9.6.2. Obaveze RA 60](#_Toc23413076)

[9.6.3. Obaveze Korisnika 60](#_Toc23413077)

[9.6.4. Obveze trećih strana 61](#_Toc23413078)

[9.7. Odgovornosti učesnika 61](#_Toc23413079)

[9.7.1. Odgovornosti PKSCA 61](#_Toc23413080)

[9.7.2. Odgovornosti Korisnika 62](#_Toc23413081)

[9.7.3. Odgovornosti trećih strana 62](#_Toc23413082)

[9.8. Odricanje od odgovornosti 63](#_Toc23413083)

[9.9. Ograničenja odgovornosti 63](#_Toc23413084)

[9.10. Naknada štete 63](#_Toc23413085)

[9.11. Trajanje i prestanak važenja 63](#_Toc23413086)

[9.11.1. Trajanje 63](#_Toc23413087)

[9.11.2. Prestanak važenja 64](#_Toc23413088)

[9.11.3. Posledice prestanka važenja i nastavak delovanja 64](#_Toc23413089)

[9.12. Individualna obaveštenja i komunikacija sa učesnicima 64](#_Toc23413090)

[9.13. Izmene i dopune 64](#_Toc23413091)

[9.13.1. Procedure izmena i dopuna 64](#_Toc23413092)

[9.13.2. Mehanizmi obaveštavanja i vremenski periodi 65](#_Toc23413093)

[9.13.3. Okolnosti pod kojima se mora mijenjati OID 65](#_Toc23413094)

[9.14. Postupak rešavanja sporova 65](#_Toc23413095)

[9.15. Važeći propisi 66](#_Toc23413096)

[9.16. Usklađenost sa primenjivim propisima 66](#_Toc23413097)

[9.17. Ostale odredbe 66](#_Toc23413098)

[8.4. Predmeti ocjenjivanja uskljađenosti 67](#_Toc23413099)

[8.5. Mere u slučaju neusklađenosti 67](#_Toc23413100)

[8.6. Saopštavanje rezultata 67](#_Toc23413101)

[9. Istorija dokumenta 68](#_Toc23413102)

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 usluge izdavanja kvalifikovanog elektronskog sertifikata za elektronski potpis u oblaku i kvalifikovanog elektronskog sertifikata za elektronski pečat u oblaku**

# Uvod i pregled osnovnih pretpostavki

Sertifikaciono telo Privredne komore Srbije (u nastavku: PKSCA) kao registrovani pružalac usluga od poverenja, vrši usluge izdavanja kvalifikovanog elektronskog sertifikata za elektronski potpis u oblaku i kvalifikovanog elektronskog sertifikata za elektronski pečat u oblaku, u skladu sa Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima. (u daljem tekstu - Zakon).

PKSCA inicijalno je osmišljeno i uspostavljeno u Privrednoj komori Srbije kao treća strana od poverenja (*Trusted Third Party*), sa ciljem pružanja usluga od poverenja za građane, poslovne subjekte i organe javne uprave. PKSCA kao kvalifikovani pružalac usluga od poverenja omogućuje stvaranje odnosa poverenja potrebnog za korišćenje i razvoj elektronskog poslovanja (e-poslovanje) i elektronske javne uprave (e-uprava). Promovisanjem ovih usluga od poverenja i njihovim korišćenjem PKSCA želi da podstakne i olakša razvitak e-poslovanja i e-uprave u Srbiji.

## Pregled osnovnih pretpostavki

PKS CA utvrđuje Praktična pravila pružanja usluge od poverenja (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.

PKSCA je PKI infrastruktura uspostavljena u Privrednoj komori Srbije kojom PKSCA pruža usluge od poverenja, a koje se odnose na izdavanje i upravljanje životnog ciklusa kvalifkovanih elektronskih sertifikata za elektronski potpis, kvalifikovanih elektronskih sertiikata za elektronski pečat, izdavanje kvalifikovanog elektronskog sertifikata, sredstva za formiranje elektronskog potpisa (u daljem tekstu ePotpis u oblaku) i usluge validacije elektronski potpisanih dokumentata. Set ovih usluga objedinjeno je pod imenom Usluge kaligrafije.

Hijerarhijska struktura PKSCAzasnovana je na PKSCA Root CA i temelji se na dvojnoj arhitekturi produkcionih sertifikacionih tela (engl.: *Certification Authorities,* u daljem tekstu: CA ili CA-ovi).

Infrastrukturu Sertifikacionog tela PKS čine dva sertifikaciona tela:

* „*PKS CA Root*“ server,kao *Root* sertifikaciono telo.
* „*PKS CA Class1*“server,kao podređeno sertifikaciono telo za kvalifikovane elektronske sertifikate na karticama
* „*PKS CA Cloud*“server,kao podređeno sertifikaciono telo za usluge kaligrafije

„*PKS CA Root*“ **server** radikao*Root* sertifikaciono telo na osnovu sertifikata izdatog samom sebi (*self-signed certificate*) u procesu generisanja privatnog kriptografskog klјuča aplikacije sertifikacionog tela (*Root Key Generation Ceremony*). „*PKS CA Root*“ server izdaje sertifikate podređenim sertifikacionim telima koja su deo infrastrukture Sertifikacionog tela PKS.

„*PKS CA* Class1“ server kao podređeno (*subordinate*) sertifikaciono telo izdaje kvalifikovane elektronske sertifikate pravnim i fizičkim licima, a zaposlenima koji rade na poslovima sertifikacije, u Sertifikacionom telu PKS, se izdaju administratorski sertifikati. Ova instanca izdaje i pripadajući sertifikat za OCSP servis.

„*PKS CA* Cloud“ server kao podređeno (*subordinate*) sertifikaciono telo izdaje kvalifikovane elektronske sertifikate za elektronski potpis u oblaku pravnim i fizičkim licima, kvalifikovane elektronske sertifikate za elektronski pečat u oblaku pravnim licima, kao i elektronske sertifikate za TSA (Time Stamp Authority), i pripadajuće OCSP sertifikate.

Kvalifikovani elektronski sertifikati su standardni *X*.509 verzija 3 sertifikati koji su namenjeni za verifikovanje kvalifikovanog elektronskog potpisa.

Korisnici kvalifikovanih elektronskih sertifikata Sertifikacionog tela PKS, poseduju jedan par kriptografskih klјučeva (javni i privatni klјuč). Privatni kriptografski klјuč koristi se za kvalifikovano elektronsko potpisivanje, a javni kriptografski klјuč koristi se za verifikovanje kvalifikovanog elektronskog potpisa.

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

### Opseg i namena

Ovaj CPS dokument pružanja usluga od poverenja sadrže detaljna pravila i skup načela pružanja usluga od poverenja kojim PKSCA kao kvalifikovani pružalac usluga od poverenja pruža usluge izdavanja kvalifikovanih sertifikata za elektronske potpise i pruža usluge izdavanja kvalifikovanih sertifikata za elektronske pečate, usluge udaljenog potpisivanja i pečatiranja, usluge izdavanja vremenskog žiga i usluge validacije elektronski potpisanog dokumenta.

Opseg ovog CPS dokumenta su kvalifikovane usluge od poverenja koje pruža PKSCA, a koje se odnose na izdavanje i upravljanje životnim ciklusom kvalifikovanih elektronskih sertifikata koji se izdaju na sigurnim kriptografskim uređajima i njihova primena u uslugama kaligrafije..

Produkcioni sertifikati iz opsega ovog CPS dokumenta sastavni su deo Registra digitalnih sertifikata (PKSCA), a koje izdaju sertifikaciona tela (CA) iz opsega ovog CSP dokumenta: PKSCA CLASS1 i PKSCA CLOUD. U daljem tekstu, gde je to primenljivo, radi jednostavnosti sva CA koja se nalaze u okviru PKSCA označavaju se zajedničkim nazivom subordinirani PKSCA CA ili samo PKSCA CA.

Namena ovog dokumenta je definisanje pravila iz područja određenog opsegom ovog dokumenta, a prema kojima postupaju korisnici PKSCAnavedeni u tački 1.3. ovog CSP dokumenta.

Ovaj CPS dokument usklađen je sa CP dokumentom Politika sertifikacije, a koji je objavljen na internet stranici PKSCA.

### Tipovi sertifikata

Ovim Praktičnim pravilima definisana su pravila sertifikovanja za kvalifikovane sertifikate koje izdaju PKSCA CA-ovi, a koji su usklađeni sa zahtevima Zakona o elektronskoj identifikaciji, elektronskom dokumentu i uslugama od poverenja u elektronskom poslovanju.

Ovim Praktičnim pravilima definisane su grupe sertifikata, tipovi sertifikata i pripadajući nivoi sigurnosti. Grupe sertifikata određene su vrstom Subjekta sertifikovanja. Jedna grupa sertifikata može imati jedan ili više tipova sertifikata. Svaki tip sertifikata ima dodeljen PKSCA i ETSI OID opštih pravila sertifikovanja (CP OID). Pomoću CP OID-a Potpisnici, Autori pečata i Pouzdajuće strane određuju prikladnost sertifikata za određenu primenu. Svaki tip sertifikata ima dodeljen nivo sigurnosti kojim je određen stepen pouzdanosti u sertifikat.

U sledećim tabelama prikazane su grupe i tipovi kvalifikovanih elektronskih sertifikata iz opsega ovog CP dokumenta sa nazivima sertifikata i pripadajućim PKSCA i OID-ima (u daljem tekstu: CP OID). Tabela 1.1. prikazuje grupe i tipove kvalifikovanih sertifikata koje izdaje PKSCA CLASS1, a tabela 1.2. prikazuje grupe i tipove kvalifikovanih sertifikata koje izdaje PKSCA CLOUD .

|  |  |  |  |
| --- | --- | --- | --- |
| **Kvalifikovani sertifikati koje izdaje PKSCA CLASS1 CA** | | | |
| **Naziv grupe sertifikata** | **Naziv tipa sertifikata** | **PKSCA i ETSI CP OID** | **Nivo sigurnosti** |
| **PKSCA CLASS1 kvalifikovani elektronski sertifikati za elektronski potpis** | Kvalifikovani elektronski sertifikatsertifikat za elektronski potpis za fizičko lice | PKSCA CP OID:  1.3.6.1.4.1.31266.10.2.1.4  PKSCA CP OID:  1.3.6.1.4.1.31266.10.2.1.5  PKSCA CP OID:  1.3.6.1.4.1.31266.10.2.1.6 | Srednji |
| Kvalifikovani elektronski sertifikatsertifikat za elektronski potpis za ovlašćeno (zaposleno) lice u okviru pravnog lica |
| Kvalifikovani elektronski sertifikatsertifikat za elektronski potpis za nerezidenta |

Tabela 1.1

|  |  |  |  |
| --- | --- | --- | --- |
| **Kvalifikovani sertifikati koje izdaje PKSCA CLOUD CA** | | | |
| **Naziv grupe sertifikata** | **Naziv tipa sertifikata** | **PKSCA i ETSI CP OID** |  |
| **PKSCA CLOUD**  **kvalifikovani elektronski sertifikati za elektronski potpis** | Kvalifikovani elektronski sertifikatsertifikat za elektronski potpis za fizičko lice | PKSCA CP OID:  1.3.6.1.4.1.31266.10.2.2.4  ETSI CP OID: 0.4.0.194112.1.2 | Srednji |
| Kvalifikovani elektronski sertifikatsertifikat za elektronski potpis za ovlašćeno (zaposleno) lice u okviru pravnog lica | PKSCA CP OID:  1.3.6.1.4.1.31266.10.2.2.5  ETSI CP OID: 0.4.0.194112.1.0 | Srednji |
| Kvalifikovani elektronski sertifikatsertifikat za elektronski potpis za nerezidenta | PKSCA CP OID:  1.3.6.1.4.1.31266.10.2.2.6  ETSI CP OID: 0.4.0.194112.1.0 | Srednji |
| **PKSCA CLOUD**  **Kvalifikovani elektronski sertifikati za elektronski pečat** | kvalifikovani sertifikat za e-pečat (QCP-l-qscd) | PKSCA CP OID: 1.3.6.1.4.1.31266.10.2.2.7  ETSI CP OID: 0.4.0.194112.1.3 | Srednji |

Tabela 1.2

### PKSCA CLASS1 kvalifikovani elektronski sertifikati

PKSCA CLASS1 kvalifikovani elektronski sertifikati za elektronski potpis generisani su na pametnim karticama. Politika sertifikacije ovih sertifikata ima OID 1.3.6.1.4.1.31266.10.2.1

### PKSCA CLOUD kvalifikovani elektronski sertifikati za udaljeni potpis (potpis u oblaku)

PKSCA CLASS1 lični sertifikati namenjeni su fizičkim licima – građanima za udaljeno elektronsko potpisivanje. Ovim praktičnim pravilima određeni su sledeći tipovi ličnih kvalifikovanih sertifikata:

* **kvalifikovani elektronski sertifikat za udaljeni elektronski potpis za fizičko lice** – Lični kvalifikovani sertifikat za udaljeni elektronski potpis, koji se izdaje fizičkim licima – građanima, čiji se pripadajući privatni ključ čuva u sigurnom kriptografskom uređaju. Ovaj tip sertifikata u skladu je sa „QCP-n“ EU praktičnim pravilima za kvalifikovane elektronske sertifikate iz norme ETSI EN 319 411-2
* **kvalifikovani elektronski sertifikat za udaljeni elektronski potpis za ovlašćeno (zaposleno) lice u okviru pravnog lica** – Lični kvalifikovani sertifikat za e-potpis, koji se izdaje fizičkim licima – zaposlenima u okviru nekog pravnog lica, a čiji se pripadajući privatni ključ čuva u sigurnom kriptografskom uređaju. Ovaj tip sertifikata u skladu je sa „QCP-n“ EU praktičnim pravilima za kvalifikovane elektronske sertifikate iz norme ETSI EN 319 411-2
* **kvalifikovani elektronski sertifikat za udaljeni elektronski pečat** – Kvalifikovani sertifikat za kvalifikovani elektronski pečat, koji se izdaje pravnom licu, a čiji se pripadajući privatni ključ čuva u sigurnom kriptografskom uređaju. Ovaj tip sertifikata u skladu je s „QCP-l“ EU praktičnim pravilima za kvalifikovane sertifikate iz norme ETSI EN 319 411-2 [12].

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

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

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

Opšti uslovi za pružanje usluga PKS CA su u skladu sa zahtevima standarda EN 319 401 koji se odnose na dokument iz odeljka “6.2 Terms and Conditions”.

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 ostvarivanja usluga od poverenja. Posebna pravila su privatni dokument i predstavljaju poslovnu tajnu sertifikacionog tela.

Posebna interna pravila sadrže detaljne odredbe o:

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

PKS CA je evidentirano i akreditovano od strane Nadležnog organa za poslove akreditacije i supervizije PKI (Public Key Infrastructure) sistema u Srbiji (Ministarstvo za trgovinu, turizam i telekomunikacije) i biće predmet periodične supervizije u cilju osiguravanja usaglašenosti sa zahtevima iz Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima.

## 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 (1.3.6.1.4.1.31266.10.1.2)**

## Učesnici u PKI sistemu PKS

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

### PKS CA

Sertifikaciono telo je organizacija koja je pružaoc kvalifikovanih usluga od poverenja. PKS CA je sertifikaciono telo (CA). PKS CA je odgovorna za publikaciju ove Praktična pravila rada u cilju podrške izdavanju određenih usluga od poverenja. U tom smislu, ova Praktična pravila rada (CPS Politike Certificate Practice Statement), predstavljaju odgovarajuće politike i pravila koja se primenjuju pri izvršavanju PKS CA kvalifikovanih usluga od poverenja.

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

PKS CA predstavlja hijerarhijsku PKI strukturu za izdavanje elektronskih sertifikata. U pomenutoj arhitekturi, postoji:

* PKS Root CA – centralno samopotpisano sertifikaciono telo koje izdaje sertifikate intermediate CA telima i potpisuje CRL listu na root nivou.

PKSCA Root CA ne izdaje sertifikate Korisnicima.

* PKS Intermediate CA – sertifikaciono telo koje izdaje kvalifikovane sertifikate:
  + fizičkim licima
  + fizičkim licima u okviru pravnog lica
  + nerezidentima

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

### Registraciona tela PKS CA

RA tela interaktivno komuniciraju i sa korisnicima i sa PKS CA u cilju isporuke usluga od poverenja krajnjim korisnicima. U tom smislu, registraciona tela PKS CA:

* Analiziraju, potvrđuju ili odbijaju registraciju odgovarajućih korisničkih zahteva za Usluge od poverenja (aplikacije za usluge).
* Registruju korisnike za korišćenje PKS CA usluga od poverenja.
* Sprovode sve korake u proceduri identifikacije korisnika što je definisano važećim zakonskim dokumentima i Opštim pravilima rada PKS CA.
* Koriste službene dokumente u cilju provere korisnikove aplikacije.
* Iniciraju proces opoziva i zahtevaju opoziv sertifikata od strane PKS CA.

Registraciona tela PKS CA deluju lokalno u okviru njihovog sopstvenog konteksta geografskog ili poslovnog partnerstva koje je potvrđeno i autorizovano od strane PKS CA. PKS CA registraciona tela deluju u skladu sa praksom, procedurama i osnovnim dokumentima rada PKS CA. Ne postoji ograničenje na broj registracionih tela koja mogu biti pridružena PKS CA PKI infrastrukturi.

Poslovima registracije u RA PKSCA mreži koordinira centralni RA.

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

### Korisnici

Korisnici predstavljaju korisnike sertifikacionih usluga PKS CA. To su fizička lica koja zastupaju pravna lica i ostala fizička lica.

Korisnici su strane koje:

* Apliciraju za usluge od poverenja,
* Identifikovani su kao vlasnici sertifikata u samom sertifikatu,
* Poseduju privatni ključ koji matematički odgovara javnom ključu koji je

naveden u korisnikovom sertifikatu.

### Treće strane

Treće strane su entiteti, kao na primer fizička lica (pojedinci) i/ili pravna lica (kompanije), koji se oslanjaju na uslugu od poverenja. Treća strana na osnovu kvalifikovanih elektronskih sertifikata sprovodi validaciju elektronskog potpisa ili elektronskog pečata i deluje na osnovu razumne pouzdanosti u sertifikat potpisnika generisan od strane PKS CA. Verifikacija digitalnog potpisa se vrši na bazi javnog ključa koji se nalazi u korisnikovom sertifikatu.

U cilju provere validnosti primenjenog elektronskog sertifikata, treće strane moraju uvek da provere status opozvanosti datog sertifikata u okviru PKS CA CRL liste ili kroz OCSP servis, pre nego što prihvate informacije koje su navedene u sertifikatu.

## Korišćenje usluga od poverenja PKS CA

U ovom poglavlju se definiše korišćenje usluga od poverenja za koje je akreditovano PKS CA.

### Prihvatljivo korišćenje usluga od poverenja

PKS CA usluge od poverenja se mogu koristiti za većinu transakcija elektronskog poslovanja i elektronske trgovine koje se baziraju na upotrebi kvalifikovanih elektronskih sertifikata.

U takve transakcije spadaju:

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

#### Primerena upotreba kvalifikovanih sertifikata za udaljeni elektronski potpis i pečat

Kvalifikovani elektronski sertifikati za udaljeni elektronski potpis upotrebljavaju se samo za podršku u elektronskih potpisima, a pripadajuće privatne ključeve ovih sertifikata upotrebljavaju fizička lica – građani samo za izradu elektronskih potpisa.

#### Primerena upotreba kvalifikovanih sertifikata za udaljeni elektronski pečat

Kvalifikovani elektronskji sertifikati za udaljeni elektronski pečat upotrebljavaju se samo za podršku u elektronskim pečatima, a pripadajuće privatne ključeve ovih sertifikata upotrebljavaju Autori pečata samo za izradu elektronskih pečata.

### Zabranjeno korišćenje usluga od poverenja

Osim upotrebe u elektronskim potpisima i elektronskim pečatima, navedenih u prethodnoj tački ovog dokumenta, sve ostale upotrebe usluga od poverenja PKSCA, u skladu sa ovim Opštim pravilima, su zabranjene.

## Administracija Praktičnih pravila rada PKS CA

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

### 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](mailto:dusan.berdic@pks.rs)

### Osoba koja određuje pogodnost CPS dokumenta

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

**mr Dušan Berdić**

**Privredna Komora Srbije**

**Resavska 13-15**

**11000 Beograd, Srbija**

**Tel.: 011 3304 545**

**Fax: 011 3304 556**

**Email:** [dusan.berdic@pks.rs](mailto:dusan.berdic@pks.rs)

### 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.

# Odgovornosti za publikovanje i repozitorijume

## 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 kvalifikovanog elektronskog sertifikata

Na PKSCA PKI repozitoriumu javno su objavljeni dokumenti i informacije o pružanju usluga izdavanja kvalifikovanog elektronskog sertifikata:

* aktuelna politika sertifikacije pružanja usluga od poverenja,
* aktuelni CPS dokument o postupcima pružanja usluge izdavanja kvalifikovanog elektronskog sertifikata za elektronski potpis u oblaku i kvalifikovanog elektronskog sertifikata za elektronski pečat u oblaku,
* ranije verzije praktičnih pravila pružanja usluge izdavanja kvalifikovanog elektronskog sertifikata za elektronski potpis u oblaku i kvalifikovanog elektronskog sertifikata za elektronski pečat u oblaku
* uslovi pružanja usluga izdavanja elektronskih sertifikata (engl. *Terms and conditions* i *PKI disclosure statement*)
* PKSCARoot CA sertifikat i sertifikati subordiniranih CA,
* CRL svakog pojedinačnog PKSCA CA,
* cenovnik usluga izdavanja kvalifikovanog elektronskog sertifikata,
* način podnošenja zahteva za izdavanja kvalifikovanog elektronskog sertifikata,
* aktuelne lokacije PKSCA RA/LRA tela,
* Korisnička uputstva,
* obaveštenja korisnicima vezane za pružanje usluga izdavanja kvalifikovanog elektronskog sertifikata,
* ostale informacije vezane za rad PKSCA.

Javno objavljeni sadržaj PKSCA 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 kvalifikovanog elektronskog sertifikata, 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 ovlašćee osobe PKSCA.

# IDENTIFIKACIJA I POTVRĐIVANJE IDENTITETA SUBJEKTA

## Određivanje imena

### Tipovi imena

U svaki sertifikat upisuju se podaci o imenu, odnosno nazivu Subjekta sertifikovanja kao i podatak o mestu prebivališta fizičkog lica, odnosno mestu sedišta Pravnog lica. Podaci o imenu ili nazivu koji se upisuju u sertifikat odnose se na autentično ime ili naziv Subjekta. Polje *Subject* u sertifikatu usklađeno je s dokumentom IETF RFC 5280.

Polje *Subject* u sertifikatima koji se izdaju za fizička lica sadrži ime i prezime osobe. U poslovnim sertifikatima i sertifikatima za Elektronski pečat polje *Subject* dodatno sadrži i puni registrovani naziv pravnog lica i njegov identifikator.

### Jednoznačnost imena

Imena i nazivi u atributima polja *Subject* koji identifikuju fizičko lice i Poslovni subjekt su jednoznačni.

Za atribute u polju *Subject* u sertifikatima koje izdaju PKSCA CA-ovi primenjuju se sledeća pravila:

* + - * lično ime i prezime moraju biti identični kako su navedeni u identifikacionoj ispravi, odnosno u službenim matičnim registrima,
      * naziv Pravnog lica mora biti identičan onom navedenom u službenim nadležnim nacionalnim registrima.

Sadržaj ekstenzije sertifikata *Subject Alternative Name* može biti e-mail adresa Subjekta koja ne mora biti jedinstvena.

### Anonimnost korisnika ili pseudonimi

Anonimnost i pseudonimi Korisnika nisu podržani.

### Pravila tumačenja raznih oblika imena

Tumačenje oblika imena u polju *Subject* po normi X.520 u **PKSCA** određeno je na sledeći način:

* + - * Serial Number

Vrednost atributa *Serial Number* u polju *Subject* jamči jedinstvenost pojedinog Subjekta. Vrednost ovog atributa garantuje i jedinstvenost polja *Subject* u sertifikatima unutar **PKSCA** produkcione hijerarhije zasnovane na PKSCA Root CA.

U sertifikatima za elektronske potpise atribut *Serial Number* sastoji se od dvoslovnog ISO koda države prebivališta Potpisnika, trinaestobrojnog jedinstvenog identifikatora fizičkog lica kao i karaktera koji predstavljaju oznake koje imaju interno značenje za PKSCA PKI. Trinaestobrojni jedinstveni identifikator fizičkog lica je JMBG ako fizičko lice ima dodeljen JMBG u Republici Srbiji. Ako fizičko lice nema dodeljen JMBG, tada PKSCA generiše podatke na osnovu pasoša ili odgovarajućeg dokumenta matične države osobe koja zahteva sertifikat.

U sertifikatima za elektronske pečate atribut *Serial Number* sastoji se od osmobrojnog jedinstvenog identifikatora Pravnog lica kao i karaktera koji predstavljaju oznake koje imaju interno značenje za PKSCA PKI. Osmobrojni jedinstveni identifikator Pravnog lica je MB ako Pravno lice ima dodeljen MB u Republici Srbiji.

* Common Name

U sertifikatima za elektronske potpise ovaj atribut sadrži ime i prezime fizičkog lica kako je navedeno u identifikacionoj ispravi.

U sertifikatima za elektronske pečate ovaj atribut sadrži naziv pravnog lica kako ga pravno lice koristi u poslovnoj primeni. Ovaj naziv ne mora biti jednak punom registrovanom nazivu pravnog lica iz službenog nadležnog nacionalnog registra.

* Given Name

Atribut *Given Name* sadrži ime fizičkog lica kako je navedeno u identifikacionoj ispravi.

* Surname

Atribut *Surname* sadrži prezime fizičkog lica kako je navedeno u identifikacionoj ispravi.

* Organizational Unit Name

U sertifikatima za elektronske pečate i sertifikatima za elektronske potpise za pravna lica ovaj atribut sadrži naziv organizacione jedinice povezane sa Poslovnim subjektom imenovanim u atributu *Organization Name*.

* Organization Name

U sertifikatima izdatim fizičkim licima koje nisu povezane sa Poslovnim subjektom atribut *Organization Name* sadrži vrednost „LIČNI“.

U sertifikatima za elektronske pečate i sertifikatima za elektronske potpise izdatim fizičkim licima koje su povezane s Poslovnim subjektom atribut *Organization Name* sadrži puni registrovani naziv Pravnog lica.

* Organization Identifier

U sertifikatima za elektronske potpise izdatim fizičkim licima koje su povezane s Poslovnim subjektom atribut *Organization Identifier* sadrži dvoslovni ISO kod države sedišta Pravnog lica te osmobrojni jedinstveni identifikator Pravnog lica. Osmobrojni identifikator Pravnog lica je MB ako Poslovni subjekt ima dodeljen MB u Republici Srbiji.

* Locality Name

Za poslovne sertifikate za elektronske potpise i sertifikate za elektronske pečate atribut *Locality Name* sadrži naziv mesta u kojem je sedište Pravnog lica.

Za lične sertifikate za elektronske potpise atribut *Locality Name* sadrži mesto prebivališta Potpisnika

* Country Name

Atribut *Country Name* sadrži oznaku dvoslovnog ISO koda Republike Srbije.

* Subject Alternative Name

*Subject Alternative Name* je opciona ekstenzija sertifikata koja može sadržati e- mail adresu i/ili interni identifikator Subjekta.

### Jedinstvenost imena

Različitost imena Subjekta jedinstveno je unutar **PKSCA** produkcione hijerarhije zasnovane na PKSCA Root CA. Jedinstvenost različitih imena osigurana je vrednošću atributa *Serial Number* u polju *Subject* sertifikata

## Inicijalno utvrđivanje identiteta

Putem PKSCA RA mreže i mreže spoljnih ugovorenih RA-ova PKSCA prikuplja lične podatke fizičkih osoba i podatke Poslovnih subjekata isključivo za potrebe registracije u cilju izdavanja elektronskih sertifikata i korišćenja pripadajućih korisničkih privatnih ključeva za usluge od poverenja ukoliko korisnik zatraži izdavanje sertifikata za udaljeni elektronski potpis ili elektronski pečat.

Proveru podataka iz zahteva za izdavanje sertifikata, PKSCA sprovodi preko RA mreže njihovim poređenjem sa podacima iz dostavljene ili samostalno prikupljene dokumentacije iz merodavnog i nadležnog izvora, u skladu sa važećim nacionalnim zakonima i propisima.

### Metoda dokazivanja poseda privatnog ključa

Privatni ključ koji odgovara javnom ključu koji se dostavlja za izradu sertifikata za elektronski potpis ili elektronski pečat generiše potpisnik, odnosno autor pečata, ili ga generiše PKSCA .

U slučaju kad PKSCA generiše par korisničkih ključeva tehnološkim procesima i metodama provere osigurava se povezanost potpisnika, odnosno autora pečata sa privatnim ključem, koji odgovara javnom ključu, za koji PKSCA izdaje sertifikat, kao i kontrola potpisnika, odnosno ovlašćenog predstavnika nad privatnim ključem.

U slučaju kad potpisnik, odnosno autor pečata generše par ključeva PKSCA tehnološkim procesom i metodom zahtevanja sertifikata obuhvata proveru poseduje li i kontroliše li Potpisnik, odnosno Ovlašćeni predstavnik privatni ključ koji je povezan sa javnim ključem koji se na zaštićeni način dostavlja u PKSCA za izradu sertifikata.

U slučaju kada pravila pružanja usluga od poverenja propisuju da se za određeni tip kvalifikovanog sertifikata generisanje i zaštita privatnog ključa sprovodi odgovarajućim uređajem PKSCA ili spoljnim ugovorenim RA tehnološkim procesima i metodama provere osigurava da je javni ključ koji se dostavlja na sertifikovanje iz para ključeva generisanog u odgovarajućem bezbednosnom uređaju i da je povezan sa privatnim ključem potpisnika, odnosno autora pečata.

### Potvrda identiteta pravnog lica

Provera i potvrda identiteta Pravnog lica ssprovodi se proverom:

* registrovanog naziva Pravnog lica,
* pravnog postojanja Pravnog lica,
* upisa u nadležni registar,
* identifikatora iz nadležnog registra,
* adrese sedišta Pravnog lica.

Provera i potvrda naziva organizacione jedinice pravnog lica sprovodi se uvidom u važeći zakon ili drugi propis na osnovu kojeg je pravno lice osnovano, ili uvidom u drugi dokument u kojem je navedeno postojanje te organizacione jedinice.

### Potvrda identiteta fizičkog lica

Inicijalna identifikacija i potvrđivanje identiteta fizičkog lica sprovodi se postupcima neposredne ili posredne identifikacije.

Za potrebe inicijalne identifikacije i potvrđivanje identiteta fizičkog lica PKSCA prikuplja i proverava sledeće lične podatke:

* ime i prezime,
* datum, mesto i državu rođenja,
* JMBG (ako je JMBG dodeljen), ili podatke iz odgovarajuće isprave za nerezidente
* podatke sadržane na identifikacionoj ispravi,
* kontakt podatke.

Za izdavanje sertifikata za elektronske potpise koji se izdaju fizičkim licima povezanim sa pravnim licem, RA mreža, u skladu sa priznatim i prihvatljivim postupcima, prikuplja i dokaz o povezanosti fizičkog lica sa tim pravnim licem.

Za izdavanje sertifikata za elektronske pečate RA mreža, u skladu sa priznatim i prihvatljivim postupcima, prikuplja dokaz o povezanosti Ovlašćenog predstavnika sa pravnim licem kome se izdaje Elektronski pečat.

#### Postupak neposredne identifikacije

Neposredna identifikacija fizičkog lica sprovodi se u njenoj fizičkoj prisutnosti temeljem važeće identifikacione isprave iz tačke 3.2.3. ovog CPS dokumenta.

#### Postupak posredne identifikacije

PKSCA sprovodi postupak posredne identifikacije fizičkog lica pomoću sertifikata kvalifikovanog elektronskog potpisa izdatog na osnovu neposredne identifikacije fizičkog lica. Ovaj postupak pruža jednak nivo sigurnosti utvrđivanja identiteta fizičkog lica kao i postupak neposredne identifikacije.

#### Prihvatljive vrste identifikacijskih isprava

Fizička lica dokazuju svoj identitet ličnom kartom ili pasošem koji je u roku važenja.

Fizička lica koja nemaju ličnu kartu ili pasoš izdatu u Republici Srbiji svoj identitet dokazuju valjanom identifikacijskom ispravom za ulazak u Republiku Srbiju.

### Informacije o korisniku koje se ne proveravaju

PKSCA ne proverava telefonski broj za kontakt Korisnika.

### Provera identiteta ovlašćenih osoba

Pre izdavanja sertifikata za elektronske potpise sprovodi se utvrđivanje identiteta osobe Ovlašćene za dobijanje elektronskog sertifikata proverom podataka iz dostavljene dokumentacije za utvrđivanje pravnog subjektiviteta pravnog lica navedene u tački 3.2.2., i uporedo sa podacima iz važeće identifikacione isprave osobe ovlašćene za dobijanje elektronskog serttifikata.

Pre izdavanja sertifikata za elektronske pečate sprovodi se provera i potvrda identiteta ovlašćenog predstavnika postupcima neposredne ili posredne identifikacije u skladu sa tačkama 3.2.3.1. i 3.2.3.2. ovog dokumenta.

Utvrđivanje identiteta punomoćnika sprovodi se na jednak način kao i provera identiteta osobe koja je ovlašćeni predstavnik.

## Identifikacija i potvrđivanje identiteta kod podnošenja zahteva za obnovu sertifikata uz generisanje novog para ključeva

PKSCA sprovodi postupke identifikacije i potvrde identiteta podnosioca zahteva za:

* + redovnu obnovu sertifikata uz generisanje novog,
  + izdavanje sertifikata nakon isteka,
  + aktivaciju suspendovanog sertifikata,
  + ponovno izdavanje sertifikata nakon opoziva

.

### Identifikacija i potvrđivanje identiteta kod redovne obnove sertifikata uz generisanje novog para ključeva

Redovna obnova sertifikata uobičajeno se obavlja pred kraj isteka sertifikata i uključuje postupak generisanja novog para Subjektovih ključeva, a za kvalifikovane elektronske sertifikate za elektronske pečate može uključivati korišćenje postojećeg javnog ključa.

#### Identifikacija pri podnošenju zahteva u RA mreži

Identifikacija i potvrđivanje identiteta podnosioca zahteva sprovodi se u skladu sa tačkom 3.2.3. ovog dokumenta, podnošenjem vlastitog potpisanog zahteva uz neposrednu identifikaciju podnosioca zahteva u RA mreži.

Proveru i potvrdu identiteta pravnog lica RA mreža sprovodi upoređivanjem podataka iz zahteva sa podacima iz dostavljene ili samostalno prikupljene dokumentacije iz merodavnog i nadležnog izvora, u skladu sa važećom zakonskom regulativom i u skladu sa tačkom 3.2.2. ovog dokumenta. Identifikacija opisana u ovoj tački primenjuje se za sve tipove sertifikata iz opsega opisanog u ovom dokumentu.

Ukoliko se podaci o pravnom licu, koji su sadržani u sertifikatu razlikuju, od važećih podataka u PKSCA RA sistemu, sprovodi se postupak izmene podataka u sertifikatu u skladu sa tačkom 4.8. ovog dokumenta.

#### Identifikacija pri podnošenju online zahteva

Za identifikaciju i potvrđivanje identiteta podnosioca zahteva kod redovne obnove sertifikata koja se sprovodi podnošenjem *online* zahteva koristiti se dokumentacija i podaci za proveru identiteta fizičkog lica koji su prikupljeni pri zadnjoj neposrednoj identifikaciji podnosioca zahteva u RA mreži u skladu sa tački 3.3.1.1. ovog CPS dokumenta, pod uslovom da od zadnje neposredne identifikacije podnosioca zahteva nije prošlo više od 6 godina, kao i da je identifikaciona isprava korišćena u toj identifikaciji još uvek važeća. Skup podataka iz zahteva za obnovu sertifikata elektronski se potpisuje naprednim elektronskim potpisom, odnosno pečatom uz korišćenje sertifikata čija se obnova traži.

U suprotnom sprovodi se postupak u skladu sa tačkom 3.3.1.1. ovog dokumenta.

### Identifikacija i potvrđivanje identiteta korisnika za ponovno izdavanje sertifikata nakon opoziva

Identifikacija i potvrđivanje identiteta podnosioca zahteva za ponovno izdavanje sertifikata nakon opoziva sprovodi se u skladu sa procedurom inicijalnog utvrđivanja identiteta iz tačke 3.2. ovog dokumenta.

### Identifikacija i potvrđivanje identiteta korisnika za ponovno izdavanje sertifikata nakon isteka

Identifikacija i potvrđivanje identiteta podnosioca zahteva za ponovno izdavanje sertifikata nakon isteka, sprovodi se u skladu sa procedurom inicijalnog utvrđivanja identiteta iz tačke 3.2. ovog dokumenta.

### Identifikacija i potvrđivanje identiteta korisnika za oporavak sertifikata

Oporavak sertifikata sprovodi se iz razloga i uz uslove navedene u tački 4.7.1. ovog dokumenta.

Identifikacija i potvrđivanje identiteta podnosioca zahteva za oporavak sertifikata sprovodi se u skladu sa procedurom inicijalnog utvrđivanja identiteta iz tačke 3.2. ovog CPS dokumenta.

## Identifikacija i potvrđivanje identiteta kod zahteva za opoziv i suspenziju sertifikata

PKSCA sprovodi opoziv, suspenziju i reaktivaciju sertifikata na osnovu podnesenog zahteva. Potvrđivanje identiteta podnosioca zahteva sprovodi se kako bi se utvrdeo identitet fizičkog lica u svojstvu podnosioca zahteva, odnosno da je li ta osoba ovlašćena za njegovo podnošenje.

### Identifikacija i potvrđivanje identiteta podnosioca zahteva kod opoziva i suspenzije sertifikata

PKSCA ili RA sprovodi identifikaciju i potvrđivanje identiteta podnosioca zahteva za opoziv ili suspenziju sertifikata, u zavisnosti od načina dostave zahteva:

* Lično podnošenje zahteva za opoziv ili suspenziju u registracijskoj kancelarijiji RA mreže.

Identifikacija i potvrđivanje identiteta sprovodi se neposrednom identifikacijom podnosioca zahteva na osnovu njegove identifikacione isprave ili upoređivanjem potpisa podnosioca zahteva i podataka na zahtevu sa potpisom i podacima prikupljenih prilikom registracije.

* Podnošenje zahteva za opoziv ili suspenziju poštanskom dostavom ili dostavom preko dostavljača.

Identifikacija i potvrđivanje identiteta podnosioca zahteva sprovodi se u RA upoređivanjem potpisa podnosioca zahteva i podataka na zahtevu sa potpisom i podacima prikupljenih prilikom registracije.

* Elektronska dostava zahteva za opoziv ili suspenziju preko registrovanog naloga korisnika.

Identifikacija i potvrđivanje identiteta podnosioca zahteva sprovodi se:

* verifikacijom i validacijom zahteva potpisanog naprednim elektronskim potpisom ili pečatiranog najmanje naprednim elektronskim pečatom, kreiranim na osnovu kvalifikovanog sertifikata koji je generisan od strane PKSCA CA, ili su kreirani na osnovu kvalifikovanog sertifikata koji je izdao kvalifikovani pružalac usluga od poverenja, ili
* autentikacijom putem lozinke registrovanog podnosioca zahteva.
* Podnošenje zahteva za opoziv ili suspenziju telefonskim putem

Identifikacija podnosioca zahteva sprovodi se predstavljanjem podnosioca svojim imenom i prezimenom, kao i navođenjem naziva pravnog lica ukoliko je sertifikat za koji se podnosi zahtev povezan sa pravnim licem. Potvrđivanje identiteta podnosioca zahteva sprovodi se na osnovu podataka unetih prilikom registracije korisnika. Telefonskim putem se može izvršiti samo privremena suspenzija, dok se puna supenzija ili opoziv vrše na osnovu zahteva koji se popunjava elektronski.

### Identifikacija i potvrđivanje identiteta podnosioca zahteva kod reaktivacije sertifikata

Potvrđivanje identiteta podnosioca zahteva sprovodi se kako bi se utvrdio identitet fizičkog lica u svojstvu podnosioca zahteva, kao i da li je ta osoba ovlašćena za podnošenje zahteva.

PKSCA ili RA sprovodi identifikaciju i potvrđivanje identiteta podnosioca zahteva za reaktivaciju sertifikata postupkom neposredne identifikacije podnosioca zahteva, u skladu sa tačkom 3.2.3.1. ovog dokumenta.

# Operativni zahtevi vezani za životni ciklus sertifikata

Za pristup nekoj od usluga od poverenja, korisnik je dužan da:

* popuni i potpiše zahtev za uslugu od poverenja,
* popuni i potpiše ugovor,
* ispuni zahteve za identifikaciju,
* ispuni finansijske obaveze prema cenovniku koji je objavljen na javno dostupnim internet stranicama.

## Izdavanje sertifikata

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

### Ko može podneti zahtev za kvaligifkovani elektronski sertifikat

Zahtev za uslugu od poverenja podnose sledeći subjekti, osim ako im propisi, odnosno akti doneti na osnovu propisa isto sprečavaju:

* Zahtev za izdavanje kvalifikovanog elektronskog sertifikata za elektronski potpis za fizička lica mogu podneti ta fizička lica – građani.
* Zahtev za izdavanje kvalifikovanog elektronskog sertifikata za elektronski potpis za ovlašćeno (zaposleno) lice mogu podneti to lice ili lice koje je ovlašćeno za podnošenje ovog tipa dokumenata.
* Zahtev za izdavanje kvalfikovanog elektronskog sertifikata za elektronski pečat mogu podneti ovlašćeni predstavnici.
* Zahtev za usluge potpisivanja, validacije i Usluge izdavanja vremenskog žiga mogu podneti fizicka lica ili ovlašćeni predstavnici pravnog lica.

Zahtev za korišćenje usluge od poverenja sadrži podatke na osnovu kojih Sertifikaciono telo PKS može da stupi u kontakt sa korisnikom te usluge od poverenja.

Ugovor sadrži uslove izdavanja i korišćenja usluge od poverenja, a stupa na snagu potpisivanjem obe ugovorne strane.

Obrada zahteva na strani RA vrši se na licu mesta. Obrada zahteva na strani Sertifikacionog tela vrši se u periodu ne dužem od 10 radnih dana. Ukoliko postoji potreba da ovaj rok bude duži, PKSCA je dužno da o tome obavesti korisnike na svojoj internet stranici.

Korišćenje usluge od poverenja regulisano je ugovorom i vezuje se za dan pokretanja usluge.

Sertifikaciono telo PKS će odobriti zahtev za uslugu od poverenja, ukoliko su ispunjeni sledeći uslovi:

* korisnik je lično podneo identifikacionu dokumentaciju,
* sva dokumentacija je uspešno primlјena i proverena,
* svi podaci uneti u zahtev smatraju se odgovarajućim i kompletnim.

Ako korisnik ne ispuni uslove iz prethodnog stava Sertifikaciono telo PKS će odbiti zahtev za uslugu od poverenja.

### Postupak prijave korisnika sa podnošenjem zahteva za izdavanje kvalifikovanog elektronskog sertifikata

Za svako izdavanje novog sertifikata obvezno je podnošenje zahteva za izdavanje sertifikata.

Za svako inicijalno izdavanje sertifikata korisnik sa PKSCA sklapa ugovor o obavljanju usluga od poverenja.

Zahtev za izdavanje sertifikata može se podneti u elektronskom obliku u okviru portal usluga PKS.

#### Proces podnošenja zahtjeva za izdavanje sertifikata

Izdavanje kvalifikovanih elektronskih sertifikata, vrši se na sledeći način:

* Korisnik se registruje na portalu PKS
* Nakon provere, dobija pravo pristupa i popunjava odgovarajući zahtev uz ličnu odgovornost za istinitost unetih podataka
* Zahtev se proverava i automatski prosleđuje u RA deo PKSCA
* RA služba PKSCA proverava podatke i prosleđuje ih u centralni sistem za generisanje odgovarajuće usluge od poverenja
* Korisnički privatni kriptografski klјuč, generiše se u sigurnom hardverskom kriptografskom modulu u sertifikacionom telu, za usluge od poverenja gde je to i neophodno
* Korisnik preuzima informacije o pristupu uslugama od poverenja u lokalnom registracionom telu za nove korisnike, ili putem interneta za ranije identifikovane korisnike.
* Na osnovu dobijenih informacija, korisnik aktivira nalog i bira model multifaktorske autentikacije.

Prvom upotrebom elektronkog sertifikata od strane korisnika, ta usluga se smatra prihvaćenom. Predviđeno je da prva upotreba bude potpisivanje izjave da je usluga aktivna.

Ukoliko se naknadno utvrdi da u podacima za korišćenje usluge od poverenja postoje pogrešni podaci, korisnik je dužan da se obrati Sertifikacionom telu PKS, radi korekcije podataka.

Zamena javnog klјuča i izmena podataka u kvalifikovanom elektronskom sertifikatu se ne vrši. Ceo proces se izvršava izdavanjem novog kvalifikovanog elektronskog sertifikata.

Sertifikaciono telo PKS je dužno da opozove kvalifikovani elektronski sertifikat iz sledećih razloga:

* gubitka, oštećenja ili zloupotrebe tehničkih sredstava (hardvera ili softvera) ili privatnog kriptografskog klјuča, odnosno kompromitovanja ili sumnje u kompromitovanje privatnog kriptografskog klјuča,
* promene podataka u sertifikatu, koje zahtevaju izdavanje novog sertifikata,
* neispunjavanja obaveza korisnika sertifikata određenih praktičnim pravilima i ugovorom,
* naknadnog utvrđivanja da podaci koje je dostavio korisnik pri identifikaciji nisu tačni,
* ukoliko opoziv kvalifikovanog elektronskog sertifikata zahteva korisnik sertifikata,
* ukoliko korisnik kvakifikovanog elektronskog sertifikata izgubi poslovu sposobnost ili pravno lice kojem pripada korisnik prestane da postoji,
* ukoliko se promene okolnosti koje bitno utiču na važenje sertifikata,
* iz drugih razloga koji su utvrđeni Zakonom i drugim propisima koji regulišu ovu oblast.

Opoziv kvalifikovanog elektronskog sertifikata može da zahteva:

* korisnik kvalifikovanog elektronskog sertifikata,
* Sertifikaciono telo PKS,
* nadležni državni organ na osnovu zakona.

Posle opoziva kvalifikovanog elektronskog sertifikata, korisnik može da zahteva izdavanje novog kvalifikovanog elektronskog sertifikata.

Registar opozvanih sertifikata je stalno dostupan za *on-line* proveru opozvanosti kvalifikovanih elektronskih sertifikata.

Korisnici i treća lica su dužni da provere status kvalifikovanog elektronskog sertifikata na osnovu javno dostupnog registra opozvanih sertifikata Sertifikacionog tela PKS.

Ako korisnik zna ili sumnja u kompromitaciju njegovog privatnog klјuča dužan je da odmah prestane sa njegovim korišćenjem i podnese zahtev za opoziv kvalifikovanog elektronskog sertifikata.

Sertifikaciono telo PKS može da suspenduje kvalifikovani elektronski sertifikat u toku proveravanja okolnosti u vezi sa mogućim opozivom sertifikata.

Korisnik prestaje sa korišćenjem kvalifikovane usluge od poverenja posle:

* isteka roka korišćenja kvalifikovanog elektronskog sertifikata,
* isteka roka važnosti kvalifikovanog elektronskog sertifikata,
* izvršenog opoziva kvalifikovanog elektronskog sertifikata.
* isteka uplate za korišćenje usluga od poverenja koje podrazumevaju plaćanje.

#### Odgovornosti i obveze u procesu podnošenja zahteva za kvalifikovanim uslugama od poverenja

Korisnici sa PKSCA sklapaju ugovor o obavljanju usluga od poverenja kojim prihvataju ova Praktična pravila i uslove pružanja usluga od poverenja.

Ugovor se potpisuje kvalifikovanim elektronskim potpisom ili naprednim elektronskim potpisom na osnovu kvalifikovanom elektronskom sertifikatu koji je izdao PKSCA.

# Obrada zahteva za izdavanje kvalifikovanog elektronskog sertifikata

### Provera identifikacije i potvrđivanje identiteta

Identifikacija i potvrđivanje identiteta fizičkih i pravnih lica iz zahteva provodi se u skladu sa poglavljem 3. ovog dokumenta.

Pri preuzimanju zahteva za izdavanje sertifikata obliku Službenik za registraciju u RA mreži provodi sljedeći postupak:

* Nakon primanja zahtjeva za izdavanje sertifikata na kom je označeno izdavanje kvalifikovanog sertifikata, službenik za registraciju pregleda primljeni zahtev zbog kontrole, u skladu sa postupcima opisanim u tačkama 3.2.2., 3.2.3. i 3.2.5. ovog dokumenta.
* Ako zahtev nije tačno i u celini pravilno popunjen, službenik za registraciju odbija takav zahtjev u skladu sa tačkom 4.2.2. ovog dokumenta i podnosioca zahteva upućuje na ispravno i tačno popunjavanje zahtjeva.

### Odobravanje ili odbijanje zahteva za izdavanje kvalifikovanog sertifikata

Službenik za registraciju u RA mreži proverava podatke iz dostavljenih ili prikupljenih dokumenata i potvrđuje tačnost i integritet informacija u zahtevu za izdavanje elektronskog sertifikata. Službenik za registraciju potvrđuje uspešnu i pravilnu identifikaciju podnosioca zahteva

Odobravanje ili odbijanje zahteva za uslugu izdavanja kvalifikovanog elektronskog sertifikata sprovodi službenik za registraciju u RA u kojem je korisnik podneo zahtev. On prosleđuje zahtev na dalju realizaciju, ili ga odbija.

Ukoliko službenik za registraciju ili PKSCA RA sistem odbije zahtev za izdavanje sertifikata, podnosioc zahteva se o tome, kao i o razlozima odbijanja obaveštava na isti način na koji je podneo zahtev. Ukoliko je podnosioc zahteva fizički prisutan u kancelariji RA mreže, podnosioc se obaveštava usmenim putem.

Zahtjev za izdavanje kvalifikovanog elektronskog sertifikata može se odbiti zbog:

* + - * nepravilno podnesenog zahteva, odnosno ugovora,
      * netačnih ili nepotpunih podataka,
      * nepotpune ili neispravne priložene dokumentacije,
      * prethodnih neodgovarajućih postupaka i nepoštivanja ugovornih obveza korisnika,
      * zakonske zabrane.

### Vreme obrade zahteva za izdavanje sertifikata

U redovnim okolnostima vreme obrade zahteva za izdavanje kvalifikovanih elektronskih sertifikata je do pet radnih dana od momenta prijema kompetne dokumentacije i registrovane uplate u RA mreži.

Ako podnosioc zahteva ne kompletira dokumentaciju za izdavanje kvalifikovanog elektronskog sertifikata u roku od 60 dana od dana podnošenja zahteva, smatra se da je odustao od zahteva za izdavanje kvalifikovanog elektronskog sertifikata.

## Izdavanje sertifikata

PKSCA izdaje kvalifikovani elektronski sertifikat nakon sprovođenja svih procesa provere podataka, odobrenja zahteva za izdavanje sertifikata od strane službenika zaposlenog na tim poslovima. Generisanje sertifikata sprovodi se na siguran način kako bi se osigurala autentičnost sertifikata. Iz tog razloga PKSCA ima implementirane mere kojima se spečava falsifikovanje sertifikata.

Mere protiv falsifikovanja sertifikata uključuju:

* korišćenje propisanih algoritama i parametara kao i mera zaštite privatnih ključeva,
  + - * korišćenje propisanih metoda dokazivanja pristupa privatnim korisničkim ključevima,
      * sprečavanje fizičkog i logičkog (online) pristupa sistemu za izdavanje sertifikata od strane neovlašćenih osoba,
      * proveru integriteta kritičnih komponenti sistema,
      * zaštitu računarske mreže,
      * implementaciju i odvajanje poverljivih uloga.

## Prihvatanje kvalifikovanih elektronskih sertifikata

Prihvatanje kvalifikovanih elektronskih sertifikata od strane potpisnika, odnosno ovlašćenog predstavnika preduslov je za korišćenje tog sertifikata.

Prihvatajući kvalifikovani elektronski sertifikat, potpisnik, odnosno ovlašćeni predstavnik prihvata da su sve informacije koje će biti sadržane u tom sertifikatu tačne u trenutku njegovog prihvatanja.

## Par ključeva i upotreba kvalifikovanog elektronskog sertifikata

### Korištenje privatnog ključa i sertifikata od strane korisnika

Korisničkim parom ključeva iz ovog dokumenta u ime potpisnika, odnosno autora pečata upravlja PKSCA kao kvalifikovani pružaoc usluga od poverenja, tako da PKSCA ima obvezu da osigura ove ključeve:

• da je korišćenje privatnog ključa za elektronski potpis isključivo pod kontrolom potpisnika,

• da je korišćenje privatnog ključa za elektronski pečat pod kontrolom autora pečata,

• da se izrada elektronskog potpisa, odnosno elektronskog pečata sprovodi isključivo HSM modulom koji zadovoljava zahteve iz tačke 6.2.1. ovog dokumenta,

• korišćenje para ključeva Subjekta u skladu sa pravilima određenim u tački 1.4.1. ovog dokumenta.

### Korišćenje javnog ključa i sertifikata od strane treće strane

Treća strana koja namerava ostvariti poverenja u sertifikat generisan prema ovom dokumentu treba:

* + - * voditi računa o primerenoj upotrebi i ograničenjima upotrebe sertifikata koja su naznačena u sertifikatu ili na njih upućuju reference u sertifikatu,
      * upotrebljavati sertifikat za elektronski potpis i pripadajući javni ključ isključivo za validaciju elektronskog potpisa, u skladu sa tačkom 1.4.1. ovog dokumenta,
      * upotrebljavati sertifikat za elektronski pečat i pripadajući javni ključ isključivo za validaciju elektronskog pečata, u skladu sa tačkom 1.4.1. ovog dokumenta,
      * proveriti da su svi podaci o identitetu subjekta u sertifikatu ispravno prikazani aplikacijom u koju se može pouzdati,
      * u slučaju validacije elektronskog potpisa, odnosno elektronskog pečata proveriti da je elektronski potpis, odnosno elektronski pečat izrađen privatnim ključem koji odgovara javnom ključu u sertifikatu, za vreme perioda validnosti sertifikata,
      * obaviti proveru roka važenja svih sertifikata u sertifikacionom lancu, pa provesti proveru sertifikata prema postupcima za validaciju lanca sertifikata, u skladu sa dokumentom IETF RFC 5280,
      * obaviti proveru statusa opozvanosti i suspendovanosti sertifikata upotrebom aktuelnih informacija o tim statusima na način opisan u tački 4.10.1. ovog dokumenta.

Kod validacije elektronskog potpisa, odnosno elektronskog pečata treća strana ne sme ostvariti poverenja u sertifikat koji je u vreme izrade elektronskog potpisa, odnosno elektronskog pečata:

* + - * bio van perioda važenja sertifikata, ili
      * bio opozvan.

Poverenjem u tako istekli ili opozvani sertifikat, treća strana gubi garancije dobijena od PKSCA kao pružaoca usluge od poverenja.

## Obnavljanje sertifikata

PKSCA sprovodi obnavljanje sertifikata tako da se za postojeći Subjekt čiji je sertifikat pred istekom generiše novi par ključeva i izdaje sertifikat.

Postupak obnove sertifikata opisan je u sledećoj tački.

## Obnova sertifikata uz generisanje novog para ključeva

PKSCA sprovodi obnavljanje sertifikata na način da se za postojeći Subjekt čiji je sertifikat pred istekom generiše novi par ključeva i izdaje sertifikat.

PKSCA izdaje sertifikat čiji su DN ime i drugi parametri isti kao i parametri sertifikata na koji se zahtev odnosi, ali sa novim serijskim brojem sertifikata, novim vremenskim periodom važenja i novim potpisom istog PKSCA CA, i to nakon sprovedene identifikacije i potvrde identiteta podnosioca zahtjeva za:

* redovnu obnovu sertifikata,
* izdavanje sertifikata nakon isteka,
* ponovno izdavanje sertifikata nakon opoziva

## Izmene u sertifikatu

Korisnici, kao i autori pečata imaju obvezu informisanja PKSCA o potrebi promene podataka koji ulaze u sadržaj sertifikata u roku od sedam dana od nastalih promena, odnosno zatražiti izmene podataka u sertifikatu.

PKSCA sprovodi izmenu podataka u sertifikatu samo u periodu njegovog važenja i ako sertifikat nije opozvan ili suspendovan.

## Opoziv i suspenzija sertifikata

Opoziv ili suspenzija kvalifikovanih elektronskih sertifikata koje generiše PKSCA sprovodi se u skladu sa niže navedenim tačkama..

### Razlozi za opoziv

PKSCA opoziva sertifikat:

* + - * ako neka od informacija sadržanih u sertifikatu postane netačna,
      * u slučaju kompromitovanja privatnog ključa ili ako se pojavi osnovana sumnja da je privatni ključ kompromitovan,
      * ako privatni ključ ili aktivacioni podaci nisu više u jedinstvenom posedu potpisnika, odnosno autora pečata,
      * u slučaju gubitka ili trajne nedostupnosti privatnog ključa,
      * ako prestane odnos između potpisnika i pravnog lica na osnovu kog je generisan sertifikat,
      * ako je PKSCA primila službeno obaveštenje o smrti potpisnika,
      * ako je PKSCA primila službeno obaveštenje o gubitku poslovne sposobnosti potpisnika,
      * u slučaju da sertifikat više nije u skladu sa CP i CPS dokumentima prema kojima je bio generisan,
      * ako sertifikat nije generisan u skladu sa zahtevom,
      * ako sertifikat nije generisan u skladu sa ovim dokumentom,
      * u slučaju otkaza ugovora o obavljanju usluge od poverenja, od strane korisnika,
      * u slučaju službenog obaveštenja o korišćenju sertifikata u nezakonite svrhe,
      * ako PKSCA proceni da sertifikat svojim tehničkim karakteristikama, profilom ili sadržajem ne pruža dovoljan nivo poverenja trećim stranama,
      * u slučajevima kada to nalaže zakon ili drugi propis.

### Ko može tražiti opoziv

Zahtev za opoziv kvalifikovanog elektronskog sertifikata za elektronski potpis može podneti potpisnik.

Zahtev za opoziv kvalifikovanog elektronskog sertifikata za elektronski pečat može podneti ovlašćeni predstavnik.

Zahtev za opoziv kvalifikovanog elektronskog sertifikata moće podneti RA.

PKSCA može opozvati kvalifikovani elektronski sertifikat i na osnovu autentičnog obaveštenja treće strane ili na osnovu autentičnog službenog obaveštenja nadležnog tela.

### Učestalost izdavanja CRL

Sledeća CRL se objavljuje najkasnije 24 sata od prethodnog izdavanja CRL.

### 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/ocsp 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.

### Razlozi za suspenziju

PKSCA vrši suspenziju sertifikata:

* ako potpisnik, ovlašćeni predstavnik ili osoba ovlašćena za zastupanje, zbog sumnji navedenih u tački 4.9.1. podnese zahev za suspenziju sertifikata,
* privremeno do opoziva koji je zatražen iz razloga navedenih u tački 4.9.1., a za vreme dok službenik za registraciju sprovodi sve potrebne provere, neophodne za opoziv sertifikata,
* u slučaju neizvršenja ugovornih obveza od strane korisnika, a koje se odnose na plaćanje pruženih usluga.

### Ko može tražiti suspenziju

Zahtev za suspenziju kvalifikovanog elektronskog sertifikata za elektronski potpis za fizičko lice podnosi potpisnik.

Zahtev za suspenziju kvalifikovanog elektronskog sertifikata za elektronski potpis za ovlašćeno (zaposleno) lice u okviru pravnog lica podnosi potpisnik ili osoba ovlašćena za zastupanje tog pravnog lica.

Zahtev za suspenziju kvalifikovanog elektronskog sertifikata za elektronski pečat podnosi ovlašćeni predstavnik.

Zahtev za suspenziju kvalifikovanog elektronskog sertifikata može podneti RA mreža.

PKSCA može suspendovati kvalifikovani elektronski sertifikat i na osnovu autentičnog obaveštenja treće strane ili na osnovu autentičnog službenog obaveštenja nadležnog tela.

Zahtev za reaktivaciju kvalifikovanog elektronskog sertifikata za elektronski potpis za fizičko lice podnosi potpisnik.

Zahtev za reaktivaciju kvalifikovanog elektronskog sertifikata za elektronski potpis za ovlašćeno (zaposleno) lice u okviru pravnog lica podnosi potpisnik ili osoba ovlašćena za zastupanje tog pravnog lica.

Zahtev za reaktivaciju kvalifikovanog elektronskog sertifikata za elektronski pečat podnosi ovlašćeni predstavnik.

## Usluge provere statusa sertifikata

### Operativna svojstva

PKSCA daje informacije o statusu opozvanosti ili suspendovanosti sertifikata kroz pružanje OCSP servisa i objave CRL.

Informacija o statusu opozvanosti kvalifikovanog elektronskog sertifikata dostupna je putem OCSP servisa i CRL i nakon isteka sertifikata.

Preporuka trećim stranama je da za proveru statusa sertifikata koriste PKSCA OCSP servis, a da se provera statusa upitom u CRL koristiti kao alternativna metoda provere u slučaju nedostupnosti OCSP servisa ili u slučaju da aplikacija treće strane podržava proveru statusa sertifikata samo putem CRL.

Adresa PKSCA OCSP servisa je http://v3.pksca.rs/ocsp, a upisuje se u ekstenziji *Authority Information Access* svih sertifikata koje izdaju PKSCA CA.

CRL za sertifikate koje izdaju PKSCA CA objavljuju se na internet serverima. Na internet serveru objavljuje se objedinjena CRL.

Adrese objave CRL sadržane su u ekstenziji *CRLDistributionPoints* u svakom izdanom sertifikatu.

## Kraj korištenja

Ako Korisnik otkaže ugovor pre isteka sertifikata, PKSCA CA će opozvati sve sertifikate na koje se odnosi taj ugovor.

## Sigurno skladištenje i oporavak privatnog ključa

Sigurno skladištenje privatnih korisničkih ključeva kvalifikovanih elektronskih sertifikata nije dozvoljeno.

# PROVERA SISTEMA, UPRAVLJANJA I RADNIH POSTUPAKA

PKSCA osigurava primerenu zaštitu imovine koja se upotrebljava za pružanje usluga izdavanja kvalifikovanog elektronskog sertifikata 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 kvalifikovanog elektronskog sertifikata 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 kvalifikovanog elektronskog sertifikata primenjuje mere fizičke zaštite PKSCA 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 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 sistema.

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

### 5.1.2. Fizički pristup

Fizički pristup PKSCA 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 ovlastima, a u skladu sa internim pravilom koje reguliše pristupe u zaštićenu zonu.

Osobama koje nemaju ovlašćenje fizičkog pristupa PKSCA 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 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 dodijeljene odgovarajuće poverljive uloge, i uz prethodno ovlašćeje.

Fizički pristup podacima registrovanih korisnika koje prikuplja RA mreža imaju samo ovlašćei zaposlenici PKSCA PKI i ovlašćei zaposleni PKSCA RA mreže, koji lične podatke o fizičkim osobama prikupljaju, čuivaju, 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 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 sistem, PKSCA RA sistem i repozitorium zaštićena je od poplave.

### 5.1.5. Protivpožarna zaštita

PKSCA 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 zazaštićeni 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 kvalifikovanog elektronskog sertifikata, administriranje i implementacije sigurnosnih postupaka, kao i poslovi nadzora delovanja PKSCA PKI obavljaju se unutar odvojenih organizacionih jedinica PKSCA.

Poslovi, obaveze i odgovornosti zaposlenih podijeljene su prema odgovarajućim poverljivim ulogama. Poverljive uloge čine osnovu poverenja u PKSCA PKI i dodeljuju se ovlašćeim 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 kvalifikovanog elektronskog sertifikata sprovodi se odvajanje sledećih dužnosti:

* osobi kojoj je dodijeljena poverljiva uloga Glavni administrator bezbednosti ili Operater registracionog tela ne dodeljuje se poverljiva uloga Sistem evidentičar,
* osobi kojoj je dodijeljena 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 obveze prema Kolektivnom ugovoru, a eventualne kaznene mere određuju se disciplinskim postupkom.

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

### Zahtevi za spoljne saradnike

Za ugovorene spoljne saradnike koji za PKSCA obavljaju deo usluga iz opsega usluga izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata 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 inormacionog 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 dodijeljenom poverljivom ulogom i pripadajućim ovlašćenjima.

## Postupci upravljanja revizionim zapisima

### Tipovi događaja koji se zapisuju

Revizioni zapisi PKSCA sistema sadrže zapise o događajima vezanim za:

* datum i vreme događaja,
* vrstu događaja,
* identitet osobe ili jedinice sistema koja je odgovorna za radnju,
* uspešnost ili neuspešnost događaja koji se prati.

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.

Datum i vreme koji se koriste za revizione zapise događaja u elektronskom obliku serveri u PKSCA PKI svakog sata usklađuju sa NTP serverom koji je sinhronizovan sa izvorom tačnog vremena, a ima odstupanje manje od +/- 1 s u odnosu na UTC vreme.

PKSCA prikuplja revizione zapise u elektronskom ili papirnom obliku o događajima u PKSCA PKI vezanim za:

* upravljanje životnim ciklusom CA ključeva PKSCA CA,
* upravljanje životnim ciklusom HSM modula kojim su zaštićeni privatni ključevi PKSCA CA,
* upravljanje životnim ciklusom korisničkih ključeva koje generiše PKSCA,
* pripremu i izdavanje sigurnih kriptografskih uređaja na kojima se izdaju i kvalifikovani sertifikati,
* upravljanje životnim ciklusom sertifikata koje izdaju PKSCA CA,
* registraciju fizičkog i pravnog lica,
* zahteve za izdavanje, obnovu, opoziv, suspenziju i reaktivaciju sertifikata, kao i prihvatanje i odbijanje tih zahteva,
* sve propisane aktivnosti za proverama,
* izradu CRL-ova i OCSP odgovora,
* autentikaciju korisnika, aktivaciju i upotrebu korisničkih privatnih ključeva u servisu kaligrafije,
* sigurnosne događaje, uključujući događaje uspešnog i neuspešnog pokušaja pristupa PKI sistemu, aktivnosti na PKI i sigurnosnim sistemima, podizanja i spuštanja sistema, ispada sistema i kvara hardvera, aktivnosti zaštitnih uređaja i aktivne mrežne opreme, izmene sigurnosnih postavki Sistema i ulaske u PKSCA zaštićene prostore, kao i izlaske iz tih prostora.

Podaci i događaji koji se zapisuju u revizionim zapisima PKSCA PKI sistema opisani su u internim dokumentima.

Eksterni ugovoreni RA zapisuje revizione zapise onih događaja navedenih u ovoj tački, a koji su obuhvaćeni poslovima koje na osnovu ugovora, za PKSCA obavlja eksterni RA.

### Učestalost obrade revizionih zapisa

Preglede revizionih zapisa PKSCA 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 neovlašćeog 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 kvalifikovanog elektronskog sertifikata,
  + Pravilnici o postupcima izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata,
  + Uslovi pružanja usluga izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata,
  + Zahtevi za izdavanje kvalifikovanih kvalifikovanog elektronskog sertifikata,
  + Ugovor o pružanju usluge izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata,
* Podaci i pripadajuća dokumentacija prikupljena postupkom registracije pravnih i fizičkih lica i poslovnih subjekata,
* podaci i dokumentacija vezana uz sigurne kriptografske uređaje,
* sertifikati i podaci vezani za životni ciklus pojedinog sertifikata, uključujući sve zahteve i obaveštenja za opoziv, suspenziju i reaktivaciju sertifikata, kao i pripadajuće izvršene radnje,
* evidencija opozvanih i suspendovanih sertifikata, podaci o opozivu, suspenziji i reaktivaciji sertifikata, kao i pripadajuća dokumentacija,
* revizioni zapisi iz tačke 5.4.1. ovog dokumenta,
* drugi PKSCA interni dokumenti.

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 zaštićen 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 (unutarnji ili spoljašni)

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 CA ključa

Radi potrebe osiguranja kontinuiteta pružanja usluge izdavanja kvalifikovanih sertifikata PKSCA će dovoljno vremena pre isteka PKSCA CA sertifikata, generisati novi par ključeva za PKSCA CA. Takođe, PKSCA će dovoljno vremena ranije generisati novi par CA ključeva i u slučaju kada tu promenu zahteva nivo sigurnosti kriptografskog algoritma privatnog PKSCA CA ključa u upotrebi.

Par ključeva PKSCA CA generiše se na način opisan u tački 6.1 ovog dokumenta. Novi sertifikat PKSCA CA sa novo generiranim javnim ključem potpisuje se privatnim ključem PKSCA Root CA.

O planiranoj promeni ključa PKSCA CA, PKSCA će pravovremeno obavestiti učesnike PKSCA PKI objavom informacija na stranicama PKSCA PKI repozitoriuma iz tačke 2.2.1. ovog dokumenta. Novi sertifikat PKSCA CA dostupan je učesnicima PKSCA PKI putem internet stranica repozitoriuma.

Novi sertifikat PKSCA CA će se dostaviti potpisnicima, autorima pečata i trećim stranama na način na koji se dostavlja postojeći PKSCA CA sertifikat, u skladu sa tačkom 6.1.4. ovog dokumenta.

## 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 kvalifikovanog elektronskog sertifikata.

Plan kontinuiteta poslovanja revidira se jednom godišnje.

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

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

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

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

### Postupci u slučaju kompromitovanja privatnog ključa ili incidenata

U slučaju kompromitovanja privatnog ključa za PKSCA sistem pripadajući sertifikat biti će 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 ili gubitka kalibracije PKSCA će putem internet stranica PKSCA repozitoriuma za sve korisnike i pouzdajuće strane objaviti informacije za jasnu identifikaciju izdatih kvalifikovanog elektronskog sertifikata koji sadrže neispravne podatke.

PKSCA će o opozivu sertifikata za PKSCA sistem obaveštavati korisnike PKSCA:

* 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 Praktičnim pravilima.

### Mogućnost nastavka poslovanja nakon nepogode

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

## Prestanak rada PKSCA CA ili RA

U slučaju prestanka rada eksternog ugovorenog RA raskida se ugovor između PKSCA i eksternog RA, pa se ukidaju i sva ovlašćenja tog RA, uključujući ovlašćenja svih službenika u tom RA, kao i sva ovlašćenja eksternog RA za dostavu zahteva za izdavanje, opoziv suspenzije i reaktivacije sertifikata u PKSCA PKI sistem. Poslove ugovorenog RA koji prestaje sa radom može preuzeti PKSCA RA mreža. Detaljnije odredbe vezane za prekid rada eksternog ugovorenog RA određuju se ugovorom.

O planiranom prestanku pružanja usluga izdavanja kvalifikovanih sertifikata Fina će:

* obavestiti sve korisnike usluge, treće strane i centralno nadležno telo državne najmanje tri meseca pre planiranog prestanka pružanja usluga izdavanja kvalifikovanih sertifikata,
* za svaki raskinuti ugovor između PKSCA i eksternog RA ukidaju se sva ovlašćenja eksternog RA u skladu sa opiom navedenim prethodno u ovoj tački,
* uložiti sav napor da kod drugog kvalifikovanog pružaoca usluga od poverenja osigura nastavak pružanja usluga izdavanja kvalifikovanih sertifikata i da će tom pružaocu usluga dostaviti svu dokumentaciju prikupljenu u postupku registracije korisnika kao i svu dokumentaciju o izdatim sertifikatima,
* na tog pružaoca usluga preneti svoju obavezu da trećim stranama u toku razumnog vremena omogući raspoloživost PKSCA CA sertifikata u kojima su javni ključevi PKSCA CA-ova, kao i raspoloživost drugih sertifikata sa javnim ključevima PKSCA usluga od poverenja,
* na tog pružaoca usluga preneti svoju obavezu omogućavanja raspoloživosti CRL za sve opozvane korisničke sertifikate i sertifikate PKSCA CA-ova koji prestaju sa radom,
* na tog pružaoca usluga preneti svoju obavezu pružanja informacija putem OCSP servisa o opozvanim korisničkim i PKSCA CA sertifikatima,
* opozvati sve generisane kvalifikovane sertifikate i uništiti privatne ključeve korisnika u slučajevima kad PKSCA čuva i upravlja korisničkim ključevima u servisu kaligrafije,
* opozvati sertifikate PKSCA CA-ova koji prestaju sa radom i uništiti pripadajuće privatne ključeve tih CA-ova.

U slučaju prestanka pružanja usluga izdavanja kvalifikovanih sertifikata PKSCA će arhivirati, zaštititi i čuvati zapise prema odredbama iz tačke 5.5. ovog dokumenta, 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 pravnim licem 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 i za izdavanje kvalifikovanog elektronskog sertifikata.

Konkretni postupci i mere zaštite koje se preduzimaju u cilju postizanja zahtevanog nivoa sigurnosti interne su prirode i ne objavljuju se javno.

## Generisanje i instalacija para ključeva

### 6.1.1. Generisanje para ključeva

PKSCA provodi generisanje para ključeva za PKSCA sistem koristeći kriptografske algoritme za generisanje ključeva koji su uskladjeni sa standardom ETSI TS 119 312.

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

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

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

O sprovedenom generisanju PKSCA QTSA TSU ključeva vodi se zapisnik.

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

Javni ključ PKSCA servisa služi za proveru potpisa vremenskog žiga, a nalazi se u sertifikatu za PKSCA 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 kvaliteta parametara javnog ključa

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

### 6.1.5. Namene ključeva

Sertifikat PKSCA CA u ekstenziji *Key Usage* ima postavljene vrednosti *keyCertSign* i *cRLSign*. PKSCA CA pripadajući privatni ključ koristi samo za:

* potpisivanje korisničkih sertifikata i sertifikata za RA,
* potpisivanje sertifikata za potpis odgovora OCSP servisa,
* potpisivanje sertifikata za PKSCA servis izdavanja kvalifikovanih vremenskih žigova,
* potpisivanje pripadajuće CRL.

Kvalifikovani sertifikat namenjen za službenika u PKSCA RA mreži u ekstenziji *Key Usage* koja je označena kritičnom (*critical*) ima postavljenu vrednost *nonRepudiation*. Službenik u PKSCA RA mreži pripadajući privatni ključ sme upotrebljavati samo za izradu elektronskih potpisa.

Kvalifikovani sertifikat za elektronske potpise u ekstenziji *Key Usage* koja je označena kritičnom (*critical*) ima postavljenu vrednost *nonRepudiation*. Potpisnik pripadajući privatni ključ sme upotrebljavati samo za izradu elektronskih potpisa.

Kvalifikovani sertifikat za elektronske pečate u ekstenziji *Key Usage* koja je označena kritičnom (*critical*) ima postavljenu vrednost *digitalSignature*. Autor pečata pripadajući privatni ključ sme upotrebljavati samo za izradu elektronskih pečata.

Sertifikat za servis izdavanja kvalifikovanih vremenskih žigova u ekstenziji *Key Usage* ima postavljene vrednosti *digitalSignature* i *nonRepudiation*. Servis izdavanja kvalifikovanih vremenskih žigova pripadajući privatni ključ upotrebljava samo za potpisivanje kvalifikovanih vremenskih žigova.

## Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

### Standardi i tehničke mere zaštite kriptografskog modula

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

Zaštita privatnih ključeva za kvalifikovane sertifikate. koji se koriste u sklopu servisa kaligrafje sprovodi se HSM modulom koji zadovoljava zahteve prema FIPS 140-2 nivo 3.

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

HSM moduli kojim se štite privatni ključevi PKSCA CA-ova i servisa kaligrafije u oblaku smešteni su u prostoru najvišeg nivoa sigurnosti u okviru PKSCA PKI zaštićenog prostora. Fizički pristup ovim HSM modulima sprovodi se uz dualnu kontrolu ovlašćenih osoba sa poverljivim ulogama u PKSCA PKI.

Upravljanje PKCA CA privatnim ključevima potpisnika sprovodi se uz najmanje dualnu kontrolu osoba sa poverljivim ulogama u PKSCA PKI. Pri upravljanju privatnim ključevima PKSCA CA osobe sa poverljivim ulogama koriste pripadajuće upravljačke kartice kriptografskog modula na principu n od m.

### Sigurno skladištenje privatnog ključa

Nije dozvoljeno skladištenje privatnih ključeva PKSCA CA-ova.

Nije dozvoljeno skladištenje privatnih korisničkih ključeva povezanih sa kvalificikovanim sertifikatima.

### Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje privatnih ključeva PKSCA sistema provodi se uz dualnu kontrolu ovlašćenih osoba sa poverljivim ulogama u PKSCA, u prostoru najvišeg nivoa sigurnosti u okvru zaštićenog prostora PKSCA. Privatni ključ koristi se iz HSM 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 ključeva PKSCA sistema imaju isključivo ovlašćene osobe sa poverljivim ulogama u PKSCA.

### Arhiviranje privatnog ključa

Nije dozvoljeno arhiviranje privatnih ključeva PKSCA CA-ova.

Nije dozvoljeno arhiviranje privatnih ključeva povezanih sa kvalifikovanim sertifikatima.

### Prenos privatnog ključa

Za vreme dok je izvan HSM modula privatni 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. Privatni ključevi prenose se iz HSM modula isključivo u svrhe izrade sigurnosne kopije.

Kod prenosa privatnog TSU ključa iz jednog HSM modula u drugi HSM privatni ključ se smije prenositi samo u HSM jednake ili više razine sigurnosti u odnosu na HSM iz kojega se privatni ključ prenosi.

### Čuvanje privatnog ključa u kriptografskom modulu

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

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

### Metoda aktivacije privatnog ključa

Aktivacija privatnih ključeva za PKSCA 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 HSM-a upotrebljava upravljačku karticu kriptografskog modula i pripadajući tajni PIN.

Jednom aktiviran, privatni ključ ostaje aktiviran bez vremenskog ograničenja.

### Metoda deaktivacije privatnog ključa

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

Deaktivacija privatnih 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 ključevi subordinanatnih PKSCA CA-ova deaktiviraju se:

* zaustavljanjem PKSCA CA serverskog procesa,
* isključenjem HSM-a,
* isključenjem servera povezanog sa HSM-om.

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

### Metoda uništavanja privatnog ključa

Postupak uništavanja privatnog ključa provodi se nakon isteka perioda važenja privatnog ključa, zbog kompromitovanja ili opravdane sumnje u kompromitovanost privatnog ključa, ili zbog prestanka njegovog korišćenja, a sprovode ga ovlašćene osobe sa poverljivim ulogama u PKSCA, uz minimalno dualnu kontrolu. Postupkom uništavanja privatnog 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 arhiviraju se u svrhu pružanja dokaza o izdatim elektronskim vremenskim žigovima u sudskim, upravnim i drugim postupcima.

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

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

Rok važenja sertifikata po vrstama je dat u tabeli:

|  |  |
| --- | --- |
| **Sertifikat** | **rok** |
| PKSCA CA sertifikat | 10 godina |
| Kvalifikovani sertifikati za elektronski potpis | 3 godine |
| Kvalifikovani sertifikati za elektronski pečate | 3 godine |

PKSCA CA sertifikat se izdaje sa vremenom validnosti koje ne prelazi period validnosti PKSCA Root CA sertifikata.

Vremenski period validnosti privatnog ključa jednak je vremenskom periodu validnosti pripadajućeg sertifikata. Nije dozvoljena upotreba privatnih ključeva nakon isteka perioda validnosti pripadajućih sertifikata, nakon opoziva sertifikata ili za vreme dok je sertifikat suspendovan.

### Upravljanje životnim ciklusom kriptografskih modula

PKSCA 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 koje ima ovlašćenja za izvršavanje operacija upravljanja kriptografskim modulom.

PKSCA 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 ključem za PKSCA generišu se i instaliraju prilikom postupka generisanja pripadajućeg privatnog ključa.

### Zaštita aktivacionih podataka

Aktivacioni podaci povezani s privatnim ključem za PKSCA podijeljeni 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 ovlašćee osobe nakon autentikacije. Kontrola pristupa operativnim sistemima PKSCA servera dopušta pristup samo ovlašćenom osoblju sa poverljivim ulogama u PKSCA.

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

Identifikacija i potvrđivanje identiteta za svaku poverljivu ulogu u PKSCA sprovodi se korištenjem 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 sistem zaštite od zlonamernog koda, a zabranjeno je korištenja 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 kvalifikovanog elektronskog sertifikata 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 kvalifikovanog elektronskog sertifikata u odnosu na bezbednost, pouzdanost i kvalitet delovanja, a u skladu sa važećim propisima.

U slučaju povrede sigurnosti PKSCA 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 uticaj 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 kvalifikovanog elektronskog sertifikata i informacija štiti se antivirusnom zaštitom i upotrebom autorizovanog softvera.

Sprovodi se praćenje raspoloživih kapaciteta PKSCA PKI Sistema, a procjenjuje 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 zastitnim 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 ograničena 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 neovlašćeog pristupa, uključujući pristup korisnika i trećih strana.

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

## Upotreba vremenskog žiga

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

# SADRŽAJ SERTIFIKATA, LISTA OPOZVANIH SERTIFIKATA I OCSP PROFILI

## Profil sertifikata PKSCA QTSA

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

Subordinantni PKSCA CA izdaju sertifikate prema profilima koji su određeni ovim dokumentom. Zavisno od namene sertifikata, pravilima prema kojima je sertifikat generisan, nivou sigurnosti i načinu čuvanja pripadajućih privatnih ključeva, svaki tip sertifikata ima definisan jedinstveni PKSCA OID (CP OID)

### 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 Tablici 7.1.

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

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

### 7.1.4. Oblici naziva

Oblici naziva za PKSCA Root CA i za subordinantne PKSCA CA opisani su u tački 1.3.1. ovog dokumenta.

Oblici naziva za sertifikate koje izdaju subordinantni PKSCA CA opisani su u tačkama 3.1.1. i 3.1.4. ovog dokumenta.

### 7.1.5. Ograničenja u nazivima

Ekstenzija *Name Constraints* se ne koristi.

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

Ekstenzija *Certificate Policies* sertifikata sadrži odgovarajuće PKSCA OID-ove. U delu 1.1.2. ovog dokumenta naveden je popis tipova kvalifikovanih sertifikata kao i pripadajući PKSCA OID-ovi politike sertifikacije u ekstenziji *Certificate Policies*.

### 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 sa preporukom IETF RFC 6960.

### Broj(evi) verzije

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

### OCSP ekstenzije

Ekstenzije odgovora PKSCA OCSP servisa prikazane su:

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

Ni jedna od ovih ekstenzija nije postavljena kao kritična

# PROVERA USKLJAĐENOSTI

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 uskljađenosti obavlja se u cilju potvrđivanja da PKSCA kao kvalifikovani pružalac usluga od poverenja, koje PKSCA pruža, uključujući uslugu izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata, 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 uskljađenosti

Eksterna provera uskljađenosti sprovodi se najmanje svaka 24 mjeseca, u skladu sa zahtevima Uredbe (EU) br. 910/2014 i standarda 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 ocjenjuje

Kontrolno telo za ocenjivanje usklađenosti i pripadajući ocenjivači nezavisni su od PKSCA i sistema 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 kvalifikovanog elektronskog sertifikata 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 pravo 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 kvalifikovanog elektronskog sertifikata 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 kvalifikovanog elektronskog sertifikata.

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 svezi sa uspostavom i pružanjem usluga izdavanja kvalifikovanog elektronskog sertifikata, a koje učesnici označe poverljivim, ili određenom vrstom ili stepenom tajnosti, ili koji su po 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 kvalifikovanog elektronskog sertifikata, 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 obvezan 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 kvalifikovanog elektronskog sertifikata 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 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 kvalifikovanog elektronskog sertifikata, 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 kvalifikovanog elektronskog sertifikata. 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 usluge 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 kvalifikovanog elektronskog sertifikata.

### Ovlašćenje za korištenje ličnih podataka

PKSCA je ovlašćena, osim za potrebe ispunjenja zakonskih obveza, odnosno ugovornih obveza po ugovoru o pružanju usluga izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata, 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 pravo intelektualnog vlasništva na softver koji se koristi u PKSCA PKI, a koji je u vlasništvu trećih strana.

Privatni ključevi i pripadajući sertifikati za PKSCA sistem, koji se koriste za potpisivanje kvalifikovanog elektronskog sertifikata, vlasništvo su PKSCA.

## Obaveze učesnika

### Obveze PKSCA

PKSCA kao kvalifikovani pružalac usluga izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata obavezuje se:

* + - * sprovoditi pružanje usluga izdavanja kvalifikovanog elektronskog sertifikata 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 kvalifikovanog elektronskog sertifikata,
      * sprovoditi zahtevane sigurnosne mere za zaštitu prostora i opreme sistema za izdavanje kvalifikovanog elektronskog sertifikata,
      * osigurati nesmetan rad i maksimalnu raspoloživost usluga izdavanja kvalifikovanog elektronskog sertifikata 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 kvalifikovanog elektronskog sertifikata sa pažnjom dobrog stručnjaka,
      * primenjivati u svom poslovanju organizacione i tehničke mere zaštite podataka prikupljenih od korisnika pri ugovaranju korišćenja ove usluge i te podatke čuvati kao poslovnu tajnu, a koristiti ih isključivo za potrebe usluga izdavanja kvalifikovanog elektronskog sertifikata 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 sistema za izdavanje kvalifikovanog elektronskog sertifikata u najkraćem mogućem roku,
      * planirati održavanje i dalji razvoj sistema za izdavanje kvalifikovanog elektronskog sertifikata 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 korištenje usluga izdavanja kvalifikovanog elektronskog sertifikata o javno objavljenim i dostupnim uslovima pružanja usluge izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata.

### Obaveze Korisnika

Korisnik je obvezan:

* prilikom predaje zahteva za korištenje usluga izdavanja kvalifikovanog elektronskog sertifikata u zahtevu navesti tačne i istinite lične podatke, a odmah obavestiti PKSCA, kao pružaoca usluga, o svakoj promeni tih podataka,
* čuvati privatni ključ i pripadajuće aktivacione podatke koji se odnose na način kojim pristupa usluzi izdavanja kvalifikovanog elektronskog sertifikata,
* za korišćenje usluge od poverenja plaćati PKSCA naknadu u skladu sa cenovnikom usluga iz tačke 9.1. ovih Praktičnih pravila.

Korisnik se obvezuje 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

Treća strana dužna je samostalno i svesno doneti odluku o razumnom poverenju u sertifikat.

Razumnim poverenjem smatra se odluka treće strane da veruje u sertifikat ako je u vreme ostvarenja pouzdanja:

* preduzela potrebne mere opreza i koristila sertifikat u svrhe propisane ovim dokumentom, odnosno uslovima pružanja usluge, pod okolnostima u kojima je poverenje razumno i u dobroj nameri, pod okolnostima koje su poznate ili bi trebale biti poznate trećoj strani pre ostvarenja poverenja,
* koristila aplikacijsko rešenje i IT okolinu u koju se može verovati,
* proverila period važenja sertifikata,
* proverila status opozvanosti ili suspendovanosti sertifikata, a što treća strana utvrđuje sprovodeći proveru statusa sertifikata putem OCSP servisa ili na osnovu zadnje objavljene CRL, kako je propisano ovim dokumentom,
* proverila da je elektronski potpis, odnosno elektronski pečat izrađen privatnim ključem koji odgovara javnom ključu u sertifikatu za vreme perioda validnosti sertifikata.

Korišćenje javnog ključa i sertifikata od strane treće strane opisano je u tački 4.5.2., a zahtevi za proveru opoziva sertifikata navedeni su u tački 4.9.6. ovog dokumenta.

Treća strana koja nije poštovala propise i ovaj dokument i nije postupala u skladu sa obvezama i odgovornostima iz ove tačke, sama snosi sve rizike poverenja u takav sertifikat.

Treća strana snosi sve rizike poverenja u sertifikat ako zna, ili ima razloga da smatra da postoje činjenice koje mogu prouzrokovati ličnu ili poslovnu štetu prouzrokovanu korišćenjem sertifikata.

## Odgovornosti učesnika

### Odgovornosti PKSCA

PKSCA kao kvalifikovani pružalac usluge izdavanja kvalifikovanog elektronskog sertifikata za elektronski potpis u oblaku i kvalifikovanog elektronskog sertifikata za elektronski pečat u oblaku ima punu odgovornost za pružanje usluga izdavanja kvalifikovanog elektronskog sertifikata i za ispunjenje svih zahteva propisanih ovim Praktičnim pravilima.

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

Ova Praktična pravila sastavni su deo ugovora o pružanju usluga izdavanja kvalifikovanog elektronskog sertifikata koji sklapaju korisnik i PKSCA kao pružalac usluga izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata.

### Odgovornosti Korisnika

Korisnik je dužan:

* u procesu registracije predstaviti se na način propisan u poglavlju 3. i u tački 4.1.2.2. ovog dokumenta,
* pažljivo koristiti i čuvati sredstvo za izradu elektronskog potpisa ili pečata, privatne ključeve i aktivacione podatke u skladu sa ovim dokumentom,
* preduzeti odgovarajuće mere zaštite sredstva za izradu elektronskog potpisa, odnosno elektronskog pečata, privatnog ključa i aktivacionih podataka od neovlašćenog pristupa i upotrebe u skladu sa poglavljem 6. ovog dokumenta,
* pregledati i proveriti tačnost sadržaja sertifikata,
* u najkraćem mogućem roku zatražiti opoziv, odnosno suspenziju sertifikata u slučaju kompromitovanja privatnog ključa, gubitka ili oštećenja sredstva za izradu elektronskog potpisa, odnosno elektronskog pečata, privatnog ključa i aktivacionih podataka, u skladu sa tačkom 4.9. ovog dokumenta,
* dostaviti u RA sve potrebne podatke i informacije o promenama koje utiču ili mogu uticati na tačnost elektronskog potpisa, odnosno elektronskog pečata u roku iz tačke 4.8. ovog dokumenta,
* koristiti sertifikat i pripadajući privatni ključ u skladu sa zakonima i drugim propisima Republike Srbije, a u skladu sa odredbama iz tačke 1.4.1. i 1.4.2. ovog dokumenta,
* delovati u skladu sa svim ostalim odredbama iz ovog dokumenta koje se odnose na obveze korisnika.

Potpisnik, odnosno pravno lice odgovorni su za tačnost i ispravnost podataka dostavljenih u postupku registracije.

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

U slučaju promene kontakt podataka, nastale promene korisnik je dužan dostaviti u PKSCA koristeći podatke navedene u tački 9.11. ovog dokumenta.

Pravno lice, odnosno osoba ovlašćena za zastupanje tog pravnog lica, dužna je u najkraćem mogućem roku zatražiti opoziv elektronskog sertifikata izdanog ovlašćenoj (zaposlenoj) osobi koja više nije zaposlena u tom pravnom licu ili više nije na drugi način povezana sa tim pravnim licem.

Autor pečata dužan je u najkraćem mogućem roku dostaviti u PKSCA eventualnu promenu ovlašćenog predstavnika povezanog sa sertifikatom za elektronski pečat.

Korisnik odgovara za nepravilnosti koje su nastale zbog neispunjavanja obaveza utvrđenih gore navedenim odredbama iz ove tačke.

Korisniku koji ne postupa u skladu sa preuzetim obvezama može biti opozvan sertifikat, tako da će izgubiti sva prava proizašla iz ugovora o korišćenju usluga od poverenja.

### Odgovornosti trećih strana

Treća strana dužna je samostalno i svesno doneti odluku o razumnom poverenju u kvalifikovani elektronski sertifikat.

Razumnim poverenjem smatra se odluka treće strane da sertifikat smatra ispravnim ako je u vreme ostvarenja poverenja:

* preduzela potrebne mere opreza i koristi sertifikat u svrhe propisane ovim dokumentom, odnosno uslovima pružanja usluge, pod okolnostima u kojima je poverenje razumno i u dobroj nameri, pod okolnostima koje su poznate ili bi trebale biti poznate trećoj strani pre ostvarenja poverenja,
* koristila aplikaciono rešenje i IT okolinu u koju se može verovati,
* proverila period validnosti kvalifikovanog elektronskog sertifikata,
* proverila status opozvanosti ili suspendovanosti sertifikata, što treća strana utvrđuje sprovodeći proveru statusa sertifikata putem OCSP servisa ili na osnovu zadnje objavljene CRL, kako je propisano ovim dokumentom,
* proverila da je elektronski potpis, odnosno elektroniski pečat izrađen privatnim ključem koji odgovara javnom ključu u kvalifikovanom elektronskom sertifikatu za vreme perioda validnosti sertifikata.

Korišćenje javnog ključa i sertifikata od strane treće strane opisano je u tački 4.5.2., a zahtevi za proveru opoziva sertifikata navedeni su u tački 4.9.6. ovog dokumenta.

Treća strana koja nije poštovala propise i ovaj dokument i nije postupala u skladu sa obavezama i odgovornostima iz ove tačke, sama snosi sve rizike poverenja u takav sertifikat.

Treća strana snosi sve rizike poverenja u sertifikat ako zna ili ima razloga smatrati da postoje činjenice koje mogu prouzrokovati ličnu ili poslovnu štetu prouzrokovanu korišćenjem kvalifikovanog elektronskog sertifikata.

## 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 kvalifikovanog elektronskog sertifikata.

PKSCA nije odgovorna za štete u sledećim slučajima:

* kad je šteta nastala zbog neautorizovane upotrebe korisničkih ključeva i sertifikata,
* kad je šteta nastala upotrebom sertifikata koja nije dopuštena ovim dokumentom,
* kad je šteta prouzrokovana prevarnom ili nemarnom upotrebom sertifikata, CRL ili OCSP servisa,
* kad je šteta nastala kao rezultat neispravnosti i grešaka u softveru i hardveru korisnika i treće strane,
* kad je šteta nastala kao rezultat prevarnog davanja podataka i prevarnog predstavljanja fizičkog ili pravnog lica tokom procesa identifikacije i potvrde identiteta, ako je identifikaciju i proveru podataka RA mreža sprovodila u skladu sa zahtevima iz ovog dokumenta i radnim procedurama.

## Ograničenja odgovornosti

Ukupna finansijska odgovornost PKSCA za kvalifikovane elektronske sertifikate izdate prema ovim Praktičnim pravilima, kao i za transakcije obavljene na osnovu poverenja u tako izdate sertifikate iznosi najviše 1.000.000 eura u dinarskoj protivvrednosti, a osigutranje po jednom štetnom događaju maksimalno 20.000 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 kvalifikovanog elektronskog sertifikata odgovora oštećenom, odnosno svakom drugom učesniku, ako koristi uslugu na osnovu lažnog predstavljanja prilikom prijave na servis za izdavanje kvalifikovanog elektronskog sertifikata.

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

PKSCA je odgovorna osobi koja veruje u izdati elektronski sertifikat samo ako je ta odgovornost jasno uspostavljena ugovorom, ovim Praktičnim 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 dodijeljuje 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 kvalifikovane elektronske sertifikate izdate od tog dana primenjuju se odredbe iz tog dokumenta.

Novi dokument Praktičnih pravila ne utiče na važenje kvalifikovanog elektronskog sertifikata koji su izdati primenom prethodnih dokumenata Praktičnih pravila.

## 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 korišćenjem 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 |

## Izmene i dopune

### Procedure izmena i dopuna

Ova Praktična pravila rada PKSCA revidira po potrebi.

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 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 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 novoobjavljenog dokumenta Praktičnih pravila naznačeni su na njegovoj naslovnoj strani 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 kvalifikovanog elektronskog sertifikata 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, ETSI EN 319 421. ETSI EN 319 401-1 i ETSI EN 319 411-2.

## Usklađenost sa primenjivim propisima

Ova Praktična pravila i pružanje usluga izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata 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 kvalifikovanog elektronskog sertifikata 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 kvalifikovanog elektronskog sertifikata.

Pre sklapanja ugovora o pružanju usluga izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata korisnici se informišu o uslovima pružanja usluga izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata. Prihvatanje uslova pružanja usluga izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata preduslov je za izdavanje kvalifikovanih kvalifikovanog elektronskog sertifikata.

Pre sklapanja ugovora o obavljanju usluga izdavanja kvalifikovanog elektronskog sertifikata korisnici se informiraju o uslovima pružanja usluga izdavanja kvalifikovanih kvalifikovanog elektronskog sertifikata

# Istorija dokumenta

|  |  |  |  |
| --- | --- | --- | --- |
| Verzija | Datum | Opis | Autor |
| 1.0 | 25.10.2019. | Radna verzija | Dušan Berdić |
| 2.0 | 25.12.2019 | Finalna verzija | Dušan Berdić |

PRIVREDNA KOMORA SRBIJE

02.01-Broj:

28. decembar 2019 godine

B e o g r a d