Praktična pravila rada

za pružanje kvalifikovane usluge izdavanja kvalifikovanih elektronskih sertifikata u cloud-u

OID CPS dokumenta (1.3.6.1.4.1.31266.10.1.4)

- verzija 3.1.-

Sadržaj

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

Praktična pravila rada za pružanje kvalifikovaneusluge izdavanja kvalifikovanih elektronskih sertifikata u cloud-u

1. UVOD

Sertifikaciono telo Privredne komore Srbije (u nastavku: PKSCA), kao registrovani pružalac usluga od poverenja, izdaje kvalifikovane elektronske sertifikate u cloud-u u skladu sa Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima (Službeni glasnik RS, br. 94/2017 - u daljem tekstu: Zakon).

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

1.1. Pregled

Hijerarhijska struktura PKSCA zasnovana je na dvoslojnoj arhitekturi sertifikacionih tela (engl. *Certification Authorities*, u daljem tekstu: CA tela), koju čine:

- ***PKS CA Root***, kao korensko sertifikaciono telo;
- ***PKS CA Class1***, kao podređeno sertifikaciono telo za pružanje kvalifikovane usluge izdavanja kvalifikovanih sertifikata za elektronski potpis na smart karticama;

- ***PKS CA Cloud***, kao podređeno sertifikaciono telo za pružanje kvalifikovane usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa odnosno pečata.
- ***PKS CA TSA,*** kao podređeno sertifikaciono telo za pružanje kvalifikovane usluge izdavanja kvalifikovanih vremenskih žigova.

U okviru ovako definisane hijerarhije, **PKS CA Cloud** je sertifikaciono telo koje vrši uslugu izdavanja kvalifikovanih elektronskih sertifikata u cloud-u.

PKSCA utvrđuje Praktična pravila pružanja usluge izdavanja kvalifikovanog elektronskog sertifikata u cloud-u (u daljem tekstu: Praktična pravila) u skladu sa Zakonom i Politikom pružanja kvalifikovanih usluga od poverenja PKSCA (u daljem tekstu: CP). Praktična pravila obezbeđuju korisnicima dovoljno informacija na osnovu kojih se mogu upoznati sa obimom usluge i odlučiti o prihvatanju usluge.

Politika pružanja kvalifikovanih usluga od poverenja PKSCA i Praktična pravila rada za uslugu izdavanja kvalifikovanog sertifikata u cloud-u su javni dokumenti.

PKSCA je odgovorno za pružanje kompletnih usluga sertifikacije, koje uključuju sledeće servise:

- Registracija korisnika
- Formiranje asimetričnog para ključeva korisnika za elektronsko potpisivanje/ pečaćenje
- Formiranje kvalifikovanih elektronskih sertifikata
- Upravljanje procedurom opoziva kvalifikovanih elektronskih sertifikata i
- Obezbeđivanje statusa opozvanosti kvalifikovanih elektronskih sertifikata.

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

PKSCA je evidentirano i akreditovano od strane nadležnog organa za poslove akreditacije i supervizije PKI (Public Key Infrastructure) sistema u Srbiji (Ministarstvo trgovine, turizma i telekomunikacija) i predmet je periodične supervizije u cilju ocene usaglašenosti sa zahtevima Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima.

PKSCA kao pružalac usluga izdavanja kvalifikovanih elektronskih sertifikata uključuje svoj vlastiti OID u sertifikate koje izdaje. U kvalifikovanim elektronskim sertifikatima koje PKSCA

izdaje u cloud-u nalazi se identifikator ovih Praktičnih pravila (PKSCA OID: 1.3.6.1.4.1.31266.10.1.4).

1.1.1. Opseg i namena

Praktična pravila definišu način na koji pružalac usluge izdavanja kvalifikovanog sertifikata u cloud-u ispunjava tehničke, organizacione i proceduralne zahteve poslovanja koji su određeni u CP dokumentu.

Praktična pravila pokrivaju organizacione i tehničke mere koje PKSCA primenjuje u praksi prilikom utvrđivanja identiteta korisnika, izdavanja i upravljanja životnim ciklusom kvalifikovanih elektronskih sertifikata i upravljanja sredstvima elektronske identifikacije (eID means) u okviru usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa/pečata (QSCD). Ovaj dokument je usaglašen sa odredbama standarda ETSI TS 119 431-1 “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part1: TSP service components operating a remote QSCD/SCDev” i CEN EN 419 241-1 “Trustworthy Systems Supporting Server Signing – Part1: General System Security Requirements”.

Produkcioni sertifikati iz opsega Praktičnih pravila sastavni su deo Registra digitalnih sertifikata PKSCA.

Namena ovog dokumenta je definisanje pravila i operativnih procedura iz područja određenog njegovim opsegom, a prema kojima postupaju korisnici PKSCA navedeni u tački 1.3. ovog dokumenta.

Struktura ovog dokumenta izrađena je na osnovu standardizovanog dokumenta IETF RFC 3647 (November 2003) Internet X.509 Public Key Infrastructure; Certificate Policy and Certification Practices Framework.

1.1.2. Tipovi sertifikata

PKS CA Cloud izdaje kvalifikovane elektronske sertifikate za:

- Fizička lica
- Ovlašćena lica u okviru pravnih lica
- Pravna lica (za elektronske pečate)
- Nerezidente (fizička lica koja nemaju državljanstvo Republike Srbije u okviru pravnih lica registrovanih na teritoriji Republike Srbije)

Grupe, tipovi i profili sertifikata koje izdaje PKS CA Cloud sertifikaciono telo dati su u poslednjoj verziji dokumenta „Pregled profila sertifikata PKSCA“.

1.2. Naziv dokumenta i identifikacija

Praktična pravila definišu konkretne detalje implementacije, pravila i procedure rada PKSCA tokom izdavanja kvalifikovanih elektronskih sertifikata u cloud-u.

Ovaj dokument se identifikuje na sledeći način:

- **Naziv:** Praktična pravila rada za pružanje usluge izdavanja kvalifikovanog elektronskog potpisa u cloud-u
- **Verzija:** 3.1
- **OID:** 1.3.6.1.4.1.31266.10.1.4
- **Internet adresa na kojoj je dokument objavljen:** http://v3.pksca.rs.

Identifikacioni podaci PKS CA su:

PKS CA
Privredna Komora Srbije
Resavska 13-15
11000 Beograd
Srbija

1.3. Učesnici u PKI sistemu PKS

Učesnici u PKI sistemu PKS CA su:

- Sertifikaciona tela (CA)
- Registraciona tela (RA)
- Pružalac usluga udaljenog elektronskog potpisivanja/pečaćenja (Server Signing application Service Provider – SSASP)
- Korisnici
- Pouzdajuće strane (treće strane)

1.3.1. Sertifikaciona tela PKSCA

Hijerarhijska PKI infrastruktura PKSCA, uspostavljena za pružanje usluge izdavanja kvalifikovanih elektronskih sertifikata za interne i eksterne korisnike u cloud-u, sastoji se od sledećih sertifikacionih tela:

- **PKS CA Root** – korensko samopotpisano sertifikaciono telo koje izdaje sertifikate podređenim CA telima i potpisuje CRL listu na root nivou.
- **PKS CA Cloud** – Podređeno CA telo koje izdaje kvalifikovane elektronske sertifikate za korisnike i sertifikat za sopstveni OCSP servis. Ovo CA telo potpisuje i CRL listu za sertifikate izdate u svom domenu.

Sertifikat PKS CA Root je samopotpisani sertifikat.

PKS CA Cloud sertifikat je potpisan od strane PKS CA Root.

Sertifikati korisnika su digitalno potpisani privatnim ključem PKS CA Cloud.

Sertifikati PKS korisnika se generišu na osnovu validnog zahteva za izdavanjem sertifikata, formiranog na osnovu podataka o korisniku koji se prikupljaju u procesu registracije korisnika. Korisnički sertifikati i pripadajući asimetrični parovi ključeva su namenjeni za kreiranje i validaciju kvalifikovanog elektronskog potpisa/pečata u cloud-u.

Detaljni podaci o sertifikatima dati su u dokumentu “Pregled profila sertifikata PKS CA”.

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

PKS CA Cloud sertifikat dostupan je na internet adresi:
http://v3.pksca.rs/certs/PKSCloud.cer.

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

1.3.2. Registraciona tela PKS CA

Poslovi registracije korisnika za uslugu izdavanja kvalifikovanih elektronskih sertifikata u cloud-u obavljaju se u registracionim telima Sertifikacionog tela PKS. PKSCA ima organizovanu mrežu registracionih tela (u daljem tekstu: PKSCA RA mreža) koja obavlja poslove registracije korisnika za PKS CA.

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

PKSCA može odrediti i drugi odgovarajući način registracije korisnika.

PKSCA 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.

1.3.3. Pružalac usluga udaljenog elektronskog potpisivanja/pečaćenja

PKSCA je pružalac usluga upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa/pečata (Server Signing Application Service Provider – SSASP) i upravlja okruženjem za pružanje ove usluge. Kvalifikovane sertifikate koji se koriste u ovom okruženju izdaje PKS CA Cloud sertifikaciono telo.

SSASP je okruženje koje se koristi za:

- generisanje privatnih ključeva korisnika
- skladištenje privatnih ključeva i sertifikata korisnika
- povezivanje sertifikata korisnika sa privatnim ključem
- povezivanje autentikacionog sredstva sa privatnim ključem
- aktiviranje podataka za kreiranje kvalifikovanog elektronskog potpisa/pečata
- uništavanje (brisanje) privatnih ključeva korisnika

Upravljanje podacima za kreiranje udaljenog elektronskog potpisa/pečata u ime korisnika u SSASP se obavlja u kvalifikovanom sredstvu za kreiranje elektronskog potpisa/pečata (*QSCD*), koje se sastoji od:

- HSM (Hardware Security Module) uređaja
- SAM (Signature Activation Module) softvera

QSCD ispunjava zahteve standarda navedenih u Zakonu o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i Pravilniku o uslovima koje mora da ispunjava kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata i uslovima koje mora da ispunjava imenovano telo (Službeni glasnik RS, br. 94/17). Takođe, QSCD je u okruženju zaštićenom od slučajnog ili namernog modifikovanja (tamper protected).

1.3.4. Korisnici

Korisnike usluga od poverenja koje pruža PKSCA predstavljaju fizička lica, pravna lica, ovlašćena lica u okviru pravnih lica i nerezidenti (strani državljani u okviru pravnog lica registrovanog u Republici Srbiji).

Uslugu od poverenja upotrebljava korisnik čije se ime ili funkcija registruju kod prijave za korišćenje usluge od poverenja.

1.3.5. Pouzdajuće strane (treće strane)

Treće strane su fizička i pravna lica koja se pouzdaju u kvalifikovanu uslugu od poverenja na osnovu razumne pouzdanosti u sertifikat potpisnika, generisan od strane PKS CA.

1.3.6. Ostali učesnici

Nije primenljivo.

1.4. Upotreba sertifikata

1.4.1. Dozvoljena upotreba sertifikata

Sertifikat PKS CA Root sertifikacionog tela i pripadajući par asimetričnih ključeva se koriste isključivo za izdavanje sertifikata njemu podređenih CA tela i potpisivanje liste opozvanih sertifikata (CRL), kao i za validaciju elektronskog potpisa PKS CA Root.

Sertifikati PKS CA Cloud sertifikaciong tela i pripadajući parovi asimetričnih ključeva se koriste za izdavanje korisničkih sertifikata, potpisivanje pripadajuće CRL, izdavanje sertifikata za sopstveni OCSP servis, kao i za validaciju elektronskog potpisa PKS CA Cloud.

Korisnički sertifikati koje izdaje PKS CA Cloud se koriste u usluzi upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa/pečata za većinu transakcija elektronskog poslovanja i elektronske trgovine koje se baziraju na upotrebi kvalifikovanih elektronskih sertifikata i služe za validaciju elektronskog potpisa/pečata korisnika.

1.4.2. Zabranjena upotreba sertifikata

Zabranjena je svaka upotreba PKSCA sertifikata za druge namene, osim dozvoljenih u tački 1.4.1. ovog dokumenta.

1.5. Administracija Praktičnih pravila rada PKS CA

1.5.1. Organizacija administriranja Praktičnih pravila rada

PKSCA je odgovorno za izradu i administraciju Praktičnih pravila i to u smislu periodične kontrole i ažuriranja, kao i vanrednih izmena odgovarajućih odredbi koje proističu iz eventualnih promena u zakonskoj regulativi ili tehničkim karakteristikama primenjenih kriptografskih algoritama i dužina ključeva.

1.5.2. Kontakt osoba

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

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

1.5.3. Osoba koja određuje pogodnost CPS dokumenta

Osoba u PKSCA, odgovorna da su ova Praktična pravila rada (CPS) u saglasnosti sa Politikom pružanja usluga od poverenja (CP), koja je takođe publikovana od strane PKSCA, je:

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

1.5.4. Procedura odobravanja CPS dokumenta

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

Ovaj dokument se može analizirati i po potrebi ažurirati i češće nego jednom godišnje, ukoliko se steknu uslovi za to. Takvi uslovi se odnose, između ostalog, na vanredne promene u zakonskoj regulativi ili odgovarajuća saznanja o kritičnim slabostima primenjenih kriptografskih algoritama i dužine kriptografskih ključeva.

Definicije i skraćenice

1.6.1. Definicije

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

Cloud (Cloud computing – Računarstvo u oblaku) – Predstavlja platformu za isporuku IT resursa (podataka, aplikacija, hardvera) preko računarske mreže, najčešće interneta.

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

1.6.2. Skraćenice

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

CEN – European Committee for Standardization

SAM – Signature Activation Module

SAP – Signature Activation Protocol

SSASP – Server Signing Application Service Provider

2. PUBLIKOVANJE I ODGOVORNOST ZA REPOZITORIJUM

2.1. Repozitorijum

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

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

Sve podatke i dokumentaciju koja se odnosi na pružanje kvalifikovanih usluga od poverenja PKS CA objavljuje na svom repozitorijumu koji se nalazi na internet adresi: http://v3.pksca.rs. Repozitorijum je javno dostupan 24 sata na dan, 7 dana u nedelji.

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

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

2.2. Publikovanje informacija o sertifikatima

PKS CA publikuje informacije o sertifikatima na repozitorijumu iz tačke 2.1. ovog CPS, i to:

- Sertifikate PKS CA (Root i intermediate CA sertifikate),
- Informacije o statusima opozvanosti za sva CA tela (CRL)
- Online informacije o statusu sertifikata izdatih izdatih od strane podređenih CA tela (OCSP)
- Osnovne dokumente rada PKSCA (CP, CPS, standardne forme zahteva za izdavanje sertifikata, standardne korisničke ugovore, itd.).

Korisnički sertifikati se ne objavljuju.

2.3. Učestalost publikovanja

PKSCA analizira i ažurira Praktična pravila za pružanja kvalifikovane usluge izdavanja kvalifikovanih elektronskih sertifikata u cloud-u na godišnjem nivou ili prema ukazanoj potrebi. Ažurirana Praktična pravila se, nakon odobrenja, objavljuju na repozitorijumu iz tačke 2.1. ovog dokumenta.

PKS CA publikuje informacije o statusu opozvanosti izdatih digitalnih sertifikata (CRL liste) periodično i to u tačno određenim intervalima, kako je to precizirano u tački 4.9.7. ovog CPS dokumenta.

2.4. Kontrola pristupa repozitorijumu

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

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

- Preuzimanja CA sertifikata PKSCA,
- Preuzimanja CRL liste PKSCA u cilju validacije sertifikata izdatog od strane PKSCA,

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

Pristup PKSCA repozitorijumu je besplatan. PKSCA zadržava pravo da naplaćuje određena specifična korišćenja svojih servisa.

IDENTIFIKACIJA I AUTENTIKACIJA KORISNIKA

Procedure identifikacije i autentikacije navedene u ovom dokumentu se odnose na sertifikate koje izdaje PKS CA Cloud sertifikaciono telo.

PKSCA autentikuje zahteve strana koje žele da opozovu sertifikate u skladu sa CP i ovim Praktičnim pravilima.

3.1. Dodeljivanje imena

3.1.1. Vrste imena

PKS CA Cloud upisuje u svaki korisnički sertifikat podatke o imenu, odnosno nazivu korisnika i podatak o prebivalištu fizičkog lica, odnosno sedištu pravnog lica. Podaci o imenu ili nazivu odnose se na autentično ime ili naziv korisnika. Polje *Subject* u sertifikatu je usklađeno sa dokumentom IETF RFC 5280 5280 (May 2008) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Sertifikati koji se izdaju fizičkom licu i nerezidentu u polju *Subject* sadrže ime i prezime fizičkog lica.

Sertifikati koji se izdaju ovlašćenom licu u okviru pravnog lica i nerezidentu u polju *Subject* dodatno sadrže i pun naziv pravnog lica, kao i identifikator pravnog lica.

Sertifikati koji se izdaju pravnom licu za elektronski pečat u polju *Subject* sadrže pun naziv pravnog lica, kao i identifikator pravnog lica.

3.1.2. Potreba da imena budu sa realnim značenjem

Podnosilac zahteva za izdavanje sertifikata mora dostaviti autentično lično ime, odnosno naziv pravnog lica u čije ime podnosi zahtev. PKSCA odobrava samo ispravno popunjene zahteva sa imenom, odnosno nazivom koji se može verifikovati.

Imena koja se upisuju u atribute polja *Subject* korisničkog sertifikata moraju imati realno značenje.

PKSCA primenjuje sledeća pravila za atribute polja *Subject*:

- Ime i prezime fizičkog lica mora biti identično onome iz identifikacione isprave,
- Naziv pravnog lica mora biti identičan onome iz nadležnog nacionalnog registra.

Sadržaj ekstenzije sertifikata Subject Alternative Name može biti e-mail adresa korisnika, koja ne mora biti smislena.

Pravila za popunjavanje polja Subject u različitim grupama sertifikata su sledeća:

Naziv grupe sertifikata	Pravilo za realno značenje elemenata polja Subject
PKS CA Cloud kvalifikovani sertifikat za fizička lica	• commonName: Ime i prezime korisnika • givenName: Ime korisnika • surname: Prezime korisnika • localityName: Prebivalište korisnika • countryName: Država korisnika (RS)
PKS CA Cloud kvalifikovani sertifikat za ovlašćena lica u okviru pravnog lica	• commonName: Ime i prezime korisnika • givenName: Ime korisnika • surname: Prezime korisnika • organizationName: Puni ili skraćeni naziv pravnog lica • organizationalIdentifier: PIB i MB pravnog lica • localityName: Sedište pravnog lica • countryName: Država korisnika (RS)
PKS CA Cloud kvalifikovani sertifikat za nerezidente	• commonName: Ime i prezime korisnika • givenName: Ime korisnika • surname: Prezime korisnika • organizationName: Puni ili skraćeni registrovani naziv pravnog lica • organizationalIdentifier: PIB i MB pravnog lica • localityName: Sedište pravnog lica • countryName: Država korisnika
PKS CA Cloud kvalifikovani sertifikat za pravna lica za elektronski pečat	• commonName: Naziv korisnika • givenName: • surname: • organizationName: Puni ili skraćeni registrovani naziv pravnog lica • organizationalIdentifier: PIB i MB pravnog lica • localityName: Sedište pravnog lica • countryName: Država korisnika

Tabela 1. – Pravila za popunjavanje polja *Subject* u različitim profilima sertifikata

3.1.3. Anonimnost korisnika

Anonimnost i pseudonimi korisnika nisu podržani.

3.1.4. Pravila za interpretaciju različitih formi imena

Interperetacija atributa polja Subject po standardu X.520 za različite vrste korisnika je sledeće:

Atribut po X.520	Objašnjenje
Sertifikat koji se izdaje fizičkom licu	
serialNumber (1)	"PNORS" i JMBG
serialNumber (2)	"CA:RS – " i jedinstveni serijski broj u okviru PKSCA sistema
commonName (CN)	Ime i prezime korisnika kako je navedeno u identifikacionoj ispravi
givenName (GN)	Ime korisnika kako je navedeno u identifikacionoj ispravi
surname (SN)	Prezime korisnika kako je navedeno u identifikacionoj ispravi
localityName (L)	Prebivalište korisnika
countryName (C)	Dvoslovčana ISO oznaka države, RS za Republiku Srbiju
Sertifikat koji se izdaje ovlašćenom licu u okviru pravnog lica	
serialNumber (1)	"PNORS" i JMBG
serialNumber (2)	"CA:RS – " i jedinstveni serijski broj u okviru PKSCA sistema
commonName (CN)	Ime i prezime korisnika kako je navedeno u identifikacionoj ispravi
givenName (GN)	Ime korisnika kako je navedeno u identifikacionoj ispravi
surname (SN)	Prezime korisnika kako je navedeno u identifikacionoj ispravi
organizationName (O)	Puni ili skraćeni registrovani naziv pravnog lica
organizationalIdentifier (1)	"VATRS – " i PIB (poreski identifikacioni broj pravnog lica)
organizationalIdentifier (2)	"MB:RS – " i MB (matični broj pravnog lica)
localityName (L)	Sedište pravnog lica
countryName (C)	Dvoslovčana ISO oznaka države, RS za Republiku Srbiju
Sertifikat koji se izdaje nerezidentu	
serialNumber (1)	"PAS" i dvoslovčana ISO oznaka države korisnika i broj putne isprave
serialNumber (2)	"CA:RS – " i jedinstveni serijski broj u okviru PKSCA sistema
commonName (CN)	Ime i prezime korisnika kako je navedeno u identifikacionoj ispravi
givenName (GN)	Ime korisnika kako je navedeno u identifikacionoj ispravi

Atribut po X.520	Objašnjenje
surname (SN)	Prezime korisnika kako je navedeno u identifikacionoj ispravi
organizationName (O)	Puni ili skraćeni registrovani naziv pravnog lica
organizationalIdentifier (1)	"VATRS – " i PIB (poreski identifikacioni broj pravnog lica)
organizationalIdentifier (2)	"MB:RS – " i MB (matični broj pravnog lica)
localityName (L)	Sedište pravnog lica
countryName (C)	Dvoslovčana ISO oznaka države korisnika
Sertifikat koji se izdaje pravnom licu za elektronski pečat	
serialNumber	Jedinstveni serijski broj u okviru PKSCA sistema
commonName (CN)	Naziv korisnika kako je navedeno u identifikacionoj ispravi
organizationName (O)	Puni ili skraćeni registrovani naziv pravnog lica
organizationalIdentifier (1)	"VATRS – " i PIB (poreski identifikacioni broj pravnog lica)
organizationalIdentifier (2)	"MB:RS – " i MB (matični broj pravnog lica)
localityName (L)	Sedište pravnog lica
countryName (C)	Dvoslovčana ISO oznaka države korisnika

Tabela 2. – Interpretacija atributa polja *Subject* za različite vrste korisnika

3.1.5. Jedinstvenost imena

Imena pridružena korisnicima sertifikata izdatih od strane PKS CA Cloud su jedinstvena. Jedinstvenost imena u polju *Subject* sertifikata garantuje se atributima *serialNumber* i *commonName*.

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

PKSCA ne prihvata "trademark" oznake, logoe ili druge grafičke ili tekstualne materijale koji su zaštićeni od kopiranja, a predloženi su za uključenje u sertifikate koje izdaje PKSCA.

3.2. Inicijalna provera identiteta

Službenici RA mreže su dužni da pribave sva potrebna dokumenta za utvrđivanje identiteta podnosioca zahteva za uslugom od poverenja, u skladu sa internim procedurama PKSCA i odgovarajućom zakonskom regulativom.

Provera identiteta lica sa poverljivim ulogama zaposlenih u Sertifikacionom telu PKS sporovodi

se prema internim pravilima PKS i obavlja ih nadležna organizaciona jedinica PKS.

3.2.1. Metoda dokazivanja posedovanja privatnog ključa

Par asimetričnih ključeva korisnika se generiše u okviru samog sertifikacionog tela u procesu izdavanja sertifikata, tako da ne postoji potreba za dokazivanjem posedovanja privatnog ključa od strane krajnjeg korisnika.

Prilikom generisanja para asimetričnih ključeva korisnika sertifikaciono telo se pridržava najbolje prakse i postupaka iz standarda kojim je regulisana ova oblast.

3.2.2. Utvrđivanje identiteta pravnog lica

Zahtevi PKSCA u smislu identifikacije i autentikacije organizacija koje su podnele zahtev za PKSCA sertifikate, uključuju, ali nisu ograničeni, na konsultovanje određenih baza podataka treće strane koje jednoznačno identifikuju organizacije ili proverom dokumenata date organizacije.

U cilju identifikacije i autentikacije organizacije koja je ovlastila svog predstavnika za podnošenje zahteva za kvalifikovani sertifikat, PKSCA može primeniti korake koji uključuju:

- Proveru identifikacionih dokumenata pojedinca, ovlašćenog predstavnika date organizacije, kao što su lična karta ili pasoš, u skladu sa važećim zakonom.
- Utvrđivanje identiteta organizacije koja se bazira na dostavljenoj dokumentaciji.
- Zahtev da osoba bude fizički prisutna u PKS RA u odgovarajućoj fazi procedure, pre nego što se sertifikat izda.

PKSCA može imati i dodatne zahteve za organizaciju podnosioca zahteva, kao što su elektronski potpisani autorizacioni dokumenti (ovlašćenja) ili pribavljanje neke druge identifikacione oznake organizacije, uz poštovanje uslova navedenog u prethodnom stavu.

3.2.3. Utvrđivanje identiteta fizičkog lica

U cilju identifikacije i autentikacije individualnog korisnika koji podnosi zahtev za dobijanje sertifikata, PKSCA može primeniti korake koji uključuju:

- Proveru identifikacionih dokumenata kao što su lična karta ili pasoš, u skladu sa važećim zakonom.
- Utvrđivanje identiteta datog pojedinca koja se bazira na proveri ličnih identifikacionih dokumenata.
- Zahtev je da se pojedinac fizički pojavi u PKS RA u odgovarajućoj fazi procedure, pre nego što se sertifikat izda.

3.2.4. Informacije o korisniku koje se ne proveravaju

Nije primenljivo.

3.2.5. Provera identiteta ovlašćenih lica

Lice koje podnosi zahtev za izdavanje sertifikata u ime pravnog lica mora da obezbedi validnu dokumentaciju od strane pravnog lica koje će biti upisano u sertifikat, u skladu sa tačkom 3.2.2. ovog dokumenta. Naziv pravnog lica koje će biti upisano u sertifikat mora biti identično registrovanom punom ili skraćenom nazivu pravnog lica, na način kako je upisano u podnetoj dokumentaciji.

Službenik PKSCA RA mreže je dužan da proveri identičnost podataka o ovlašćenom fizičkom licu sa ovlašćenja i iz zahteva za izdavanje certifikata. Ovlašćenje mora biti overeno pečatom i potpisom.

PKSCA može zahtevati posebno, elektronski potpisano ovlašćenje od strane datog pravnog lica.

3.2.6. Kriterijumi za interoperabilnost

Nije primenljivo.

3.3. Identifikacija i provera identiteta kod podnošenja zahteva za obnovu sertifikata uz generisanje novog para ključeva

Nije primenljivo.

3.3.1. Identifikacija i provera identiteta za rutinsko obnavljanje ključeva

Nije primenljivo.

3.3.2. Identifikacija i provera identiteta za obnavljanje ključeva nakon opoziva

Nije primenljivo.

3.4. Identifikacija i provera identiteta kod zahteva za opoziv i suspenziju sertifikata

PKSCA vrši opoziv i suspenziju sertifikata na osnovu podnetog zahteva. Zahtevi za opoziv ili suspenziju sertifikata se podnose odgovarajućem PKSCA RRA. PKSCA RRA, nakon provere, prosleđuje zahtev PKSCA, koje realizuje proceduru opoziva ili suspenzije sertifikata.

Provera identiteta podnosioca zahteva se vrši da bi se utvrdio fizički identitet lica koje podnosi zahtev i da li to lice ima ovlašćenja za podnošenje zahteva za opoziv ili suspenziju sertifikata.

Način provere identiteta lica koje podnosi zahtev opisan je u tačkama 3.2.2. i 3.2.3. ovog dokumenta.

4. OPERATIVNI ZAHTEVI TOKOM ŽIVOTNOG CIKLUSA SERTIFIKATA

Procedure upravljanja sertifikatima navedene u ovom dokumentu se odnose na sertifikate koje izdaje PKS CA Cloud sertifikaciono telo.

4.1. Zahtev za izdavanje sertifikata

4.1.1. Ko može da podnese zahtev za izdavanje sertifikata

Zahtev za izdavanje sertifikata od strane PKSCA može da podnese svako fizičko ili pravno lice koje ispunjava sledeće uslove:

- Mora biti prihvatljiv krajnji korisnik PKS kako to definišu politika sertifikacije i ova Praktična pravila.
- Zahtev koji predaje korisnik mora da u sebi sadrži sve neophodne podatke, uključujući dovoljan broj identifikacionih podataka kako bi korisnik mogao da bude identifikovan na jedinstven način.

4.1.2. Proces obrade zahteva za izdavanje sertifikata (enrollment) i odgovornosti

Korisnici sprovode enrolment proces (proces identifikacije, autentikacije i registracije) sa registracionim autoritetom koji zahteva:

- Prihvatanje pravila izdavanja i korišćenja kvalifikovanog elektronskog sertifikata.
- Popunjavanje forme zahteva za izdavanje sertifikata.
- Prihvatanje korisničkog ugovora.

Podnosioci zahteva za izdavanje sertifikata imaju odgovornost da dostave pouzdane i tačne informacije u svojim zahtevima za dobijanje sertifikata.

Registraciju korisnika PKS CA vrše Registracioni autoriteti. RA mogu biti i druga pravna lica sa kojima su posebnim ugovorima regulisani odnosi, prava i obaveze.

Operateri registracionog autoriteta vrše proveru sledećih podataka o korisniku:

- Ime,
- Prezime,
- JMBG,
- Naziv organizacije (privrednog subjekta) koju korisnik predstavlja,
- Matični broj firme,
- Sedište organizacije (naziv grada),
- Poštanski broj grada,
- Adresu organizacije (ulica i broj) i

- E-mail adresu korisnika u navedenoj organizaciji.

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

4.2. Procesiranje aplikacije za dobijanje sertifikata

4.2.1. Postupak identifikacije i autentikacije korisnika

Nakon registracije datog korisnika i prijema aplikacije, centralni PKSCA RA ili PKS RRA vrše identifikacionu i autentikacionu proceduru, definisanu u tačkama 3.2.2. i 3.2.3. ovog dokumenta, u cilju validacije zahteva za izdavanje sertifikata.

4.2.2. Odobravanje ili odbijanje zahteva za izdavanje kvalifikovanog sertifikata korisnika

Nakon validacije zahteva korisnika za izdavanje kvalifikovanog sertifikata, centralni PKSCA RA ili PKS RRA potvrđuju ili odbijaju aplikaciju za izdavanje kvalifikovanog sertifikata.

Ukoliko zakonski uslovi nisu ispunjeni ili podnosilac zahteva nije priložio sve neophodne dokumente, zahtev se odbija.

Ukoliko je zahtev za izdavanje kvalifikovanog sertifikata potvrđen, registracioni autoritet ga prosleđuje do PKSCA radi izdavanja sertifikata.

4.2.3. Potrebno vreme za procesiranje aplikacije korisnika

PKSCA mora da izvrši sve identifikacione aktivnosti i procesira zahtev za izdavanje kvalifikovanog sertifikata u okviru vremenskog perioda od sedam (7) radnih dana od dana dobijanja validnog zahteva.

4.3. Izdavanje sertifikata

4.3.1. Aktivnosti CA tokom procesa izdavanja kvalifikovanog sertifikata

Izdavanje sertifikata za OCSP servis sprovodi se prema formalnoj proceduri uspostave ovog sistema i generisanja para asimetričnih ključeva. Ovu proceduru sprovode lica sa poverljivim ulogama u zaštićenom prostoru PKSCA, uz primenu propisanih mera bezbednosti.

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

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

Kvalifikovani sertifikat se izdaje korisniku ukoliko su ispunjeni sledeći uslovi:

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

PKSCA generiše dve vrste asimetričnih parova ključeva za različite tipove korisnika, i to:

- Asimetrični par ključeva i kvalifikovani sertifikat korisnika za kvalifikovani elektronski potpis – generiše se na QSCD uređaju u PKSCA.
- Asimetrični par ključeva i kvalifikovani sertifikat korisnika za kvalifikovani elektronski pečat – generiše se na QSCD uređaju u PKSCA.

4.3.2. Obaveštenje korisnika od strane CA o izdatom sertifikatu

Sertifikat za autentikaciju i enkripciju i kvalifikovani sertifikat se generišu u okviru PKSCA i upisuju u QSCD.

Korisnik se o izdavanju kvalifikovanog sertifikata obaveštava notifikacijom preko aplikacije na svom mobilnom uređaju.

Ukoliko je zahtev odbijen, korisnik se informiše o razlozima odbijanja koji su definisani Zakonom.

4.4. Prihvatanje sertifikata

4.4.1. Sprovođenje procesa prihvatanja sertifikata

Sertifikat izdat od strane PKSCA se smatra prihvaćenim od strane korisnika ukoliko nastupi bilo koji od dole navedenih događaja:

- Korišćenjem certifikata prvi put (tokom procesa elektronskog potpisivanja ugovora) uz odgovarajući kvalifikovani elektronski potpis korisnika,
- Ukoliko korisnik ne javi da postoje bilo kakvi problemi u izdatom sertifikatu u periodu od 10 (deset) dana od dana izdavanja sertifikata.

Primedba na prihvatanje izdatog sertifikata, bilo koje vrste, mora biti eksplicitno dostavljena PKSCA, kao sertifikacionom telu – pružaocu usluge. Potvrda o odbijanju koja uključuje sva eventualna polja u sertifikatu koja sadrže pogrešne informacije mora takođe biti dostavljena PKSCA.

4.4.2. Objavljivanje sertifikata

Korisnički sertifikati se javno ne objavljuju.

4.4.3. Obaveštenje ostalih učesnika o izdavanju sertifikata

Ostali učesnici se ne obaveštavaju o izdavanju korisničkih sertifikata.

4.5. Korišćenje sertifikata i asimetričnog para ključa

4.5.1. Korišćenje privatnog ključa i sertifikata od strane korisnika

Korisnik se obavezuje da će koristiti privatni ključ i pripadajuće sertifikate izdate od strane PKSCA samo u predviđenim aplikacijama, kao i u skladu sa definisanim načinom korišćenja ključa u samom sertifikatu (*Key Usage* i *Enhanced Key Usage* ekstenzije).

Korišćenje privatnih ključeva i sertifikata predstavlja deo korisnikovog ugovora sa PKSCA. U tom smislu, korisnik može koristiti svoje privatne ključeve samo nakon prihvatanja odgovarajućih sertifikata i aktivacionih podataka.

Korisnik mora da prestane sa korišćenjem svojih privatnih ključeva nakon isticanja perioda validnosti ili opoziva izdatih sertifikata.

4.5.2. Korišćenje javnog ključa i sertifikata od strane pouzdajućih strana

Ukoliko namerava da koristi usluge od poverenja koje pruža PKSCA, pouzdajuća strana je obavezna da prihvata izdate sertifikate PKSCA sa predviđenim načinom korišćenja sertifikata definisanim u samom sertifikatu. Takođe, pouzdajuća strana je obavezna da, u skladu sa propisima, koristi javni ključ koji ekstrahuje iz izdatog sertifikata na dozvoljen način, u skladu sa tačkom 1.4. ovog dokumenta i odgovorna je da sprovodi proveru statusa datog sertifikata korišćenjem metoda validacije lanca sertifikata, prema dokumentu RFC 5280 ili RFC 6960.

Pouzdajuća strana je obavezna da, u slučaju zloupotrebe ili sumnje u zloupotrebu sertifikata koji je izdao PKSCA sistem, odmah obavesti PKSCA (vidi kontakt informacije u tački 1.5.2.).

4.6. Obnavljanje sertifikata bez promene ključa

Obnova sertifikata bez promene ključa je proces u kome sertifikaciono telo izdaje sertifikata za isti javni ključ. PKSCA ne vrši obnovu sertifikata bez promene ključa.

4.7. Obnova sertifikata sa novim ključem (Re-Key)

Obnova sertifikata sa novim ključem (Re-Key) je proces u kome sertifikaciono telo izdaje korisniku novi sertifikat. Novi sertifikat sadrži iste identifikacione podatke o korisniku kao i stari, s tim da sadrži novi korisnički javni ključ.

4.7.1. Uslovi za obnovu sertifikata

Obnova sertifikata uz generisanje novog para ključeva korisnika se vrši kada je:

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

4.7.2. Ko može da zahteva obnovu sertifikata sa novim javnim ključem

Obnovu sertifikata mogu da zatraže svi korisnici PKSCA koji ispunjavaju uslove iz tačke 4.7.1.

4.7.3. Procesiranje zahteva za novi par ključeva i sertifikat

Korisnici kojima je sertifikat istekao, ukoliko žele da dobiju novi sertifikat, moraju da podnesu zahtev za izdavanje novog sertifikata identičan prvobitnom zahtevu za izdavanje sertifikata. U tom slučaju, uvek se generiše novi par asimetričnih ključeva.

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

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

4.7.4. Obaveštenje korisnika da mu je izdat novi sertifikat

Procedura je identična proceduri iz tačke 4.3.2.

4.7.5. Sprovođenje procesa prihvatanja novog sertifikata

Procedura je identična proceduri iz tačke 4.4.1.

4.7.6. Objavljivanje novog sertifikata od strane CA

Procedura je identična proceduri iz tačke 4.4.2.

4.7.7. Obaveštenje drugih entiteta od strane CA o izdavanju novog sertifikata

Ostali učesnici se ne obaveštavaju o izdavanju korisničkih sertifikata.

4.8. Modifikacije sertifikata korisnika

Modifikacija sertifikata je postupak koji omogućava korisnicima da zahtevaju promenu podataka sadržanih u sertifikatu. Ovaj postupak zahteva obnovu sertifikata i obrađuje se kao prvobitni zahtev za izdavanje sertifikata.

4.8.1. Uslovi za modifikaciju sertifikata korisnika

Korisnik može zahtevati modifikaciju sertifikata u slučaju promene bilo kog identifikacionog podatka.

4.8.2. Ko može zahtevati modifikaciju sertifikata

Modifikaciju sertifikata može zatražiti bilo koji korisnik koji ispunjava uslove iz tačke 4.8.1.

4.8.3. Procesiranje zahteva za modifikacijom sertifikata

Modifikacija sertifikata izvodi se na isti način kao i prvobitni zahtev za izdavanje sertifikata.

4.8.4. Obaveštenje korisnika da mu je izdat modifikovani sertifikat

Procedura je identična proceduri iz tačke 4.3.2.

4.8.5. Postupak prihvatanja modifikovanog sertifikata

Procedura je identična proceduri iz tačke 4.4.1.

4.8.6. Objavljivanje modifikovanog sertifikata od strane CA

Procedura je identična proceduri iz tačke 4.4.2.

4.8.7. Obaveštenje ostalih učesnika o izdavanju modifikovanog sertifikata

Ostali učesnici se ne obaveštavaju o izdavanju korisničkih sertifikata.

4.9. Opoziv i suspenzija sertifikata

4.9.1. Uslovi za opoziv sertifikata korisnika

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

- kompromitacije privatnog ključa korisnika sertifikata;
- kompromitacije aktivacionih podataka;
- kompromitacije ili nefunkcionalnosti QSCD;
- prijavljene zloupotrebe ili neautorizovanog korišćenja QSCD;
- ako je korisnik sertifikata narušio materijalne obaveze definisane u CP ili u ovom CPS dokumentu;
- promene informacija sadržanih u sertifikatu datog lica;
- prestanka povezanosti lica koje je korisnik sertifikata i organizacije koja je podnela zahtev;

- prestanka valjanosti sertifikata pre isteka roka trajanja zbog smrti korisnika ili ukoliko više ne postoji osnova po kojoj je sertifikat izdat;
- vanrednih okolnosti ili više sile;
- zahteva suda, javnog tužioca ili istražnog organa, kako bi se sprečilo vršenje krivičnog dela;
- utvrđenih grešaka u podacima na sertifikatu ili QSCD;
- ako korisnik zahteva opoziv iz njemu ličnih razloga.

4.9.2. Ko može zahtevati opoziv sertifikata

Opoziv sertifikata može zahtevati sam korisnik, zakonski zastupnik pravnog lica u slučaju ako se radi o sertifikatima izdatim fizičkim licima koja zastupaju pravna lica ili pravnim licima za potrebe izrade elektronskog pečata, kao i ovlašćeni službenik PKS RA ili PKSCA. Zahtev za opoziv sertifikata može da podnese vlasnik sertifikata, nakon propisne autentikacije, ili odgovarajući službenik PKSCA ili PKS RA uz dokaz da je ispunjen jedan od uslova za opoziv sertifikata naveden u članu 4.9.1.

4.9.3. Procedura zahteva za opoziv sertifikata

U slučaju da je potrebno izvršiti opoziv sertifikata usled ispunjenja uslova iz tačke 4.9.1., korisnik ili ovlašćeni predstavnik pravnog lica mora, u najkraćem mogućem roku, da kontaktira operatera RA i popuni zahtev za opozivom. Zahtev za opozivom je poseban formular koji mora biti elektronski potpisan i dostavljen RA lično, on-line ili nekim drugim kanalom komunikacije.

PKSCA opoziva sertifikat nakon provere identiteta strane koja je zahtevala opoziv (službenik PKS RA ili PKSCA, sam korisnik ili ovlašćeni predstavnik pravnog lica) i potvrdom da je zahtev podnet u skladu sa procedurom zahtevanom u CP i CPS dokumentu.

Provera identiteta podnosioca zahteva za opozivom se vrši na osnovu tačke 3.4. ovog dokumenta.

Operaciju opoziva korisničkih sertifikata vrši RAO. Ona podrazumeva sledeće akcije:

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

Opoziv sertifikata obavezno sadrži datum i vreme opoziva, a proizvodi dejstvo od trenutka unošenja u evidenciju opozvanih sertifikata.

4.9.4. Rok za predaju zahteva za opoziv sertifikata

Subjekt koji je postao svestan okolnosti koje zahtevaju opoziv sertifikata mora da zatraži opoziv u najkraćem mogućem roku i bez nepotrebnog odlaganja.

4.9.5. Vreme za koje CA mora da obradi zahtev za opoziv sertifikata

Registraciono telo odmah i bez odlaganja sprovodi postupak za opoziv sertifikata, a najkasnije 24 sata po prijemu validnog zahteva.

4.9.6. Zahtevi za pouzdajuće strane u vezi provere statusa sertifikata

Pouzdajuće strane imaju obavezu da koriste on-line resurse koje PKSCA čini raspoloživim putem repozitorijuma u cilju provere statusa sertifikata u koje se pouzdaju.

Pouzdajuće strane moraju biti saglasne sa PKSCA politikom sertifikacije a posebno sa obavezama pouzdajućih strana propisanim ovim dokumentom.

4.9.7. Frekvencija izdavanja CRL liste

PKSCA objavljuje listu opozvanih sertifikata (CRL – Certificate Revocation List) na svaka 24 sata.

4.9.8. Maksimalno kašnjenje u izdavanju CRL liste

U regularnim okolnostim kašnjenje u objavi liste opozvanih certifikata nije duže od 1 minuta.

U slučaju vanrednih okolnosti PKSCA će preduzeti sve mere i postupke u okviru svojih mogućnosti da kumulativno kašnjenje objavljivanja liste opozvanih certifikata na godišnjem nivou ne bude duže od 10 dana.

4.9.9. Raspoloživost procedure online provere statusa sertifikata

PKS CA Cloud sertifikaciono telo podržava online proveru statusa izdatih certifikata putem OCSP servisa čiji je rad usaglašen s dokumentom IETF RFC 6960.

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

Adresa OCSP servisa se upisuje u ekstenziji *Authority Information Access* svakog korisničkog sertifikata koji izdaje PKS CA Cloud.

4.9.10. Zahtevi online provere statusa sertifikata

Korišćenje OCSP servisa omogućeno je svim pouzdajućim stranama uz uslov da poseduju aplikaciu koja može da koristi OCSP servis upotrebom GET ili POST HTTP metode.

4.9.11. Raspoloživost drugih formi objavljivanja statusa sertifikata

Nije primenljivo.

4.9.12. Specijalni zahtevi u odnosu na kompromitaciju privatnog ključa

Nije primenljivo.

4.9.13. Uslovi za suspenziju sertifikata

Suspenzija sertifikata se može izvršiti ukoliko je korisnik prekršio odgovarajuća pravila korišćenja sertifikata ili zna da u dužem vremenskom periodu neće koristiti sertifikat i svoj privatni ključ.

Sertifikat se suspenduje u sledećim situacijama:

- Ako suspenziju sertifikata zahteva korisnik sertifikata, zakonski zastupnik pravnog lica (ako je sertifikat izdat fizičkim licima koja zastupaju pravno lice) ili odgovarajući službenik PKSCA ili PKS RA;
- Ako suspenziju sertifikata zahteva nadležni organ za zaštitu podataka ili neki drugi viši organ koji ima opravdane sumnje da sertifikat sadrži neispravne podatke ili da se privatni ključ koji odgovara javnom ključu iz sertifikata može koristiti bez saglasnosti vlasnika;
- Ako suspenziju sertifikata zahteva sud, tužilac ili institucije koje vrše istražne radnje, kako bi sprečili dalje zloupotrebe.

4.9.14. Ko može zahtevati suspenziju sertifikata

Suspenziju korisničkog sertifikata može zahtevati sam korisnik, zakonski zastupnik pravnog lica (ako je sertifikat izdat fizičkim licima koja zastupaju pravno lice ili pravnim licima za potrebe izrade elektronskog pečata), ovlašćeni službenik PKS RA, PKSCA, sud, tužilac ili institucije koje vrše istražne radnje.

4.9.15. Procedura suspenzije sertifikata

Zahtev za suspenzijom sertifikata može biti dostavljen od strane korisnika ili PKS RA. Zahtev se dostavlja u obliku odgovarajućeg dokumenta, elektronski potpisan od strane korisnika ili PKSRA.

Operacija suspenzije sertifikata je identična opozivu s tim što se navodi drugačiji razlog opoziva (Certificate Hold).

4.9.16. Ograničenje perioda suspenzije sertifikata

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

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

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

Sertifikat se aktivira u sledećim situacijama:

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

Operaciju aktiviranja sertifikata vrši operater RA, preduzimajući sledeće akcije:

1. Brisanje serijskog broja sertifikata korisnika iz CRL.
2. Promenu stanja sertifikata korisnika u OCSP-u.

4.10. Servisi provere statusa sertifikata

4.10.1. Operativne karakteristike

PKSCA publikuje sve opozvane i suspendovane sertifikate u svojoj CRL listi.

PKSCA publikuje informacije o statusu korisničkih sertifikata koje izdaje PKS CA Cloud i putem OCSP servisa.

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

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

Adresa OCSP servisa PKS CA Cloud sertifikacionog tela se upisuje se u ekstenziji *Authority Information Access* svih sertifikata koje ovo sertifikaciono telo izdaje.

Adrese objave CRL sadržane su u ekstenziji *CRLDistributionPoints* u svakom izdatom certifikatu.

4.10.2. Raspoloživost servisa

CRL i OCSP servis PKSCA su raspoloživi neprekidno, 24 sata na dan, 7 dana u nedelji.

U slučaju prestanka rada sistema, nastanka okolnosti koje su izvan kontrole PKSCA ili uticaja više sile, usluga će biti dostupna u skladu sa planom kontinuiteta poslovanja PKSCA.

Vreme odziva na zahtev za pristup CRL ili dobijanje OCSP odgovora u normalnim radnim uslovima je manje od 1 sekunde.

4.10.3. Dodatne funkcije

Nije primenljivo.

4.11. Prestanak korišćenja sertifikata

Prestanak korišćenja sertifikata se može ostvariti biti iz sledećih razloga:

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

Nakon prestanka korišćenja sertifikata izdatog od strane PKSCA, sertifikat mora biti opozvan.

4.12. Čuvanje i rekonstrukcija privatnog ključa korisnika

PKSCA čuva privatne ključeve korisnika u bezbednom okruženju QSCD. QSCD ispunjava zahteve standarda navedenih u Zakonu i Pravilniku o uslovima koje mora da ispunjava kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata i uslovima koje mora da ispunjava imenovano telo. Takođe, QSCD je u okruženju zaštićenom od slučajnog ili namernog modifikovanja (tamper protected).

5. BEZBEDNOSNA PROVERA SISTEMA, UPRAVLJANJA I RADNIH POSTUPAKA

PKSCA obezbeđuje odgovarajuću zaštitu imovine koja se upotrebljava za pružanje usluga od poverenja i u tu svrhu vodi celokupni popis imovine sa pripadajućom klasifikacijom koja je u skladu sa procenom rizika.

Mere fizičke zaštite, postupci koje PKSCA primenjuje u zaštiti sistema za pružanje usluga od poverenja (u daljem tekstu: sistem usluga), kao i postupci upravljanja i provere sistema su interne prirode i njihovi detalji se ne objavljuju javno.

5.1. Mere fizičke bezbednosti

PKSCA, kao pružalac usluga od poverenja, primenjuje mere fizičke zaštite sistema usluga sa ciljem minimiziranja rizika vezanih uz fizički zaštitu, u skladu sa poslovnom politikom PKSCA i važećom zakonskom regulativom.

5.1.1. Lokacija i konstrukcija objekta

Primarni produkcioni sistem PKSCA smešten je u zgradi PKS, u posebnom zaštićenom prostoru izdvojenom za tu namenu, uz primenu više nivoa fizičke i tehničke zaštite koje onemogućavaju neovlašćen fizički pristup sistemu i podacima i time sprečavaju kompromitovanje sistema i usluga. Fizička zaštita zasnovana je na konceptu upotrebe bezbednosnih zona, tako da se nivoi zaštite povećavaju svakim prelaskom u sledeću zonu. Zaštita od fizičkog upada ostvarena je bezbednosnim parametrima koji razdvajaju zone postavljene oko sistema za izdavanje usluga od poverenja, u kome se sprovode operacije izrade i opoziva kvalifikovanih sertifikata.

Obezbeđeni prostori i podprostori u kojima se nalaze komponente PKSCA sistema u daljem tekstu nazivaju se zajedničkim nazivom PKSCA zaštićeni prostor.

5.1.2. Fizički pristup

Fizički pristup sistemu usluga u PKSCA zaštićenom prostoru i pripadajućim podprostorima, ostvaruje se dvostrukom kontrolom pristupa ovlašćenih lica PKSCA, a u skladu s njihovim ulogama i ovlašćenjima.

Licima koja nemaju ovlašćenje za fizički pristup sistemu ulaz je dozvoljen samo uz pratnju i stalni nadzor ovlašćenih lica PKSCA, kao i uz dvostruku kontrolu pristupa, u skladu s internim procedurama PKSCA.

O svakom pristupu sistemu vodi se evidencija.

Oprema, informacije, mediji i softver iz PKSCA zaštićenog prostora iznose se isključivo uz minimalno dvostruku kontrolu ovlašćenih lica PKSCA, kojima su dodeljene odgovarajuće uloge

od poverenja i uz prethodno ovlašćenje.

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

5.1.3. Električno napajanje i klimatizacija

Uređaji i prostor u kojem se nalaze PKSCA CA, PKSCA RA sistem, repozitorijum i sistemi tehničke zaštite imaju neprekidno napajanje električnom energijom i klimatizacijom koja je dimenzionirana na način koji osigurava odgovarajuće radne uslove u slučaju prekida napajanja.

5.1.4. Izloženost poplavama i vremenskim nepogodama

Lokacija na kojem se nalaze PKSCA sistem i repozitorijum zaštićena je od poplave.

5.1.5. Prevencija i zaštita od požara

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

5.1.6. Skladištenje medija za čuvanje podataka

Mediji na kojima se nalaze arhivske i sigurnosne kopije PKSCA podataka u elektronskom obliku, kopije sadržaja nosioca i sigurnosne kopije programske opreme skladište se na dve odvojene zaštićene lokacije sa uspostavljenom protivpožarnom zaštitom i zaštitom od poplava. Ovi mediji su zaštićeni od oštećenja, krađe i neovlašćenog pristupa.

5.1.7. Odlaganje otpada

Uređaji i mediji koji sadrže poverljive informacije u elektronskom obliku, a koji više nisu u upotrebi, uništavaju se na bezbedan način, tako da poverljive informacije ne mogu više biti čitljive, niti obnovljene. Uništavanje ovih uređaja i medija odvija se pod nadzorom ovlašćenih lica u PKSCA.

Papirni dokumenti i materijali koji sadrže poverljive informacije se bezbednosno tretiraju pre odlaganja u otpad.

5.1.8. Odlaganje rezervnih kopija

Nije primenljivo.

5.2. Organizacione mere bezbednosti

5.2.1. Poverljive uloge

Poslovi upravljanja informacionim i komunikacionim sistemom, poslovi upravljanja životnim ciklusom sertifikata, administriranje i implementacija sigurnosnih postupaka i poslovi nadzora PKSCA se obavljaju u okviru organizacionih jedinica PKSCA.

Poslovi, obaveze i odgovornosti zaposlenih podeljene su prema odgovarajućim poverljivim ulogama. Poverljive uloge čine osnovu poverenja u PKSCA i dodeljuju se zaposlenima iz nadležnih jedinica PKSCA. Svaka poverljiva uloga je dokumentovama sa jasno definisanim opisom poslova i pripadajućom odgovornošću.

U poverljive uloge PKSCA spadaju:

- Glavni administrator bezbednosti,
- Administrator sistema,
- Sistem operater i
- Sistem evidentičar
- Operater sertifikacionog tela
- Operater registracionog tela

5.2.2. Broj osoba potrebnih za obavljanje aktivnosti

Poslove u PKSCA obavljaju isključivo ovlašćena lica. PKSCA ima dovoljan broj stalno zaposlenih stručnih osoba sa znanjem, iskustvom i kvalifikacijama koji je potreban u PKSCA za pružanje usluga od poverenja.

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

Za obavljanje pojedinih bezbednosno osetljivih zadataka u PKSCA zaštićenom prostoru zahteva se angažovanje više osoba sa određenim poverljivim ulogama.

5.2.3. Identifikacija i provera identiteta za svaku ulogu

Prilikom prijave na kritične aplikacije i servise unutar PKSCA sprovodi se identifikacija i provera identiteta lica koje pristupa aplikaciji ili servisu. Identifikacija i provera identiteta se sprovodi odgovarajućom metodom autentikacije. Pristup aplikacijama i servisima unutar PKSCA omogućen je samo ovlašćenim licima u skladu sa poverljivom ulogom koju obavljaju. Tokom korišćenja kritičnih aplikacija i servisa se beleže, skladište i čuvaju podaci o aktivnosti prijavljene osobe.

5.2.4. Uloge koje zahtevaju razdvajanje dužnosti

Bezbednosni zahtevi usluga od poverenja uzrokuju razdvajanje sledećih dužnosti:

- osobi kojoj je dodeljena poverljiva uloga glavni administrator bezbednosti, sistem operater ili sitem evidentičar ne dodeljuje se poverljiva uloga administrator sistema.
- osobi kojoj je dodeljena poverljiva uloga administrator sistema ne dodeljuje se poverljiva uloga glavni administrator bezbednosti ili sistem evidentičar.

5.3. Kadrovske bezbednosne mere

5.3.1. Kvalifikacije i radno iskustvo

Zaposleni na poslovima PKSCA moraju posedovati odgovarajuća stručna znanja, iskustvo, kvalifikacije i obučenost za rad sa kriptografskim tehnologijama, zaštitom računarskih sistema, informacionom bezbednošću i zaštitom ličnih podataka iz delokruga rada PKSCA.

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

5.3.2. Procedura provere

PKSCA izvršava neophodne aktivnosti u cilju provere biografije, kvalifikacija, kao i neophodnog iskustva u okviru kompetencija neophodnih za specifične poslove. Zaposleni u PKSCA moraju imati potvrdu da nisu zakonski kažnjavani.

PKSCA realizuje relevantne provere kandidata za zasnivanje radnog odnosa na bazi statusnih izveštaja izdatih od strane kompetentnih autoriteta, izjava trećih strana ili izjava samih kandidata.

5.3.3. Usavršavanje osoblja

Zaposlenima koji obavljaju poslove unutar PKSCA obezbeđuje se obuka i usavršavanje u skladu sa njihovim poverljivim ulogama.

Zaposleni PKSCA sa poverljivim ulogama u PKSCA imaju obavezu da se edukuju i usavršavaju.

5.3.4. Periodična provera znanja

Provera znanja o informacionoj bezbednosti sprovodi se jednom godišnje za sve zaposlene u PKSCA.

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

5.3.5. Učestalost i redosled rotacije poslova

Nije primenljivo.

5.3.6. Kaznene mere za neovlašćene radnje

Nepridržavanjem propisanih mera, ovlašćene osobe na radu u PKSCA čine povredu radne obaveze. Kaznene mere za povredu radne obaveze izriču se u disciplinskom postupku.

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

5.3.7. Zahtevi za spoljne saradnike

Spoljni saradnici koji, na osnovu ugovora, obavljaju poslove iz domena pružanja usluga izdavanja kvalifikovanih sertifikata za PKSCA imaju iste obaveze i odgovornosti kao i stalno zaposleni.

Obaveze dobavljača roba i usluga za PKSCA regulisane su internim dokumentima o poslovanju sa dobavljačima. Pristup spoljnih saradnika informacionim uređajima u PKSCA odobrava se isključivo ugovorom, za one informacione uređaje koji su predmet ugovora i samo za aktivnosti navedene u ugovoru.

5.3.8. Dokumentacija koja se dostavlja zaposlenima

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

5.4. Upravljanje audit logovima

5.4.1. Tipovi zabeleženih događaja

PKSCA beleži audit logove događaja u PKSCA vezanih za:

- upravljanje životnim ciklusom CA ključeva PKSCA CA-ova,
- registraciju fizičkog ili pravnog lica,
- pripremu QSCD uređaja na kome se izdaju kvalifikovani sertifikati,
- dostavu aktivacionih podataka korisniku
- autentikaciju korisnika i aktivaciju privatnog ključa na QSCD,
- životni ciklus ključeva i upravljanje ključevima korisnika,
- životni ciklus sertifikata koje izdaju PKSCA CA-ovi,
- zahteve za opoziv, suspenziju i reaktivaciju sertifikata i pripadajuće sprovedene radnje.

Audit logovi uključuju i bezbednosne događaje u PKSCA vezane za promene bezbednosnih politika, fizičku i tehničku zaštitu PKSCA prostora, pokretanje i zaustavljanje rada sistema, sistemske greške i kvarove hardvera, aktivnosti mrežnih barijera i aktivne mrežne opreme i pokušaja pristupa sistemu.

5.4.2. Učestalost procesiranja logova

Audit logovi u PKSCA se kontrolišu redovno na dnevnom nivou. Kontrola audit logova se vrši i u svrhu praćenja i utvrđivanja zlonamernih aktivnosti na sistemu. PKSCA koristi automatske mehanizme za upozorenje i dojavu o mogućim kritičnim bezbednosnim događajima. Takva obaveštenja dostavljaju se ovlašćenim licima u PKSCA. Radnje preduzete na osnovu prikupljanja audit logova se dokumentuju.

5.4.3. Period čuvanja audit logova

Audit logovi sa zapisima iz tačke 5.4.1. čuvaju se najmanje 10 godina od prestanka važnosti sertifikata na koji se odnose.

5.4.4. Zaštita audit logova

Audit logovi u PKSCA su zaštićeni tokom celog perioda čuvanja. Zaštita audit logova obuhvata zaštitu zapisa od neovlašćenog pristupa i očuvanje integriteta zapisa.

Zaštićeni audit logovi su raspoloživi samo ovlašćenim licima, na zahtev, a posebno u svrhu pružanja dokaza za potrebe sudskih postupaka.

5.4.5. Procedure back-up-a audit logova

Audit logovi PKSCA sistema arhiviraju se u dve kopije na fizički odvojenim lokacijama.

Kopije audit logova na sekundarnoj lokaciji štite se jednakim ili višim nivoom zaštite u odnosu na audit logove na primarnoj lokaciji.

5.4.6. Sistem prikupljanja audit logova

Audit logovi se, u zavisnosti od vrste podataka, prikupljaju automatski ili ih prikuplja ovlašćena osoba.

Audit logovi nastali u PKSCA i PKS RA mreži se prikupljaju interno.

5.4.7. Obaveštenje subjekta uzročnika događaja

U slučaju uočavanja zapisa o značajnom događaju u radu PKSCA koji je povezan sa određenim učesnikom, PKSCA zadržava pravo odluke o obaveštavanju učesnika koji je taj događaj prouzrokovao.

5.4.8. Procena ranjivosti sistema

PKSCA obavlja redovnu procenu rizika vezanu za informacionu imovinu, kao i procenu ranjivosti za prepoznate javne i privatne adrese i penetraciono testiranje.

Procena rizika se sprovodi jednom godišnje.

Procena ranjivosti sistema za prepoznate javne i privatne adrese PKSCA sprovodi se kvartalno.

Penetracioni test sprovodi se jednom godišnje.

Svaku novu kritičnu ranjivost PKSCA će razmotriti u roku od 48 sati od njenog prepoznavanja i postupiti u skladu sa utvrđenim procedurama.

5.5. Arhiviranje zapisa/logova

5.5.1. Tipovi arhiviranih zapisa

PKSCA arhivira sledeće podatke koji, u zavisnosti od tipa, mogu biti u elektronskom ili papirnom obliku:

- dokumenti PKSCA politika sertifikacije i praktičnih pravila rada o pružanju usluga od poverenja,
- uslovi pružanja usluga od poverenja,
- ugovori povezani s pružanjem usluga od poverenja,
- podaci i pripadajuća dokumentacija prikupljena postupkom registracije fizičkih osoba i poslovnih subjekata,
- podaci i dokumentacija vezana za kriptografske uređaje,
- podaci vezani za životni ciklus pojedinog sertifikata,
- podaci i dokumentacija vezani za promenu statusa sertifikata,
- audit logovi iz tačke 5.4.1. ovog dokumenta,
- drugi PKSCA interni dokumenti.

Svaki zapis koji se arhivira sadrži podatke o vremenu koji se odnose na taj zapis.

5.5.2. Period čuvanja arhive

Sve arhivirane podatke i dokumentaciju iz tačke 5.5.1. ovog CP dokumenta PKSCA čuva najmanje 10 godina od prestanka važnosti usluge na koju se odnosi.

5.5.3. Zaštita arhive

Arhivirani podaci i dokumentacija štite se mehanizmima i postupcima propisanog nivoa bezbednosti koji garantuju poverljivost i integritet arhive. Arhiva se štiti od neovlašćenog pristupa, izmena i brisanja podataka.

Arhivirani zapisi su raspoloživi samo ovlašćenim licima, na zahtev, a posebno u svrhu pružanja dokaza o usluzi od poverenja za potrebe sudskih postupaka.

5.5.4. Procedura izrade back-up-a arhive

Back-up kopija arhiviranih podataka u elektronskom obliku izrađuje se u PKSCA zaštićenom prostoru i čuva se na bezbedan način, na drugoj lokaciji, izdvojenoj od primarnog produkcionog sistema.

5.5.5. Zahtevi za zaštitu zapisa vremenskim žigom

Nije primenljivo.

5.5.6. Sistem prikupljanja arhivskih zapisa

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

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

5.5.7. Procedure za dobijanje i proveru informacija iz arhive

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

5.6. Promena CA ključeva

PKSCA obezbeđuje da CA tela kontinuirano pružaju kvalifikovane usluge od poverenja sa svojim validnim parom ključeva i pripadajućim CA sertifikatima. Iz tog razloga CA tela će pravovremeno, pre isteka CA sertifikata, generisati novi par CA ključeva. Takođe, CA tela će dovoljno vremena ranije generiseti novi par CA ključeva i u slučaju kada tu promenu zahteva nivo bezbednosti kriptografskog algoritma privatnog CA ključa u upotrebi. U oba slučaja za novi javni CA ključ izdaće se odgovarajući CA sertifikat.

CA tela PKSCA će o promeni svog javnog ključa i o svom novom CA sertifikatu pravovremeno obavestiti korisnike.

Novi pripadajući javni ključevi CA tela biće dostupni korisnicima PKSCA na način na koji su to bili i prethodni, u skladu sa ovim dokumentom.

5.7. Kompromitacija i oporavak u slučaju katastrofe

5.7.1. Procedure za postupanje u incidentnim i kompromitujućim situacijama

Planom kontinuiteta poslovanja PKSCA regulisani su postupci u slučaju nastanka incidenta ili kompromitovanja sistema, koji obuhvataju postupke za oporavak sistema i uspostavu bezbednih uslova za pružanje usluga od poverenja.

Plan kontinuiteta poslovanja PKSCA revidira se najmanje jednom godišnje.

5.7.2. Računarski resursi, softver ili podaci koji su oštećeni

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 sistema obezbeđeno je ugovorima o podršci i održavanju sa dobavljačima opreme.

Plan kontinuiteta poslovanja PKSCA reguliše postupke oporavka sistema usluga u slučaju kvarova ili oštećenja opreme i mrežnih resursa i način oporavka podataka.

5.7.3. Procedure koje se sprovode kod kompromitacije privatnog ključa korisnika

U slučaju kompromitovanja ili sumnje u kompromitovanost privatnog ključa CA, PKSCA će odmah prekinuti sa upotrebom kompromitovanog ključa.

Nakon potvrde kompromitovanosti privatnog ključa, PKSCA donosi odluku o njegovu opozivu i pripadajući CA sertifikat će biti opozvan.

O opozivu PKSCA CA sertifikata PKSCA će obaveštavati sledeće subjekte:

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

Nakon otkrivanja i otklanjanja uzroka koji su prouzrokovali kompromitaciju CA ključa, PKSCA će preduzeti mere za sprečavanje ponavljanja takvog događaja. PKSCA Root CA generisaće novi par CA ključeva za CA čiji je sertifikat opozvan. PKSCA Root CA će za novi javni CA ključ izdati novi CA sertifikat.

CA će upotrebom novog privatnog CA ključa izdati sertifikate postojećim registrovanim korisnicima. Sve naredne informacije o opozvanosti sertifikata će potpisivati upotrebom novog ključa. Novi CA sertifikat biće dostupan korisnicima PKSCA na način na koji je bio dostupan i prethodni CA sertifikat, u skladu sa ovim dokumentom.

U slučaju da korišćeni kriptografski algoritmi i parametri prestanu da pružaju odgovarajuću sigurnost i zaštitu, PKSCA će, ukoliko je to moguće, pravovremeno o tome obaveštavati:

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

PKSCA će razmotriti mogućnost korišćenja odgovarajućih preporučenih sigurnih kriptografskih algoritama i, ukoliko to bude moguće, doneti odluku o korišćenju drugog algoritma. PKSCA će izraditi konkretne planove i postupke koji će obavezno uključivati i sprovođenje opoziva svih sertifikata na koje utiču kriptografski algoritmi i parametri čija je sigurnost narušena. O planovima i rokovima sprovođenja PKSCA će obaveštavati korisnike i treće strane kao korisnike usluga od poverenja.

U slučaju kompromitovanja ili sumnje u kompromitovanost korisničkog privatnog ključa, autentikacionih ili aktivacionih podataka, PKSCA će odmah prekinuti sa upotrebom kompromitovanog ključa.

Nakon potvrde kompromitovanosti korisničkog privatnog ključa, PKSCA donosi odluku o opozivu i opoziva pripadajući korisnički sertifikat.

5.7.4. Mogućnosti kontinuiteta poslovanja nakon katastrofe

U Planu kontinuiteta poslovanja PKSCA predviđeni su postupci za nastavak poslovanja nakon elementarnih nepogoda. U zavisnosti od vrste nepogode, PKSCA će nastojati da pružanje usluge od poverenja nastavi na svom primarnom produkcionom sistemu.

5.8. Završetak rada CA ili RA

PKSCA će, u slučaju planiranog prestanka pružanja usluga izdavanja kvalifikovanih sertifikata:

- obavestiti sve korisnike usluga, treće strane i nadležni organ državne uprave najmanje tri meseca pre planiranog prestanka pružanja usluga od poverenja,
- uložiti sav napor da kod drugog kvalifikovanog pružaoca usluga od poverenja osigura nastavak pružanja usluga izdavanja kvalifikovanih sertifikata i tom pružaocu usluga dostaviti svu dokumentaciju prikupljenu u postupku registracije korisnika kao i svu dokumentaciju o izdatim sertifikatima,
- opozvati sve izdate kvalifikovane sertifikate i uništiti privatne ključeve korisnika u slučajevima kad PKSCA čuva i upravlja korisničkim ključevima,
- opozvati sertifikate PKSCA CA koji prestaju sa radom i uništiti pripadajuće privatne ključeva tih CA.

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 važećom zakonskom regulativom, ili će sa drugim poslovnim subjektom ugovoriti takvo arhiviranje, zaštitu i čuvanje zapisa.

6. TEHNIČKE BEZBEDNOSNE MERE

PKSCA primenjuje sve neophodne tehničke bezbednosne mere u cilju zaštite kriptografskih ključeva i aktivacionih podataka. Kriptografski ključevi koji se štite merama i postupcima opisanim u ovom poglavlju mogu pripadati samom sertifikacionom telu, servisima ili krajnjim korisnicima. Primena pomenutih mera je kritična u smislu garantovanja da su svi ključevi i aktivacioni podaci zaštićeni i da se koriste isključivo od strane autorizovanih zaposlenih, odgovarajućih servisa ili krajnjih korisnika.

Takođe, definisane su i druge tehničke bezbednosne mere koje se primenjuju da bi se bezbedno izvršavale funkcije generisanja ključeva, autentikacije korisnika, registracije korisnika, izdavanja sertifikata, opoziva sertifikata, auditinga i arhiviranja.

U ovom poglavlju se takođe definišu tehničke bezbednosne mere za zaštitu repozitorijuma, registracionih tela, korisnika i drugih učesnika.

6.1. Generisanje i instalacija asimetričnog para ključeva

6.1.1. Generisanje asimetričnog para ključeva

PKSCA prilikom generisanja i upravljanja sopstvenim privatnim ključevima primenjuje odredbe Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i podzakonskih akata koji proizilaze iz njega, kao i evropske i internacionalne standarde u vezi bezbednih i pouzdanih sistema.

PKSCA primenjuje sve mere, postupke i metode propisane ovim dokumentima u cilju bezbednog i pouzdanog generisanja kriptografskih ključeva i sprečavanja njihove kompromitacije ili neautorizovanog korišćenja. Procedure generisanja ključeva su implementirane i dokumentovane u skladu sa CP i ovim Praktičnim pravilima.

PKSCA generiše sledeće asimetrične parove ključeva:

- Za potrebe PKS CA Root sertifikacionog tela – asimetrični par ključeva se generiše na hardverskom bezbednosnom modulu (HSM – Hardware Security Module).
- Za potrebe podređenih CA tela – asimetrični par ključeva se generiše na hardverskom bezbednosnom modulu (HSM – Hardware Security Module).
- Za potrebe korisnika – elektronski potpis – asimetrični par ključeva se generiše na hardverskom bezbednosnom modulu (HSM – Hardware Security Module) i čuva u QSCD uređaju u PKSCA.
- Za potrebe korisnika – elektronski pečat – asimetrični par ključeva se generiše na hardverskom bezbednosnom modulu (HSM – Hardware Security Module) i čuva u QSCD uređaju u PKSCA.

PKSCA koristi bezbedan proces generisanja korenskog privatnog ključa korenskog sertifikacionog tela u skladu sa dokumentovanom procedurom.

PKSCA distribuira deljene tajne za svoje privatne ključeve, vlasnik je privatnih ključeva i poseduje autoritet da prenese odgovarajuće deljene tajne na autorizovane nosioce deljenih tajni, odnosno lica sa poverljivim ulogama u PKSCA.

Privatni ključ korenskog sertifikacionog tela PKSCA se koristi za napredno elektronsko potpisivanje sertifikata podređenih CA tela i liste opozvanih sertifikata (CRL) i u druge svrhe se ne sme koristiti.

Privatni ključ podređenog sertifikacionog tela se koristi za napredno elektronsko potpisivanje sertifikata koji se izdaju korisnicima sa ovog sertifikacionog tela, odgovarajuće CRL i sertifikata za sopstveni OCSP servis i u druge svrhe se ne sme koristiti.

6.1.2. Isporuka privatnog ključa korisniku

Privatni ključevi korisnika se čuvaju na QSCD uređaju i ne isporučuju se korisniku. PKSCA, u svojstvu SSASP, koristi identifikacione procedure koje obezbeđuju da korisnik ima isključivu kontrolu nad upotrebom svog privatnog ključa.

6.1.3. Dostava javnog ključa do sertifikacionog tela

Dostava javnog ključa podređenog sertifikacionog tela vrši se u okviru procedure uspostavljanja sertifikacionog tela.

Dostava javnog ključa OCSP servisa vrši se u okviru formalne procedure uspostavljanja ovog sistema.

Javni ključ korisnika, kao deo asimetričnog para ključeva, se dostavlja do CA u obliku zahteva za izdavanje sertifikata u PKCS#10 formatu.

6.1.4. Dostava javnog ključa sertifikacionog tela trećim stranama

PKSCA dostavlja javne ključeve korenskog i podređenih CA tela, u obliku X.509 v3 sertifikata putem svog online repozitorijuma kome mogu da pristupaju svi korisnici i treće strane.

6.1.5. Dužine ključeva

Za privatni ključ korenskog sertifikacionog tela i odgovarajuće elektronsko potpisivanje, PKSCA koristi SHA-256/RSA kombinaciju hash i asimetričnog algoritma sa dužinom ključa od 4096 bita sa peridom validnosti od 20 godina i periodom izdavanja sertifikata od 20 godina.

Za privatni ključ podređenih CA tela i odgovarajuće elektronsko potpisivanje, PKSCA koristi SHA-256/RSA kombinaciju hash i asimetričnog algoritma sa dužinom ključa od 3072 bita, sa periodom validnosti od 10 godina i periodom izdavanja sertifikata od 10 godina.

Za potrebe OCSP servisa podređenih certifikacionih tela koristi se RSA asimetrični par ključeva dužine 2048 bita sa periodom validnosti certifikata od 3 meseca.

Za kvalifikovane sertifikate za kvalifikovani elektronski potpis/pečat krajnjim korisnicima, koristi se RSA asimetrični par ključeva dužine 2048 bita i periodom izdavanja sertifikata od 5 godina.

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

6.1.6. Generisanje kriptografskih parametara i provera kvaliteta

Asimetrični parovi ključeva se generišu pomoću hardverskih generatora slučajnih brojeva koji su realizovani na kriptografskim hardverskim uređajima (HSM-ovima).

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

HSM uređaji su sertifikovani po standardima propisanim Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i Pravilniku o uslovima koje mora da ispunjava kvalifikovano sredstvo za kreiranje elektornskog potpisa odnosno pečata i uslovima koje mora da ispunjava imenovano telo.

6.1.7. Svrha upotrebe ključeva (X509 „Key Usage")

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

Root CA sertifikat:

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

Intermediate CA sertifikat:

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

Kvalifikovani sertifikat za kvalifikovani elektronski potpis korisnika:

- Digital Signature, Non-Repudiation

Kvalifikovani sertifikat za kvalifikovani elektronski pečat korisnika:

- Digital Signature, Non-Repudiation

6.2. Zaštita privatnog ključa i kontrola kriptografskog hardverskog modula

PKSCA koristi odgovarajuće kriptografske uređaje u cilju realizacije zadataka upravljanja životnim ciklusom i zaštite kriptografskih ključeva. Pomenuti kriptografski uređaji su poznati pod imenom hardverski bezbednosni moduli (HSM - Hardware Security Module). HSM-ovi u PKSCA su u skladu sa svim relevantnim standardima zaštite kriptografskih uređaja navedenim u Zakonu o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i Pravilniku o uslovima koje mora da ispunjava kvalifikovano sredstvo za kreiranje elektornskog potpisa odnosno pečata i uslovima koje mora da ispunjava imenovano telo.

Privatni ključevi PKS CA tela se nalaze samo u okviru HSM uređaja i mogu se koristiti samo nakon sprovedenog postupka aktivacije od strane lica sa poverljivim ulogama u PKSCA.

Korisnički ključevi se čuvaju u QSCD uređaju i mogu se koristiti nakon što je sproveden postupak njihove aktivacije od strane korisnika.

6.2.1. Standardi i mere zaštite hardverskog kriptografskog modula

Generisanje korisničkih i PKS CA (root i podređena CA tela) privatnih ključeva se vrši u okviru bezbednog kriptografskog uređaja – HSM, koji zadovoljava odgovarajuće zahteve u skladu sa međunarodnim standardima. Ispunjenje zahteva ovih standarda garantuje, između ostalog, nemogućnost nedetektovanog narušavanja integriteta uređaja ili kriptografske memorije.

HSM uređaji ne smeju da napuštaju PKS CA prostorije, izuzev u retkim prilikama unapred definisanih premeštanja i preseljenja. PKS CA vodi evidenciju u vezi svih premeštanja ili preseljenja.

U slučaju da odgovarajući HSM zahteva održavanje ili popravku, koja se ne može izvršiti u okviru PKSCA prostorija, oni se bezbedno prenose do njihovog proizvođača uz poštovanje svih neophodnih bezbednosnih mera.

6.2.2. k od n distribucija odgovornosti kontrole privatnog ključa

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

Procedura deljenja tajni PKSCA koristi višestruke autorizovane nosioce u cilju zaštite poverljivosti privatnih ključeva i obezbeđenja odgovarajuće procedure oporavka ključa. S tim

u vezi, sertifikaciono telo implementira politiku 2 od 3 distribucije odgovornosti kontrole privatnog ključa.

Prilikom generisanja ili upotrebe kriptografskog ključa sertifikacionog tela potrebno je da minimalno dve osobe sa povjerljivim ulogama autorizuju generisanje ili upotrebu privatnog ključa. Autorizacija se vrši aktivacijom HSM slota na kojem se generiše i čuva privatni ključ. Kada se slot aktivira on ostaje aktiviran sve dok se eksplicitno ne deaktivira, ugasi HSM uređaj ili se ugasi aplikacija sertifikacionog tela.

Privatni ključ CA tela se koristi pod uslovima definisanim u okviru k=2 od n=3 kontrole od strane više zaposlenih sa poverljivim ulogama.

Pre nego što nosilac deljene tajne prihvati deljenu tajnu (upotreba PIN-a, korisničkog naloga i pripadajuće lozinke, upotreba smart kartice i pripadajućeg PIN-a) on mora lično da se upozna sa kreiranjem, zamenom i upotrebom aktivacionih parametara. Nosilac aktivacionih parametara može primiti te parametre na fizičkom mediju, kao što je određeni hardverski kriptografski modul (npr. smart kartica) koji je odobren od strane sertifikacionog tela.

PKS CA čuva zapise u vezi distribucije deljene tajne u pisanom obliku.

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

6.2.3. Deponovanje (Key Escrow) privatnog ključa

Nije primenljivo.

6.2.4. Back-up privatnog ključa

Privatni ključevi sertifikacionih tela i korisnika se backup-uju u skladu sa procedurom definisanom u internim pravilima rada PKSCA. Koriste se procedure backup-a ključa koje su podržane od strane HSM uređaja i koje su u skladu sa zahtevanim standardima. Procedura čuvanja privatnih ključeva zahteva višestruke odgovarajuće kontrole od strane autorizovanih lica PKSCA sa poverljivim ulogama.

Hardverske i softverske mehanizme zaštite privatnih ključeva obezbeđuje HSM uređaj. Mehanizmi zaštite privatnih ključeva su minimalno ekvivalentne snage kao i sami privatni ključevi koji se štite, a po specifikaciji proizvođača HSM-a. Sertifikaciono telo pravi rezervne kopije privatnih ključeva u skladu sa procedurom opisanom u pratećoj dokumentaciji proizvođača HSM, što je definisano internim pravilima rada.

Kopije privatnog ključa PKSCA se čuvaju na eksternoj memoriji (flash memorija, CD,…) na bezbednom mestu, u šifrovanom obliku, u dva primerka, na odvojenim lokacijama.

6.2.5. Arhiviranje privatnog ključa

Arhiviranje privatnog ključa se ne vrši.

6.2.6. Transfer privatnog ključa na hardverski kriptografski modul

Procedura bezbednog eksportovanja privatnog ključa PKSCA u cilju backup- a, kao i procedura bezbednog importa backup-ovanog privatnog ključa na HSM su opisane u posebnim internim pravilima rada PKSCA i dokumentaciji proizvođača HSM.

6.2.7. Čuvanje privatnog ključa na hardverskom kriptografskom modulu

Privatni ključ sertifikacionog tela, koji se nalazi i koristi na HSM uređaju, čuva se u šifrovanom obliku u memoriji HSM uređaja.

6.2.8. Metoda aktivacije privatnog ključa

Nosioci deljenih tajni PKSCA imaju zadatak da aktiviraju i deaktiviraju privatni ključ. Jednom aktiviran, privatni ključ je aktivan sve dok se ne deaktivira.

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

Korisnički privatni ključ se aktivira upotrebom aktivacionih podataka opisanih u poglavlju 6.4. Ovi aktivacioni podaci se dostavljaju SAM aplikaciji na bezbedan način, kroz protokol (Signature Activation Protocol – SAP) koji je definisan između aplikacije i SAM-a.

6.2.9. Metoda deaktiviranja privatnog ključa

Privatni ključ se deaktivira gašenjem ili restartom aplikacije sertifikacionog tela, gašenjem ili restartom HSM uređaja ili deaktivacijom privatnog ključa putem logoff mehanizma.

Korisnički privatni ključ se deaktivira nakon izvršenja usluge od poverenja koja je zahtevala aktivaciju.

6.2.10. Metoda uništenja privatnog ključa

Privatni ključ sertifikacionog tela se ne obnavlja.

Privatni ključ sertifikacionog tela se uništava na kraju svog životnog ciklusa, kako bi se garantovalo da neće nikada biti ponovo aktiviran i korišćen.

Nakon generisanja novog asimetričnog para ključeva i novog sertifikata sertifikacionog tela, prethodni privatni ključ se briše iz HSM-a, a backup kopije koje se čuvaju na mediju se fizički uništavaju na odgovarajućem uređaju.

PKSCA vodi odgovarajući zapisnik o uništenju privatnog ključa sertifikacionog tela, koji se arhivira.

Korisnički privatni ključ se uništava na kraju svog životnog veka, kako bi se onemogućilo njegovo ponovno aktiviranje i korišćenje.

6.2.11. Nivo bezbednosti kriptografskih modula

Kao što je definisano u tački 6.2.1.

6.3. Drugi aspekti upravljanja parom ključeva

6.3.1. Arhiviranje javnog ključa

PKSCA arhivira javne ključeve pojedinačnih CA tela (korenskog i podređenih sertifikacionih tela).

6.3.2. Periodi validnosti sertifikata i privatnog ključa

PKS CA Cloud izdaje korisničke privatne ključeve i sertifikate za periodom korišćenja do 5 godina.

Vreme validnosti privatnog ključa PKS CA Root je 20 godina. PKS CA Root sertifikat je validan 20 godina.

Vreme validnosti privatnog ključa PKS CA Cloud je 20 godina. PKS CA Cloud sertifikat je validan 20 godina.

Sertifikat za OCSP servis je validan 5 godina, sa validnošću privatnog ključa od 5 godina.

Sertifikat podređenih CA tela izdaje se sa vremenom važenja koje ne prelazi period važenja sertifikata korenskog CA tela.

Vremenski period važenja privatnog ključa može biti jednak vremenskom periodu važenja pripadajućeg sertifikata.

Nije dozvoljena upotreba privatnih ključeva nakon isteka perioda njihovog važenja, nakon isteka perida važenja pripadajučih sertifikata, nakon opoziva sertifikata ili za vreme dok je sertifikat suspendovan.

6.4. Aktivacioni podaci

6.4.1. Generisanje i instalacija aktivacionih podataka

Aktivacioni podaci za privatni ključ korenskog certifikacionog tijela, podređenih setifikacionih tela i OCSP servisa, generišu se prilikom sprovođenja formalne procedure uspostavljanja ovih sistema. Aktivacioni podaci se instaliraju na pripadajuće upravljačke kartice HSM modula koje se koriste za aktivaciju slotova na HSM modulu, a na kojima su smešteni odgovarajući privatni ključevi, u skladu sa tačkom 6.2.2. ovog dokumenta.

Podaci za upravljačke kartice HSM modula generišu se u bezbednom prostoru PKSCA od strane lica sa poverljivim ulogama PKSCA.

Aktivacioni podatak za kvalifikovani certifikat za elektronski potpis-pečat u cloud-u predstavlja simetrični ključ AES256, koji se generiše i čuva na mobilnom uređaju korisnika prilikom generisanja ključeva za potpisivanje/pečaćenje.

6.4.2. Zaštita aktivacionih podataka

Aktivacioni podaci za privatni ključ korenskog sertifikacionog tela, podređenih setifikacionih tela i OCSP servisa koji su smešteni na upravljačke kartice HSM modula, zaštićeni su odgovarajućim lozinkama. Lozinke se generišu u bezbednom prostoru PKSCA. Upravljačke kartice HSM modula i pripadajuće lozinke dodeljuju se ovlašćenim licima sa poverljivim ulogama. Upravljačke kartice i pripadajuće lozinke smešaju se u posebne koverte i čuvaju na dve lokacije.

Aktivacioni podaci za privatne ključeve korisnika se štite bezbednosnim mehanizmima implementiranim u korisničkoj aplikaciji.

6.4.3. Drugi aspekti u vezi aktivacionih podataka

Nije primenljivo.

6.5. Bezbednosne kontrole računara

6.5.1. Specifični zahtevi za bezbednost računara

PKSCA implementira specifične bezbednosne kontrole pristupa računarima koji se koriste u okviru PKI Sistema.

Računarska i komunikaciona oprema koja se koristi u okviru sertifikacionog tela fizički je obezbeđena unutar specijalne prostorije sertifkacionog tela.

Računari koji se koriste u okviru PKSCA čuvaju se unutar specijalne prostorije koja je fizički obezbeđena. Pristup preko računarske mreže se štiti pomoću specijalnih aplikativnih firewall

uređaja - kripto komunikacionih servera. Neautorizovan pristup računarima PKSCA nije dozvoljen. PKSCA sistem mogu startovati najmanje dva ili više ovlašćenih lica.

6.5.2. Rangiranje bezbednosti računara

HSM moduli sertifikacionog tela imaju ocenu bezbednosti predviđenu Zakonom i na osnovu njega donetim podzakonskim aktima.

Računari i operativni sistemi koje koristi sertifikaciono telo su komercijalni proizvodi koji su dodatno bezbednosno ojačani.

6.6. Životni ciklus tehničkih bezbednosnih mera

6.6.1. Mere bezbednosti tokom razvoja sistema

PKSCA nadgleda i kontroliše razvoj sistema za izdavanje sertifikata. Softver koji se koristi u PKSCA sistemu potiče iz pouzdanog izvora. Nove verzije softvera testiraju se kod proizvođača u fazi razvoja, a nakon toga i u PKSCA sistemu u okviru testnog okruženja. Nakon pozitivnih testova, vrši se implementacija softvera u produkcionom okruženju, u skladu sa internom procedurom upravljanja izmenama na IT sistemima i aplikacijama PKSCA.

6.6.2. Mere upravljanja bezbednošću

PKSCA nadgleda i kontroliše bezbednost i upravljanje bezbednošću sistema za izdavanje sertifikata.

6.6.3. Životni ciklus bezbednosnih mera

Sertifikaciono telo sprovodi sva testiranje pre implementacije u okviru testnog okruženja.

6.7. Bezbednosne mere u računarskoj mreži

Bezbednost računarske mreže PKSCA zasnovana je na konceptu segmentacije mreže na mrežne zone različitih nivoa. Mrežne zone razgraničavaju se firewall-ovima koji propuštaju samo neophodan mrežni saobraćaj. Na sve sisteme locirane unutar jedne mrežne zone primjenjuju se iste sigurnosne mjere.

Mrežni segment u kome se nalaze radne stanice za administraciju sertifikacionog tela firewall-om je odvojen od ostalih mrežnih segmenata i računara koji se nalaze u tim mrežnim segmentima.

Oprema za zaštitu računarske mreže beleži tok saobraćaja i pokušaje pristupa servisima i javnim internet stranicama PKSCA. Samo ovlašćena lica sa poverljivim ulogama PKSCA imaju administratorska ovlašćenja za podešavanje i upravljanje opremom za zaštitu računarske mreže. Udaljeno podešavanje opreme za zaštitu računarske mreže nije dozvoljeno.

Nepotrebne komunikacije, nalozi, portovi, protokoli i servisi su eksplicitno zabranjeni ili deaktivirani.

Interna računarska mreža sertifikacionog tela zaštićena je od neovlašćenog pristupa, uključujući i pristup korisnika i trećih lica.

Svi kritični sistemi za pružanje usluga od poverenja smešteni su u bezbednoj zoni PKSCA i raspoređeni su u više različitih bezbednosnih mrežnih zona.

Mrežne komponente sertifikacionog tela čuvaju se u fizički i logički bezbednom okruženju i usaglašenost njihove konfiguracije periodično se proverava.

6.8. Vremenski žig

Nije primenljivo.

7. PROFILI SERTIFIKATA I CRL

Ovo poglavlje sadrži opis profila certifikata, liste opozvanih certifikata (CRL) i odgovora OCSP servisa koje izdaje PKSCA, kao pružalac usluga od poverenja, kroz korensko sertifikaciono telo i podređena sertifikaciona tela, u skladu sa opsegom ovog dokumenta.

7.1. Profili sertifikata

PKSCA izdaje sledeće vrste sertifikata:

- PKS CA Root CA sertifikat
- PKS CA Cloud CA sertifikat
- Sertifikat za PKS CA Cloud OCSP servis
- PKS CA Cloud izdaje kvalifikovane sertifikate za:
  - Fizička lica,
  - Ovlašćena fizička lica u okviru pravnih lica
  - Pravna lica (za potrebe izrade elektronskog pečata)
  - Nerezidente

PKS CA Cloud izdaje sertifikate prema profilima koji su određeni ovim dokumentom.

U zavisnosti od namene sertifikata, nivoa bezbednosti i načina čuvanja pripadajućih ključeva, svaki tip sertifikata ima definisan jedinstveni OID politike sertifikacije, a pored njega sadrži i odgovarajući ETSI OID politike sertifikacije, ukoliko je takav OID primenljiv.

7.1.1. Broj verzije

Sertifikaciona tela u okviru PKSCA izdaju X.509 V3 certifikate u skladu sa RFC 5280. Koriste se slijedeća X.509 osnovna polja sertifikata:

X509 Naziv osnovnog polja	Opis
signature	Napredni elektronski potpis kvalifikovanog elektronskog certifikata privatnim kriptografskim ključem aplikacije CA tela. Algoritam potpisa je RSA-SHA256.
issuer	Jedinstveno ime sertifikacionog tela
Valid From	Datum i vreme početka važenja kvalifikovanog elektronskog sertifikata
Valid To	Datum i vreme prestanka važenja kvalifikovanog elektronskog sertifikata.

X509 Naziv osnovnog polja	Opis
subject	Jedinstveno ime korisnika sertifikata
subjectPublicKeyInformation	Javni kriptografski ključ korisnika sertifikata, dužina javnog ključa i naziv algoritma javnog ključa
version	Verzija X.509 certifikata, verzija 3
serialNumber	Jedinstveni serijski broj sertifikata

Tabela 3. – Opis X.509 osnovnih polja sertifikata

7.1.2. Ekstenzije sertifikata

PKSCA u svojim sertifikatima koristi sledeće ekstenzije:

X509 Naziv polja ekstenzije	Opis
Authority Key Identifier	Identifikator javnog kriptografskog ključa sertifikacionog tela koji se računa kao RSA-SHA256 hash polja Subject Public Key Info sertifikata sertifikacionog tela.
Subject Key Identifier	Identifikator javnog kriptografskog ključa korisnika sertifikata koji se računa kao hash polja *Subject Public Key Info* kvalifikovanog elektronskog sertifikata korisnika.
Key Usage	Namena javnog kriptografskog ključa korisnika kvalifikovanog elektronskog sertifikata kao što je navedeno u **Error! Reference source not found.**. Polje je u svim sertifikatima označeno kao kritično.
Extended Key Usage	Proširena namena javnog kriptografskog ključa korisnika kvalifikovanog elektronskog sertifikata kao što je navedeno u 6.1.7.
Certificate Policies	Identifikacija politike sertifikacije i adrese Web strane na kojoj se nalaze ova praktična pravila.
Issuer Alternative Name	Alternativno ime sertifikacionog tela koje sadrži naziv, poreski identifikacioni broj i oznaku države u kojoj je davalac usluga registrovan.

X509 Naziv polja ekstenzije	Opis
Subject Alternative Name	Alternativno ime korisnika kvalifikovanog elektronskog sertifikata. U ovom polju može da se navede adresa elektronske pošte korisnika certifikata, ako je adresa elektronske pošte navedena u zahtevu za izdavanjem sertifikata.
CRL Distribution Points	Lokacija na kojoj se nalaze CRL
Qualified Certificate Statements	Oznaka da je certifikat izdat kao kvalifikovani elektronski certifikat (*OID*: 1.3.6.1.5.5.7.1.3), koja sadrži oznake u skladu sa tehničkim standardom ETSI EN 319 412-5. Sadržaj oznaka pojedinog tipa certifikata naveden je u **Error! Reference source not found.**.
Authority Information Access (authorityInfoAccess)	Informacije o lokaciji na kojoj je dostupan certifikat na kom se zasniva napredni elektronski potpis sertifikacionog tela (polje id-ad-caIssuers).

Tabela 4. – Ekstenzije sertifikata

Osim ekstenzija navedenih u tabeli 4. u sertifikatima koji se izdaju nerezidentima uvode se i dodatne ekstenzije (custom extensions): Broj putne isprave - PassportNumber (OID 1.3.6.1.0.1), Oznaka zemlje koja je izdala putnu ispravu - PassportIssuer (OID 1.3.6.1.0.2) i Datum do koga važi putna isprava - PassportDate (OID 1.3.1.6..1.0.3).

7.1.2.1. Polje Qualified Certificate Statements (qCStatements)

Polje qCStatements (1.3.6.1.5.5.7.1.3) sadrži oznake u skladu sa tehničkim standardom ETSI EN 319 412-5 .

U kvalifikovanom sertifikatu za kvalifikovani elektronski potpis izdat u cloud-u polje qCStatements sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
- QCstatement QcType (0.4.0.1862.1.6)
    - id-etsi-qct-esign (0.4.0.1862.1.6.1)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

U kvalifikovanom sertifikatu za kvalifikovani elektronski pečat izdat u cloud-u polje qCStatements sadrži oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
- QCstatement QcType (0.4.0.1862.1.6)
    - id-etsi-qct-eseal (0.4.0.1862.1.6.2)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

7.1.3. Objektni identifikatori algoritama

PKSCA u sertifikatima koje izdaje koristi sledeće algoritme sa pripadajućim OID:

Algoritam	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1
Sha1WithRSAEncryption	1.2.840.113549.1.1.5

Tabela 5. – Identifikatori algoritama

7.1.4. Forme imena

Sertifikati izdati od strane PKSCA sistema sadrže kompletno X.500 jedinstveno ime izdavaoca sertifikata i korisnika sertifikata u sledećim poljima: issuer name (CA ime) i subject name. Jedinstvena imena su tekstualna polja u X.501 printable, teletex ili UTF8 formatu.

Za potrebe profila kvalifikovanog sertifikata ovlašćenog korisnika u okviru pravnog lica obavezno je uneti i sledeće podatke:

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

7.1.5. Ograničenja za imena

Ograničenja koja se odnose na imena korisnika u kvalifikovanim elektronskim sertifikatima proističu iz Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i Pravilnika o uslovima koje moraju da ispunjavaju kvalifikovani elektronski sertifikati, kao njegovog podzakonskog akta. U nastavku su navedena pomenuta ograničenja:

- Polje *Subject* kvalifikovanog elektronskog sertifikata mora da sadrži atribut *CommonName*.
- U atribut *commonName* treba da bude upisano puno ime i prezime potpisnika i jedinstveni identifikator potpisnika unutar sertifikacionog tela. Prema Pravilniku o uslovima koje moraju da ispunjavaju kvalifikovani elektronski sertifikati atribut c*ommonName* ne sme da se završava sa 13 ili više uzastopnih numeričkih karaktera, niti da se završava crticom iza koje slede dva slovna karaktera i niz numeričkih. Za atribut *commonName* treba koristiti UTF8String kodiranje, tako da sva slova iz imena i prezimena budu verno predstavljena odgovarajućim karakterima.
- Sertifikaciono telo je dužno da korisniku jasno stavi do znanja da li će sertifikat sadržati JMBG.
- Sertifikati koji se koriste u opštenju državnih organa, opštenju državnih organa i stranaka, dostavljanju i izradi odluke državnih organa u elektronskom obliku u upravnom, sudskom i drugom postupku pred državnim organom, treba da sadrže JMBG. Sertifikate koji sadrže JMBG ili lični broj sertifikaciono telo ne sme učiniti javno dostupnim.
- Sertifikati koji ne sadrže JMBG mogu se koristiti za potpisivanje statisičkih izveštaja u skladu sa članom 35 stav 6 Zakona o računovodstvu (“Službeni glasnikRS”, broj 62/13) i potpisivanje finansijskih izveštaja i pratećih izjava u skladu sa članom 33 stav 6 tog zakona, ukoliko je potpisnik stranac u smislu Zakona o strancima (“Službeni glasnik RS”, broj 97/08).

PKSCA u imenima ne dozvoljava korišćenje sledećih specijalnih znakova: ? (upitnik), \ (backslash), / (slash), # (taraba), $ (dolar), % (procenat), = (jednako), + (plus), | (uspravna crta), ; (tačka-zarez), < (manje), > (veće) i , (zarez). Iste je potrebno izostaviti ili zameniti drugim znacima.

7.1.6. Identifikator objekta politike sertifikacije

Identifikator objekta politike sertifikacije upisuje se u polje ekstenzije *Certificate Policies*.

7.1.7. Korišćenje „Policy Constraints“ ekstenzije

Ekstenzija *Policy Constraints* se ne koristi.

7.1.8. Sintaksa i semantika „Policy Qualifier“-sa

Kvalifikator politika sertifikacije u ekstenziji *Certificate Policies* sadrži link u URI formatu sa internet adresom politike sertifikacije. Dokument se nalazi na naznačenoj internet lokaciji i obavezno je u verziji na srpskom jeziku, a može biti preveden i na engleski jezik.

7.1.9. Semantika procesiranja kritične ekstenzije „Certificate Policies“

U sertifikatima izdatim od strane PKSCA, neophodno je da ekstenzija *Certificate Policies* ima sledeće vrednosti:

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

Klijentske aplikacije, u saglasnosti sa RFC 5280, moraju da procesuiraju ekstenzije označene kao kritične.

7.2. Profil CRL

Profil PKSCA CRL je usklađen sa odredbama dokumenta IETF RFC 5280.

7.2.1. Broj verzije

PKS CA generiše i objavljuje CRL liste verzije 2 prema X509 specifikaciji (X.509v2).

7.2.2. CRL i CRL entry ekstenzije

Ekstenzije CRL koje se koriste u CRL listama i u elementima unosa CRL lista definisane su u skladu sa standardom RFC 5280.

7.3. OCSP profil

Profil odgovora PKS CA Cloud OCSP servisa usaglašen je s dokumentom IETF RFC 6960.

7.3.1. Broj verzije

Profil odgovora PKS CA Cloud OCSP servisa je u skladu sa verzijom 1 prema dokumentu IETF RFC 6960.

7.3.2. OCSP ekstenzije

PKS CA Cloud OCSP servis koristi sledeće ekstenzije:

- *Nonce* – Vrednost Nonce iz zahteva za status sertifikata
- *Extended Revoked Definition* – Kod razloga opoziva sertifikata (Reason code)

8. PROVERA USAGLAŠENOSTI I DRUGE PROCENE

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

Provera usaglašenosti obavlja se u cilju potvrđivanja da PKSCA, za usluge koje pruža, ispunjava zahteve utvrđene Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, Uredbom EU br. 910/2014 i standardom CEN EN 419 241-1 (July 2018) Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements i tehničkim specifikacijama ETSI TS 119 431-1 V1.1.1 (2018-12) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/SCDev.

8.1. Učestalost ili uslovi ocenjivanja

Provere usaglašenosti rada PKSCA mogu biti interne i eksterne.

Interne i eksterne provere usaglašenosti rada PKSCA sprovode se i u PKSCA RA mreži.

8.1.1. Eksterna provera usaglašenosti

Potpuna eksterna provera usaglašenosti sprovodi se pre početka pružanja usluga od poverenja i najmanje jednom u 24 meseca, u skladu sa Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju.

8.1.2. Interna provera usaglašenosti

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

8.2. Identitet/kvalifikacije ocenjivača

Eksternu proveru usaglašenosti sprovodi telo za ocenjivanje usaglašenosti. Osposobljenost tela za ocenjivanje usaglašenosti i osposobljenost pripadajućih ocenjivača dokazuje se akreditacijom tela za ocenjivanje usaglašenosti pružaoca kvalifikovanih usluga od poverenja, u skladu sa zakonom kojim se uređuje akreditacija.

Internu proveru usaglašenosti sprovode interni ocenjivači koji raspolažu znanjima i razumevanjem:

- odredbi standarda CEN EN 419 241-1,
- tehničkih specifikacija ETSI TS 119 431-1

- PKI područja i područja informacione bezbednosti,
- zakonske regulative iz područja pružanja usluga od poverenja.

8.3. Odnos ocenjivača prema ocenjivanom entitetu

Telo za ocenjivanje usaglašenosti i pripadajući ocenjivači nezavisni su od PKSCA i internih sistema ocenjivanja.

Interni ocenjivači usaglašenosti ne ocenjuju u domenu sopstvenog delokruga odgovornosti.

8.4. Predmet ocenjivanja usaglašenosti

Predmet ocenjivanja usaglašenosti su sledeća područja pružanja kvalifikovanih usluga od poverenja:

- integritet i tačnost dokumentacije,
- implementiranost zahteva za kvalifikovane usluge od poverenja,
- organizacioni procesi i procedure,
- tehnički procesi i procedure,
- implementirane mere informacione bezbednosti,
- fizička bezbednost predmetnih lokacija.

Opis predmetnog ocenjivanja usaglašenosti definisan je planom ocenjivanja usaglašenosti.

8.5. Aktivnosti preduzete kao rezultat utvrđenih nedostataka

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

Za vreme prekida izdavanja kvalifikovanih usluga od poverenja zbog utvrđene značajne neusaglašenosti, PKSCA će pružati samo one usluge u kojima je naznačeno da služe za interne i testne svrhe i osiguraće da te usluge ne budu dostupne ni jednom drugom korisniku.

8.6. Objavljivanje rezultata

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

Izveštaj o ocenjivanju usaglašenosti koje primi od tela za ocenjivanje usaglašenosti, PKSCA će dostaviti nadzornom organu u roku od tri radna dana od dana prijema.

PKSCA javno objavljuje kratak izveštaj ili potvrdu o sprovedenoj eksternoj proveri usaglašenosti. Neusaglašenosti utvrđene tokom eksterne provere usaglašenosti se smatraju poverljivim informacijama i ne objavljuju se.

9. DRUGI POSLOVNI I PRAVNI ASPEKTI

9.1. Naknade za usluge

PKSCA, u skladu sa uslovima iz sklopljenog ugovora o pružanju usluge izdavanja kvalifikovanih elektronskih sertifikata u cloud-u, obaveštava korisnike i pouzdajuće strane o naplati usluge. Ukoliko posebnim ugovorom nije drugačije određeno, usluga se naplaćuje u skladu sa cenovnikom PKSCA. Cenovnik svih usluga koje se naplaćuju objavljen je na internet stranici repozitoriuma iz tačke 2.1. ovih Praktičnih pravila.

PKSCA zadržava pravo izmene cenovnika. Izmene cenovnika objavljuju se na internet stranici repozitoriuma iz tačke 2.1. ovog dokumenta.

9.1.1. Naknade za izdavanje ili obnovu sertifikata

PKSCA naplaćuje korisnicima naknadu za uslugu izdavanja kvalifikovanog elektronskog sertifikata u cloud-u u skladu sa objavljenim cenovnikom.

9.1.2. Naknade za pristup sertifikatima

PKSCA ne naplaćuje naknadu za pristup sertifikatima.

9.1.3. Naknade za pristupa informacijama o statusu sertifikata i opoziv sertifikata

PKSCA ne naplaćuje proveru statusa sertifikata putem OCSP servisa ili putem liste opozvanih sertifikata (CRL).

Sertifikaciono telo ne naplaćuje uslugu opoziva sertifikata.

9.1.4. Naknade za ostale usluge

PKSCA može odrediti da se naplaćiuju naknade i za ostale usluge, kao što su: registracija pravnog lica ili korisnika, promena podataka u sertifikatu i slično.

Za pristup ovom dokumentu naknade se ne naplaćuju.

9.1.5. Politika povraćaja novca

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

9.2. Finansijska odgovornost

PKSCA, kao pružalac kvalifikovanih usluga od poverenja, poseduje stabilnost i raspolaže dovoljnim sredstvima koja osiguravaju nesmetano pružanje usluga od poverenja u skladu s ovim dokumentom.

9.2.1. Pokrivenost osiguranjem

PKSCA, kao pružalac kvalifikovanih usluga od poverenja, ima osiguran rizik od odgovornosti za štete koje nastanu obavljanjem usluga od poverenja.

PKS dodatno osigurava imovinu polisom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda, poplava, eksplozija, udara groma, pada ili udara letilice, demonstracija, kao i osiguranje opreme, električne opreme, elektronskih i komunikacijskih uređaja, instalacija i slično.

9.2.2. Ostala sredstva

Nije primenljivo.

9.2.3. Osiguranje ili garancijsko pokrivanje za krajnje korisnike

Korisnik izdatih sertifikata dužan je da nadoknadi nastalu štetu koju bi PKSCA moglo da ima kao rezultat sledećih nedozvoljenih radnji:

- Lažno predstavljanje prilikom registracije korisnika,
- Bilo kog propusta korisnika za koji korisnik ne može da dokaže da je propust nenamerno učinjen,
- Ako korisnik ne obezbedi korišćenje privatnih ključeva u skladu sa Zakonom i ovim dokumentom,
- Ukoliko upotrebom privatnih ključeva krši bilo koji važeći zakon,
- U svim drugim slučajevima koji su u suprotnosti sa Zakonom, ovim dokumentom i drugim zakonskim aktima Republike Srbije.

Korisnik izdatih certifikata i treća lica isključivo su odgovorni za obezbeđenje adekvatnog osiguranja ili garancije pokrivenosti osiguranjem za korišćenje sertifikata u okviru njihovih servisa ili aplikacija.

9.3. Poverljivost poslovnih informacija

9.3.1. Opseg poverljivih poslovnih informacija

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

9.3.2. Informacije koje nisu u opsegu poverljivih poslovnih informacija

Podaci koji se ugrađuju u sadržaj sertifikata, podaci o statusu sertifikata i podaci i dokumenti javno objavljeni u PKSCA repozitorijumu se ne smatraju poverljivim poslovnim podacima.

9.3.3. Odgovornost za zaštitu poverljivih informacija

Svaki učesnik u pružanju usluga od poverenja je obavezan da štiti poverljive poslovne podatke iz tačke 9.3.1. ovog dokumenta, bez obzira na način na koji je do njih došao, u skladu sa Zakonom o zaštiti poslovne tajne (Službeni glasnik RS, br. 72/2011) i Zakonom o zaštiti podataka o ličnosti (Službeni glasnik RS, br. 87/2019).

9.4. Privatnost i zaštita podataka o ličnosti

PKSCA posvećuje pažnju zaštiti ličnih podataka koje prikuplja, skladišti i upotrebljava u svrhu pružanja usluge sertifikovanja iz opsega ovog dokumenta i sa ličnim podacima postupa u skladu sa Zakonom o zaštiti podataka o ličnosti i Uredbom EU 2016/679.

Podnošenjem zahteva za uslugom i sklapanjem ugovora o pružanju usluga od poverenja fizička lica daju PKSCA saglasnost za korišćenje i obradu njihovih ličnih podataka prikupljenih u postupku registracije i saglasnost za čuvanje tih podataka u trajanju od najmanje 10 godina od prestanka važnosti usluge na koju se podaci odnose, u skladu sa važećom zakonskom regulativom.

9.4.1. Plan zaštite podataka o ličnosti

PKSCA sprovodi politiku zaštite ličnih podataka u skladu sa zakonskom regulativom, kojom se utvrđuju načela obrade ličnih podataka fizičkih lica i kojom se izražava svest, znanje i predanost za poštovanje prava i sloboda pojedinaca pri obradi ličnih podataka. Lične podatke prikupljene za potrebe pružanja usluga od poverenja PKSCA obrađuje u opsegu koji je primeren, relevantan i ograničen samo za pružanje te usluge.

PKSCA svojim stručnim znanjem, pouzdanošću, resursima, poštovanjem propisanih tehničkih, organizacionih i bezbednosnih mera garantuje obradu ličnih podataka u skladu sa Zakonom o zaštiti podataka o ličnosti i Uredbom EU 2016/679 .

Mere zaštite poverljivosti i integriteta ličnih podataka primenjuju se i prilikom razmene ličnih podataka korisnika između RA mreže i sistema usluga, kao i prilikom čuvanja i arhiviranja ličnih podataka korisnika, do njihovog brisanja iz arhive i uništavanja.

9.4.2. Poverljivi podaci o ličnosti

U postupku registracije korisnika i nakon toga, PKSCA je ovlašćeno za prikupljanje ličnih podataka koji su potrebni za pouzdano utvrđivanje identiteta korisnika i druge podatke potrebne za valjano pružanje usluga od poverenja. Lični podaci koje prikupi PKSCA, a koji nisu sadržaj sertifikata, poverljivi su lični podaci koje PKSCA štiti na propisani način.

9.4.3. Podaci o ličnosti koji nisu poverljivi

Lični podaci koje u postupku registracije korisnika i nakon toga prikupi PKSCA i koji su sadržaj sertifikata, lični su podaci koji, zbog dostupnosti svim zainteresovanim stranama, nisu poverljivi.

Sklapanjem ugovora o pružanju usluga od poverenja potpisnici daju saglasnost za objavu sertifikata u javnom imeniku.

9.4.4. Odgovornost za zaštitu podataka o ličnosti

PKSCA je odgovorno za zaštitu ličnih podataka prikupljenih u svrhu pružanja usluga od poverenja.

9.4.5. Ovlašćenje i saglasnost za korišćenje podataka o ličnosti

PKSCA je ovlašćeno, osim za potrebe ispunjenja zakonskih obaveza, odnosno ugovornih obaveza po ugovoru o uslugama od poverenja, da koristi ili objavljuje lične podatke samo na osnovu pismene saglasnosti fizičkih lica na koje se ti podaci odnose.

9.4.6. Dostupnost podataka o ličnosti nadležnim telima

PKSCA ne čini dostupnima podatke iz tačaka 9.4.1. i 9.4.2. ovog dokumenta osim u slučajevima propisanim zakonom ili kada to pismenim putem zahteva sud, upravno ili neko drugo nadležno državno telo.

9.4.7. Ostale okolnosti za otkrivanje podataka o ličnostima

PKSCA će, u svim ostalim okolnostima, otkriti podatke o ličnostima samo uz pismenu saglasnost krajnjeg korisnika.

9.5. Prava intelektualnog vlasništva

Ovaj dokument je, kao i druga dokumentacija PKSCA objavljena na njegovim internet stranicama, intelektualno vlasništvo PKSCA.

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

Vlasnik korisničkog para asimetričnih ključeva je korisnik. Za upotrebu privatnog ključa ovlašćen je isključivo potpisnik, bez obzira na način na koji je privatni ključ zaštićen.

PKSCA je, kao pružalac usluga od poverenja, vlasnik usluga koje pruža.

9.6. Obaveze i odgovornosti

9.6.1. Obaveze i odgovornosti CA

PKSCA je odgovorno za usklađenost svojih pravila sa zakonskom regulativom i za sprovođenje odredbi propisanih ovim dokumentom, CP dokumentom, Uslovima pružanja usluga od poverenja i za poštovanje obaveza iz ugovora o obavljanju usluga od poverenja sklopljenog sa korisnikom.

PKSCA na svojim internet stranicama objavljuje uslove pružanja usluga od poverenja, ovaj dokument, CP dokument i sva obaveštenja i informacije o promenama u radu koje na bilo koji način mogu uticati na korisnike usluga PKSCA.

PKSCA je, kao kvalifikovani pružalac usluga od poverenja, odgovorno za štetu nastalu tokom pružanja usluge, pouzrokovane od strane pravnog lica sa kojim je PKSCA ugovorila deo usluga od poverenja. Odnos PKSCA i pravnog lica koje obavlja deo usluga od poverenja uređuje se posebnim ugovorom.

PKSCA je kao kvalifikovani pružalac usluga od poverenja odgovorno za:

- usklađenost pružanja usluga od poverenja sa odredbama svoje CP i politike informacione bezbednosti, uključujući i kada je deo svoje usluge od poverenja ugovorom poverila drugom poslovnom subjektu,
- ispravnu proveru identiteta i podataka fizičkog i/ili pravnog lica u cilju pružanja usluga od poverenja,
- pružanje usluga od poverenja na siguran način radi očuvanja integriteta i autentičnosti,
- usklađenost sa svojim obavezama.

U skladu sa obavezama i odgovornostima, PKSCA:

- primenjuje odredbe važećih propisa pri pružanju usluge od poverenja,
- pruža uslugu od poverenja na siguran način radi očuvanja integriteta i autentičnosti, u skladu sa pouzdano utvrđenim identitetom fizičkog i/ili pravnog lica,
- generiše parove korisničkih ključeva na bezbedan način, uz garantovanje tajnosti privatnog ključa, u skladu sa ovim dokumentom,
- garantuje bezbedan način generisanja privatnog ključa i dostave pripadajućih aktivacionih podataka korisniku, odnosno ovlašćenom predstavniku, za sertifikate koji se izdaju u cloud-u,
- uspostavlja proceduru deljenja tajni za sve poverljive uloge, u skladu sa svojom PKI infrastrukturom,
- na osnovu autentičnog i ažuriranog zahteva, po sprovedenom propisanom postupku, opoziva, suspenduje ili reaktivira sertifikat i objavljuje ga na listi opozvanih sertifikata,

- pruža informaciju o statusu opozvanosti, odnosno suspendovanosti sertifikata,
- sprovodi zahtevane bezbednosne mere za zaštitu prostora i opreme sistema usluga,
- primenjuje organizacione i tehničke mere za zaštitu ključeva i sertifikata u skladu sa ovim dokumentom,
- u najkraćem mogućem roku obaveštava korisnike i treća lica o kompromitaciji sopstvenog privatnog ključa,
- omogućava nesmetan rad i maksimalnu raspoloživost usluga od poverenja, u skladu sa planom kontinuiteta poslovanja PKSCA,
- prati raspoloživost kapaciteta, planira održavanje i dalji razvoj sistema usluga od poverenja u skladu sa budućim potrebama, zahtevima standarda i razvojem tehnologije,
- štiti podatke koji se smatraju poverljivim i te podatke koristiti isključivo za potrebe usluga od poverenja iz opsega ovog dokumenta,
- obezbeđuje da se interne i spoljne provere usklađenosti PKSCA, kao kvalifikovanog pružoaca usluga od poverenja, sprovode u skladu sa ovim dokumentom.

U slučaju prekida poslovanja PKSCA će postupiti u skladu sa tačkom 5.8. ovog dokumenta.

9.6.2. Obaveze i odgovornosti RA

Obaveze i odgovornosti PKSCA RA mreže su:

- sprovođenje postupka registracije i identifikacije fizičkih i pravnih lica i provere podataka na način propisan u ovom dokumentu,
- prosleđivanje potpunih, tačnih i proverenih podataka o korisnicima na dalju obradu u PKSCA CA,
- čuvanje, arhiviranje i zaštita podataka i dokumentacije u periodu od najmanje 10 godina od prestanka validnosti usluge od poverenja na koji se odnose,
- obezbeđenje od gubitka ili narušavanja poverljivosti, integriteta i raspoloživosti arhiviranih podataka korisnika, na način propisan ovim dokumentom,
- obaveštavanje podnosioca zahteva za uslugom o javno objavljenim i dostupnim uslovima pružanja usluga od poverenja i odredbama ovog dokumenta.

9.6.3. Obaveze i odgovornosti korisnika

Korisnik je dužan:

- da se, u procesu registracije, predstavi na način propisan u ovom dokumentu,
- da preduzima odgovarajuće mere zaštite sredstva za izradu elektronskog potpisa i aktivacionih podataka od neovlašćenog pristupa i upotrebe,
- da pregleda i proveri tačnost podataka koji se unose u sadržaj sertifikata i potvrdi te podatke pre izdavanja sertifikata,

- da u najkraćem mogućem roku zatražiti opoziv, odnosno suspenziju sertifikata u slučaju kompromitovanja privatnog ključa, gubitka ili oštećenja sredstva za izradu elektronskog potpisa i aktivacionih podataka,
- da dostavi u RA sve potrebne podatke i informacije o promenama koje utiču ili mogu uticati na tačnost elektronskog potpisa u roku naznačenom u ovom dokumentu,
- da koristi sertifikat i pripadajući privatni ključ u skladu sa zakonima i drugim propisima Republike Srbije i u skladu sa odredbama ovog dokumenta,
- da deluje u skladu sa svim ostalim odredbama iz ovog dokumenta koje se odnose na obveze korisnika.

Potpisnik zahteva za izdavanje sertifikata, odnosno odgovorna osoba za zastupanje pravnog lica, odgovorni su za tačnost i ispravnost podataka dostavljenih u postupku registracije.

U slučaju promene kontakt podataka, korisnik je dužan da nastale promene dostavi PKSCA.

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

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

Korisniku koji ne postupa u skladu s preuzetim obavezama može biti uskraćeno pružanje usluga od poverenja, pa će, na taj način, izgubiti sva prava proizašla iz ugovora o obavljanju usluga.

9.6.4. Obaveze i odgovornosti treće strane

Treća strana dužna je da samostalno i svesno donese odluku o razumnom poverenju u usluge od poverenja koje pruža PKSCA.

Razumnim poverenjem smatra se odluka treće strane, kao korisnika usluga od poverenja, da se pouzdaje u sertifikat ako je u vreme ostvarenja poverenja:

- preduzela potrebne mere opreza i koristi usluge u svrhe propisane ovim dokumentom, odnosno uslovima pružanja usluge, pod okolnostima u kojima je poverenje razumno i u dobroj nameri i pod okolnostima koje su poznate ili bi trebale biti poznate trećoj strani pre ostvarenja poverenja,
- koristila aplikaciona rešenja i IT okolinu u koju ima poverenja,
- proverila period važenja sertifikata koji se koriste,
- proverila status opozvanosti ili suspendovanosti sertifikata, a što treća strana utvrđuje sprovodeći proveru statusa sertifikata putem OCSP servisa ili na osnovu

zadnje izdate CRL, kako je propisano u ovom dokumentu,
- proverila da je elektronski potpis izrađen privatnim ključem koji odgovara javnom ključu u sertifikatu za vreme perioda važenja sertifikata.

Treća strana sama snosi sve rizike ukoliko nije poštovala propise i odredbe ovog dokumenta i nije postupala u skladu sa obavezama i odgovornostima iz ove tačke.

9.6.5. Obaveze i odgovornosti ostalih učesnika

Nije primenljivo.

9.7. Odricanje od odgovornosti

PKSCA nije odgovorna za direktne i indirektne štete, kao i za bilo koji gubitak dobiti, gubitak podataka ili druge oblike štete u sledećim slučajevima:

- kada je šteta nastala zbog neautorizovane upotrebe korisničkih usluga od poverenja,
- kad je šteta nastala upotrebom usluge koja nije dopuštena ovim dokumentom,
- kad je šteta prouzrokovana prevarom ili nemarnom upotrebom usluga od poverenja, CRL ili OCSP servisa,
- kad je šteta nastala kao rezultat neispravnosti i grešaka u softveru i hardveru korisnika ili treće strane kao korisnika usluga od poverenja,
- kad je šteta nastala kao rezultat lažnog davanja podataka i predstavljanja pravnog lica ili fizičkog lica tokom procesa identifikacije i potvrde identiteta, ukoliko je RA mreža sprovodila identifikaciju i proveru podataka u skladu sa zahtevima iz ovog dokumenta i radnim uputstvima.

9.8. Ograničenja odgovornosti

Ukupna finansijska odgovornost za sertifikate izdate prema ovom dokumetu i za transakcije obavljene na osnovu usluga od poverenja ne može biti viša od 2.000.000,00 RSD.

Ukoliko posebnim ugovorom ili na drugi način nije drugačije određeno, maksimalna finansijska odgovornost prema korisniku i trećoj strani koja se razumno pouzdaje u usluge od poverenja ograničava se u skladu sa preporučenim limitima.

Kategorija sertifikata	Maksimalna PKSCA odgovornost	
	Po transakciji	Ukupno
Kvalifikovani sertifikati za elektronski potpis srednjeg nivoa sigurnosti	do 80.000 RSD	2.000.000 RSD

Tabela 6. - Maksimalna PKSCA odgovornost

9.9. Naknada štete

Svaki učesnik odgovara oštećenom za štetu koju je počinio zbog nepoštovanja odredbi ovog dokumenta i važećih relevantnih propisa.

Potpisnik, odnosno pravno ili fizičko lice, u čije ime potpisnik deluje i koju predstavlja, odgovara oštećenom, odnosno svakom drugom učesniku, ako koristi PKSCA uslugu od poverenja na osnovu lažno datih podataka u zahtevu za kvalifikovanom uslugom od poverenja.

Treća strana odgovara oštećenom, odnosno svakom drugom učesniku ako se pouzda u usluge od poverenja bez provere njihove ispravnosti, opisane u ovom dokumentu, ili ih koristi protivno svrsi određenoj ovim dokumentom.

9.10. Trajanje i prestanak važenja Praktičnih pravila

9.10.1. Trajanje

Dokument Praktična pravila važi do stupanja na snagu novog dokumenta praktičnih pravila ili do objave prestanka njegovog važenja.

Nova verzija Praktičnih pravila ili objava prestanka važenja biće publikovana na internet stranici PKSCA sa naznačenim danom stupanja na snagu. Novom dokumentu praktičnih pravila biće dodeljena nova verzija i u novom OID će biti naznačene izmene.

9.10.2. Prestanak važenja

Prestanak važenja ovog dokumenta nije vezan i ne utiče na važenje usluga definisanih primenom ovog dokumenta.

PKSCA može za pojedine odredbe važećeg dokumenta izraditi izmene i dopune.

9.10.3. Posledice prestanka važenja i nastavak delovanja

Stupanjem na snagu nove verzije Praktičnih pravila, na sve usluge od poverenja definisane u njemu se od tog dana primenjuju odredbe iz tog dokumenta.

Usluge definisane primenom prethodnog dokumenta važe do njihovog isteka pri čemu se

mogu obnoviti primenom pravila iz novog dokumenta praktičnih pravila.

9.11. Individualna obaveštenja i komunikacija sa učesnicima

Individualna komunikacija sa korisnicima se primarno odvija preko PKSCA on line HelpDesk sistema na adresi: http://helpdesk.pksca.rs/.

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

Kontaktni podaci za dostavu dopisa prema PKSCA	
Poštanska adresa:	Privredna komora Srbije Sertifikaciono telo Resavska 15 11000 Beograd

9.12. Izmene i dopune Praktičnih pravila

9.12.1. Procedure za izmene i dopune

Praktična pravila se revidiraju po potrebi, a najmanje jednom u 12 meseci.

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

Svi korisnici mogu na kontakt adresu PKSCA poslati dopis s predlogom za ispravke grešaka, predlog izmena ili dopuna ovog dokumenta. U dopisu se navode kontakt podaci osobe koja je poslala predlog izmene. PKSCA može prihvatiti, prilagoditi ili odbiti predložene izmene, nakon razmatranja istih.

9.12.2. Mehanizam i vremenski period obaveštavanja

Sve izmene i dopune Praktičnih pravila objavljuju se u elektronskom obliku na repozitorijumu PKSCA.

Nove verzije Praktičnih pravila sa izmenjenim OID-om dokumenta objavljuju se u elektronskom obliku na repozitorijumu PKSCA.

Datum stupanja na snagu izmena i dopuna ili novoobjavljenog dokumenta praktičnih pravila naznačen je na njegovoj naslovnoj strani kao i na internet stranicama na kojima je objavljen.

9.12.3. Uslovi promene identifikatora objekta (OID)

Veće izmene u Praktičnim pravilima, koje mogu uticati na korisnike zahtevaju i izmenu OID-a

ovog dokumenta. OID za novu verziju dokumenta određuje PKSCA.

9.13. Procedure rešavanja sporova

Sporovi ili neslaganja između PKSCA i drugih učesnika povodom radnji i/ili postupaka pružanja usluga od poverenja uređenih ovim dokumentom će se rešavati sporazumno. Ako sporazumno rešenje spora nije moguće, isti će se rešavati pred nadležnim sudom u Republici Srbiji.

Korisnici mogu u PKSCA uputiti prigovor ako smatraju da postoji odstupanje sadržaja usluge u odnosu na objavljene uslove pružanja usluga. PKSCA će razmotriti prigovor i odgovoriti podnosiocu. Prigovor se upućuje pismeno i dostavlja, u papirnom obliku, na adrese navedene u ovom dokumentu.

9.14. Važeći propisi

Kvalifikovane usluge od poverenja iz opsega Praktičnih pravila PKSCA pruža u skladu sa Zakonom o elektronkom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i podzakonskim aktima donetim na osnovu njega.

9.15. Usaglašenost sa važećim zakonima

Ovaj dokument i u njemu opisana usluga od poverenja usaglašeni su sa zakonskom regulativom Republike Srbije.

Svi korisnici saglasni su sa primenom prava Republike Srbije u tumačenju odredbi ovog dokumenta.

9.16. Ostale odredbe

Gde je to moguće, usluge od poverenja koje pruža PKSCA i proizvodi za krajnjeg korisnika koji se koriste pri pružanju tih usluga dostupni su licima sa invaliditetom.

PKS CA Cloud izdaje testne sertifikate. Testni sertifikati se prvenstveno izdaju PKSCA za potrebe testiranja PKSCA sistema, a mogu se izdati i drugom poslovnom subjektu u svrhu testiranja sistema. Testni sertifikati izdaju se isključivo u svrhu testiranja i nemaju nikakvo pravno dejstvo. PKSCA ne preuzima nikakvu odgovornost za korišćenje testnih sertifikata.

PKSCA javno objavljuje ovaj dokument i uslove pružanja usluga od poverenja.

Pre sklapanja ugovora o obavljanju usluga od poverenja, korisnici se informišu o uslovima pružanja tih usluga. Prihvatanje uslova pružanja usluga od poverenja preduslov je za izdavanje sertifikata.

U postupcima obnove sertifikata, ponovnog izdavanja sertifikata nakon isteka, opoziva ili izmene podataka u sertifikatu, PKSCA obaveštava korisnika o eventualnim izmenama uslova o pružanju usluga od poverenja.

10. ISTORIJAT DOKUMENTA

Verzija	Datum	Opis	Autor
1.0	25.10.2019.	Radna verzija	Dušan Berdić
2.0	25.12.2019	Finalna verzija	Dušan Berdić
3.0	22.10.2020.	Izmene i dopune	Tanja Grujović
3.1	01.06.2021.	Finalna verzija	Jelena Radić

11. ODOBRENJE DOKUMENATA

Ime i prezime	Radno mesto	Potpis	Datum
Dušan Berdić	Rukovodilac CA		01.06.2021.

PRIVREDNA KOMORA SRBIJE

mr Dušan Berdić

Sertifikaciono telo