Sertifikaciono telo
Privredne komore Srbije

Politika sertifikacije
Kvalifikovani elektronski sertifikati

Sertifikati koji se izdaju u okviru ove Politike sertifikacije:

Kvalifikovani sertifikati

OID Politike (1.3.6.1.4.1.31266.1.1.3)

– verzija 2.0.2 –

Beograd, mart 2015.

Sadržaj

1. Uvod i pregled osnovnih pretpostavki 1

1.1. Pregled osnovnih pretpostavki 1

1.2. Ime dokumenta i identifikacija 3

1.3. Učesnici u PKI sistemu PKS 3

1.3.1. PKS CA 3

1.3.2. Registraciona tela PKS CA 4

1.3.3. Korisnici 5

1.3.4. Treće strane 5

1.3.5. Drugi učesnici 5

1.4. Korišćenje sertifikata izdatih od strane PKS CA 5

1.4.1. Prihvatljivo korišćenje sertifikata 6

1.4.2. Zabranjeno korišćenje sertifikata 6

1.5. Administracija Politike sertifikacije PKS CA 6

1.5.1. Organizacija administriranja Politike sertifikacije 6

1.5.2. Kontakt osoba 6

1.5.3. Osoba koja određuje pogodnost CPS dokumenta 7

1.5.4. Procedura odobravanja CPS dokumenta 7

1.6. Definicije i skraćenice 7

2. Odgovornosti za publikovanje i repozitorijume 12

2.1. Repozitorijumi 12

2.2. Publikovanje informacija o sertifikatima 12

2.3. Vreme i frekvencija publikovanja 12

2.4. Kontrole pristupa repozitorijumima 13

3. Identifikacija i autentikacija korisnika 13

3.1. Nazivi 13

3.2. Inicijalna provera identiteta 14

3.2.1. Autentikacija identiteta organizacije 14

3.2.2. Autentikacija identiteta pojedinca 14

3.3. Identifikacija i autentikacija zahteva za obnavljanje ključeva ... 15

3.4. Identifikacija i autentikacija zahteva za opoziv sertifikata 15
4. Operativni zahtevi u vezi životnog ciklusa sertifikata.....15
4.1. Aplikacija za dobijanje sertifikata.....15
4.2. Procesiranje aplikacije za dobijanje sertifikata 16
4.3. Izdavanje sertifikata 16
4.4. Prihvatanje sertifikata.....16
4.5. Korišćenje kvalifikovanog sertifikata i asimetričnog para ključa 17
4.6. Obnavljanje sertifikata.....17
4.7. Generisanje novog para ključeva i sertifikata korisnika 17
4.8. Modifikacije sertifikata korisnika.....18
4.9. Suspenzija i opoziv sertifikata 18
4.10. Servisi provere statusa sertifikata 19
4.11. Prestanak korišćenja sertifikata.....19
4.12. Čuvanje i rekonstrukcija privatnog ključa korisnika namenjenog za autentikaciju 19
5. Upravne, operativne i fizičke bezbednosne kontrole.....20
5.1. Fizičke bezbednosne kontrole.....20
5.2. Proceduralne kontrole.....20
5.3. Kadrovske bezbednosne kontrole.....21
5.3.1. Kvalifikacija i iskustvo 21
5.3.2. Procedura provere biografije 21
5.3.3. Zahtevi za obučenošću..... 21
5.3.4. Ponovna obuka..... 22
5.3.5. Rotacija poslova 22
5.3.6. Kaznene mere u odnosu na zaposlene 22
5.3.7. Kontrole nezavisnih ugovarača..... 22
5.3.8. Dokumentacija za inicijalnu obuku i ponovnu obuku 22
5.4. Procedure bezbednosnih provera/auditing.....22
5.5. Arhiviranje zapisa.....23
5.6. Izmena ključeva 23

5.7. Kompromitacija i oporavak u slučaju katastrofe 24
5.8. Završetak rada CA ili RA.....24
6. Tehničke bezbednosne kontrole 24
6.1. Generisanje i instalacija asimetričnog para ključeva 25
6.2. Zaštita privatnog ključa 25
6.3. Drugi aspekti upravljanja parom ključeva 27
6.4. Aktivacioni podaci 27
6.5. Bezbednosne kontrole računara 27
6.6. Mrežne bezbednosne kontrole.....27
6.7. Vremenski pečat 27
7. Profili sertifikata i CRL lista 28
7.1. Profili sertifikata.....28
7.1.1. Opšti profil sertifikata 28
7.1.2. Profil Root CA sertifikata PKS CA 29
7.1.3. Profil Intermediate CA sertifikata PKS CA 29
7.1.4. Profil sertifikata korisnika 29
7.2. Profil CRL liste 30
7.3. OCSP profil.....31
8. Provera saglasnosti sa Politikom sertifikacije 31
9. Drugi poslovni i pravni aspekti.....32
9.1. Cene 32
9.2. Finansijska odgovornost 32
9.3. Poverljivost poslovnih informacija 33
9.4. Privatnost i zaštita personalnih informacija 33
9.5. Prava intelektualnog vlasništva 33
9.6. Predstavljanje i garancije 33
9.7. Nepriznavanje garancije.....33
9.8. Ograničenja odgovornosti 34
9.9. Odštete 34
9.10. Period važnosti i kraj validnosti Politike sertifikacije 34

9.11. Pojedinačna obaveštenja i komunikacija sa učesnicima 34
9.12. Ispravke 34
9.13. Procedure rešavanja sporova 34
9.14. Zakon koji se poštuje 35
9.15. Saglasnost sa primenljivim zakonima 35
9.16. Razne odredbe 35
9.17. Druge odredbe 35
10. Istorija dokumenta.....35
11. Reference.....35
12. Kompanije i organizacije.....36

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

Upravni odbor Privredne komore Srbije, na sednici održanoj 31. marta 2015. godine, donosi

Politiku sertifikacije
Kvalifikovani elektronski sertifikati

1. Uvod i pregled osnovnih pretpostavki

Sertifikaciono telo Privredne komore Srbije (u nastavku: PKS CA) izdaje kvalifikovane elektronske sertifikate tako što formira elektronski potpis sertifikata na osnovu svog privatnog ključa i asimetričnog kriptografskog algoritma. U tako formiranom elektronskom sertifikatu, PKS CA se identifikuje kao izdavač kvalifikovanog elektronskog sertifikata u skladu sa Zakonom o elektronskom potpisu i odgovarajućim podzakonskim aktima.

PKS CA izdaje kvalifikovane elektronske sertifikate korisnika u skladu sa dokumentima ETSI ESI TS 101 862 „Qualified Certificate Profile", RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" i ETSI TS 102 280 „X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons" i sa obaveznim sadržajem definisanim u članu 17. Zakona o elektronskom potpisu (u daljem tekstu - Zakon).

1.1. Pregled osnovnih pretpostavki

PKS CA je odgovorno za pružanje kompletnih usluga sertifikacije, koje uključuju sledeće servise, i to:

- Registraciju korisnika,
- Formiranje asimetričnog para ključeva za korisnike,
- Formiranje kvalifikovanih elektronskih sertifikata,
- Distribuciju privatnog ključa i kvalifikovanih elektronskih sertifikata korisnicima na način propisan Zakonom (SSCD),
- Upravljanje procedurom opoziva kvalifikovanih elektronskih sertifikata i
- Obezbeđivanje statusa opozvanosti kvalifikovanih elektronskih sertifikata.

PKS CA obezbeđuje sredstvo za formiranje kvalifikovanog elektronskog potpisa korisnicima (SSCD) i pridruženi PIN kod za aktivaciju sredstva, kao i njihovu bezbednu distribuciju do korisnika.

PKS CA utvrđuje Opšta pravila pružanja usluge sertifikacije (u daljem tekstu: Opšta pravila) u skladu sa Zakonom koja korisnicima obezbeđuju dovoljno informacija na

osnovu kojih se mogu odlučiti o prihvatanju usluga i o obimu usluga. Opšta pravila sertifikacije PKS CA ugrađuju se u dokumenta:

1. Politika sertifikacije (Certificate Policy) – ovaj dokument;
2. Praktična pravila pružanja usluge Sertifikacije (Certification Practices Statement) (u daljem tekstu: Praktična pravila).

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

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

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

Opšta pravila funkcionisanja PKS CA su u skladu sa dokumentima RFC 3647 „Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework" i ETSI TS 101 456 „Policy Requirements for Certification Authorities Issuing Qualified Certificates".

PKS CA utvrđuje i Posebna interna pravila rada sertifikacionog tela i zaštite sistema sertifikacije (u daljem tekstu: Posebna pravila) u kojima su sadržani i detaljno opisani postupci i mere koji se primenjuju prilikom izdavanja i rukovanja elektronskim sertifikatima i kvalifikovanim elektronskim sertifikatima. Posebna pravila su privatni dokument i predstavljaju poslovnu tajnu sertifikacionog tela.

Posebna interna pravila sadrže detaljne odredbe o:

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

PKS CA je evidentirano i akreditovano od strane Nadležnog organa za poslove akreditacije i supervizije PKI (Public Key Infrastructure) sistema u Srbiji (Ministarstvo za telekomunikacije i informaciono društvo) i biće predmet periodične supervizije u cilju osiguravanja saglasnosti sa zahtevima iz Zakona o elektronskom potpisu i odgovarajućim podzakonskim aktima.

1.2. Ime dokumenta i identifikacija

Ovaj dokument predstavlja Politiku sertifikacije (u daljem tekstu CP – Certificate Policy) PKS CA za sve korisnike.

PKS CA izdaje kvalifikovane elektronske sertifikata za potrebe realizacije funkcija autentikacije i kvalifikovanog elektronskog potpisa.
Identifikacioni podaci PKS CA su:

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

Jedinstveno ime (Dname – issuer):

OU=PKS CA
O=Privredna komora Srbije
C=RS

Ovaj dokument ima jedinstvenu oznaku (OID – Object Identifier):

CP (Certificate Policy)
OID Politike (1.3.6.1.4.1.31266.1.1.3)

1.3. Učesnici u PKI sistemu PKS

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

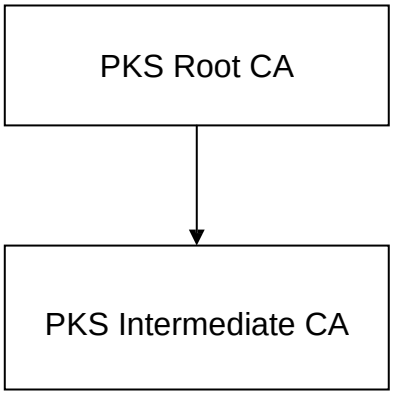
1.3.1. PKS CA

Sertifikaciono telo je organizacija koja izdaje elektronske sertifikate. PKS CA je sertifikaciono telo (CA). PKS CA je odgovorna za publikaciju ove politike sertifikacije u cilju podrške izdavanju određenih tipova elektronskih sertifikata. U tom smislu, ova Politike sertifikacije (CP), kao i pridruženi dokument PKS CA CPS (Certificate Practice Statement), predstavljaju odgovarajuće politike i pravila koja se primenjuju pri izdavanju PKS CA kvalifikovanih elektronskih sertifikata.

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

PKS CA predstavlja hijerarhijsku PKI strukturu za izdavanje elektronskih sertifikata. U pomenutoj arhitekturi (slika 1), postoji:

- PKS Root CA – centralno samopotpisano sertifikaciono telo koje izdaje sertifikate intermediate CA telima i potpisuje CRL listu na root nivou.
- PKS Intermediate CA – sertifikaciono telo koje izdaje kvalifikovane sertifikate:
  - fizičkim licima
  - fizičkim licima koja zastupaju pravna lica



Slika 1: Hijerarhijska struktura PKS PKI sistema

Sva navedena sertifikaciona tela se nalaze i upravljaju na centralnoj lokaciji PKS, a u okviru Centra za informatiku i elektronsko poslovanje PKS.

1.3.2. Registraciona tela PKS CA

Zahtevi za izdavanjem sertifikata za korisnike PKS CA se prikupljaju u regionalnim komorama, kao i u samoj centrali PKS, koje igraju ulogu Registracionih autoriteta (RA – Registration Authority), tj. PKS CA pristupa svojim korisnicima putem mreže registracionih tela (centralno RA i mreža RA).

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

- Prihvataju, analiziraju, potvrđuju ili odbijaju registraciju odgovarajućih korisničkih zahteva za sertifikatima (aplikacije za sertifikate).
- Registruju korisnike za korišćenje PKS CA sertifikacionih usluga.
- Sprovode sve korake u proceduri identifikacije korisnika što je definisano važećim zakonskim dokumentima i Opštim pravilima rada PKS CA.
- Koriste službene i overene dokumente u cilju provere korisnikove aplikacije.

- Nakon potvrde aplikacije korisnika, obaveštavaju PKS CA u cilju izdavanja sertifikata.
- Iniciraju proces opoziva i zahtevaju opoziv sertifikata od strane PKS CA.

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

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.

1.3.3. Korisnici

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

Korisnici su strane koje:

- Apliciraju za dobijanje sertifikata,
- Identifikovani su kao vlasnici sertifikata u samom sertifikatu,
- Poseduju privatni ključ koji matematički odgovara javnom ključu koji je naveden u korisnikovom sertifikatu.

1.3.4. Treće strane

Treće strane su entiteti, kao na primer fizička lica (pojedinci) i/ili pravna lica (kompanije), koja prihvataju sertifikate i verifikuju elektronski potpis određenih elektronskih dokumenata koja su potpisana od strane korisnika PKS CA, kao i koja vrše validaciju sertifikata izdatih od strane PKS CA. Verifikacija digitalnog potpisa se vrši na bazi javnog ključa koji se nalazi u korisnikovom sertifikatu.

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

1.3.5. Drugi učesnici

Ovo poglavlje nije primenljivo u okviru ove CP.

1.4. Korišćenje sertifikata izdatih od strane PKS CA

U ovom poglavlju se definiše korišćenje kvalifikovanih elektronskih sertifikata izdatih od strane PKS CA.

1.4.1. Prihvatljivo korišćenje sertifikata

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

U takve transakcije spadaju:

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

1.4.2. Zabranjeno korišćenje sertifikata

Ovo poglavlje nije primenljivo u okviru ove CP.

1.5. Administracija Politike sertifikacije PKS CA

U ovom poglavlju su opisane aktivnosti u vezi administracije ove CP.

1.5.1. Organizacija administriranja Politike sertifikacije

PKS CA je odgovorno za propisnu 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 tehničkim karkateristikama primenjenih kriptografskih algoritama i dužina ključeva.

1.5.2. Kontakt osoba

Osoba u PKS CA, odgovorna za ovu CP je:

Nebojša Garić
Privredna Komora Srbije
Resavska 13-15
11000 Beograd, Srbija
Tel.: 011 3304 550
Fax: 011 3304 556

Email: nebojsa.garic@pks.rs

1.5.3. Osoba koja određuje pogodnost CPS dokumenta

Ovo poglavlje nije primenljivo u okviru ove CP.

1.5.4. Procedura odobravanja CPS dokumenta

Ovo poglavlje nije primenljivo u okviru ove CP.

1.6. Definicije i skraćenice

U ovom dokumentu pojedini izrazi imaju sledeće značenje:

Aktivacioni podaci – Podaci, koji nisu ključevi, koji su zahtevani u cilju rada kriptografskih modula i koji moraju biti zaštićeni (kao na primer PIN ili passphrase).

CA sertifikat – Sertifikat za dato CA izdat (digitalno potpisan) od strane drugog CA ili samopotpisan (ukoliko se radi o Root CA).

Politika sertifikacije – Imenovan skup pravila koji indicira primenljivost sertifikata na određeno okruženje i/ili na klasu aplikacija sa zajedničkim bezbednosnim zahtevima.

Lanac (put) 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.

Certificate Practice Statement (CPS) – Javna Praktična pravila i procedure koje sertifikaciono telo primenjuje u proceduri izdavanja sertifikata.

Sertifikaciono telo – izdavač sertifikata (issuing CA) – U kontekstu određenog sertifikata, sertifikaciono telo – izdavač sertifikata je ono CA koje je izdalo (digitalno potpisalo) sertifikat.

Kvalifikator politike – Informacija koja zavisi od politike sertifikacije i koja je pridružena identifikatoru politike sertifikacije u okviru X.509 sertifikata. Može da uključi i URL na kome se nalazi publikovan CPS datog sertifikacionog tela.

Registraciono telo (RA) – Entitet koji je odgovoran za identifikaciju i autentikaciju korisnika/vlasnika sertifikata, kao i kreiranje zahteva za izdavanje sertifikata, ali koji ne izdaje i ne potpisuje sertifikat (tj. RA vrši odgovarajuće poslove (identifikaciju korisnika) i u tom smislu je delegirano od CA). Često se i termin LRA (Local Registration Authority) koristi u istom kontekstu.

Treća strana – Primalac sertifikata koji proverava dati sertifikat i/ili proverava digitalni potpis dobijenog elektronskog dokumenta primenom javnog ključa

potpisnika iz sertifikata. Takođe, treća strana proverava validnost sertifikata u istom procesu. Treća strana može biti i korisnik sertifikata izdatog od strane istog sertifikacionog tela ali i ne mora.

Elektronski dokument – dokument u elektronskom obliku koji se koristi u pravnim poslovima i drugim pravnim radnjama, kao i u upravnom, sudskom i drugom postupku pred državnim organom.

Elektronski potpis – skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika.

Kvalifikovani elektronski potpis – Elektronski potpis koji se kreira primenom sredstva za kreiranje kvalifikovanog elektronskog potpisa (SSCD – Secure Signature Creation Device) i koji se proverava putem kvalifikovanog elektronskog sertifikata potpisnika. Ovaj potpis je pravno ekvivalentan svojeručnom potpisu po Zakonu o elektronskom potpisu.

Potpisnik – lice koje poseduje sredstva za elektronsko potpisivanje i vrši elektronsko potpisivanje u svoje ime ili u ime pravnog ili fizičkog lica.

Podaci za formiranje elektronskog potpisa – jedinstveni podaci, kao što su kodovi ili privatni kriptografski ključevi, koje potpisnik koristi za izradu elektronskog potpisa;

Sredstva za formiranje elektronskog potpisa – odgovarajuća tehnička sredstva (softver i hardver) koja se koriste za formiranje elektronskog potpisa, uz korišćenje podataka za formiranje elektronskog potpisa.

Sredstva za formiranje kvalifikovanog elektronskog potpisa – sredstva za formiranje kvalifikovanog elektronskog potpisa koja ispunjavaju dodatne uslove utvrđene Zakonom o elektronskom potpisu.

Podaci za proveru elektronskog potpisa – podaci, kao što su kodovi ili javni kriptografski ključevi, koji se koriste za proveru i overu elektronskog potpisa.

Sredstva za proveru elektronskog potpisa – odgovarajuća tehnička sredstva (softver i hardver) koja služe za proveru elektronskog potpisa, uz korišćenje podataka za proveru elektronskog potpisa.

Sredstva za proveru kvalifikovanog elektronskog potpisa – sredstva za proveru elektronskog potpisa koja ispunjavaju dodatne uslove utvrđene Zakonom o elektronskom potpisu.

Elektronski sertifikat – elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika.

Kvalifikovani elektronski sertifikat – elektronski sertifikat koji je izdat od strane sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata i sadrži podatke predviđene Zakonom o elektronskom potpisu.

Korisnik – pravno lice, preduzetnik, državni organ, organ teritorijalne autonomije, organ lokalne samouprave ili fizičko lice kome se izdaje elektronski sertifikat.

Sertifikaciono telo - pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama Zakona o elektronskom potpisu.

Akreditacija – Formalna deklaracija od strane potvrdnog autoriteta da izvesne funkcije/entiteti zadovoljavaju specifične formalne zahteve.

Aplikacija za sertifikat - Zahtev poslat od strane korisnika koji zahteva sertifikat (aplikant) ka Sertifikacionom telu u cilju izdavanja elektronskog sertifikata.

Arhiva – Specifična baza podataka za čuvanje zapisa za određeni period vremena u cilju bezbednosti, backup-a ili audit-a.

Authentikacija – proces utvrđivanja identiteta pojedinca ili organizacije. U kontekstu PKI sistema, autentikacija se odnosi na dva procesa:

- Utvrđivanje da dato ime pojedinca ili organizacije odgovara realnom identitetu pojedinca ili organizacije
- Utvrđivanje da je pojedinac ili organizacija koji se prijavljuje za određeni servis pod datim imenom u stvari baš taj (pod tim imenom) pojedinac ili organizacija.

Identifikacija – procedura bezbednog logičkog predstavljanja korisnika, tj. utvrđivanja njegovog elektronskog identiteta, odgovarajućoj aplikaciji ili servisu.

Autorizacija – procedura utvrđivanja prava koje neki autentikovani korisnik ima za korišćenje odgovarajuće aplikacije ili servisa.

Ekstenzije u sertifikatu – Dodatna polja u sertifikatu, pored osnovnih, koja daju bliže informacije o vlasniku (korisniku) i izdavaču (CA) sertifikata.

Hijerarhija sertifikata – Sekvenca sertifikata bazirana na nivoima koja ima jedan root CA sertifikat i subordinate/intermediate entitete, kao što su sertifikati drugih CA i korisnici.

Upravljanje sertifikatima – Aktivnosti pridružene upravljanju sertifikatima uključuju generisanje čuvanje, isporuku, objavljivanje i opoziv sertifikata.

Lista opozvanih sertifikata (CRL – Certificate Revocation List) – Lista izdata i elektronski potpisana od strane CA koja uključuje serijske brojeve opozvanih sertifikata, vreme kada je opoziv izvršen i razlog opoziva. Takva lista se mora koristiti od strane trećih strana uvek kada treba proveriti validnost sertifikata i/ili verifikaciju elektronskog potpisa.

Serijski broj sertifikata – Sekvencijalni broj koji jedinstveno identifikuje sertifikat u domenu datog CA.

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

Sertifikacija – Proces izdavanja elektronskog sertifikata.

Asimetrični par ključeva (key pair) – Privatni ključ i javni ključ, kao matematički par koji se koriste za potrebe rada asimetričnog kriptografskog algoritma, kao što je na primer RSA algoritam.

Privatni ključ – Matematički podatak koji se koristi kao ključ za kreiranje elektronskog potpisa i za raspakivanje digitalne envelope - dešifrovanje simetričnog ključa kojim je šifrovan dokument za datog korisnika primenom asimetričnog kriptografskog algoritma.

Javni ključ – Matematički podatak koji može biti javno objavljen (najčešće se objavljuje u formi X.509v3 elektronskog sertifikata) i koji se koristi za verifikaciju elektronskog potpisa, kreiranog pomoću odgovarajućeg privatnog ključa koji je matematički par sa datim javnim ključem, kao i za šifrovanje podataka za korisnika koji poseduje odgovarajući privatni ključ.

Šifrovanje – transformacija koja primenom odgovarajućeg kriptografskog algoritma i odgovarajućeg kriptografskog ključa pretvara originalnu informaciju u oblik u kojem sadržaj informacije postaje nedostupan neovlašćenim licima (šifrat).

Dešifrovanje – transformacija kojom se iz šifrata dobija originalna informacija primenom odgovarajućeg kriptografskog algoritma i odgovarajućeg kriptografskog ključa.

Kriptografija – nauka o zaštiti tajnosti informacija.

Kriptografski algoritmi – algoritmi po kojima se vrši transformacija originalne informacije u šifrovanu informaciju (šifrat) i obratno, iz šifrata u originalnu infomaciju, korišćenjem odgovarajućeg kriptografskog ključa.

Kriptografski ključ – tajna i slučajna informacija odgovarajuće dužine u bitovima koja se koristi u kriptografskim algoritmima, u procedurama šifrovanja i dešifrovanja.

Simetrični kriptografski algoritmi – kriptografski algoritmi koji se koriste za realizaciju šifrovanja u cilju zaštite tajnosti informacija. Algoritmi se nazivaju simetričnim zato što se isti kriptografski ključ koristi za šifrovanje i za dešifrovanje.

Asimetrični kriptografski algoritmi – kriptografski algoritmi koji se koriste za realizaciju tehnologije digitalnog potpisa (kojom se obezbeđuje: autentičnost, integritet i neporecivost transakcija) i digitalne anvelope (kojom se obezbeđuje čuvanje simetričnog ključa u šifrovanom obliku). Algoritmi se nazivaju asimetričnim zato što se različiti kriptografski ključevi koriste za šifrovanje i za dešifrovanje. Asimetrični kriptografski algoritam koristi par ključeva, javni i privatni.

Hash algoritmi – jednosmerni kriptografski algoritmi pomoću kojih se vrši kriptografska transformacija informacije proizvoljne veličine u hash vrednost fiksne veličine (160, 224, 256, 374, 512 bitova (ili više)).

Identifikator objekta (Object identifier) – Sekvenca intedžerskih komponenti koja može biti pridružena nekom registrovanom objektu i koja ima karakteristiku da je jedinstvena u svim identifikatorima objekata u okviru specifičnog domena.

Repozitorijum – Baza podataka i/ili direktorijum na kome su publikovani osnovni dokumenti rada CA, kao i eventualne druge informacije koje se odnose na pružanje sertifikacionih usluga od strane datog CA.

Opoziv sertifikata – Permanentno ukidanje validnosti datog sertifikata i njegovo smeštanje na CRL listu.

Deljena tajna – Deo kriptografske tajne koja je podeljena na unapred definisan broj fizičkih tokena, kao na primer smart kartica.

Smart kartica – Hardverski token koji sadrži čip na kome može da se izvrše odgovarajuće kriptografske funkcije, kao što su: elektronski potpis, šifrovanje, generisanje para asimetričnih ključeva, itd.

Korisnički ugovor – Ugovor između korisnika i CA u cilju obezbeđenja sertifikacionih usluga.

Skraćenice koje se koriste u ovom dokumentu:

CA – Certification Authority

RA – Registration Authority

PKS – Privredna Komora Srbije PKI – Public Key Infrastructure OID – Object IDentifier

TSA – Time Stamping Authority CRL – Certificate Revocation List CSR – Certificate Service Request CDP – CRL Distribution Point

AIA – Authority Information Access

AKI – Authority Key Identifier

SKI – Subject Key Identifier

RFC – Request For Comments

ETSI – European Telecommunication Standardization Institute

CP – Certificate Policy

CPS – Certificate Practise Statement

URL – Uniform Resource Locator

2. Odgovornosti za publikovanje i repozitorijume

Ovo poglavlje se odnosi na sve aspekte publikovanja informacija, kao i na lokacije gde se te informacije publikuju, u okviru PKS CA.

2.1. Repozitorijumi

PKS CA publikuje informacije u vezi elektronskih sertifikata koje izdaje na on- line repozitorijumima koji mogu biti na web serveru ili LDAP serveru. PKS CA zadržava pravo da publikuje statusne informacije o sertifikatima i na repozitorijumu neke treće strane ukoliko je to pogodno.

PKS CA ima on-line repozitorijum dokumenata u kojima se objavljuju informacije o praktičnim pravilima i procedurama rada, uključujući CPS kao i ovu CP. PKS CA zadržava pravo da učini raspoloživim i publikuje informacije u vezi sopstvenih politika i procedura rada putem bilo kog pogodnog načina.

2.2. Publikovanje informacija o sertifikatima

PKS CA publikuje informacije o sertifikatima na prethodno pomenutim repozitorijumima, i to:

- Sertifikate PKS CA (Root i intermediate CA sertifikate),
- Informacije o statusima opozvanosti sertifikata (CRL).

Učesnici u sertifikacionim uslugama se obaveštavaju da će PKS CA publikovati pojedine informacije koje su oni dostavili na javno pristupačnim direktorijumima uz pridružene statusne informacije o elektronskim sertifikatima u formatu i sadržaju koji propisuje Zakon.

Iz razloga njihove osetljvosti i poslovne tajne, PKS CA neće publikovati interna pravila rada koja se odnose na izvesne podkomponente i elemente koji uključuju izvesne bezbednosne kontrole, procedure koje se odnose na upravljanje ključevima, distribuiranu odgovornost, bezbednost registraciona tela, root signing proceduru i sve ostale bezbednosno osetljive procedure.

2.3. Vreme i frekvencija publikovanja

PKS CA publikuje informacije o statusu opozvanosti izdatih digitalnih sertifikata (CRL liste), kao što je naznačeno i precizirano u CPS dokumentu.

2.4. Kontrole pristupa repozitorijumima

PKS CA održava raspoloživim pristup do svog javnog repozitorijuma trećim stranama sa svrhom:

- Dobavljanja CA sertifikata PKS CA,
- Dobavljanja CRL liste PKS CA u cilju validacije sertifikata izdatog od strane PKS CA,
- Eventualnog dobavljanja sertifikata izdatih od strane PKS CA.

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

Iako je pristup PKS CA repozitorijumu i direktorijumima besplatan, PKS CA zadržava pravo da naplaćuje određena specifična korišćenja svojih servisa.

3. Identifikacija i autentikacija korisnika

PKS CA održava dokumentovana praktična pravila i procedure u cilju autentikacije identiteta i/ili drugih atributa aplikanata/krajnjih korisnika PKS CA sertifikata što se izvršava pre izdavanja sertifikata.

PKS CA koristi potvrđene procedure u cilju prihvatanja aplikacija od entiteta koji žele da postanu članovi PKS CA PKI hijerarhije.

PKS CA autentikuje zahteve strana koje žele da opozovu sertifikate u skladu sa ovom politikom.

PKS CA održava odgovarajuće procedure u cilju određivanja praktičnih pravila za dodeljivanje imena, uključujući i prepoznavanje “trademark” prava u izvesnim imenima.

3.1. Nazivi

U cilju identifikacije korisnika, PKS CA sprovodi odgovarajuća pravila dodeljivanja imena i identifikacije koja uključuje tipove imena pridruženih subjektu, kao na primer X.500 “distinguished” imena.

Kada aplicira za PKS CA sertifikat, ime aplikanta mora biti u potpunosti sa odgovarajućim značenjem sem ako to nije eksplicintno dozvoljeno u relevantnom proizvodnom opisu i u PKS CA CPS dokumentu. PKS CA izdaje sertifikate aplikantima koji dostavljaju dokumentovane aplikacije koje sadrže ime koje se može verifikovati.

PKS CA ne izdaje anonimne sertifikate korisnicima.

Imena pridružena korisnicima sertifikata su jedinstvena u domenu PKS CA pošto se uvek koriste zajedno sa jedinstvenim identifikacionim brojem korisnika (u CN polju Subject-a).

PKS CA ne prihvata “trademark” oznake, loga ili druge grafičke ili tekstualne materijale koji su zaštićeni od kopiranja, a razmatrani su za uključenje u sertifikate.

3.2. Inicijalna provera identiteta

U cilju realizacije procedure identifikacije i autentikacije za inicijalnu korisnikovu registraciju za svaki tip subjekta (CA, RA, korisnici ili drugi učesnici) PKS CA sprovodi sledeće korake:

3.2.1. Autentikacija identiteta organizacije

Zahtevi PKS CA u smislu identifikacije i autentikacije organizacija koje su aplicirale za PKS CA sertifikate, uključuju, ali nisu ograničene na konsultovanje određenih baza podataka treće strane koje jednoznačno identifikuju organizaciju ili proverom dokumenata o udruživanju date organizacije.

U cilju identifikacije i autentikacije organizacije koja je ovlastila svog predstavnika za apliciranje za kvalifikovani sertifikat, PKS CA može primeniti korake koji uključuju, ali nisu ograničeni na:

- Provera dokumenata pojedinca, ovlašćenog predstavnika date organizacije, kao što su identifikacione kartice, pasoš, u skladu sa važećim zakonom,
- Utvrđivanje identiteta organizacije koja se bazira na dostavljenoj dokumentaciji,
- Zahtev je da se pojedinac fizički pojavi u PKS RA u odgovarajućoj fazi pre nego što se sertifikat izda,
- Primenu dodatnih zahteva za organizaciju aplikanta, kao što su potpisani autorizacioni dokumenti (ovlašćenja) ili neka druga identifikaciona oznaka organizacije, imajući u vidu uslov iz prethodnog stava.

3.2.2. Autentikacija identiteta pojedinca

U cilju identifikacije i autentikacije individualnog korisnika koji aplicira za dobijanje PKS CA sertifikata, PKS CA može primeniti korake koji uključuju, ali nisu ograničeni na:

- Provera dokumenata kao što su identifikacione kartice, pasoš, u skladu sa važećim zakonom,
- Utvrđivanje identiteta datog pojedinca koja se bazira na dostavljenoj dokumentaciji,

- Zahtev je da se pojedinac fizički pojavi u PKS RA u odgovarajućoj fazi pre nego što se sertifikat izda.

Kada PKS CA uključuje informaciju koja indicira odgovarajuću autorizaciju kao što su specifična prava, ovlašćenja, ili dozvole uključujući dozvolu da realizuje odgovarajuće aktivnosti u ime date organizacije da bi dobio kvalifikovani sertifikat, PKS CA može zahtevati specijalnu pisanu dozvolu od strane date organizacije.

3.3. Identifikacija i autentikacija zahteva za obnavljanje ključeva

Ovo poglavlje nije primenljivo u okviru ove CP.

3.4. Identifikacija i autentikacija zahteva za opoziv sertifikata

U cilju sprovođenja procedura identifikacije i autentikacije zahteva za opozivom sertifikata za odgovarajuće tipove subjekata (CA, RA, korisnici ili drugi učesnici), PKS CA zahteva korišćenje obrazca koji se prosleđuje odgovarajućem PKS, koji sprovodi takve zahteve do PKS CA u cilju realizacije procedure opoziva sertifikata.

Primeri bezbednog dostavljanja zahteva za opozivom mogu biti i digitalno potpisani zahtevi od strane samih korisnika koji žele da im se opozove sertifikat (ukoliko je takva mogućnost dozvoljena u okviru CPS) ili od strane RA ili CA ovlašćenih službenika.

4. Operativni zahtevi u vezi životnog ciklusa sertifikata

Za sve korisnike ili druge učesnike postoji stalna obaveza da informišu PKS CA o svim promenama u informacijama koje su objavljene u sertifikatu za čitav period operativnog rada takvog sertifikata. Određene druge obaveze se takođe mogu dodatno primeniti.

4.1. Aplikacija za dobijanje sertifikata

Aplikanti za dobijanje kvalifikovanih sertifikata su odgovorni da dostave pouzdane i tačne informacije u svojim aplikacijama za dobijanje kvalifikovanih sertifikata. PKS CA zahteva da aplikant lično podnese aplikaciju za kvalifikovan sertifikat.

Korisnici sprovode enrolment proces (proces identifikacije, autentikacije i registracije) sa PKS CA ili njegovim partnerom koji zahteva:

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

4.2. Procesiranje aplikacije za dobijanje sertifikata

Nakon prijema aplikacije datog korisnika, PKS CA ili PKS RA vrše definisanu identifikacionu i autentikacionu proceduru u cilju validacije aplikacije za izdavanje kvalifikovanog sertifikata.

Nakon toga, PKS CA ili PKS RA potvrđuju ili odbijaju aplikaciju za izdavanje kvalifikovanog sertifikata ukoliko zakonski uslovi nisu ispunjeni.

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

Nakon potvrđivanja dostavljenih informacija u aplikaciji za izdavanje kvalifikovanog sertifikata, PKS RA potvrđuje ili odbija aplikaciju za izdavanje kvalifikovanog sertifikata ukoliko zakonski uslovi nisu ispunjeni.

Nakon potvrđivanja aplikacije za izdavanje kvalifikovanog sertifikata, PKS RA šalje zahtev za izdavanje kvalifikovanog sertifikata do PKS CA.

4.3. Izdavanje sertifikata

Nakon dostave validnog zahteva korisnika za izdavanjem sertifikata, PKS CA sprovodi proces izdavanja odgovarajućeg sertifikata koji se sastoji od:

- Generisanja asimetričnih parova ključeva na SSCD, kao i generisanje sertifikata i njihov upis na SSCD.
- Mehanizama notifikacije koji se koriste od strane CA da bi se informisao korisnik o tome da mu je sertifikat izdat i da može da ga preuzme. U tom smislu, CA na siguran način dostavlja korisniku SSCD i odgovarajući PIN.

Ova procedura se detaljno opisuje u CPS dokumentu.

4.4. Prihvatanje sertifikata

Izdati sertifikat od strane PKS CA se smatra prihvaćenim od strane korisnika ukoliko se ispuni bilo koji od dole navedenih uslova:

- Korišćenje standardne on-line forme uz odgovarajući elektronski potpis korisnika gde je to moguće primeniti,
- Korišćenje sertifikata prvi put uz odgovarajući elektronski potpis korisnika,
- Petnaest (15) dana nakon preuzimanja ukoliko korisnik ne javi da postoje bilo kakvi problemi u izdatom sertifikatu.

Bilo koja primedba na prihvatanje izdatog sertifikata mora biti eksplicitno dostavljena do PKS CA, kao sertifikacionom telu – izdavaocu. Potvrda odbijanja koja uključuje sva eventualna polja u sertifikatu koja sadrže pogrešne informacije mora takođe biti dostavljena.

4.5. Korišćenje kvalifikovanog sertifikata i asimetričnog para ključa

U ovom poglavlju se definišu odgovornosti koje se odnose na korišćenje asimetričnog para ključeva i kvalifikovanog sertifikata, i to:

- Odgovornosti korisnika – korisnik se obavezuje da će koristiti privatni ključ i izgenerisani kvalifikovani sertifikat od strane PKS CA u skladu sa definisanim načinom korišćenja ključa u samom sertifikatu (Key Usage i Enhanced Key Usage ekstenzije). Korišćenje privatnog ključa i sertifikata predstavlja deo korisnikovog ugovora sa CA. U tom smislu, korisnik može koristiti svoj privatni ključ samo nakon prihvatanja odgovarajućeg sertifikata. Takođe, korisnik mora prestati da koristi svoj privatni ključ nakon isticanja perioda validnosti ili opoziva izdatog sertifikata.
- Odgovornost treće strane – treća strana je obavezna da prihvata izdate kvalifikovane sertifikate PKS CA sa predviđenim načinom korišćenje sertifikata definisanim u samom sertifikatu. Treća strana je obavezna da propisno i uspešno primenjuje operaciju javnog ključa koji ekstrahuje iz izdatog kvalifikovanog sertifikata i odgovorna je da sprovodi proveru statusa opozvanosti datog kvalifikovanog sertifikata korišćenjem metoda koji je definisan u CP i CPS dokumentima PKS CA.

4.6. Obnavljanje sertifikata

Ovo poglavlje nije primenljivo u okviru ove CP.

4.7. Generisanje novog para ključeva i sertifikata korisnika

Korisnici kojima je sertifikat istekao, ukoliko žele da dobiju novi sertifikat, moraju da podnesu zahtev za izdavanje novog sertifikata koji je isti kao i svaki novi zahtev za dobijanje sertifikata. U tom slučaju, uvek se generiše novi par asimetričnih ključeva.

Takođe, ukoliko je sertifikat korisnika opozvan, a razlog za opoziv je kompromitacija ključa, korisnik može dobiti novi sertifikat samo na osnovu generisanog novog para

asimetričnih ključeva i putem procedure koja je identična dostavljanju prvobitnog zahteva za izdavanje novog sertifikata.

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

4.8. Modifikacije sertifikata korisnika

Ovo poglavlje nije primenljivo u okviru ove CP.

4.9. Suspenzija i opoziv sertifikata

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

- Gubitka, krađe, modifikacije, neautorizovanog objavljivanja ili neke druge kompromitacije privatnog ključa korisnika sertifikata.
- Ako je subjekt sertifikata narušio materijalne obaveze koje su definisane ovom CP ili u CPS dokumentu.
- Ako izvršenje odgovarajućih obaveza lica koja su navedena u ovoj CP kasni ili je sprečeno usled prirodne katastrofe, računarskog ili komunikacionog otkaza, ili usled drugog uzroka koji izlazi van kontrole datog lica,
- Ako se desila promena određenih informacija koja se sadrže u sertifikatu datog lica,
- Ako korisnik zahteva opoziv iz njemu ličnih razloga.

Ako se desi neki od gore pomenutih događaja, korisnik ili neki drugi ovlašćeni predstavnik pravnog lica (u slučaju ako se radi o sertifikatima izdatim fizičkim licima koja zastupaju pravna lica) mora što pre da kontaktira PKS RA ili PKS CA u cilju dostavljanja zahteva za opozivom sertifikata. Pomenuti kontakt može biti on-line ili putem drugih kanala komunikacije. PKS CA opoziva sertifikat promptno nakon verifikacije identiteta strane koja je zahtevala opoziv (službenik PKS RA ili sam korisnik) i potvrdom da je zahtev podnet u skladu sa procedurom zahtevanom u ovoj CP, kao i u CPS dokumentu. Verifikacija identiteta može biti izvršena na osnovu informacionih elemenata koji su sadržani u identifikacionim podacima koje je korisnik dostavio do PKS RA. Nakon ispunjenja pomenutih uslova, PKS CA izvršava promptnu aktivnost u cilju opoziva sertifikata.

Treće strane moraju koristiti listu opozvanih sertifikata (CRL – Certificate Revocation List) koju PKS CA čini raspoloživom putem javno dostupnog repozitorijuma u cilju provere statusa sertifikata na koje oni žele da se oslone. Lista opozvanih sertifikata se ažurira na svaka 24 sata.

Treće strane moraju biti u saglasnosti sa PKS CA politikom, a posebno sa obavezama trećih strana publikovanim u ovoj CP ili CPS dokumentu.

Funkcija suspenzije PKS CA sertifikata je podržana.

Zahtev za suspenzijom može biti dostavljen od strane korisnika ili PKS RA.

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

PKS CA publikuje sve opozvane i suspendovane sertifikate u svojoj CRL listi. Za vreme suspenzije, ili nakon opoziva sertifikata, period operativnog rada datog sertifikata se istovremeno smatra završenim.

4.10. Servisi provere statusa sertifikata

PKS CA publikuje sve opozvane i suspendovane sertifikate u svojoj CRL listi. Lista opozvanih sertifikata (CRL – Certificate Revocation List) PKS CA se ažurira na svaka 24 sata. PKS CA objavljuje listu opozvanih sertifikata na web lokaciji koja je upisana u korisničke sertifikate u polje CRL Distribution Points. Treće strane moraju koristiti listu opozvanih sertifikata u cilju provere statusa opozvanosti sertifikata na koje oni žele da se oslone.

4.11. Prestanak korišćenja sertifikata

Nakon prestanka korišćenja sertifikata izdatog od strane PKS CA, dati sertifikat mora biti opozvan. Prestanak korišćenja sertifikata može biti iz sledećih razloga:

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

4.12. Čuvanje i rekonstrukcija privatnog ključa korisnika namenjenog za autentikaciju

PKS CA obezbeđuje uslove za generisanje višestrukih parova asimetričnih ključeva za korisnike. Pri tome, jedan par ključeva se generiše u okviru CA i služi za autentikaciju korisnika i za šifrovanje dokumenata putem procedure digitalne envelope za datog korisnika. U cilju omogućavanja dešifrovanja dokumenata šifrovanih za datog korisnika u incidentnim slučajevima, kao i za eventualne službene potrebe, neophodno je da se dati privatni ključ čuva u okviru CA. U vezi toga su definisane i odgovarajuće procedure za bezbedno čuvanje privatnog ključa, za postupak aktiviranja datog privatnog ključa, kao i definicije u kojim sve slučajevima privatni ključ određenog korisnika može biti rekonstruisan iz arhivnog servera. Napominjemo još jednom da se ovde radi o privatnom ključu koji isključivo služi za dešifrovanje digitalne envelope. Privatni ključ korisnika kojim se vrši digitalni potpis se nigde ne čuva izuzev na smart kartici korisnika.

5. Upravne, operativne i fizičke bezbednosne kontrole

Ovo poglavlje opisuje sve one bezbednosne kontrole koje ne spadaju direktno u tehničke kontrole, a koje se koriste od strane PKS CA kao podrška u cilju realizacije funkcija generisanja ključeva, autentikacije subjekata, izdavanja sertifikata, opoziva sertifikata, audita i arhiviranja.

Ove ne-tehničke bezbednosne kontrole su kritične za poverenje u sertifikate izdate od strane PKS CA pošto nedostatak bezbednosti može kompromitovati operativni rad CA rezultujući na primer u kreiranju sertifikata i CRL sa pogrešnim informacijama ili kompromitacijom privatnog ključa CA.

5.1. Fizičke bezbednosne kontrole

PKS CA implementira fizičke kontrole u svojim prostorijama uključujući sledeće:

- PKS CA bezbedne prostorije su locirane u prostoru koji odgovara potrebama izvršenja operacija visoke bezbednosti. Postoje označene zone sa fizičkom kontrolom pristupa i zaključane kancelarije sa odgovarajućim sefovima.
- Fizički pristup je ograničen implementacijom odgovarajućih mehanizama kontrole pristupa iz jedne u drugu zonu bezbednosti, kao i u zonu visoke bezbednosti. U tom smislu, CA operacije su locirane u okviru bezbedne računarske sobe koja je podržana fizičkim monitorisanjem i bezbednosnim alarmima, a obezbeđena je i podrška da prelazak iz zone u zonu može biti izveden samo korišćenjem tokena (beskontaktnih kartica), kao i listi kontrole pristupa.
- Napajanje i ventilacija se izvršavaju sa redundansom visokog nivoa.
- Prostorije PKS CA su zaštićene od poplava.
- Prevencija i zaštita od požara su implementirane.
- Medijumi se čuvaju na bezbedan način. Backup medijumi se takođe čuvaju na odvojenoj lokaciji koja je fizički obezbeđena i zaštićena od požara i poplava.
- Iznošenje smeća se takođe kontroliše.

5.2. Proceduralne kontrole

PKS CA sprovodi kadrovsku i upravnu praksu koja obezbeđuje razumnu sigurnost u poverljivost i kompetenciju zaposlenih, kao i zadovoljavajuće performance u vezi sa njihovim dužnostima u domenu tehnologija koje se odnose na elektronski potpis i PKI sisteme.

Svaki zaposleni PKS CA potpisuje izjavu da će se pridržavati pravne regulative u vezi zaštite podataka, kao i da će zadovoljiti sve postavljene zahteve u vezi sa poverljivošću.

Svi zaposleni u PKS CA koji izvršavaju operacije povezane sa upravljanjem ključevima, kao i bilo koje druge operacije koje materijalno utiču na takve operacije, smatraju se dužnostima na poverljivim pozicijama. Poverljive uloge/dužnosti u PKS CA, između ostalih, su:

- Administrator bezbednosti,
- Sistem administratori,
- Sistem operater i
- Sistem evidentičar

PKS CA sprovodi inicijalno istraživanje svih zaposlenih koji su kandidati za poverljive uloge u cilju razumnog pokušaja sticanja uvida u njihovu poverljivost i kompetencije.

Tamo gde se zahteva dualna kontrola, potrebno je da najmanje dva poverljiva zaposlena PKS CA iskažu njihova podeljena znanja u cilju omogućavanja izvršenja tekućih operacija. Drugim rečima, u okviru PKS CA, nijednu osetljivu operaciju ne može izvršiti samo jedan zaposleni. Takođe, svaka uloga/dužnost definiše odgovarajuće zahteve u pogledu identifikacije i autentikacije korisnika.

Takođe, definisano je koje uloge/dužnosti mogu biti kombinovane od strane jednog zaposlenog, a koje to ne smeju.

5.3. Kadrovske bezbednosne kontrole

5.3.1. Kvalifikacija i iskustvo

PKS CA izvršava neophodne aktivnosti u cilju provere zahtevane biografije, kvalifikacija, kao i neophodnog iskustva u cilju realizacije u okviru konteksta kompetencije specifičnog posla. Takve provere biografije tipično uključuju:

- Kriminalne osude za ozbiljne zločine,
- Pogrešne prezentacije informacija od strane kandidata,
- Odgovarajuće reference.

5.3.2. Procedura provere biografije

PKS CA realizuje relevantne provere eventualnih zaposlenih na bazi statusnih izveštaja koji su izdati od strane kompetentnih autoriteta, izjava trećih strana ili izjava samih potencijalnih zaposlenih.

5.3.3. Zahtevi za obučenošću

PKS CA obezbeđuje obuku za svoje zaposlene u cilju realizacije funkcija poslovanja CA i RA.

5.3.4. Ponovna obuka

Periodično ažuriranje obuke može takođe biti izvršeno u cilju uspostave kontinuiteta i ažurnosti znanja zaposlenih, kao i odgovarajućih procedura.

5.3.5. Rotacija poslova

Ovo poglavlje nije primenljivo u okviru ove CP.

5.3.6. Kaznene mere u odnosu na zaposlene

PKS CA ima odgovarajuće mere za kažnjavanje zaposlenih za neovlašćene aktivnosti, neovlašćeno korišćenje autoriteta, kao i neovlašćeno korišćenje sistema u cilju sprovođenja sankcija za određeno neposlovno i rizično ponašanje, koje može biti različito u zavisnosti od različitih okolnosti.

5.3.7. Kontrole nezavisnih ugovarača

Nezavisni ugovarači su subjekti istih procedura zaštite privatnosti i uslova poverljivosti kao i zaposleni u PKS CA.

5.3.8. Dokumentacija za inicijalnu obuku i ponovnu obuku

PKS CA čini dostupnom svu dokumentaciju zaposlenima koja se odnosi na inicijalnu obuku, doobuku ili za druge svrhe.

5.4. Procedure bezbednosnih provera/auditing

Procedure audit logovanja uključuju logovanje događaja i auditing sistema, i implementirane su za svrhu održavanja bezbednog okruženja. U tom smislu, PKS CA implementira sledeće kontrole:

- PKS CA zapisuje događaje koji uključuju ali nisu ograničeni na operacije vezane za životni ciklus sertifikata, pokušaje pristupa sistemu, kao i zahteve dostavljene sistemu.
- PKS CA čuva audit logove u realnom vremenu. U slučaju alarma ili incidentnog događaja, obaveštava se administrator mreže PKS CA.
- Audit logovi se mogu videti samo od strane autorizovanog osoblja – sistem auditori.
- PKS CA implementira procedure backup-a audit logova.

Subjekat koji je prouzrokovao određeni audit događaj se ne obaveštava o samoj audit aktivnosti.

PKS CA realizuje s vremena na vreme procenu ranjivosti sistema.

5.5. Arhiviranje zapisa

Zahtevi za čuvanjem zapisa se primenjuju kako na PKS CA tako i na PKS RA. Opšte politike čuvanja zapisa PKS CA uključuju sledeće:

- Tipove zapisa – PKS CA čuva na bezbedan način zapise o izdatim elektronskim sertifikatima, audit podacima, informacijama o aplikacijama za dobijanjem sertifikata, kao i dokumentaciju o samim aplikacijama za izdavanje sertifikata.
- Period čuvanja – PKS CA čuva na bezbedan način pomenute zapise o PKS CA kvalifikovanim elektronskim sertifikatima za period koji je naznačen u PKS CA CPS dokumentu, a što je usklađeno sa Zakonom.
- Zaštita arhive – uslovi za zaštitu arhive uključuju:
  - Zapise koje samo sistem auditori (zaposleni kojima su pridružene dužnosti čuvanja podataka) mogu da vide i arhiviraju.
  - Zaštitu u odnosu na modifikaciju arhive, kao što je čuvanje podataka na medijumu na koga se može upisati samo jednom.
  - Zaštitu u odnosu na brisanje arhive.
  - Zaštitu u odnosu na kvarenje karakteristika medijuma vremenom na kojima se arhiva čuva, kao na primer realizacija zahteva da se podaci periodično migriraju na sveže medijume.
- Proceduru back-up-a arhive.
- Zahteve za definisanjem vremenskog pečata zapisa u arhivi.
- Zahteve za procedurom čuvanja barem dve odvojene kopije arhive koje su pod kontrolom dve različite osobe.
- Procedure u cilju dobijanja i verifikacije arhivskih informacija – U cilju dobijanja i verifikacije arhivskih informacija, PKS CA i PKS RA održavaju zapise pod jasnom hijerarhijskom kontrolom i sa jasnim opisom posla. PKS CA čuva zapise u elektronskoj ili papirnoj formi. PKS CA može zahtevati od svojih RA, korisnika ili njihovih agenata da dostave odgovarajuća dokumenta u cilju podrške ovog zahteva. Ovi zapisi mogu biti čuvani u elektronskoj, papirnoj i u bilo kojoj drugoj formi za koju PKS CA smatra da je odgovarajuća. PKS CA može da izmeni način čuvanja zapisa ako je to eventualno potrebno da bude u saglasnosti sa određenim akreditacionim šemama.

5.6. Izmena ključeva

PKS CA poseduje proceduru, detaljno opisanu u CPS dokumentu, koja se sprovodi u slučaju isteka sertifikata sertifikacionog tela ili opoziva sertifikata sertifikacionog tela u skladu sa uslovima definisanim u ovoj CP. U oba slučaja, vrši se generisanje novog para ključeva seritifikacionog tela i distribucija sertifikata CA svim korisnicima i zainteresovanim stranama, kao i u slučaju prvog generisanog sertifikata CA.

5.7. Kompromitacija i oporavak u slučaju katastrofe

U Posebnim internim pravilima rada, PKS CA dokumentuje procedure koje treba izvršiti pri rešavanju incidenata, kao i izveštavanja u vezi sa eventualnom kompromitacijom ključeva CA.

PKS CA takođe dokumentuje procedure oporavka koje se koriste ukoliko su računarski resursi, softver, i/ili podaci neispravni ili se sumnja da su neispravni.

PKS CA teži da ponovo uspostavi bezbedno okruženje u koracima koji uključuju, ali nisu ograničeni samo na, opoziv neispravnih sertifikata odgovarajućih entiteta. Nakon toga, PKS CA može ponovo izdati novi sertifikat datom entitetu.

Plan kontinualnog poslovanja se implementira da osigura nastavak poslovanja nakon prirodne ili druge katastrofe.

5.8. Završetak rada CA ili RA

Pre nego što prekine svoje aktivnosti pružanja sertifikacionih usluga, PKS CA:

- Obezbeđuje svojim korisnicima koji imaju validne sertifikate obaveštenje o nameri da prestane sa pružanjem sertifikacione usluge, tj. da prestane da izvršava aktivnosti u svojstvu CA.
- Opoziva sve sertifikate koji su još uvek validni (tj. one koji nisu opozvani ili im je istekao rok važnosti) nakon obaveštenja, a bez zahteva za saglasnošću korisnika.
- Blagovremeno obaveštava o opozivu sertifikata sve korisnike na koje se to odnosi.
- Čini razumne mere u cilju zaštite zapisa koje čuva u skladu sa ovom CP,
- Ukoliko je to moguće, obezbeđuje odgovarajuće mere obezbeđenja sukcesije u smislu ponovnog izdavana sertifikata od strane drugog CA koje je sukcesor – nastavljač izdavanja sertifikata datog CA – i koje poštuje isti CP dokument.

6. Tehničke bezbednosne kontrole

Ovo poglavlje definiše tehničke bezbednosne mere koje primenjuje PKS CA u cilju zaštite kriptografskih ključeva i aktivacionih podataka (kao na primer PIN- ovi, lozinke, itd.). Bezbednosno upravljanje ključevima je kritično u cilju osiguranja da su svi ključevi i aktivacioni podaci zaštićeni i da se koriste isključivo od strane autorizovanih zaposlenih.

Takođe, definisane su i druge tehničke bezbednosne kontrole koje se koriste od strane CA da se bezbedno izvršavaju funkcije generisanja ključeva, autentikacije korisnika, registracije korisnika, izdavanja sertifikata, opoziva sertifikata, auditinga i arhiviranja. Tehničke kontrole uključuju životni ciklus bezbednosnih kontrola kao i operativne bezbednosne kontrole.

U ovom poglavlju se takođe definišu tehničke bezbednosne kontrole nad repozitorijumima, registracionim telima, korisnicima i drugim učesnicima.

6.1. Generisanje i instalacija asimetričnog para ključeva

PKS CA bezbedno generiše i štiti svoje sopstvene privatne ključeve, korišćenjem bezbednih i pouzdanih sistema, i primenjuje neophodne preventivne mere u cilju sprečavanja kompromitacije ili neautorizovanog korišćenja. PKS CA implementira i dokumentuje procedure generisanja ključeva u skladu sa ovom CP. PKS CA primenjuje javne, internacionalne i Evropske standarde propisane Zakonom u vezi bezbednih i pouzdanih sistema.

PKS CA koristi bezbedan proces generisanja svog root privatnog ključa u skladu sa dokumentovanom procedurom. PKS CA distribuira deljene tajne za svoje privatne ključeve. PKS CA je vlasnik privatnih ključeva i poseduje autoritet da prenese odgovarajuće deljene tajne na autorizovane nosioce deljenih tajni.
Privatni root ključ PKS CA se koristi za elektronsko potpisivanje PKS CA sertifikata (pre svega za izdavanje intermediate CA sertifikata) i liste opozvanih sertifikata. Druge svrhe korišćenja privatnog ključa root PKS CA su zabranjene.

Za potrebe svog root privatnog ključa i odgovarajuće potpisivanje, PKS CA koristi SHA-256/RSA kombinaciju hash i asimetričnog algoritma sa dužinom ključa od 4096 bita, periodom validnosti sertifikata od 20 godina sa periodom izdavanja sertifikata od 10 godina

Za svoj intermediate CA privatni ključ i odgovarajući algoritam za elektronsko potpisivanje, PKS CA koristi SHA-256/RSA kombinaciju hash i asimetričnog algoritma sa dužinom ključa od 3072 bita, periodom validnosti od 10 godina sa periodom izdavanja sertifikata od 3 godine.

PKS CA će izvršiti izmenu gore navedenih kombinacija algoritama i dužina ključeva ukoliko se u kriptografskoj teoriji i praksi pokažu slabosti navedenih algoritama i svetska kriptografska javnost preporuči pouzdanije algoritme, kao i u slučajevima definisanja novih standarda za hash i asimetrične algoritme.

6.2. Zaštita privatnog ključa

PKS CA koristi odgovarajuće kriptografske uređaje u cilju realizacije zadataka upravljanja ključevima CA. Pomenuti kriptografski uređaji su poznati pod imenom Hardverski bezbednosni moduli (HSM - Hardware Security Modules).

Generisanje privatnog ključa PKS CA se dešava u okviru bezbednog kriptografskog uređaja koji zadovoljava odgovarajuće zahteve u skladu sa međunarodnim standardima, kao na primer FIPS 140-2 L3 ili Common Criteria EAL4+ standardom (CWA 14169). Ovi standardi garantuju, između ostalog da je bilo koji pokušaj narušavanja integriteta uređaja ili kriptografske memorije istovremeno detektovan, i da privatni ključevi ne mogu da napuste uređaj.

Generisanje privatnog ključa PKS CA zahteva kontrolu od više od jednog, na odgovarajući način autorizovanog, zaposlenog koji imaju poverljive pozicije i dužnosti. Autorizacija procedure generisanja ključeva se mora izvršiti od strane više od jednog člana upravne strukture PKS CA.

Hardverski i softverski mehanizmi koji štite privatne ključeve CA su dokumentovani u Posebnim internim pravilima rada.

HSM uređaji ne smeju da napuštaju PKS CA prostorije izuzev retkih prilika unapred definisanih premeštanja i preseljenja. PKS CA čuva zapise u vezi svih tih premeštanja ili preseljenja.

U slučaju da odgovarajući HSM zahteva održavanje ili popravku, koja se ne može izvršiti u okviru PKS CA prostorija, oni se onda bezbedno prenose do njihovog proizvođača uz poštovanje svih neophodnih bezbednosnih mera, detaljno opisanih u CPS dokumentu.

Privatni ključ PKS CA se ne obnavlja.

Privatni ključ PKS CA će biti uništen na kraju svog životnog ciklusa.

PKS CA koristi bezbedni kriptografski uređaj da čuva svoje privatne ključeve u skladu sa međunarodnim zahtevima iskazanim u FIPS 140-2 L3 ili Common Criteria EAL4+ standardu (CWA 14169).

Procedura čuvanja privatnog ključa PKS CA zahteva višestruke kontrole od strane, na odgovarajući način autorizovanog, osoblja sa poverljivim rolama.

Autorizacija procedure čuvanja ključeva i autorizacija odgovarajućeg osoblja mora biti izvršena od strane više od jednog člana upravne strukture.

PKS CA privatni ključ se backup-uje u skladu sa procedurom definisanom u CPS dokumentu.

Procedura deljenja tajni PKS CA koristi višestruke autorizovane nosioce u cilju da zaštiti i poboljša poverljivost privatnih ključeva i obezbedi odgovarajuću proceduru oporavka ključa.

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

Nosioci deljenih tajni (staraoci) PKS CA imaju zadatak da aktiviraju i deaktiviraju privatni ključ. Privatni ključ je tada aktivan u definisanom periodu vremena.

Pre nego što nosilac deljene tajne prihvati deljenu tajnu on mora lično da se upozna sa kreiranjem, ponovnim kreiranjem i distribucijom tajne na njegovog sledećeg člana lanca poverljivosti.

Nosilac deljene tajne može primiti deljenu tajnu na fizičkom medijumu, kao što je određeni hardverski kriptografski modul (na primer smart kartica) koji je odobren za

korišćenje od strane PKS CA. PKS CA čuva pisane zapise u vezi distribucije deljene tajne.

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

PKS CA privatni ključevi se uništavaju na kraju njihovog životnog veka u cilju garancije da oni neće nikada biti ponovo aktivirani i korišćeni.

Nakon generisanja novog asimetričnog para ključeva i novog sertifikata PKS CA, prethodni privatni ključ se briše iz HSM-a, a backup kopije se čuvaju na CD medijumu se fizički uništavaju na odgovarajućem uređaju.

Pri tome se kreira odgovarajući zapisnik koji se arhivira.

6.3. Drugi aspekti upravljanja parom ključeva

PKS CA arhivira svoj sopstveni javni ključ.

PKS CA izdaje korisničke sertifikate za periodom korišćenja kao što je naznačeno u sertifikatima.

6.4. Aktivacioni podaci

PKS CA bezbedno procesira aktivacione podatke pridružene privatnim ključevima CA, kao i svim drugim privatnim ključevima u datom PKI sistemu (intermediate CA, RA, korisnici).

6.5. Bezbednosne kontrole računara

PKS CA implementira bezbednosne kotrole nad računarima koji se koriste u okviru datog PKI sistema.

6.6. Mrežne bezbednosne kontrole

PKS CA održava i primenjuje visok nivo sistema mrežne bezbednosti, uključujući primenu firewall uređaja i intrusion detection/prevention sistema.

6.7. Vremenski pečat

Ovo poglavlje nije primenljivo u okviru ove CP.

7. Profili sertifikata i CRL lista

Ovo poglavlje specificira formate sertifikata i CRL lista koje izdaje PKS CA.

7.1. Profili sertifikata

PKS CA izdaje sledeće vrste sertifikata:

- Root CA
- Intermediate CA;
- Kvalifikovane sertifikate za:
  - Fizička lica koja su zakonski zastupnici pravnih lica,
  - Zaposlene u PKS i u regionalnim privrednim komorama.

Ovaj dokument predstavlja Politiku sertifikacije PKS CA za izdavanje kvalifikovanih elektronskih sertifikata za korisnike PKS.

7.1.1. Opšti profil sertifikata

Opšti profil PKS CA sertifikata:

Ime profila		
Period validnosti certifikata	1 – 20 godina	
Basic Constraints Ekstenzija	End Entity|CA, Path length=x	
Čuvanje ključeva	Smart kartica | HSM	
Zajedničke ekstenzije	Authority Key Identifier Subject Key Identifier Authority Information Access CRL Distribution Point	
Dužina ključeva	4096, 3072, 2048	
Key Usage ekstenzija – moguće vrednosti	Digital Signature Non-Repudiation Key Encipherment Data Encipherment Key Agreement	Certificate Signing CRL Signing Encipher Only Decipher Only
Enhanced Key Usage Ekstenzija – moguće vrednosti	Client Authentication Server Authentication Email Protection Code Signing Microsoft Smart Card Logon Time Stamping OCSP Signer Microsoft Encrypted File IPsec End System/IKE/Tunnel/User	

QC (Qualified Certificate) statement ekstenzija	OID ekstenzije (1.3.6.1.5.5.7.1.3) sa standardnim vrednostima
OID Politike	
URL za politiku certifikacije	

7.1.2. Profil Root CA sertifikata PKS CA

Profil Root CA sertifikata:

Ime profila	PKS Root CA
Period validnosti certifikata	20 godina
Ekstenzija osnovnih ograničenja	CA
Čuvanje ključeva	HSM
Zajedničke ekstenzije	Subject Key Identifier CRL Distribution Point
Primenljiva dužina ključeva	4096
Ekstenzija korišćenja ključa	Certificate Signing Off-Line CRL signing CRL Signing

7.1.3. Profil Intermediate CA sertifikata PKS CA

Profil Intermediate CA sertifikata:

Ime profila	PKS Intermediate CA
Period validnosti certifikata	10 godina
Ekstenzija osnovnih ograničenja	CA
Čuvanje ključeva	HSM
Zajedničke ekstenzije	Authority Key Identifier Subject Key Identifier Authority Information Access CRL Distribution
Primenljiva dužina ključeva	3072
Ekstenzija korišćenja ključa	Certificate Signing Off-Line CRL Signing CRL

7.1.4. Profil sertifikata korisnika

PKS CA publikuje u okviru CPS dokumenta profile sertifikata koje koristi za sve tipove sertifikata koje izdaje.

U sledeće dve tabele su prikazani profili kvalifikovanih sertifikata za digitalni potpis i za autentikaciju koje izdaje PKS CA.

Ime profila	Kvalifikovani sertifikat za digitalni potpis
Period validnosti certifikata	3 godine
Ekstenzija osnovnih ograničenja	End Entity
Čuvanje ključeva	Smart kartica – SSCD
Zajedničke ekstenzije	Authority Key Identifier Authority Information Access CRL Distribution Point Certificate Policies
Primenljiva dužina ključeva	2048
Ekstenzija korišćenja ključa	Digital Signature Non-Repudiation
Ekstenzija naprednog korišćenja ključa	Client Authentication (1.3.6.1.5.5.7.3.2) Email Protection (1.3.6.1.5.5.7.3.4) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
QC (Qualified Certificate) statement ekstenzija	OID ekstenzije (1.3.6.1.5.5.7.1.3) sa standardnim vrednostima uključujući SSCD ekstenziju
OID Politike	1.3.6.1.4.1.31266.1.1.3
URL za CPS	http://ca.pks.rs/v2/docs/PKSCACPSClass1.pdf

Za sertifikate koji ne sadrže JMBG, mogu biti dodata posebna polja u skladu sa opisom u Praktičnim pravilima rada Sertifikacioog tela PKS.

Ime profila	Kvalifikovani sertifikat za autentikaciju
Period validnosti certifikata	3 godine
Ekstenzija osnovnih ograničenja	End Entity
Čuvanje ključeva	Smart kartica – SSCD, PKS CA
Zajedničke ekstenzije	Authority Key Identifier Authority Information Access CRL Distribution Point
Primenljiva dužina ključeva	2048
Ekstenzija korišćenja ključa	Key Encipherment
OID Politike	1.3.6.1.4.1.31266.1.1.3

7.2. Profil CRL liste

U skladu sa IETF PKIX RFC 2459, PKS CA podržava izdavanje CRL lista koje su u saglasnosti sa sledećim uslovima:

- Brojevi verzija su podržani za CRL liste,
- CRL i CRL ekstenzije su popunjene i njihova kritičnost je posebno naznačena.

Profil PKS CA CRL (Sertificate Revocation List) liste je prikazan u sledećoj tabeli:

<table>
<tr><td>Version</td><td colspan="3">[Version 2]</td></tr>
<tr><td>Issuer Name</td><td colspan="3">CountryName=RS,
OrganizationName=Privredna komora Srbije,
CommonName= PKS CA Class1 – Kvalifikovani sertifikati</td></tr>
<tr><td>This Update</td><td colspan="3">[Date of Issuance]</td></tr>
<tr><td>Next Update</td><td colspan="3">[Date of Issuance + 24 hours]</td></tr>
<tr><td>Signature Algorithm identifier</td><td colspan="3">sha256RSA</td></tr>
<tr><td>Authority Key identifier</td><td colspan="3"></td></tr>
<tr><td>CRL Number</td><td colspan="3">Redni broj CRL liste</td></tr>
<tr><td rowspan="3">Revoked sertificates</td><td colspan="3">CRL Entries</td></tr>
<tr><td>Sertificate Serial Number</td><td>Date and Time of Revocation</td><td>CRL Reason Code</td></tr>
<tr><td>[Sertificate Serial Number]</td><td>[Date and Time of Revocation]</td><td>[CRL Reason Code]</td></tr>
</table>

7.3. OCSP profil

Ovo poglavlje nije primenljivo u okviru ove CP.

8. Provera saglasnosti sa Politikom sertifikacije

PKS CA prihvata periodičnu audit/poveru saglasnosti svojih politika, uključujući ovu CP što uključuje i periodičnu superviziju od strane Nadležnog organa Republike Srbije. Rad PKS CA je takođe u saglasnosti sa najvažnijim međunarodnim i Evropskim standardima u ovoj oblasti, kao i sa Evropskom direktivom 1999/93/EC o elektronskim potpisima.

U domenu izdavanja kvalifikovanih elektronskih serifikata, PKS CA radi u okviru ograničenja definisanim u okviru Zakona o elektronskom potpisu države Srbije, kao i odgovarajućim podzakonskim aktima.

PKS CA prihvata pod određenim uslovima i proveru/auditing internih procedura i pravila rada koja nisu javno dostupna. PKS CA evaluira rezultate ovakvih provera pre nego što ih implementira.

PKS CA sprovodi redovne interne audit-e usklađenosti poslovanja sa ovom CP, kao i sa CPS dokumentom. Interni audit sprovode odgovarajući zaposleni PKS sa datim zaduženjima.

Nakon akreditacije PKS CA za izdavanje kvalifikovanih elektronskih sertifikata u Srbiji, Nadležni organ za poslove akreditacije i supervizije PKI sistema (Ministarstvo

za telekomunikacije i informaciono društvo) vršiće obaveznu superviziju PKS CA redovno, i to barem jednom godišnje.

9. Drugi poslovni i pravni aspekti

9.1. Cene

PKS CA ne naplaćuje korišćenje PKS CA izdatih kvalifikovanih sertifikata korisnicima elektronskih servisa PKS.

PKS CA zadržava prava da menja uslove korišćenja sertifikata od strane pomenutih korisnika.

PKS CA može naplaćivati korišćenje PKS CA izdatih sertifikata onim korisnicima – trećim licima za koje PKS CA outsource-uje odgovarajuću sertifikacionu uslugu. PKS CA zadržava prava da menja cene svojih sertifikata u ovim slučajevima.

Objavljivanje cena sertifikata i drugih sertifikacionih usluga se vrši putem veb sajta PKS CA, partnera PKS CA (treća lica) ili putem odgovarajućeg ugovora tamo gde je to primenljivo.

9.2. Finansijska odgovornost

PKS CA obezbeđuje osiguranje za pokrivanje svih odgovornosti opisanih u ovoj CP i to iskazuje u okviru svog ograničenog garancijskog plana koji je raspoloživ na PKS CA repozitorijumu i predstavlja deo CPS.

PKS CA ne prihvata nikakvu drugu odgovornost koja izlazi iz pokrivanja definisanog pomenutim ograničenim garancijskim planom.

Korisnik je dužan da obešteti PKS CA u odnosu na bilo koje aktivnosti ili propuste u odgovornosti, bilo koje gubitke ili štetu, kao i za bilo kakve troškove bilo koje vrste, uključujući razumne naknade advokata, koje bi PKS CA mogao da ima kao rezultat:

- Bilo kog lažnog ili pogrešno prezentovanog podatka dostavljenog od strane korisnika ili njihovih agenata.
- Bilo kog propusta korisnika da dostavi materijalnu činjenicu da je pogrešna prezentacija ili propust učinjen iz nemarnosti ili sa namerom da se prevari PKS CA, ili bilo koje lice koje prima i odnosi se prema dobijenom sertifikatu.
- Neobezbeđivanja odgovarajuće zaštite korisnikovog privatnog ključa, nekorišćenja bezbednog sistema kako je zahtevano, ili neizvršenja odgovarajućih preventivnih mera neophodnih da se spreči kompromitacija, gubitak, objavljivanje, modifikacija ili neautorizovano korišćenje korisnikovog privatnog ključa, ili napada na integritet PKS CA Root privatnog ključa.
- Kršenja bilo kojih zakona koji su primenljivi, uključujući one koji se odnose na zaštitu intelektualnih prava, viruse, pristup računarskim sistemima, itd.

9.3. Poverljivost poslovnih informacija

Ovo poglavlje nije primenljivo u okviru ove CP.

9.4. Privatnost i zaštita personalnih informacija

PKS CA se pridržava pravila zaštite privatnosti personalnih podataka i pravila poverljivosti kako je propisano u CPS dokumentu, kao i u odgovarajućim zakonskim dokumentima.

PKS CA ne objavljuje, niti se zahteva da objavljuje, bilo koju poverljivu informaciju bez autentikovanog i potvrđenog zahteva od strane:

- Same strane za koju se takva infromacija i čuva,
- Odgovarajućeg suda.

PKS CA može naplatiti odgovarajuću administrativnu cenu za procesiranje ovakvih objavljivanja.

Strane u komunikaciji koje zahtevaju i dobijaju poverljive informacije imaju dozvolu za to na osnovu pretpostavke da će oni te informacije koristiti za zahtevane svrhe, da će ih osigurati od kompromitacije, i da će se uzdržavati od njihovog korišćenja i objavljivanja trećim stranama.

PKS CA i njegovi partneri mogu učiniti raspoloživom specifičnu politiku privatnosti u cilju zaštite personalnih podataka aplikanta koji zahteva izdavanje sertifikata od strane PKS CA ili njegovog partnera putem njihovih veb sajtova i/ili CP ili CPS dokumenata.

9.5. Prava intelektualnog vlasništva

PKS CA poseduje i zadržava sva prava intelektualnog vlasništva pridružena njegovim bazama podataka, web sajtovima, elektronskim sertifikatima koje izdaje, kao i bilo kojim drugim publikacijama koje na bilo koji način pripadaju ili potiču od strane PKS CA, uključujući i ovu CP.

9.6. Predstavljanje i garancije

Ovo poglavlje nije primenljivo u okviru ove CP.

9.7. Nepriznavanje garancije

Ovo poglavlje nije primenljivo u okviru ove CP.

9.8. Ograničenja odgovornosti

PKS CA ne prihvata bilo kakvu drugu odgovornost osim one koja je eksplicitno definisana u ovom dokumentu.

Ni u kom slučaju (izuzev zloupotrebe ili namere) PKS CA nije odgovorno za:

- Bilo kakav gubitak profita.
- Bilo kakav gubitak podataka.
- Bilo koju indirektnu ili slučajnu štetu koja je prouzrokovana ili je vezana za korišćenje, isporuku, licencu, performanse sertifikata ili elektronskih potpisa.
- Bilo koju transakciju ili uslugu ponuđenu ili u okviru obuhvata ove CP.
- Bilo koju drugu štetu izuzev onih koje potiču od opravdanog oslanjanja na verifikovane informacije koje se nalaze u izdatom sertifikatu.
- Bilo koju odgovornost koja se pojavila u slučaju namerne obmane aplikanta u procesu utvrđivanja identiteta aplikanta.

•

9.9. Odštete

Ovo poglavlje nije primenljivo u okviru ove CP.

9.10. Period važnosti i kraj validnosti Politike sertifikacije

Ovo poglavlje nije primenljivo u okviru ove CP.

9.11. Pojedinačna obaveštenja i komunikacija sa učesnicima

Ovo poglavlje nije primenljivo u okviru ove CP.

9.12. Ispravke

Ovo poglavlje nije primenljivo u okviru ove CP.

9.13. Procedure rešavanja sporova

PKS CA se referiše na arbitražu u cilju rešavanja svih sporova koji se odnose na ovu CP. Ako se spor ne reši u okviru deset (10) dana nakon inicijalnog obaveštenja shodno pravilima CP, strane u sporu dostavljaju spor na arbitražu. Arbitraža se sastoji od 3 arbitra, svaka strana predlaže po jednog, dok trećeg predlažu zajedno

obe strane u sporu. Mesto za arbitražu je Beograd, Srbija, a arbitri određuju sve troškove arbitraže.

Za sve sporove koji se odnose na tehnologiju, kao i sporove koji se odnose na samu CP, strane u sporu prihvataju arbitražno telo koje će biti izabrano od strane vlade Srbije.

9.14. Zakon koji se poštuje

Ova CP je izdata u potpunosti u skladu sa odgovarajućom zakonskom regulativom države Srbije, i to pre svega sa Zakonom o elektronskom potpisu i odgovarajućim podzakosnkim aktima. Sve pravne stvari koje se odnose na PKS CA i/ili koji se odnose na sertifikate izdate od strane PKS CA će biti procesuirane od strane odgovarajućeg suda u Srbiji.

9.15. Saglasnost sa primenljivim zakonima

Ovo poglavlje nije primenljivo u okviru ove CP.

9.16. Razne odredbe

Ovo poglavlje nije primenljivo u okviru ove CP.

9.17. Druge odredbe

Ovo poglavlje nije primenljivo u okviru ove CP.

10. Istorija dokumenta

Verzija	Datum	Opis
1.0	17.08.2012.	Radna verzija
1.1	01.09.2012.	Ažurirana verzija
2.0.1	01.03.2013.	Primereno novoj verziji sertifikata
2.0.2	10.03.2015.	Ažurirana verzija

11. Reference

- Zakon o elektronskom potpisu, Sl. glasnik Republike Srbije, br. 135/2004
- Pravilnik o bližim uslovima za izdavanje elektronskih sertifikata, Sl. glasnik Republike Srbije, broj 48/2005
- Pravilnik o dopunama Pravilnika o tehničko-tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijumima koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa, Sl. glasnik

Republike Srbije, broj 23/15

- RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework
- RFC 5280 – Request For Comments 5280, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile
- Praktična pravila sertifikacije Sertifikacionog tela Privredne komore Srbije

12. Kompanije i organizacije

1. Privredna komora Srbije, http://www.pks.rs
2. NetSeT d.o.o, http://www.netset.rs
3. IANA (Internet Assigned Numbers Authority), http://www.iana.org

PRIVREDNA KOMORA SRBIJE **PREDSEDNIK**

02.01-Broj:

31. mart 2015. godine Marko Čadež

B e o g r a d