POLITIKA

PRUŽANJA KVALIFIKOVANIH USLUGA OD POVERENJA SERTIFIKACIONOG TELA PRIVREDNE KOMORE SRBIJE

OID dokumenta 1.3.6.1.4.1.31266.10.2.3.1.0

Verzija 3.1

Sadržaj

Na osnovu Zakona o elektronskoj identifikaciji, elektronskom dokumentu i uslugama od poverenja u elektronskom poslovanju (Službeni glasnik RS 94/2017), Upravni odbor Privredne komore Srbije donosi:

POLITIKU PRUŽANJA KVALIFIKOVANIH USLUGA OD POVERENJA

SERTIFIKACIONOG TELA PRIVREDNE KOMORE SRBIJE

1. UVOD

Privredna komora Srbije (u daljem tekstu: PKS) izgradila je infrastrukturu javnih kriptografskih ključeva (*Public Key Infrastructure – u daljem tekstu: PKI*) i na tržištu je prisutna kao sertifikaciono telo koje pruža kvalifikovane usluge od poverenja, pod imenom Sertifikaciono telo PKS (u daljem tekstu: PKSCA).

PKSCA radi kao kvalifikovani pružalac usluga od poverenja u skladu sa zakonskim propisima, opštim aktima i uputstvima Sertifikacionog tela PKS, koji regulišu ovu oblast.

Zakon o elektronskoj identifikaciji, elektronskom dokumentu i uslugama od poverenja u elektronskom poslovanju (Sl. glasnik RS, br. 94/2017) i podzakonska akta doneta na osnovu njega čine pravni okvir za obavljanje usluga od poverenja PKSCA.

PKSCA vrši izdavanje kvalifikovanih elektronskih sertifikata u skladu sa odgovarajućim međunarodnim standardima i preporukama, odnosno drugim standardima, dokumentima i preporukama, koji se odnose na izdavanje kvalifikovanih elektronskoh sertifikata.

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

Poslovna mreža PKS ima nacionalnu pokrivenost poslovnicama, a njihova informatička povezanost obezbeđuje brzinu i pouzdanost izvršenja zahteva, koju koristi i registraciona služba PKSCA (u daljem tekstu: PKSCA RA mreža).

Ovim dokumentom se definiše način na koji PKSCA ispunjava tehničke, organizacione i

proceduralne zahteve poslovanja, koji su propisani za elektronske usluge od poverenja, u skladu sa standardom ETSI EN 319 401 V2.2.0 (2017-08) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

1.1. Pregled

PKSCA predstavlja PKI infrastrukturu uspostavljenu u Privrednoj komori Srbije kojom se pružaju sledeće kvalifikovane usluge od poverenja:

- izdavanje kvalifkovanih elektronskih sertifikata za elektronski potpis/pečata na smart karticama,
- izdavanje kvalifikovanih elektronskih sertifikata za elektronski potpis/pečat u cloud-u,
- izdavanje kvalifikovanih elektronskih vremenskih žigova,
- usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa/pečata i
- usluge validacije kvalifikovanog elektronskog potpisa/pečata

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.

PKS ostavlja mogućnost uspostave i drugih podređenih sertifikacionih tela u hijerarhijskoj strukturi, za potrebe izdavanja drugih tipova elektronskih sertifikata, odnosno pružanje drugih kvalifikovanih usluga od poverenja.

PKS CA Root radi kao korensko sertifikaciono telo na osnovu sertifikata izdatog samom sebi (*self-signed certificate*) u procesu generisanja privatnog kriptografskog ključa aplikacije sertifikacionog tela (*Root Key Generation Ceremony*). *PKS CA Root* izdaje sertifikate podređenim sertifikacionim telima koja su deo infrastrukture PKSCA.

PKS CA Class1, kao podređeno sertifikaciono telo, izdaje kvalifikovane elektronske sertifikate za kvalifikovani elektronski potpis pravnim i fizičkim licima, a zaposlenima koji rade na poslovima sertifikacije u PKSCA izdaje administratorske sertifikate. Ovo CA telo, takođe, izdaje sertifikate za servis za validaciju kvalifikovanih elektronskih potpisa/pečata i svoj OCSP servis.

PKS CA Cloud, kao podređeno sertifikaciono telo, izdaje kvalifikovane elektronske sertifikate za elektronski potpis fizičkim licima i ovlašćenim licima u okviru pravnog lica, kao i kvalifikovane elektronske sertifikate za elektronski pečat pravnim licima u okviru usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa, odnosno pečata.

PKS CA TSA kao podređeno sertifikaciono telo izdaje kvalifikovani sertifikat za servis izdavanja kvalifikovanih elektronskih vremenskih žigova i sertifikat za svoj OCSP servis.

Kvalifikovani elektronski sertifikati se izdaju po standardu *X*.509 verzija 3 i namenjeni su za verifikovanje kvalifikovanog elektronskog potpisa, odnosno pečata.

Korisnici kvalifikovanih elektronskih sertifikata PKSCA, poseduju jedan par asimetričnih kriptografskih ključeva (javni i privatni ključ). Privatni kriptografski ključ koristi se za kvalifikovano elektronsko potpisivanje/pečatiranje, a javni kriptografski ključ koristi se za validaciju kvalifikovanog elektronskog potpisa/pečata.

Korisnik kvalifikovanog elektronskog sertifikata može biti fizičko lice, pravno lice ili ovlašćeno lice zaposleno u pravnom licu koje se identifikuje specifičnim atributima. Ukoliko PKSCA izdaje kvalifikovani elektronski sertifikat ovlašćenom licu koje je zaposleno u pravnom licu, u okviru atributa koji identifikuju korisnika nalaze se i podaci koji označavaju naziv pravnog lica.

Kvalifikovani elektronski sertifikati i pripadajući privatni kriptografski ključevi koriste se za kvalifikovano elektronsko potpisivanje/pečatiranje elektronskih dokumenata.

Privatni kriptografski ključevi koji su pridruženi kvalifikovanim elektronskim sertifikatima koriste se u procesu kvalifikovanog elektronskog potpisivanja/pečatiranja elektronskog dokumenta, koji se može koristiti u međusobnom opštenju organa javne vlasti, opštenju organa javne vlasti i stranaka, u pravnim poslovima i drugim pravnim radnjama, kao i u upravnom, sudskom i drugom postupku pred državnim organom, ako je zakonom kojim se utvrđuje taj postupak propisana upotreba kvalifikovanog elektronskog potpisa.

Kvalifikovani elektronski sertifikati potvrđuju vezu između javnog kriptografskog ključa korisnika i identiteta korisnika koji je izvršio kvalifikovano potpisivanje elektronskog dokumenta.

Svaka upotreba kvalifikovanog elektronskog sertifikata koja nije u saglasnosti sa odredbama Zakona o elektronskoj identifikaciji, elektronskom dokumentu i uslugama od poverenja u elektronskom poslovanju i drugim aktima koji regulišu ovu oblast, nije dozvoljena.

PKSCA je uspostavilo uslugu upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa/pečata, u kome generisanje ili upravljanje privatnim ključevima u ime potpisnika i

autora pečata sprovodi PKSCA, kao kvalifikovani pružalac usluga od poverenja. Kvalifikovane sertifikate povezane sa ključevima generisanim u ovoj usluzi od poverenja za potpisnike i autore pečata izdaje PKSCA.

1.1.1. Opseg i namena

Politika pružanja kvalifikovanih usluga od poverenja Sertifikacionog tela Privredne komore Srbije (u daljem tekstu: CP) opisuje pravila i skup načela kojim PKSCA pruža kvalifikovane usluge od poverenja, kao i praktična pravila rada za korensko sertifikaciono telo PKS CA Root, odnosno za postupke i procedure koje ono primenjuje prilikom izdavanja i upravljanja sertifikatima za podređena sertifikaciona tela i sopstveni OCSP servis.

Opseg ovog CP dokumenta su kvalifikovane usluge od poverenja koje pruža PKSCA, a koje se odnose na izdavanje i upravljanje životnim ciklusom kvalifikovanih elektronskih sertifikata izdatim na bezbednim kriptografskim uređajima i njihovu primenu u kvalifikovanim uslugama od poverenja.

Produkcioni sertifikati iz opsega ovog CP dokumenta sastavni su deo Registra digitalnih sertifikata PKSCA, a izdaju ih CA tela iz opsega ovog CP dokumenta: PKS CA Class1, PKS CA Cloud i PKS CA TSA.

Namena ovog dokumenta je definisanje pravila iz područja određenog opsegom ovog dokumenta, 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.

Postupci koji se primenjuju prilikom izdavanja korisničkih sertifikata su opisani u odgovarajućim praktičnim pravilima rada (u daljem tekstu: CPS – *Certificate Practice Statement*) za konkretne kvalifikovane usluge od poverenja. CPS definišu način na koji sertifikaciono telo ispunjava tehničke, organizacione i proceduralne zahteve poslovanja koji su identifikovani u Politici pružanja kvalifikovanih usluga od poverenja.

PKSCA posebno utvrđuje i interna pravila rada pružaoca kvalifikovanih usluga od poverenja i zaštite sistema usluga od poverenja (u daljem tekstu: Interna pravila) u kojima su sadržani i detaljno opisani postupci i mere koji se primenjuju prilikom ostvarivanja usluga od poverenja, upravljanja životnim ciklusom sertifikata, kao i upravljanja IT infrastrukturom i njenom zaštitom. Interna pravila su privatni dokument i predstavljaju poslovnu tajnu pružaoca kvalifikovanih usluga od poverenja.

1.1.2. Tipovi sertifikata

Grupe, tipovi i profili sertifikata koje izdaje PKSCA su navedeni u poslednjoj verziji dokumenta „Pregled profila sertifikata PKSCA“. Ovim dokumentom definisane su grupe sertifikata, tipovi sertifikata i njima pripadajući nivoi bezbednosti.

6.2. Naziv dokumenta i identifikacija

Internet Assigned Number Authority (IANA) dodelio je Privrednoj komori Srbije sledeći OID (Object identifier): 1.3.6.1.4.1.31266.

Na osnovu ovog OID PKS je, za potrebe PKSCA PKI, dodelila OID: 1.3.6.1.4.1.31266.10.

U nastavku se navodi naziv ovog dokumenta i njegovi identifikacioni podaci:

- Naziv: Politika pružanja kvalifikovanih usluga od poverenja sertifikacionog tela Privredne komore Srbije
- Verzija: 1.0
- OID: 1.3.6.1.4.1.31266.10.2.3.1.0

Internet adresa na kojoj je objavljen ovaj CP dokument je: http://v3.pksca.rs.

1.1. Učesnici u sistemu pružanja usluga od poverenja PKS

Učesnici u pružanju usluga od poverenja PKSCA su:

- Sertifikaciona tela (CA)
- Registraciona tela (RA)
- Korisnici
- Pouzdajuće strane (treće strane)

1.1.1. Sertifikaciona tela PKSCA

Sertifikaciona tela koja učestvuju u pružanju usluga od poverenja su:

- Korensko sertifikaciono telo: PKS CA Root
- Podređeno sertifikaciono telo: PKS CA Class1
- Podređeno sertifikaciono telo: PKS CA Cloud
- Podređeno sertifikaciono telo: PKS CA TSA

Sva navedena sertifikaciona tela se nalaze i njima se upravlja na centralnoj lokaciji PKS, a u okviru Direktorata za informacione tehnologije PKS, u specijalno namenjenim prostorijama koje ispunjavaju sve zahteve propisane relevantnim pravilnicima.

1.1.2. Registraciona tela PKS CA

Poslove registracionog tela za krajnje korisnike vrše registraciona tela PKSCA i Centralno registraciono telo PKSCA.

Regionalne privredne komore predstavljaju registraciona tela za podnošenje zahteva za kvalifikovane usluge od poverenja. Uloga registracionog tela u procesu podnošenja zahteva za kvalifikovanu uslugu poverenja opisana je u CPS dokumentu konkretne usluge.

Centralno registraciono telo PKSCA je namenjeno da primi zahteve za usluge od poverenja od PKSCA RA i pokrene proces realizacije usluge od poverenja. Uloga centralnog registracionog tela u procesu realizacije usluge od poverenja opisana je u CPS dokumentu konkretne usluge.

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

Poslovima registracije u RA mreži koordinira Centralno RA PKSCA.

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

1.1.3. Korisnici

Korisnike usluga od poverenja koje pruža PKSCA predstavljaju fizička lica, pravna lica i ovlašćena lica u okviru pravnih lica.

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

1.1.4. Pouzdajuće strane (treće strane)

Pouzdajuće strane ili treće strane su fizička i pravna lica koja se pouzdaju u kvalifikovanu uslugu od poverenja na osnovu razumnog poverenja u sertifikat potpisnika generisan od strane PKSCA.

Pre nego što se pouzdaju u uslugu od poverenja, pouzdajuće strane moraju da realizuju procedure provere usluge od poverenja, definisane CPS dokumentom konkretne usluge.

1.2. Upotreba sertifikata

1.2.1. Dozvoljena upotreba sertifikata

Sertifikat PKS CA Root sertifikacionog tela i njemu pripadajući par asimetričnih ključeva se koristi isključivo za izdavanje sertifikata njemu podređenih CA tela, validaciju elektronskog potpisa njemu podređenih CA tela i elektronsko potpisivanje CRL.

Sertifikati podređenih CA tela i njima pripadajući parovi asimetričnih ključeva se koriste za izdavanje korisničkih sertifikata, validaciju korisničkih elektronskih potpisa, potpisivanje pripadajućih CRL, izdavanje sertifikata za pripadajuće OCSP servise, validaciju elektronskih potpisa OCSP servisa, kao i za izdavanje sertifikata za servis izdavanja vremenskih žigova i validaciju potpisa na elektronskim vremenskim žigovima.

Dozvoljena upotreba sertifikata koje izdaju podređena sertifikaciona tela je definisana u CPS dokumentima konkretnih usluga od poverenja.

1.2.2. Zabranjena upotreba sertifikata

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

Zabranjena upotreba sertifikata koje izdaju podređena sertifikaciona tela je definisana CPS dokumentom konkretne usluge od poverenja.

1.3. Administracija Politike sertifikacije PKS CA

1.3.1. Organizacija administriranja Politike sertifikacije

PKSCA je odgovorno za izradu i administraciju ove CP i to u smislu periodičnog pregleda i ažuriranja, kao i vanrednih promena odgovarajućih odredbi koje proističu iz eventualnih promena u zakonskoj regulativi ili promena u tehničkim karakteristikama primenjenih kriptografskih algoritama i dužine ključeva.

1.3.2. Kontakt osoba

Osoba u PKS CA, odgovorna za ovu CP je:

Dušan Berdić
Privredna Komora Srbije
Resavska 13-15
11000 Beograd, Srbija
Tel.:(011) 330 4545
E-mail: dusan.berdic@pks.rs

1.3.3. Osoba koja određuje usaglašenost CP dokumenta

Nije primenljivo.

1.3.4. Procedura odobravanja CP dokumenta

Nije primenljivo.

1.4. Definicije i skraćenice

1.4.1. Definicije

POJAM	ZNAČENJE
Aktivacioni podaci	Tajni podaci potrebni za pristup ili aktivaciju kriptografskog modula. Aktivacioni podatak može biti PIN, šifra ili elektronski ključ koji osoba zna ili poseduje.
Autentikacija	Proces provere identiteta pravnog lica, fizičkog lica ili fizičkog lica u svojstvu registrovanog subjekta uključujući proveru integriteta i porekla podataka za koje se pretpostavlja da ih je to lice stvorilo, odnosno poslalo.
Autor pečata	Sinonim za pojam “pečatilac”. Za značenje pojma pogledati odrednicu “pečatilac”.
Centralni RA	Centralna registraciona kancelarija koja je primarno zadužena za koordiniranje celokupne RA mreže, ali može obavljati i registraciju korisnika.
Deljena tajna	Deo kriptografske tajne koja je podeljena na unapred definisani broj SSCD (npr. smart kartica).
Ekstenzije sertifikata	Dodatna polja u sertifikatu, pored osnovnih, koja daju bliže informacije o vlasniku (korisniku) i izdavaču (CA) sertifikata.
Elektronski dokument	Skup podataka sastavljen od slova, brojeva, simbola, grafičkih, zvučnih i video materijala, u elektronskom obliku
Elektronski pečat	Skup podataka u elektronskom obliku koji su pridruženi ili logički povezani sa drugim (pečatiranim) podacima u elektronskom obliku tako da se elektronskim pečatom potvrđuje integritet tih podataka i identitet pečatioca;.
Elektronski potpis	Skup podataka u elektronskom obliku koji su pridruženi ili logički povezani sa drugim (potpisanim) podacima u elektronskim obliku tako da se elektronskim potpisom potvrđuje integritet tih podataka i identitet potpisnika.
Elektronski vremenski žig	Zvanično vreme pridruženo podacima u elektronskom obliku kojim se potvrđuje da su ti podaci postojali u tom vremenskom trenutku.
Fizičko lice - građanin	Fizičko lice koje uslugu sertifikovanja traži sa svrhom korišćenja sertifikata u vlastito ime i za vlastiti račun i isključuje fizičko lice sa registrovanom delatnošću, fizičko

POJAM	ZNAČENJE
	lice u obavljanju slobodnog zanimanja i fizičko lice koja nastupa u ime i za račun drugog fizičkog ili pravnog lica.
Hash algoritam	jednosmerni kriptografski algoritam koji vrši kriptografsku transformaciju informacije proizvoljne veličine u hash vrednost fiksne veličine (npr. 160, 224, 256, 374, 512 bitova)
Hash vrednost	Vrednost dobijena primenom hash algoritma na informaciju proizvoljne veličine.
Infrastruktura javnog ključa (PKI)	Infrastruktura za upravljanje javnim ključevima koji podržavaju usluge autentikacije, enkripcije, integriteti i validnosti.
Javni ključ	U infrastrukturi javnih ključeva, javno poznati ključ iz para ključeva subjekta sertifikacije.
Koordinirano svetsko vreme (UTC)	Vremenska lestvica koja se temelji na sekundi kako je definisana ITU-R preporukom TF.460-5. Za većinu primena u praksi UTC je ekvivalentan srednjem sunčevom vremenu na nultom meridijanu (0°). Tačnije, UTC je kompromis između vrlo stabilnog atomskog vremena (*Temps Atomique International* - TAI) i sunčevog vremena koje se izvodi iz nepravilne rotacije Zemlje (u odnosu na dogovoreno Greenwich srednje zvezdano vrieme (GMST).
Korisnik	Pravno ili fizičko lice koje je sklapanjem ugovora sa pružaocem usluga od poverenja preuzelo ugovorne obaveze korisnika.
Kriptografski modul	Softver ili uređaj određenog nivoa sigurnosti koji: generiše par ključeva i/ili, štiti kriptografske informacije i/ili, obavlja kriptografske funkcije.
Kvalifikovani sertifikat za elektronski pečat	Sertifikat za elektronski pečat koji izdaje kvalifikovani pružalac usluga od poverenja i koji ispunjava uslove predviđene Zakonom.
Kvalifikovani sertifikat za elektronski potpis	Sertifikat za elektronski potpis koji izdaje kvalifikovani pružalac usluga od poverenja i koji ispunjava uslove predviđene Zakonom.
Kvalifikovani elektronski pečat	Napredni elektronski pečat koji je kreiran kvalifikovanim sredstvom za kreiranje elektronskog pečata i koji je zasnovan na kvalifikovanom sertifikatu za elektronski pečat.
Kvalifikovani elektronski potpis	Napredni elektronski potpis koji je kreiran kvalifikovanim sredstvom za kreiranje elektronskog potpisa i koji se zasniva na kvalifikovanom sertifikatu za elektronski potpis.
Kvalifikovani elektronski vremenski žig	Elektronski vremenski žig koji ispunjava uslove utvrđene Zakonom za kvalifikovani elektronski vremenski žig.

POJAM	ZNAČENJE
Kvalifikovano sredstvo za izradu elektronskog pečata	Sredstvo koje ispunjava uslove propisane Zakonom.
Kvalifikovano sredstvo za izradu elektronskog potpisa	Sredstvo koje ispunjava uslove propisane Zakonom.
Lanac sertifikata	Uređena sekvenca sertifikata koja se, zajedno sa javnim ključem inicijalnog objekta u lancu (putu), procesira u cilju provere istog u poslednjem objektu na putu.
Lista opozvanih sertifikata (CRL)	Elektronski potpisana lista u kojoj su naznačeni sertifikati koje izdavalac sertifikata više ne smatra valjanim.
Napredni elektronski pečat	Elektronski pečat koji ispunjava dodatne uslove za obezbeđivanje višeg nivoa pouzdanosti potvrđivanja integriteta podataka i identiteta pečatioca u skladu sa Zakonom.
Napredni elektronski potpis	Elektronski potpis koji ispunjava dodatne uslove za obezbeđivanje višeg nivoa pouzdanosti potvrđivanja integriteta podataka i identiteta potpisnika u skladu sa Zakonom.
Opoziv sertifikata	Trajni prestanak valjanosti sertifikata pre isteka roka važenja navedenog u sertifikatu.
Osoba ovlašćena za zastupanje	Osoba koja je po zakonu ovlašćena za zastupanje korisnika (poslovnog subjekta).
Ovlaćeno lice	Fizičko lice zaposleno u poslovnom subjektu ili na drugi način povezano sa pravnim licem, a koje je od strane istog pravnog lica autorizovano za dobijanje sertifikata. Sertifikat identifikuje osobu i pravno lice i garantuje da je ta osoba povezana s pravnim licem.
Ovlašćeni predstavnik	Fizičko lice koja je po zakonu ili na temelju punomoćja ovlašćena da zastupa pečatioca u postupku izdavanja i /ili opoziva sertifikata za elektronski pečat.
Par ključeva	Dva jedinstveno povezana kriptografska ključa u sistemu asimetrične kriptografije, od kojih je jedan privatni ključ, a drugi javni ključ.
Pečatilac	Pravno lice, fizičko lice ili fizičko lice u svojstvu registrovanog subjekta u čije ime se kreira elektronski pečat i čiji su identifikacioni podaci navedeni u sertifikatu na osnovu koga je kreiran taj elektronski pečat, odnosno u sertifikatu kojim se potvrđuje veza između identiteta tog pečatioca i podataka za validaciju elektronskog pečata koji odgovaraju podacima za kreiranje elektronskog pečata koji su po ovlašćenju pečatioca korišćeni pri kreiranju tog elektronskog pečata.
PKSCA PKI	Infrastruktura javnog ključa (PKI) uspostavljena u PKSCA koja je namenjena za pružanje usluga sertifikovanja fizičkim licima – građanima, poslovnim subjektima i telima državne uprave, a koja je uspostavljena kao treća

POJAM	ZNAČENJE
	strana od poverenja (engl. *Trusted Third Party*).
PKSCA RA mreža (RA mreža)	Mreža registracionih kancelarija u PKSCA, a sastoji se od Centralnog registracionog tela PKSCA i registracionih tela PKSCA (regionalne privredne komore).
Podaci za izradu elektronskog potpisa, odnosno pečata	Jedinstveni podaci koje koristi potpisnik odnosno pečatilac za kreiranje elektronskog potpisa odnosno pečata i koji su logički povezani sa odgovarajućim podacima za validaciju elektronskog potpisa odnosno pečata.
Podaci za validaciju elektronskog potpisa, odnosno pečata	Podaci na osnovu kojih se proverava da li elektronski potpis odnosno pečat odgovara podacima koji su potpisani odnosno pečatirani.
Potpisnik	Fizičko lice koje je kreiralo elektronski potpis i čiji su identifikacioni podaci navedeni u sertifikatu na osnovu koga je kreiran taj elektronski potpis, to jest sertifikatu kojim se potvrđuje veza između identiteta tog potpisnika i podataka za validaciju elektronskog potpisa koji odgovaraju podacima za kreiranje elektronskog potpisa koje je potpisnik koristio pri kreiranju tog elektronskog potpisa.
Pouzdajuća strana (treća strana)	Pravno ili fizičko lice koje se pouzdaje u uslugu elektronske identifikacije odnosno uslugu od poverenja.
Poverljive uloge	Uloge od kojih zavisi sigurnost rada pružaoca usluga od poverenja. Poverljive uloge (engl. *Trusted Roles*) i pripadajuće odgovornosti pružaoc usluga od poverenja jasno opisuje u opisu posla zaposlenog.
Praktična pravila sertifikovanja – Certification Practice Statement (CPS)	Pravilnik operativnih postupaka koje sertifikaciono telo sprovodi u izdavanju, upravljanju, opozivu ili obnovi sertifikata, kao i prilikom pružanja neke od usluga od poverenja.
Pružalac kvalifikovanih usluga od poverenja	Pravno lice ili fizičko lice u svojstvu registrovanog subjekta koje pruža jednu ili više kvalifikovanih usluga od poverenja.
Privatni ključ	U infrastrukturi javnih ključeva, ključ iz para ključeva koji je poznat samo subjektu sertifikacije.
Pružalac usluga od poverenja	Pravno lice ili fizičko lice u svojstvu registrovanog subjekta koje pruža jednu ili više usluga od poverenja.
Reaktivacija sertifikata	Radnja koja suspendovani sertifikat ponovno čini validnim.
Redovna obnova sertifikata	Obnova sertifikata u PKSCA podrazumeva izdavanje novog sertifikata čiji su parametri jednaki kao i parametri sertifikata na koji se Zahtev odnosi, ali s novim javnim ključem, novim serijskim brojem sertifikata, novim vremenskim periodom važenja i novim potpisom istog CA, a sprovodi se u definiranom periodu pre datuma

POJAM	ZNAČENJE
	isteka važenja sertifikata.
Registracioni autoritet – Registration Authority (RA)	Telo odgovorno za identifikaciju i autentikaciju subjekata sertifikovanja, kao i drugih osoba ili organizacija.
Root CA	Sertifikaciono telo najvišeg nivoa unutar domena Pružalaca usluga od poverenja koje potpisuje sertifikate podređenih sertifikacionih tela.
Root CA sertifikat	Samopotpisujući CA sertifikat koga samom sebi izdaje root CA.
Sertifikaciona politika – Politika pružanja usluga od poverenja - Certificate Policy (CP)	Imenovani skup pravila koji ukazuje na primenjivost sertifikata za određeni skup usluga od poverenja sa zajedničkim bezbednosnim zahtevima.
Sertifikaciono telo (CA)	Telo koje izrađuje, elektronski potpisuje i distribuira sertifikate, a kojem veruje jedan ili više korisnika. Sertifikaciono telo može biti: pružalac usluge od poverenja koji izrađuje, elektronski potpisuje i distribuira sertifikate, ili tehnički servis izrade sertifikata kojeg upotrebljava pružalac usluga sertifikovanja koji izrađuje, elektronski potpisuje i distribuira sertifikate.
Sertifikat	Sertifikat za elektronski potpis odnosno pečat je elektronska potvrda kojom se potvrđuje veza između podataka za validaciju elektronskog potpisa odnosno pečata i identiteta potpisnika odnosno pečatioca.
Sertifikat za elektronski pečat	Pogledati odrednicu “sertifikat”.
Sertifikat za elektronski potpis	Pogledati odrednicu “sertifikat”.
Siguran kriptografski uređaj	Uređaj koji čuva privatni korisnički ključ, štiti ga od kompromitovanja i obavlja kriptografske funkcije za korisnika.
Službenik za opoziv sertifikata	Osoba koja je odgovorna za promenu operativnog statusa sertifikata.
Službenik za registraciju	Osoba odgovorna za proveru i potvrđivanje ličnih podataka koji su potrebni za izdavanje sertifikata i za odobravanje zahteva za izdavanje sertifikata.
Centralni RA	Centralna registraciona kancelarija koja je primarno zadužena za koordiniranje celokupne RA mreže, ali može obavljati i registraciju korisnika.
Sredstvo za kreiranje elektronskog potpisa odnosno pečata	Tehničko sredstvo (softver odnosno hardver) koje se koristi za kreiranje elektronskog potpisa odnosno pečata uz korišćenje podataka za kreiranje elektronskog potpisa odnosno pečata.
Sredstvo za izradu kvalifikovanog elektronskog pečata	Sredstvo za izradu elektronskog pečata koje *mutatis mutandis* ispunjava zahteve određene u Prilogu II. Kancelarijabe (EU) br. 910/2014 [1].
Subjekt	Korisnik identifikovan u sertifikatu kao vlasnik privatnog ključa koji je povezan s javnim ključem sadržanim u

POJAM	ZNAČENJE
	sertifikatu.
Suspenzija sertifikata	Privremeni prestanak valjanosti sertifikata pre isteka roka važenja navedenog u sertifikatu. Suspendovani sertifikat se reaktivacijom može ponovno učiniti valjanim.
Sistem usluga	Sistem IT proizvoda i komponenti organizovanih za pružanje usluga od poverenja.
Telo za ocenjivanje usaglašenosti	Telo ovlašćeno za sprovođenje ocenjivanja usaglašenosti kvalifikovanog pružaoca usluga od poverenja i kvalifikovane usluge od poverenja koju on pruža sa uslovima za pružanje kvalifikovanih usluga od poverenja.
TSA sistem	Sistem IT proizvoda i komponenti organizovanih za pružanje usluge izdavanja vremenskih žigova.
Usluge sertifikovanja	Usluge izdavanje i upravljanje životnim ciklusom sertifikata.
Usluga od poverenja	Elektronska usluga koja olakšava poslovnu aktivnost između dve ili više strana pri čemu se zasniva na tome da pružalac usluge stranama garantuje verodostojnost pojedinih podataka, a koja je kao takva određena Zakonom.
Validacija	Postupak provere i potvrđivanja ispravnosti elektronskog potpisa odnosno elektronskog pečata.

Tabela 1. – Definicije pojmova u dokumentu

1.5.1. Skraćenice

SKRAĆENICA	PUNI NAZIV	ZNAČENJE
CA	*Certification Authority*	Sertifikacioni autoritet - sertifikaciono telo
CP	*Certificate Policy*	Politika sertifikacije
CPS	*Certification Practice Statement*	Praktična pravila sertifikacije
CRL	*Certificate Revocation List*	Lista opozvanih sertifikata
ETSI	*European Telecommunication Standardization Institute*	Evropski institut za standardizaciju telekomunikacija
HSM	*Hardware Security Module*	Hardverski bezbednosni modul
OCSP	*Online Certificate Status Protocol*	Protokol za online proveru statusa sertifikata
OID	*Object Identifier*	Identifikator objekta
PIN	*Personal Identification Number*	Lični tajni broj za aktivaciju smart kartice, USB tokena ili sličnog uređaja
PKI	*Public Key Infrastructure*	
PKS	*Privredna komora Srbije*	
PKSCA	*Sertifikaciono telo PKS*	

SKRAĆENICA	PUNI NAZIV	ZNAČENJE
PKS CA Root	*Korensko sertifikaciono telo PKSCA*	
PKS CA Class1	*Podređeno sertifikaciono telo PKSCA za pružanje usluge izdavanja kvalifikovanih elektronskih sertifikata na smart karticama*	
PKS CA Cloud	*Podređeno sertifikaciono telo PKSCA za pružanje usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa, odnosno pečata*	
PKS CA TSA	*Podređeno sertifikaciono telo PKSCA za pružanje usluge izdavanja kvalifikovanih elektronskih žigova*	
QC	*Qualified Certificate*	Kvalifikovani sertifikat
QCP	*Qualified Certificate Policy*	Politika sertifikacije za kvalifikovane sertifikate
QCP-l	*Certificate policy for EU qualified certificate issued to a legal person*	Politika sertifikacije za EU kvalifikovane sertifikate izdate pravnim licima
QCP-l-qscd	*Certificate policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD*	Politika sertifikacije za EU kvalifikovane sertifikate izdate pravnim licima sa privatnim ključem i pripadajućim sertifikatom na QSCD uređaju
QCP-n	*Certificate policy for EU qualified certificate issued to a natural person*	Politika sertifikacije za EU kvalifikovane sertifikate izdate fizičkim licima
QCP-n-qscd	*Certificate policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD*	Politika sertifikacije za EU kvalifikovane sertifikate izdate fizičkim licima sa privatnim ključem i pripadajućim sertifikatom na QSCD uređaju
QSCD	*Qualified electronic Signature/Seal Creation Device*	Kvalifikovano sredstvo za izradu elektronskog potpisa/pečata
RA	*Registration Authority*	Registracioni autoritet
SSCD	*Secure Signature Creation Device*	Bezbedan uređaj za kreiranje elektronskog potpisa (npr. smart kartica)
TSA	*Time Stamp Authority*	Autoritet vremenskog žiga
TSP	*Trust Service Provider*	Pružalac usluga od poverenja
URL	*Uniform Resource Locator*	
UTC	*Coordinated Universal Time*	Koordinisano univerzalno vreme

Tabela 2. - Skraćenice

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. 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. PKSCA zadržava pravo da učini raspoloživim i publikuje informacije u vezi sopstvenih politika i procedura rada na bilo koji pogodan način.

Sertifikaciono telo PKS objavljuje podatke i svu dokumentaciju koja se odnosi na pružanje kvalifikovanih usluga od poverenja na svojoj internet stranici: http://v3.PKSCA.rs. Internet stranica je javno dostupna.

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

2.2. Publikovanje informacija o sertifikatima

PKSCA publikuje na svom repozitorijumu sledeće informacije o sertifikatima:

- Sertifikate PKSCA (Root i sertifikatepodređenih CA tela),
- Informacije o statusima opozvanosti sertifikata za sva CA tela (CRL),
- Online informacije o statusu sertifikata izdatih izdatih od strane podređenih CA tela (OCSP)

Korisnički sertifikati se ne objavljuju.

2.3. Učestalost publikovanja

PKSCA periodično i po potrebi održava, ažurira i publikuje CP i SPS za odgovarajuće usluge od poverenja. Prethodne verzije ovih dokumenata ostaju publikovane na repozitorijumu najmanje 10 godina posle isteka sertifikata izdatih u skadu sa tim dokumentima.

Ostali PKSCA dokumenti i druge relevantne informacije se objavljuju po potrebi.

Učestalost publikovanja CRL za sertifikate koje izdaju CA tela definisana je u taški 4.9.7. ovog dokumenta.

Online informacije o statusu izdatih sertifikata od strane podređenih CA tela su dostupne putem OCSP servisa u realnom vremenu.

2.4. Kontrola pristupa repozitorijumu

PKSCA održava 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,
- Publikovanja informacija u vezi pružanja kvalifikovanih usluga od poverenja

PKSCA ima uspostavljene kontrole pristupa na repozitorijumu u cilju sprečavanja neautorizovanog dodavanja, izmene ili brisanja informacija, kao i zaštitu njihovog integriteta i autentičnosti.

Pravo dodavanja, izmene ili brisanja informacija na PKSCA repozitorijumu imaju ovlašćena lica 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 PKS CA repozitorijumu je besplatan, ali PKSCA zadržava pravo da naplaćuje određena specifična korišćenja svojih servisa.

3. IDENTIFIKACIJA I AUTENTIKACIJA KORISNIKA

3.1. Dodeljivanje imena

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

Procedure identifikacije i autentikacije krajnjih korisnika definisani su u CPS dokumentima konkretne usluge od poverenja.

3.1.1. Vrste imena

PKS CA Root i njemu podređena CA tela upisuju u polje *Subject* sertifikata podatke o imenu, odnosno nazivu korisnika. Podaci o imenu ili nazivu koji se upisuju u sertifikat odnose se na autentično ime ili naziv korisnika. Polje *Subject* u sertifikatu usklađeno je s dokumentom IETF RFC 5280 (May 2008) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Atributi koji čine jedinstvena imena PKS CA Root dati su u sledećoj tabeli:

Korensko sertifikaciono telo PKS CA Root		
Atribut po X.520	Vrednost	Tumačenje
commonName	PKS CA Root	Naziv sertifikacionog tela
OrganizationName	Privredna komora Srbije	Naziv pravnog lica
organizationalUnit	PKSCA	Naziv organizacione jedinice
countryName	RS	Dvoslovni ISO kod države

Tabela 3. – Sadržaj polja *Subject* korenskog sertifikacionog tela

3.1.2. Potreba da imena imaju realno značenje

Imena i nazivi u atributima polja *Subject* imaju realno značenje i odgovaraju nazivima koji se koriste za sertifikaciona tela u produkcionoj hijerarhiji PKSCA.

Pravila za imena i nazive koji se upisuju u sertifikate izdate krajnjim korisnicima su opisana u CPS dokumentima konkretne usluge od poverenja.

3.1.3. Anonimnost korisnika i pseudonimi

Anonimnost i pseudonimi korisnika nisu podržani.

3.1.4. Pravila tumačenja različitih vrsta imena

Tumačenje oblika imena u polju *Subject* sertifikata koji izdaje PKS CA Root vrši se po tabeli 3 u

članu 3.1.1. koja je usklađena sa Zakonom i odgovarajućim standardima.

3.1.5. Jedinstvenost imena

Jedinstvenost imena u serifikatima CA garantuje se atributom commonName. Svako novo korensko ili podređeno sertifikaciono telo PKS mora imati jedinstveno ime u okviru hijerarhije sertifikacionog tela PKS koje se upisuje u atribut commonName.

3.1.6. Upotreba robnih marki („Trademarks“) u sertifikatima

Sertifikaciona tela ne koriste robne marke u svojim sertifikatima.

3.2. Inicijalno utvrđivanje identiteta

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

Metoda dokazivanja posedovanja privatnog ključa za korensko sertifikaciono telo i njemu podređenih sertifikacionih tela PKS-a obezbeđena je sprovođenjem procedure uspostave sertifikacionih tela i generisanja para asimetričnih ključeva.

Sertifikaciono telo izdaje sertifikate prema poglavlju 1.1.2.

3.2.2. Utvrđivanje identiteta pravnog lica

Nije primenljivo.

3.2.3. Utvrđivanje identiteta fizičkog lica

Nije primenljivo.

3.2.4. Informacije o korisniku koje se ne proveravaju

Nije primenljivo.

3.2.5. Provera identiteta ovlašćenih osoba

Nije primenljivo.

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

Nije primenljivo.

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

Nije primenljivo.

4. OPERATIVNI ZAHTEVI TOKOM ŽIVOTNOG CIKLUSA SERTIFIKATA

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

Procedure upravljanja sertifikatima krajnjih korisnika su opisane u CPS dokumentima konkretne usluge od poverenja.

4.1. Zahtev za izdavanje sertifikata

Izdavanje sertifikata za korensko sertifikaciono telo PKS CA Root, za podređena sertifikaciona tela i OCSP servise se sprovodi po formalnoj proceduri i po odobrenju PKSCA.

4.1.1. Ko može podneti zahtev za izdavanje sertifikata

Nije primenljivo.

4.1.2. Proces obrade zahteva za izdavanje sertifikata

Nije primenljivo.

4.2. Obrada zahteva za izdavanje sertifikata

Nakon odobrenja zahteva za izdavanje sertifikata navedenih u tački 4.1. ovog dokumenta, ovlašćene osobe sa poverljivim ulogama/dužnostima u PKSCA započinju sprovođenje ceremonije generisanja parova asimetričnih ključeva i izdavanje sertifikata za PKS CA Root ili njemu podređena CA tela.

4.3. Izdavanje sertifikata

4.3.1. Aktivnosti tokom procesa izdavanja sertifikata

Izdavanje sertifikata korenskom sertifikacionom telu PKS CA Root sprovodi se prema formalnoj proceduri uspostave korenskog sertifikacionog tela i generisanja para asimetričnih ključeva.

Izdavanje sertifikata podređenim sertifikacionim telima sprovodi se prema formalnoj proceduri uspostave konkretnog podređenog sertifikacionog tela i generisanja para asimetričnih ključeva.

Proceduru uspostave korenskog ili podređenog sertifikacionog tela sprovode lica sa poverljivim ulogama/dužnostima u zaštićenom prostoru PKSCA uz primenu propisanih bezbednosnih mera.

Izdavanje certifikata za OCSP servise sprovode lica sa poverljivim ulogoma/dužnostima, upotrebom aplikacije za OCSP servis.

4.3.2. Obaveštavanje korisnika od strane CA o izdavanju sertifikata

Sertifikati korenskog sertifikacionog tela i podređenih sertifikacionih tela objavljuju se na internet stranici PKSCA repozitorijuma, čija je adresa navedena u tački 2.1. ovog dokumenta.

4.4. Prihvatanje sertifikata

4.4.1. Sprovođenje procesa prihvatanja sertifikata

Sertifikati korenskog i podređenih sertifikacionih tela smatraju se proverenim, prihvaćenim i ispravnim, uspešnim završetkom procedure generisanja ključeva i izdavanja sertifikata.

Prihvatanje korisničkih sertifikata opisano je u CPS dokumentima konkretnih usluga od poverenja.

4.4.2. Objavljivanje sertifikata

Sertifikat korenskog sertifikacionog tela se objavljuje na internet stranici PKSCA repozitorijuma.

Sertifikati podređenih sertifikacionih tela se objavljuju na internet stranici PKSCA repozitorijuma.

Sertifikati za OCSP servis se ne objavljuju.

Korisnički sertifikati se ne objavljuju.

4.4.3. Obaveštavanje ostalih učesnika o izdavanju sertifikata

Objavljivanjem sertifikata korenskog sertifikacionog tela i njemu podređenih CA tela na PKSCA repozitorijumu, smatra se da su ostali učesnici obavešteni o njihovom izdavanju.

4.5. Korišćenje sertifikata i pripadajućih asimetričnih parova ključeva

4.5.1. Korišćenje privatnih ključeva i sertifikata od strane korisnika

Privatni ključevi korenskog sertifikacionog tela i podređenih certifikacionih tela se koriste isključivo za potpisivanje sertifikata koje izdaju i potpisivanje pripadajuće liste opozvanih certifikata.

Svaka druga upotreba ovih privatnih ključeva je strogo zabranjena.

Korišćenje privatnog ključa i pripadajućeg korisničkog sertifikata od strane korisnika opisano je u CPS dokumentu konkretne usluge od poverenja.

4.5.2. Korišćenje javnih ključeva i sertifikata od strane trećih lica

Treća lica koja nameravaju da koriste usluge od poverenja PKSCA i da ostvare poverenje u korensko sertifikaciono telo ili u njemu podređeno sertifikaciono telo treba da:

- Vode računa o dozvoljenoj upotrebi i zabranjenoj upotrebi javnog ključa i pripadajućeg sertifikata u skladu sa tačkom 1.4. ovog dokumenta;
- Obave proveru vremena važenja svih sertifikata u lancu i proveru sertifikata prema postupcima za validaciju lanca sertifikata, u skladu sa dokumentima RFC 5280 ili RFC 6960 (June 2013) X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP ;
- Obave proveru statusa sertifikata upotrebom raspoloživih načina, u skladu sa ovim dokumentom.

4.6. Obnavljanje sertifikata bez promene ključa

Korensko sertifikaciono telo i njemu podređena sertifikaciona tela ne vrše obnovu sertifikata bez promene ključa.

Obnavljanje sertifikata bez promene ključa za pojedine usluge od poverenja definisano je CPS dokumentom konkretne usluge od poverenja.

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

Obnovu sertifikata korenskog sertifikacionog tela i njemu podređenih sertifikacionih tela uz generisanje novog para asimetričnih ključeva može zatražiti lice sa poverljivom ulogom/dužnošću.

Ovakav način obnove sertifikata odobrava PKSCA.

Nakon odobrenja obnove certifikata, lica s poverljivim ulogama/dužnostima sprovode ceremoniju uspostave sertifikacionog tela i generisanja para asimetričnih ključeva za sertifikaciono telo.

Novi sertifikat za sertifikaciono telo objavljuje se na internet stranici PKSCA repozitorijuma.

Zahtev za obnovu sertifikata OCSP servisa sprovodi lice s poverljivom ulogom/dužnošću.

Postupak obnove korisničkih sertifikata opisan je u pripadajućem CPS dokumentu konkretne usluge od poverenja.

4.8. Izmena sertifikata korisnika

Izmena podataka u sertifikatima za korensko sertifikaciono telo i podređena sertifikaciona tela se ne sprovode. Ukoliko se ustanovi da postoji greška u korenskom sertifikatu ili sertifikatu podređenog sertifikacionog tela sprovodi se nova formalna procedura uspostave sertifikacionog tela i generisanja para asimetričnih ključeva.

Postupak izmene korisničkih sertifikata opisan je u CPS dokumentu konkretne usluge od poverenja.

4.9. Suspenzija i opoziv sertifikata

Zahtev za opoziv sertifikata korenskog sertifikacionog tela ili podređenog sertifikacionog tela odobrava PKSCA.

Suspenzija sertifikata korenskog sertifikacionog tela ili podređenog sertifikacionog tela nije dozvoljena.

Suspenzija i opoziv korisničkih sertifikata opisani su u CPS dokumentu konkretne usluge od poverenja.

4.9.1. Razlozi za opoziv sertifikata

Korensko sertifikaciono telo vrši opoziv izdatog sertifikata u sledećim slučajevima:

- Na osnovu pisanog zahteva za opoziv sertifikata izdatog podređenom sertifikacionom telu od strane lica s poverljivom ulogom/dužnošću u PKSCA;
- Ukoliko PKSCA dođe do saznanja da je privatni ključ povezan sa javnim ključem u sertifikatu sertifikacionog tela kompromitovan;
- Ukoliko primenjeni kripografski algoritam i dužina pripadajućeg asimetričnog ključa više ne zadovoljavaju kriptografske kriterijume propisane odgovarajućim standardima i na osnovu posebne odluke PKSCA;
- Ako se utvrdi da su podaci u izdatom sertifikatu pogrešni;
- U slučaju zabranjene upotrebe odnosno zloupotrebe privatnog ključa sertifikacionog tela;
- Ukoliko sertifikat svojim sadržajem, tehničkim karakteristikama i profilom ne pruža odgovarajući nivo poverenja.

Razlozi za opoziv korisničkih sertifikata opisani su u CPS dokumentu konkretne usluge od poverenja.

4.9.2. Ko može zahtevati opoziv sertifikata

Opoziv sertifikata CA tela se vrši na osnovu odluke PKSCA.

4.9.3. Procedura za opoziv sertifikata

Opoziv sertifikata sprovode lica sa poverljivim ulogama/dužnostima u PKSCA u bezbednom prostoru sertifikacionog tela.

4.9.4. Rok za podnošenje zahteva za opoziv sertifikata

Nije primenljivo.

4.9.5. Rok u kome CA mora obraditi zahtev za opoziv sertifikata

Sertifikaciono telo mora da obradi zahtev za opozivom sertifikata najkasnija 24 sata nakon prijema zahteva za opoziv.

4.9.6. Zahtevi za proverom opozvanosti sertifikata od strane trećih lica

Treća lica obavezna su da preduzimaju sve mere i postupke propisane ovim dokumentom prilikom provere validnosti sertifikata. Za potrebe validacije sertifikata treća lica koriste sve *online* resurse koje im na raspolaganje stavlja sertifikaciono telo radi provere statusa sertifikata u koji će se pouzdati.

Treća lica moraju biti saglasna sa politikom pružanja usluga od poverenja i upoznata sa svojim obavezama propisanim ovim dokumentom.

4.9.7. Učestalost izdavanja liste opozvanih sertifikata

Najnovija lista opozvanih sertifikata koju izdaje korensko sertifikaciono telo mora biti izdata najkasnije šest (6) meseci od prethodnog izdavanja liste opozvanih sertifikata. Ukoliko dođe do opoziva sertifikata koji je izdalo korensko sertifikaciono telo, nova lista opozvanih sertifikata će biti objavljena u roku od osam (8) sati.

Vreme važenja izdate liste opozvanih sertifikata korenskog sertifikacionog tela je šest (6) meseci.

Učestalost izdavanja liste opozvanih certifikata podređenih sertifikacionih tela definisana je u CPS dokumentu konkretne usluge od poverenja.

4.9.8. Maksimalno kašnjenje objavljivanja liste opozvanih sertifikata

U regularnim okolnostim kašnjenje u objavi liste opozvanih sertikikata nije duže od jednog (1) minuta.

U slučaju vanrednih okolnosti sertifikaciono telo će preduzeti sve mere u okviru svojih mogućnosti da kumulativno kašnjenje objavljivanja liste opozvanih sertifikata na godišnjem nivou ne bude duže od deset (10) dana.

4.9.9. Dostupnost online provere statusa sertifikata

Korensko sertifikaciono telo ne podržava online proveru statusa opozvanosti izdatih sertifikata putem OCSP servisa.

Podređena sertifikaciona telo podržavaju online provjeru statusa opozvanosti izdatih sertifikata putem OCSP servisa čiji je rad usaglašen s dokumentom IETF RFC 6960 i način njihovog korišćenja opisan je u CPS dokumentu konkretne usluge od poverenja.

4.9.10. Zahtevi za online proveru statusa sertifikata

Nije primenljivo.

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. Razlozi za suspenziju sertifikata

Nije primenljivo.

4.9.14. Ko može zahtevati suspenziju sertifikata

Nije primenljivo.

4.9.15. Procedura suspenzije sertifikata

Nije primenljivo.

4.9.16. Maksimalno trajanje suspenzije sertifikata

Nije primenljivo.

4.10. Servisi objavljivanja statusa sertifikata

4.10.1. Operativne karakteristike

Korensko sertifikaciono telo daje informacije o statusu certifikata objavljivanjem CRL.

Podređena sertifikaciona tela daju informacije o statusu sertifikata kroz pružanje OCSP servisa i objavljivanje CRL.

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

CRL za sertifikate koje izdaju sertifikaciona tela objavljuju se na repozitorijumu PKSCA.

Adrese publikovanja CRL sadržane su u ekstenziji *CRLDistributionPoints* u svakom izdatom sertifikatu.

Adresa CRL za PKS CA Root sertifikate na repozitorijumu PKSCA je:

http://v3.pksca.rs/crl/PKSCARoot.crl

4.10.2. Raspoloživost servisa

Dostupnost CRL i OCSP servisa je 24 sata na dan, 7 dana u nedelji. U slučaju ispada sistema, nastanka okolnosti koje su izvan kontrole sertifikacionog tela ili usled uticaja više sile, usluga će biti dostupna u skladu s planom kontinuiteta poslovanja PKSCA.

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

4.10.3. Dodatne funkcije

Nije primenljivo.

4.11. Prestanak korišćenja sertifikata

Nije primenljivo.

4.12. Čuvanje i rekonstrukcija privatnog ključa

PKSCA ne čuva i ne omogućava rekonstrukciju privatnih ključeva.

5. 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 provere tog sistema, upravljanja i radnih postupaka u PKSCA su interne prirode i njihovi detalji se ne objavljuju javno.

5.1. Mere fizičke zaštite

PKSCA kao Pružalac usluga od poverenja primenjuje mere fizičke zaštite sistema usluga sa ciljem minimiziranja rizika vezanih za fizičku bezbednost i u skladu sa poslovnom politikom PKSCA i važećom zakonskom regulativom.

5.1.1. Lokacija objekta i konstrukcija

Produkcioni sistem PKSCA smešten je u zgradi PKS, u posebno zaštićenom prostoru, izdvojenom za tu namenu, uz primenu više nivoa fizičke i tehničke zaštite koje onemogućavaju neovlašćen fizički pristup sistemu i podacima i time sprečavaju kompromitovanje sistema i usluga. Fizička zaštita zasnovana je na konceptu upotrebe bezbednosnih zona i nivoi zaštite se povećavaju svakim prolaskom 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.

Sigurni 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 u PKSCA zaštićenom prostoru i pripadajućim podprostorima unutar tog prostora, ostvaruje se dvostrukom kontrolom pristupa ovlašćenih osoba 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 osoba 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 osoba u 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. Sistemi za napajanje i klimatizaciju

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. Opasnost od poplave

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

5.1.5. Protivpožarna zaštita

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

5.1.6. Skladištenje medija

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 poplave. Ovi mediji zaštićeni su od oštećenja, krađe i neovlašćenog pristupa.

5.1.7. Zbrinjavanje otpada

Uređaji i mediji koji sadrže poverljive informacije u elektronskom obliku, a koji više nisu 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 osoba u PKSCA.

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

5.1.8. Sigurnosne kopije na drugoj lokaciji

Sigurnosne kopije PKSCA CA i RA sistema, arhivske ili sigurnosne kopije podataka, kopije sadržaja nosioca i sigurnosne kopije računarskih programa, skladište se na lokaciji koja je izdvojena od primarnog produkcionog sistema. Ove sigurnosne kopije su, u odnosu na njihove originale, zaštićene jednakim ili višim nivoom mera fizičke zaštite.

5.2. Organizacione mere zaštite

5.2.1. Poverljive uloge

Poslovi upravljanja informacionim i komunikacionim sistemom, poslovi upravljanja životnim ciklusom sertifikata, administriranje i implementacija sigurnosnih postupaka i poslovi nadzora delovanja 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 odgovornosti.

Poverljive uloge uključuju uloge:

- glavnog adminmistratora bezbednosti,
- administratora sistema,
- sistem operatera,
- sistem evidentičara,
- operatera sertifikacionog tela i
- operatera registracionog tela.

5.2.2. Broj osoba potrebnih za obavljanje aktivnosti

Poslove u PKSCA obavljaju isključivo ovlašćene osobe. PKSCA ima dovoljan broj stalno zaposlenih stručnih osoba sa znanjem, iskustvom i kvalifikacijama neophodnim 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 propisanog broja osoba sa određenim poverljivim ulogama.

5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu

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

5.2.4. Uloge koje zahtevaju odvajanje dužnosti

Zbog bezbednosnih zahteva usluga od poverenja sprovodi se 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. Osoblje

5.3.1. Kvalifikacije, radno iskustvo i zahtevi za proverom osoblja

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. Procedure provere osoblja

Pre zasnivanja radnog odnosa, PKSCA sprovodi odgovarajuće provere kandidata u cilju procene njihove stručnosti, sposobnosti i pouzdanosti, u skladu s potrebama poslova PKSCA.

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 edukacije i usavršavanja.

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 zamene zaposlenih

Nema odredbi.

5.3.6. Kazne 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 ugovornim partnerom.

5.3.7. Zahtevi na spoljne saradnike

Za ugovorene spoljne saradnike koji za PKSCA obavljaju deo usluga iz opsega usluga izdavanja kvalifikovanih sertifikata važe iste obaveze kao i za interne zaposlene.

Obaveze dobavljača roba i usluga za PKSCA regulisani su internim dokumentima o radu 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 je dostupna osoblju

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

5.4. Procedure upravljanja audit logovima

5.4.1. Tipovi događaja koji se zapisuju

PKSCA vodi audit logove događaja u PKSCA vezanih za:

- upravljanje životnim ciklusom CA ključeva PKSCA CA-ova,
- registraciju fizičkog lica i pravnog lica,
- pripremu i izdavanje sigurnih kriptografskih, odnosno HSM uređaja na kojima se izdaju kvalifikovani sertifikati,
- životni ciklus ključeva i upravljanje ključevima,
- životni ciklus sertifikata koje izdaju PKSCA CA-ovi,
- zahteve za opoziv, suspenziju i reaktivaciju sertifikata i pripadajuće sprovedene radnje,
- autentikaciju korisnika, aktivaciju i upotrebu korisničkih privatnih ključeva u servisu udaljenog potpisivanja u oblaku.
- autentikaciju korisnika, aktivaciju i upotrebu korisničkih privatnih ključeva u servisu izdavanja vremenskog žiga
- autentikaciju korisnika u servisu verifikacije elektronski potpisanog dokumenta u oblaku

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 firewall-a i aktivne mrežne opreme i pokušaja pristupa sistemu.

5.4.2. Učestalost obrade audit logova

Audit logovi u PKSCA se pregledaju redovno, na dnevnom nivou. Audit logovi pregledaju se i u svrhu praćenja i utvrđivanja zlonamernih aktivnosti na sistemu. PKSCA koristi automatske mehanizme za upozorenja 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. Vremenski period skladištenja audit logova

Audit logovi sa zapisima iz tačke 5.4.1. čuvaju se najmanje 10 godina od prestanka važnosti sertifikata na koji se zapisi 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. Postupci izrade sigurnosnih kopija 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

Zavisno o vrste podataka, audit logovi se prikupljaju automatski ili ih prikuplja ovlašćena osoba.

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

5.4.7. Obaveštavanje 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

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

Procena rizika informacione imovine sprovodi se 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

5.5.1. Tipovi arhiviranih zapisa

PKSCA arhivira niže navedene podatke koji, zavisno o tipu, mogu biti u elektronskom i/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. Vremenski period arhiviranja

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 osiguravaju 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. Postupci izrade sigurnosnih kopija arhive

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

5.5.5. Zahtevi na zaštitu zapisa vremenskim žigom

Nema odredbi.

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. Postupci dobijanja i provere arhiviranih zapisa

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

5.6. Promena CA ključa

PKSCA obezbeđuje kontinuirano pružanje kvalifikovanih usluga od poverenja validnim parovima ključeva i pripadajućim sertifikatima svojih CA tela. Iz tog razloga PKSCA će dovoljno vremena pre isteka CA sertifikata, generisati novi par CA ključeva. Takođe, PKSCA će dovoljno vremena ranije generiseti novi par CA ključeva i u slučaju kada tu promenu zahteva nivo sigurnosti kriptografskog algoritma privatnog CA ključa u upotrebi. U oba slučaja za novi javni CA ključ PKS CA Root izdaće CA sertifikat.

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

Novi pripadajući javni ključ biće dostupan korisnicima PKSCA na način na koji je to bio i prethodni PKSCA CA javni ključ, na repozitorijumu PKSCA, u skladu sa ovim dokumentom.

5.7. Oporavak od kompromitovanja ili nepogode

5.7.1. Postupci u slučaju incidenta ili kompromitovanja

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

Plan kontinuiteta poslovanja PKSCA revidira se jednom godišnje.

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

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

Funkcionalnost, ispravnost rada i pravovremeno otklanjanje oštećenja komponenti sistema osigurano je kroz ugovore 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 oporavka podataka.

5.7.3. Postupci u slučaju kompromitovanja privatnog ključa

U slučaju kompromitovanja ili sumnje u kompromitovanost privatnog ključa nekog od PKSCA sertifikacionih tela, PKSCA će odmah prekinuti sa upotrebom kompromitovanog privatnog ključa.

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

O opozivu PKSCA CA sertifikata PKSCA će obaveštavati sledeće korisnike:

- PKSCA RA mrežu,
- Korisnike,
- Treće strane kao korisnike usluga od poverenja.

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

Novi 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, na repozitorijumu PKSCA, 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 obavestiti:

- PKSCA RA mrežu,
- Korisnike,
- Treće strane kao korisnike usluga od poverenja.

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.

5.7.4. Mogućnost nastavka poslovanja nakon elementarnih nepogoda

U Planu kontinuiteta poslovanja PKSCA određeni 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. Prestanak rada CA ili RA

O planiranom prestanku pružanja usluga izdavanja kvalifikovanih sertifikata PKSCA će:

- obavestiti sve korisnike usluge, treće strane kao korisnike usluga od poverenja 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 će 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-ova.

U slučaju prestanka pružanja usluga izdavanja kvalifikovanih sertifikata PKSCA će arhivirati, zaštititi i čuvati zapise prema odredbama iz tačke 5.5. ovog CP dokumenta kako bi ti zapisi bili raspoloživi za pružanje dokaza u sudskim, upravnim i drugim postupcima u skladu sa važećim odredbama zakonske regulative, ili će PKSCA sa drugim poslovnim subjektom ugovoriti takvo arhiviranje, zaštitu i čuvanje zapisa.

6. TEHNIČKE MERE ZAŠTITE

PKSCA primenjuje tehničke bezbednosne mere u cilju zaštite kripotografskih kljlučeva i aktivacionih podataka. Kripotografski ključevi koji se štite merama i postupcima opisanim u ovom poglavlju mogu pripadati samom sertifikacionom telu. Primena ovih mera kritična je u smislu obezbeđenja zaštite kriptografskih ključeva i aktivacionih podataka i njihovog korišćenja isključivo od strane autorizovanih zaposlenih i servisa.

Ovo poglavlje opisuje mere zaštite koje se preduzimaju u cilju postizanja zahtevanog nivoa bezbednosti kriptografskih ključeva, aktivacionih podataka, kritičnih bezbednosnih parametara, upravljanja ključevima, sertifikatima, kao i druge mere tehničke bezbednosti za PKSCA CA.

6.1. Generisanje i instalacija para ključeva

6.1.1. Generisanje para ključeva

PKSCA sprovodi generisanje para ključeva PKSCA CA-ova koristeći algoritme za generisanje ključeva koji su u saglasnosti sa tehničkim specifikacijama ETSI TS 119 312 V1.2.1 (2017-05) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

6.1.1.1. Generisanje para PKSCA CA ključeva

Tokom generisanja i upravljanja sopstvenim privatnim ključevima PKSCA primenjuje sve odredbe Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju i podzakonskih akata proizašlih iz njega, kao i internacionalne i evropske standarde u vezi sa bezbednošću i pouzdanošću sistema. PKSCA, takođe, primenjuje sve mere, postupke i metode propisane ovim dokumentom, u cilju bezbednog i pouzdanog generisanja i sprečavanja kompromitacije ili neautorizovanog korišćenja privatnih ključeva.

Postupak generisenja para PKS CA Root ključeva sprovodi se formalnom ceremonijom generisenja para ključeva PKSCA CA Root, a postupak generisanja parova ključeva za podređena CA tela sprovodi se formalnom ceremonijom generisanja parova ključeva za podređena PKSCA CA tela.

Za potrebe međusobne komunikacije softverskih i hardverskih komponenti i sertifikacionog tela, kao i zaštite mrežne komunikacije između komponenti sistema, generišu se neophodni simetrični i asimetrični ključevi.

Ceremonija generisanja para ključeva za PKSCA CA sprovodi se prema protokolu za generisanje ključeva u kome su dokumentovani koraci koji se izvode za vreme ceremonije. Protokol za generisanje ključeva u skladu je sa standardom ETSI EN 319 411-1 V1.2.0 (2017-08) Electronic

Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

Parovi ključeva za PKSCA CA-ove generišu se, uz minimalno dvostruku kontrolu ovlašćenih osoba sa poverljivim ulogama/dužnostima u PKSCA, u HSM modulu koji zadovoljava zahteve iz tačke 6.2.1. ovog dokumenta.

PKSCA CA-ovi se, tokom i nakon ceremonije generisanja parova ključeva, nalaze u PKSCA zaštićenom prostoru, a pristup PKSCA CA dopušten je isključivo ovlašćenim licima PKSCA sa poverljivim ulogama/dužnostima.

Sprovođenje postupka ceremonije generisanja para ključeva za PKSCA CA se snima, a o sprovođenju postupka svedoči predstavnik nadležnog organa državne uprave.

O sprovedenom generisanju CA ključeva vodi se zapisnik sa priloženim audit logovima.

6.1.2. Dostava privatnog ključa korisniku

Privatni ključevi korenskog i podređenih CA tela se generišu u okviru procedure uspostavljanja sertifikacionog tela.

PKS CA Root ne izdaje korisničke sertifikate.

Dostava privatnih korisničkih ključeva, povezanih sa korisničkim sertifikatima koje izdaju podređena CA tela, opisana je u pripadajućim CPS dokumentima konkretnih usluga od poverenja.

6.1.3. Dostava javnog ključa CA-u

Dostava javnih ključeva podređenih CA tela PKS CA Root-u regulisana je i opisana u ceremoniji generisanja parova ključeva za PKSCA sertifikaciona tela.

Dostava javnih korisničkih ključeva, povezanih sa korisničkim sertifikatima koje izdaju podređena CA tela, opisana je u pripadajućim CPS dokumentima konkretnih usluga od poverenja.

6.1.4. Dostava javnog ključa CA pouzdajućim stranama

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

Javni ključevi PKSCA CA dostupni su trećim stranama u PKSCA CA sertifikatima koje je izdao PKSCA Root CA.

Internet adrese za preuzimanje PKSCA CA sertifikata su:

- PKSCA Root CA: http://v3.pksca.rs/certs/PKSCARoot.crt
- PKSCA CLASS1 CA: http://v3.pksca.rs/certs/PKSCAClass1.crt
- PKSCA Cloud CA: http://v3.pksca.rs/certs/PKSCACloud.crt
- PKSCA TSA CA: http://v3.pksca.rs/certs/PKSCATSA.crt

6.1.5. Dužine ključeva

Dužine ključeva u **PKSCA** su sledeće:

- PKSCA Root CA upotrebljava sha512WithRSA algoritam sa ključem dužine 4096 bita,
- Subordinirani PKSCA CA-ovi (PKSCA CLASS1, PKSCA CLOUD i PKSCA TSA) upotrebljavaju sha256WithRSA algoritam sa ključem dužine 3072 bita,
- PKSCA OCSP servis upotrebljava RSA ključeve dužine 2048 bita,
- RA mreža upotrebljava RSA ključeve dužine 2048 bita,
- Korisnici upotrebljavaju RSA par ključeva dužine 2048 bita.

6.1.6. Generisanje i provera kvaliteta parametara javnog ključa

PKSCA CA sprovodi generisanje para ključeva koristeći parametre za generisanje koji su usklađeni sa standardom ETSI TS 119 312.

Parovi asimetričnih kriptografskih ključeva se generišu pomoću hardverskih generatora slučajnih brojeva koji su realizovani na kriptografskim hardverskim uređajima (HSM modulima).

Kvalitet generisanih kriptografskih parametara isključivo zavisi od kvaliteta hardverskog generatora slučajnih brojeva na HSM uređajima.

Ispunjenost zahteva za generisanje i proveru kvaliteta parametara ključeva obezbeđuje se korišćenjem sertifikovanih HSM modula, bezbednih kriptografskih uređaja prema odgovarajućim normama, kao i strogim pridržavanjem zahteva navedenih u sertifikacionoj dokumentaciji tih uređaja.

6.1.7. Namene ključeva

PKS CA Root i njemu podređena CA tela koriste privatne ključeve samo za potpisivanje sertifikata i pripadajućih CRL. U ekstenziji *Key Usage* imaju postavljene vrednosti *keyCertSign,* odnosno *cRLSign*.

Privatni ključevi OCSP servisa namenjeni su samo za potpisivanje odgovora PKSCA OCSP servisa. U ekstenziji *Key Usage* imaju postavljene vrednosti *keySignature i nonRepudiation,* a

u ekstenziji *extKeyUsage* postavljenu vrednost *OCSPSigning*.

Sertifikat za servis izdavanja kvalifikovanih vremenskih žigova u ekstenziji *Key Usage* ima postavljene vrednosti *digitalSignature* i *nonRepudiation,* a u ekstenziji *extKeyUsage* postavljenu vrednost *timeStamping*. Privatni ključ servisa za izdavanje kvalifikovanih vremenskih žigova se upotrebljava samo za potpisivanje kvalifikovanih vremenskih žigova.

Namene privatnih ključeva krajnjih korisnika opisane su u CPS dokumentima odgovarajućih usluga od poverenja.

6.2. Zaštita privatnog ključa i kontrola hardverskog kriptografskog modula

PKSCA koristi odgovarajuće kriptografske uređaje za upravljanje životnim ciklusom kriptografskih ključeva sertifikacionog tela. Sertifikaciono telo koristi hardverski bezbednosni modul – HSM koji je usaglašen sa svim relevantnim standardima zaštite kriptografskih uređaja predviđenim Zakonom.

Način zaštite, upravljanje životnim ciklusom i kontrola hardverskog kriptografskog modula za korisničke privatne ključeve koji se koriste za uslugu upravljanja kvalifikovanim sredstvom za generisanje elektronskog potpisa, osnosno pečata su opisani u odgovarajućem CPS dokumentu.

6.2.1. Standardi i tehničke mere zaštite kriptografskog modula

Privatni ključevi korenskog i podređenih CA tela se generišu i štite HSM modulima koji zadovoljavaju zahteve standarda predviđenih Zakonom i Pravilnikom o uslovima koje mora da ispunjava kvalifikovano sredstvo za kreiranje elektronskog potpisa, odnosno pečata i uslovima koje mora da ispunjava imenovano telo (Sl. glasnik RS br 34/2018, 3/2020, 87/2020). Ispunjenje ovih standarda garantuje, između ostalog, nemogućnost nedetektovanog narušavanja integriteta uređaja ili kriptografske memorije.

HSM uređaji ne smeju da napuštaju bezbednosnu zonu sertifikacionog tela, izuzev u unapred definisanim slučajevima premeštanja ili preseljenja, o kojima sertifikaciono telo vodi evidenciju.

U slučaju da je neophodna servisna ili havarijska intervencija na HSM-u, a ona se ne može izvršiti unutar bezbedne zone sertifikacionog tela, HSM se transportuje do ovlašćenog servisa proizvođača uz poštovanje svih neophodnih bezbednosnih mera.

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

Upravljanje privatnim ključem od strane više osoba je bezbednosna mera koja za generisanje i upotrebu privatnog ključa zahteva autorizaciju više osoba.

HSM moduli kojima se štite privatni ključevi svih PKSCA CA smešteni su u prostoru najvišeg nivoa bezbednosti unutar PKSCA zaštićenog prostora. Fizički pristup HSM modulima sprovodi se uz dvostruku kontrolu ovlašćenih osoba sa poverljivim ulogama/dužnostima u PKSCA.

Prilikom generisanja ili upotrebe kriptografskog ključa sertifikacionog tela potrebno je da minimalno dve osobe sa poverljivim ulogama/dužnostima autorizuju generisanje ili upotrebu privatnog ključa. Autorizacija se vrši aktivacijom HSM slota na kojem se generiše i čuva privatni ključ. Slot ostaje aktiviran sve dok se eksplicitno ne deaktivira, ugasi HSM uređaj ili se završi sa radom na aplikaciji sertifikacionog tela.

Privatni ključ sertifikacionog tela se koristi pod uslovima definisanim u okviru ***k*** od ***n*** kontrole od strane više zaposlenih sa poverljivim ulogama/dužnostima.

Nosilac aktivacionih parametara može primiti aktivacione parametre na fizičkom medijumu, kao što je određeni tip hardverskog kriptografskog modula (na primer smart kartica), odobrenom za korišćenje od strane sertifikacionog tela. Sertifikaciono telo čuva zapise u vezi distribucije deljene tajne.

Nosilac aktivacionih podataka mora lično da se upozna sa kreiranjem, zamenom i upotrebom aktivacionih parametara (upotreba PIN-a, korisničkog naloga i pripadajuće lozinke, upotreba smart kartice i pripadajućeg PIN-a), pre nego što prihvati podatke.

Sertifikaciono telo koristi deljene tajne za aktivaciju svog privatnog ključa i ima mogućnost da izmeni način distribucije smart kartica u slučaju da nosioci smart kartice zahtevaju da budu zamenjeni u njihovim rolama.

6.2.3. Bezbedno skladištenje privatnog ključa

Bezbedno skladištenje privatnih ključeva PKSCA CA tela se ne primenjuje.

6.2.4. Bezbednosno kopiranje privatnog ključa

Bezbednosno kopiranje privatnih ključeva svih PKSCA CA sprovodi se u zoni najvišeg nivoa bezbednosti unutar PKSCA zaštićenog prostora, uz višestruku kontrolu ovlašćenih osoba sa poverljivim ulogama/dužnostima u PKSCA.

Hardverske i softverske mehanizme koji štite privatne ključeve obezbeđuje bezbedni kriptografski uređaj. Mehanizmi zaštite privatnog ključa sertifikacionog tela su minimalno ekvivalentne snage kao i sami privatni ključevi koji se štite, a po specifikaciji proizvođača bezbednog kriptografskog modula.

Sertifikaciono telo vrši pravljenje rezervne kopije privatnog ključa u skladu sa procedurom definisanom pratećom dokumentacijom HSM proizvođača, što je definisano Internim pravilima rada.

Kopije privatnog ključa sertifikacionog tela se čuvaju na eksternoj memoriji (flash memorija, CD, ...), na sigurnom mestu, u šifrovanom obliku i u dva primerka. Privatni PKSCA CA ključ se izvan HSM modula nalazi isključivo u šifrovanom obliku i u tom obliku se kopira i čuva u zoni najvišeg nivoa bezbednosti unutar PKSCA zaštićenih prostora na odvojenim lokacijama.

Fizički pristup bezbednosnim kopijama privatnih ključeva PKSCA CA imaju isključivo ovlašćene osobe sa poverljivim ulogama/dužnostima u PKSCA.

6.2.5. Arhiviranje privatnog ključa

PKSCA ne vrši arhiviranje privatnih ključeva.

6.2.6. Prenos privatnog ključa

Kada se nalazi izvan HSM-a, privatni ključ je kriptografski zaštićen na način koji obezbeđuje ekvivalentan nivo bezbednosti kao i kada se nalazi u HSM-u. Prenos privatnog ključa iz HSM-a autorizuju ovlašćene osobe sa poverljivim ulogama/dužnostima u PKSCA, uz višestruku kontrolu unutar bezbednog prostora PKSCA.

Kod prenosa privatnih ključeva iz jednog HSM u drugi, privatni ključ se prenosi samo u HSM jednakog ili višeg nivoa bezbednosti.

Procedura bezbednog eksportovanja privatnog ključa sertifikacionog tela u cilju pravljenja rezervne kopije, kao i procedura bezbednog importovanja kopije privatnog ključa na HSM su definisane u Internim pravilima rada i dokumentaciji proizvođača HSM-a.

6.2.7. Čuvanje privatnog ključa u kriptografskom modulu

Privatni ključevi svih PKSCA CA nalaze se u HSM-u i čuvaju se u šifrovanom obliku u memoriji HSM uređaja.

6.2.8. Metoda aktivacije privatnog ključa

Aktivacija privatnih ključeva svih PKSCA CA tela sprovodi se prema postupcima i uz zadovoljenje zahteva određenih u sertifikacionom dokumentu upotrebljenog HSM-a kojim je privatni ključ zaštićen, uz višestruku kontrolu od strane ovlašćenih osoba sa poverljivim ulogama/dužnostima u PKSCA. Privatni ključ je aktivan sve dok se ne deaktivira.

6.2.9. Metoda deaktivacije privatnog ključa

Deaktivacija privatnog ključa svih PKSCA CA tela sprovodi se gašenjem ili restartom aplikacije sertifikacionog tela, gašenjem ili restartom HSM uređaja ili deaktivacijom privatnog ključa putem logoff mehanizma.

Deaktivirani privatni ključevi mogu se ponovno koristiti tek nakon ponovne aktivacije.

6.2.10. Metoda uništavanja privatnog ključa

Postupak uništavanja privatnog PKSCA CA ključa sprovodi se nakon isteka perioda važenja privatnog ključa, zbog kompromitovanja ili sumnje u kompromitovanost privatnog ključa, ili zbog prestanka njegovog korišćenja, a izvodi se od strane ovlašćenih osoba sa poverljivim ulogama/dužnostima u PKSCA uz minimalno dvostruku kontrolu. Postupak uništavanja privatnog PKSCA CA ključa uključuje i uništavanje svih sigurnosnih kopija tog privatnog ključa.

Uništavanje privatnog PKSCA CA ključa sprovodi se na način određen internim PKSCA dokumentima, a koji garantuje da se nakon uništenja privatni ključ ni na koji način ne može oporaviti ili ponovno koristiti.

O uništenju privatnog PKSCA CA ključa vodi se zapisnik.

6.2.11. Ocena nivoa bezbednosti kriptografskog modula

PKS CA Root i njemu podređena CA tela poseduju HSM koji u svemu odgovara zahtevima opisanim u tački 6.2.1 ovog dolumenta.

6.3. Ostali aspekti upravljanja parom ključeva

6.3.1. Arhiviranje javnog ključa

Javni ključevi svih PKSCA CA sastavni su deo pripadajućih CA sertifikata koji se arhiviraju u skladu sa internim pravilima PKSCA.

6.3.2. Vremenski period važenja sertifikata i korišćenja para ključeva

Rok važenja sertifikata po vrstama je definisan u Tabeli 4.

Sertifikat	Rok važenja sertifikata	Rok važenja para ključeva
Sertifikat PKS CA Root	20 godina	20 godina
Sertifikati podređenih CA tela	20 godina	20 godina
Sertifikat za OCSP servis	5 godina	5 godina
Sertifikat za TSA servis	5 godina	1 godina
Sertifikat za servis validacije	5 godina	5 godina

Sertifikat	Rok važenja sertifikata	Rok važenja para ključeva
Sertifikat za kvalifikovani elektronski potpis	5 godina	5 godina
Sertifikat za kvalifikovani elektronski pečat	5 godina	5 godina

Tabela 4. - Rokovi važenja sertifikata

Period važenja PKSCA CA sertifikata ne sme biti izvan perioda važenja PKSCA Root CA sertifikata.

Vremenski period važenja privatnog ključa jednak je vremenskom periodu važenja pripadajućeg sertifikata.

Privatni ključevi ne smeju se upotrebljavati nakon isteka perioda važenja pripadajućih 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 povezani sa privatnim ključevima za sva PKSCA CA tela, OCSP i TSA servise generišu se i instaliraju prilikom sprovođenja formalne procedure uspostavljanja ovih CA tela.

Aktivacioni podaci se instaliraju na pripadajuće upravljačke kartice HSM uređaja, neophodne za aktivaciju slotova HSM-a na kojima su smešteni odgovarajući privatni ključevi, po pricipu k od n, u skladu sa tačkom 6.2.2.

Podaci za upravljačke kartice HSM-a generišu se u bezbednom prostoru PKSCA od strane osoba sa poverljivim ulogama/dužnostima.

Generisanje i instalacija aktivacionih podataka za druge usluge od poverenja definisano je u CPS dokumentu konkretne usluge od poverenja.

6.4.2. Zaštita aktivacionih podataka

Aktivacioni podaci povezani sa privatnim ključem svih PKSCA CA tela, OCSP i TSA servisa čuvaju se na bezbedan način, na odgovarajućim karticama HSM-a, zaštićeni odgovarajućim lozinkama. Lozinke se generišu u bezbednom prostoru PKSCA od strane osoba sa poverljivim ulogama/dužnostima. Upravljačke kartice HSM-a se dodeljuju ovlašćenim licima sa poverljivim ulogama/dužnostima PKSCA.

Aktivacioni podaci ne smeju se čuvati zajedno sa sigurnim kriptografskim uređajem na koji se odnose. Upravljačke kartice i pripadajuće lozinke smeštaju se u zasebne koverte i čuvaju se na dve lokacije.

6.4.3. Ostale odredbe o aktivacionim podacima

Nema odredaba.

6.5. Upravljanje informacionom bezbednošću

6.5.1. Posebni tehnički zahtevi za informacionu bezbednost

Pristup IT Sistemu i aplikacijama u PKSCA imaju isključivo ovlašćene osobe nakon autentikacije.

Za sve korisničke naloge koji mogu direktno pokrenuti izdavanje sertifikata neophodna je dvofaktorska autentikacija.

Izmena i objava statusa opozvanosti sertifikata sprovodi se uz dvofaktorsku autentikaciju i obveznu kontrolu pristupa.

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

6.6. Bezbednosne mere tokom životnog ciklusa

6.6.1. Bezbednosne mere u razvoju sistema

Analiza bezbednosnih zahteva se sprovodi u fazi dizajna i specifikacije bilo kog projekta razvoja PKSCA sistema, kako bi se omogućilo da neophodan nivo bezbednosti bude ugrađen u sve zastupljene informacione tehnologije.

Softver koji se koristi za pružanje usluge od poverenja potiče iz pouzdanog izvora. Nove verzije softvera testiraju se u testnom okruženju. Implementacija softvera u produkciju sprovodi se u skladu sa dokumentovanim postupcima upravljanja izmenama na IT sistemima i aplikacijama.

Prilikom nabavke opreme i razvoja softvera od spoljnog izvođača, PKSCA ugovorom sa dobavljačem osigurava bezbednosne principe daljeg razvoja sistema.

6.6.2. Upravljanje bezbednošću

PKSCA vrši proveru svih delova sistema usluga u PKSCA produkcionoj hijerarhiji zasnovanoj na PKSCA Root CA u odnosu na bezbednost, pouzdanost i kvalitet, a u skladu sa važećim propisima.

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

uticati.

6.6.3. Bezbednosne procene tokom životnog ciklusa

PKSCA prati raspoložive kapacitete sistema usluga i procenjuje zadovoljenje kapaciteta za buduće potrebe sistema, kako bi se pravovremeno planiralo njihovo proširenje.

Integritet sistema usluga štiti se antivirusnom zaštitom i upotrebom autorizovanog softvera.

PKSCA sprovodi upravljanje izmenama na IT sistemima i aplikacijama kako bi se promene izvodile iz opravdanog razloga, na kontrolisan i formalizovan način.

6.7. Bezbednost računarske mreže

Bezbednost računarske mreže sistema PKSCA zasnovana je na konceptu segmentiranja mreže na mrežne zone različitih nivoa. Mrežne zone štite se se bezbednosnim mehanizmima koji propuštaju samo neophodan mrežni saobraćaj. Na sve delove sistema locirane unutar jedne mrežne zone primenjuju se iste bezbednosne mere.

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

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

Mrežne komponente PKSCA sistema čuvaju se u fizički i logički sigurnom okruženja i usklađenost njihove konfiguracije periodično se proverava.

Svi delovi sistema kritični za pružanje usluga od poverenja smešteni su u zaštićenom prostoru PKSCA. Sistemi sertifikacionih tela posebno su bezbednosno podešeni i osigurani.

6.8. Upotrebe vremenskog žiga

Vremenski žig se ne upotrebljava u okviru rada korenskog i njemu podređenih sertifikacionih tela.

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

7. SADRŽAJ SERTIFIKATA, LISTA OPOZVANIH SERTIFIKATA I OCSP PROFILI

7.1. Profil sertifikata

Profili sertifikata iz opsega ovog dokumenta koje izdaju podređena PKSCA CA usklađeni su sa standardima ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3 i ETSI EN 319 412-4, kao i sa normativnim dokumentima ETSI TS 119 495 i ETSI TS 119 412-1.

Podređena PKSCA CA izdaju sertifikate prema profilima koji su određeni ovim dokumentom. U zavisnosti od namene sertifikata, pravila prema kojima je sertifikat izdat, nivoa bezbednosti i načina čuvanja pripadajućih privatnih ključeva, svaki tip sertifikata ima definisan OID.

7.1.1. Verzija sertifikata

PKSCA sertifikaciona tela izdaju sertifikate koji su usklađeni sa X.509 specifikacijom, verzija 3. Koriste se sledeća X.509 osnovna polja:

X.509 naziv polja	Opis
signature	Kvalifikovani elektronski potpis kvalifikovanog elektronskog sertifikata privatnim kriptografskim ključem aplikacije CA tela. Algoritam potpisa je RSA-SHA256.
issuer	Jedinstveno ime sertifikacionog tela
Valid From	Datum i vreme početka važnosti kvalifikovanog elektronskog sertifikata
Valid To	Datum i vreme prestanka važnosti kvalifikovanog elektronskog sertifikata.
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 5. – X.509 osnovna polja sertifikata

7.1.2. Ekstenzije sertifikata

Koriste se sledeće ekstenzije sertifikata:

Naziv polja ekstenzije	Opis polja ekstenzije
Authority Key Identifier	Identifikator javnog kriptografskog ključa sertifikacionog tela koji se računa kao RSA-SHA256 hash polja *Subject Public Key* Info sertifikata sertifikacionog tijela.

Naziv polja ekstenzije	Opis polja ekstenzije
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 (*keyUsage*) javnog kriptografskog ključa korisnika kvalifikovanog elektronskog sertifikata kao što je navedeno u 6.1.7. Polje je u svim certifikatima označeno kao kritično.
Extended Key Usage	Proširena namena (*ExtendedKeyUsage*) javnog kriptografskog ključa korisnika kvalifikovanog elektronskog certifikata kao što je navedeno u 6.1.7. Polje je u sertifikatima za uslugu elektronskog vremenskog žiga označeno kao kritično.
Certificate Policies	Identifikacija politike sertifikacije i adrese Web strane na kojoj se nalazi.
Issuer Alternative Name	Alternativno ime sertifikacionog tela koje sadrži naziv, poreski identifikacioni broj i oznaku države u kojoj je davalac usluga registrovan.
Subject Alternative Name	Alternativno ime korisnika kvalifikovanog elektronskog sertifikata. U ovom polju može da se navede adresa elektronske pošte korisnika sertifikata, ako je adresa elektronske pošte navedena u zahtevu za izdavanje sertifikata.
CRL Distribution Points	Lokacija na kojoj se nalaze liste opozvanih certifikata.
Qualified Certificate Statements	Oznaka da je sertifikat izdat kao kvalifikovani elektronski sertifikat (*OID*: 1.3.6.1.5.5.7.1.3), koja sadrži oznake u skladu sa tehničkim standardom ETSI EN 319 412-5.
Authority Information Access (authorityInfoAccess)	Informacije o lokaciji na kojoj je dostupan sertifikat na kome se zasniva kvalifikovani elektronski potpis sertifikacionog tela (polje id-ad-calssuers).

Tabela 6. – Ekstenzije sertifikata

Detaljan opis profila sertifikata PKSCA nalazi se u dokumentu „Pregled profila sertifikata PKSCA“. Dokument je dostupan na internet adresi: https://v3.pksca.rs.

7.1.3. Identifikator objekta (OID) algoritama

Algoritmi sa pripadajućim OID identifikatorima za sve sertifikate koje izdaje PKSCA sistem prikazani su u sledećoj tabeli:

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 7. - Algoritmi sa pripadajućim OID identifikatorima

7.1.4. Forme naziva

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

7.1.5. Ograničenja u nazivima

Specijalni znaci čije korišćenje u imenima nije dozvoljeno su: ? (upitnik), \ (backslash), / (slash), # (taraba), $ (dolar), % (procenat), = (jednako), + (plus), | (uspravna crta), ; (tačka-zarez), < (manje), > (veće) i , (zarez). Pomenute znake je potrebno izostaviti ili zameniti drugim znacima.

Ekstenzija *Name Constraints* se ne koristi.

7.1.6. Identifikator objekta (OID) Politike pružanja kvalifikovanih usluga od poverenja

Ekstenzija *Certificate Policies* sertifikata sadrži odgovarajući OID Politike pružanja kvalifikovanih usluga od poverenja.

7.1.7. Upotrebe ekstenzije *Policy Constraints*

Ekstenzija *Policy Constraints* se ne koristi.

7.1.8. Sintaksa i semantika kvalifikatora politika

Kvalifikator politika sertifikacije u ekstenziji Certificate Policies sadrži link u URI formatu koji sadrži internet adresu ovog dokumenta. Dokument se nalazi na naznačenoj lokaciji obavezno u verziji na srpskom jeziku, a može biti preveden na engleski jezik.

7.1.9. Procesuiranje semantike za kritičnu ekstenziju CP

Klijentske aplikacije moraju procesuirati ekstenzije označene kao kritične u saglasnosti sa RFC 3280.

7.2. Profil CRL

Profil CRL koje izdaju PKSCA Catelu je usklađen sa dokumentom IETF RFC 5280.

7.2.1. Broj(evi) verzije

CRL su usklađene sa X.509 specifikacijom, verzijom 2.

7.2.2. CRL i ekstenzije unosa u CRL

Ekstenzije CRL koje se koriste u CRL listama i u elementima unosa CRL lista definisane su u skladu sa standardom RFC5280.

Ekstenzije CRL koje se koriste u CRL listama i u elementima unosa CRL lista koje izdaju PKSCA CA tela definisane su u sledećoj tabeli:

Ekstenzije	Kritično	Vrednost
crlExtensions		
cRLNumber	NE	Jednolično rastući serijski broj CRL dužine do 20 okteta.
AuthorityKeyIdentifier	NE	SHA-1 hash vrednost dužine 160 bita
crlEntryExtensions		
reasonCode	NE	Kod razloga opoziva sertifikata

Tabela 8. - Ekstenzije CRL liste i elemenata unosa CRL listi koje izdaju PKSCA CA tela

7.3. OCSP profil

Profil odgovora PKSCA OCSP servisa usklađen je sa dokumentom IETF RFC 6960.

7.3.1. Broj(evi) verzije

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

7.3.2. OCSP ekstenzije

U odgovor PKSCA OCSP servisa uključene su sledeće ekstenzije:

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

Tabela 9. – Ekstenzije uključene u odgovor OCSP servisa

8. PROVERA USAGLAŠENOSTI POLITIKE SERTIFIKACIJE

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

Provera usaglašenosti obavlja se u cilju potvrđivanja da PKSCA kao kvalifikovani pružalac usluga od poverenja koje PKSCA pruža, ispunjavaju zahteve utvrđene Zakonom o elektronskoj identifikaciji, elektronskom dokumentu i uslugama od poverenja u elektronskom poslovanju, Uredbom EU br. 910/2014 i standardom ETSI EN 319 411-2.

8.1. Učestalost ili okolnosti ocene usaglašenosti

Provere usaglašenosti rada PKSCA mogu biti interne i eksterne.

Interne i eksterne provere usaglašenosti rada PKSCA sprovode se i kod spoljnih ugovorenih RA.

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.

8.1.2. Interna Provera usaglašenosti

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

8.2. Identitet/kvalifikacije ocenjivača

Eksternu proveru usaglašenosti sprovodi Telo za ocenjivanje usaglašenosti. Osposobljenost Tela za ocenjivanje usaglašenosti i osposobljenost pripadajućih ocenjivača 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 ETSI EN 319 411-2,
- PKI područja i područja informacione bezbednosti,
- zakonske regulative iz područja pružanja usluga od poverenja.

8.3. Odnos ocenjivača sa predmetom ocenjivanja usaglašenosti

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

Interni ocenjivači usaglašenosti ne ocjenjuju u domenu sopstvenog delokruga odgovornosti.

8.4. Predmeti 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 u slučaju neusaglašenosti

Ukoliko je u pružanju kvalifikovane usluge od poverenja utvrđena neusaglašenost, PKSCA će preduzeti potrebne korake kako bi otklonila neusaglašenost, 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 poverljive su 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 one se ne objavljuju.

9. OSTALE POSLOVNE I PRAVNE ODREDBE

9.1. Naknade za usluge

PKSCA obaveštava korisnike i treće strane kao korisnike usluga od poverenja o svim uslugama koje se naplaćuju. Ukoliko posebnim ugovorom nije drugačije određeno, usluge se naplaćuju u skladu sa cenovnikom PKSCA. Cenovnik svih usluga koje se naplaćuju objavljen je na internet stranicama pružaoca usluga od poverenja.

PKSCA zadržava pravo izmene cenovnika. Izmene cenovnika objavljuju se na internet stranicama pružaoca usluga od poverenja.

9.1.1. Naknade za pružanje usluga od poverenja

PKSCA u skladu sa objavljenim cenovnikom naplaćuje naknadu za sve usluge od poverenja koje korisnicima pruža.

9.1.2. Naknade za pristup sertifikatu

PKSCA ne naplaćuje naknadu za pristup sertifikatima.

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

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

Sertifikaciono telo ne naplaćuje uslugu opoziva sertifikata.

9.1.4. Naknade za ostale usluge

PKSCA može odrediti i naplaćivati naknade i za ostale usluge, kao što su: registracija pravnog lica ili korisnika, promena podataka u sertifikatu, isporuka sertifikata i opreme na lokaciju korisnika i slično.

Za pristup ovom dokumentu i CPS dokumentima naknade se ne naplaćuju.

9.1.5. Povratak uplaćenih sredstava

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

9.2. Finansijska odgovornost

PKSCA kao kvalifikovani pružalac 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 kvalifikovani pružalac 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, udar groma, pada ili udar letilice, demonstracija, osiguranje opreme, električne opreme, elektronskih i komunikacijskih uređaja, instalacija i slično.

9.2.2. Ostala sredstva

Nije primenljivo.

9.3. Poverljivost poslovnih podataka

9.3.1. Opseg poverljivih poslovnih podataka

Poverljivi poslovni podaci su svi podaci, u bilo kom obliku, koje na bilo koji način između sebe razmene učesnici u uspostavi i pružanju usluga 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. Podaci koji se ne smatraju poverljivim poslovnim podacima

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 poslovnih podataka

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 propisima koji uređuju zaštitu tajnih podataka.

9.4. Zaštita ličnih podataka

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

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 ličnih podataka

PKSCA sprovodi politiku zaštite ličnih podataka u skladu sa zakonskom regulativom, kojom se utvrđuju načela obrade ličnih podataka fizičkih osoba 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 stručnim znanjem, pouzdanošću, resursima, poštivanjem propisanih tehničkih, organizacionih i sigurnosnih 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 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 lični podaci

U postupku registracije korisnika i nakon toga, PKSCA je ovlašćeno za prikupljanje ličnih podataka koji su potrebni za valjano 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 propisno štiti.

9.4.3. Lični podaci 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 suglasnost za objavu sertifikata u javnom imeniku.

9.4.4. Odgovornost za zaštitu ličnih podataka

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

9.4.5. Ovlašćenje za korišćenje ličnih podataka

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 nadležnim telima

PKSCA neće činiti 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.

9.5. Prava intelektualnog vlasništva

Ovaj dokument, kao i druga dokumentacija PKSCA objavljena na internet stranicama pružaoca usluge od poverenja, je 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, odnosno autor pečata, bez obzira na način na koji je privatni ključ zaštićen.

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

9.6. Obveze i odgovornosti

9.6.1. Obveze i odgovornosti CA

PKSCA je odgovorno za usklađenost svojih pravila sa zakonskom regulativom i za sprovođenje odredbi propisanih ovim dokumentom, CPS dokumentima, Uslovima pružanja usluga od poverenja i sa obavezama u ugovoru o obavljanju usluga od poverenja sklopljenim sa korisnikom.

PKSCA na svojim internet stranicama objavljuje uslove pružanja usluga sertifikovanja, ovaj dokument, CPS dokumente 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 odgovoran 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 politike informacione bezbednosti i odredbama ovog dokumenta, 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 obvezama i odgovornostima, PKSCA:

- primenjuje odredbe važećih propisa pri pružanju usluge sertifikovanja,
- 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 i dostave privatnog ključa i pripadajućih aktivacionih podataka potpisniku, odnosno ovlašćenom predstavniku, za sertifikate koji se izdaju na sigurnim kriptografskim uređajima,
- upravlja privatnim korisničkim ključevima u ime potpisnika, odnosno autora pečata na način da potpisnik/pečatilac ima pripadajući privatni ključ pod svojom isključivom kontrolom, za usluge upravljanja kvalifikovanim sredstvom za generisanje elektronskog potpisa/pečata,
- obezbeđuje odgovarajući sigurni kriptografski uređaj i njegovu bezbednu dostavu potpisniku, odnosno ovlašćenom predstavniku,
- 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,
- 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. Obveze 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 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,
- osiguravanje 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, odnosno elektronskog pečata 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, odnosno elektronskog pečata, privatnog ključa i aktivacionih podataka,
- da dostavi u RA sve potrebne podatke i informacije o promenama koje utiču ili mogu uticati na tačnost elektronskog potpisa, odnosno elektronskog pečata 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, 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.

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

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

Korisniku koji ne postupa u skladu s preuzetim obavezama može biti opozvana 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 kao korisnika usluga od poverenja

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, odnosno elektronski pečat izrađen privatnim ključem koji odgovara javnom ključu u sertifikatu za vreme perioda važenja sertifikata.

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

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

9.6.5. Obveze i odgovornosti ostalih učesnika

Nema odredbi.

9.7. Odricanje od odgovornosti

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

- kada je šteta nastala zbog neautorizovane upotrebe korisničkih usluga od poverenja,
- kad je šteta nastala upotrebom usluga 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 i treće strane kao korisnika usluga od poverenja,
- kad je šteta nastala kao rezultat davanja podataka i predstavljanja pravnog lica ili fizičkog lica tokom procesa identifikacije i potvrde identiteta, ako je identifikaciju i proveru podataka RA mreža sprovodila u skladu sa zahtevima iz ovog dokumenta i radnim uputstvima.

9.8. Ograničenja odgovornosti

Ukupna finansijska odgovornost za sertifikate izdate prema ovom dokumetu i za transakcije obavljene na osnovu usluga od poverenja iznosi najviše 2.000.000,00 RSD.

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

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

Tabela 10. - Maksimalna odgovornost PKSCA

9.9. Naknada štete

Svaki učesnik u PKI sistemu PKSCA 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, kao i autor pečata, 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

9.10.1. Trajanje

Ovaj CP dokument važi do stupanja na snagu novog CP dokumenta ili do objave prestanka njegovog važenja. Nova verzija CP dokumenta ili objava prestanka važenja biće objavljena na internet stranici PKSCA sa naznačenim danom stupanja na snagu. Novom CP dokumentu biće dodeljena nova verzija i u novom OID će biti naznačene obavljene izmene.

9.10.2. Prestanak važenja

Stupanjem na snagu nove verzije CP dokumenta za sve usluge definisane prema ovom dokumentu ostaju da važe one odredbe iz ovog dokumenta koje se ne mogu smisleno zameniti odredbama nove verzije CP dokumenta.

Prestanak važenja ovog CP 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 CP dokumenta, na sve usluge definisane od tog dana se primenjuju odredbe iz tog dokumenta.

Usluge definisane primenom prethodnog CP dokumenta važe do njihovog isteka pri čemu se mogu obnoviti primenom pravila iz novog CP dokumenta.

9.11. Individualna obaveštenja i komunikacija sa korisnicima

Individualna komunikacija sa korisnicima primarno se sprovodi preko PKSCA on line HelpDesk sistema na adresi:

http://helpdesk.pksca.rs/

Individualna obaveštenja i druga službena komunikacija u pisanom obliku sprovodi se 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

9.12.1. Procedure izmena i dopuna

Ovaj CP dokument revidira se po potrebi.

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 dopuna ili izmena ovog dokumenta. U dopisu se navode kontakt podaci osobe koja je poslala predlog promene. PKSCA može prihvatiti, prilagoditi ili odbiti predložene promene nakon razmatranja istih.

9.12.2. Mehanizmi obaveštavanja i vremenski periodi

Sve izmene i dopune CP dokumenta objavljuju se u elektronskom obliku na internet stranicama PKSCA.

Nove verzije CP dokumenta sa izmenjenim OID-om dokumenta objavljuju se u elektronskom obliku na internet stranicama PKSCA.

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

9.12.3. Okolnosti pod kojima se mora menjati OID

Veće izmene u CP dokumentu, koje mogu uticati na korisnike zahtevaju i izmenu OID-a ovog dokumenta. Novi OID za novu verziju dokumenta određuje PKSCA.

9.13. Postupak rešavanja sporova

U slučaju spora ili neslaganja između PKSCA i drugih učesnika povodom radnji i/ili postupaka pružanja usluga od poverenja uređenih ovim CP dokumentom, isti 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 pisano u papirnom obliku na adrese navedene u ovom dokumentu.

9.14. Važeći propisi

Kvalifikovane usluge od poverenja iz opsega ovih CP dokumenta PKSCA pruža u skladu sa Zakonom o elektronskoj identifikaciji, elektronkom dokumentu i uslugama od poverenja u elektronskom poslovanju, Odredbom Evropske komisije (EU) br. 910/2014, kao i dokumenatima standarda ETSI EN 319 401, ETSI EN 319 411-1 i ETSI EN 319 411-2.

9.15. Usklađenost sa primenjivim propisima

Ovaj CP dokument i pružanje usluga od poverenja, koje su obuhvaćene ovim CP dokumentom usklađeni su sa propisima.

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

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 Class1 i PKS CA Cloud CA izdaju 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 CP dokument, CPS dokumente i uslove pružanja usluga od poverenja.

Pre sklapanja ugovora o obavljanju usluga od poverenja, korisnici se informišu o uslovima pružanja tih usluga od poverenja. 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 potpisnika, odnosno autora pečata i, ukoliko je moguće, pravno lice o eventualnim izmenama uslova o pružanju usluga od poverenja.

PRIVREDNA KOMORA SRBIJE

mr Dušan Berdić

Sertifikaciono telo

10. Istorija dokumenata

Verzija	Datum	Opis	Autor
3.0.	18.10.2020.	Radna verzija	Dušan Berdić
3.1.	21.06.2021.	Izmene i dopune	Dušan Berdić

11. Odobrenje dokumenata

Ime i prezime	Radno mesto	Potpis	Datum
Dušan Berdić	Rukovodilac CA		21.06.2021.