Praktična pravila rada

za pružanje kvalifikovane usluge upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata

OID CPS dokumenta (1.3.6.1.4.1.31266.10.1.5)

- verzija 3.1.-

Sadržaj

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

Praktična pravila rada za pružanje kvalifikovane usluge upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata

1. UVOD

Sertifikaciono telo Privredne komore Srbije (u nastavku: PKSCA), kao registrovani pružalac usluga od poverenja, vrši kvalifikovanu uslugu upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata na osnovu Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju ("Službeni glasnik RS", broj 94/17; u daljem tekstu - Zakon) i Pravilnika o uslovima koje mora da ispunjava kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata i uslovima koje mora da ispunjava imenovano telo („Službeni glasnik RS", broj 34/18; u daljem tekstu - Pravilnik).

PKSCA pruža kvalifikovanu uslugu upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa, odnosno pečata (u nastavku: usluga udaljenog potpisivanja) u skladu sa standardom ETSI TS 119 431-1 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part1: TSP services components operating a remote QSCD/SCDev" i ETSI TS 119 431-2 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part2: TSP services components suporting AdES digital signature creation", uključujući i zahteve drugih standarda na koje se iz pomenutih standarda direktno ili indirektno upućuje, odgovarajućim međunarodnim standardima i preporukama, odnosno drugim standardima, dokumentima i preporukama koje se odnose na pružanje usluge udaljenog potpisivanja, utvrđenim Zakonom i Pravilnikom.

1.1. Pregled

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

- ***PKS CA Root**,* kao korensko sertifikaciono telo;

- ***PKS CA Class1***, kao podređeno sertifikaciono telo za pružanje kvalifikovanih elektronskih usluga izdavanja sertifikata za elektronski potpis na smart karticama;
- ***PKS CA Cloud***, kao podređeno sertifikaciono telo za pružanje usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa odnosno pečata.
- ***PKS CA TSA,*** kao podređeno sertifikaciono telo za pružanje usluga izdavanja kvalifikovanih vremenskih žigova.

U okviru ovako definisane hijerarhije, **PKS CA Cloud** je sertifikaciono telo koje izdaje kvalifikovane elektronske sertifikate u cloud-u i generiše korisničke privatne ključeve, kojima se, nakon autorizacije od strane korisnika, vrši kvalikokovana usluga upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata (u daljem tekstu: usluga udaljenog elektronskog potpisivanja/pečaćenja).

PKSCA utvrđuje Praktična pravila za pružanje kvalifikovane usluge upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata (u daljem tekstu: Praktična pravila), u skladu sa Zakonom i Politikom pružanja kvalifikovanih usluga od poverenja PKSCA. Praktična pravila obezbeđuju korisnicima dovoljno informacija na osnovu kojih se mogu upoznati sa obimom usluge i odlučiti o prihvatanju usluge.

Politika pružanja kvalifikovanih usluga od poverenja PKSCA i Praktična pravila su javni dokumenti.

PKSCA utvrđuje i posebna interna pravila rada sertifikacionog tela i zaštite sistema pružanja usluga od poverenja (u daljem tekstu: Interna pravila). Interna pravila su privatni dokument i predstavljaju poslovnu tajnu sertifikacionog tela i odobrava ih odgovorno lice PKSCA.

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

PKSCA je Praktičnim pravilima za pružanje usluge udaljenog elektronskog potpisivanja/ pečaćenja dodelilo OID: **1.3.6.1.4.1. 31266.10.1.5.**

Struktura Praktičnih pravila za pružanje usluge udaljenog potpisivanja/pečaćenja je usklađena sa Aneksom A standarda ETSI TS 119 431-2.

Ovaj dokument je, na osnovu smernica iz tehničkih specifikacija ETSI TS 119 432-1 usklađen sa politikom pružanja usluga od poverenja:

EU SSASC Policy (EUSCP OID: 0.4.0.19431.1.1.3)

itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops(1) policy-identifiers(1) eu-remote-qscd (3)

1.1.1. Učesnici

1.1.1.1. Pružalac usluge od poverenja

PKSCA je, kao pružalac kvalifikovanih usluga od poverenja, ujedno i pružalac usluga udaljenog potpisivanja/pečaćenja (Server Signing Application Service Provider – SSASP).

Identifikacioni podaci PKSCA su:

PKSCA
Privredna Komora Srbije
Resavska 13-15
11000 Beograd
Srbija

1.1.1.2. Korisnici

Korisnici su fizička ili pravna lica, koja sa PKSCA zaključe Ugovor o korišćenju kvalifikovane usluge upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata.

1.1.1.3. Pouzdajuće (treće) strane

Pouzdajuće (treće) strane su fizička lica i poslovni subjekti (kompanije, korporacije, ustanove, organi državne uprave i dr.) koji se pouzdaju u kvalifikovanu uslugu upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata.

Pre pouzdanja u elektronsku uslugu od poverenja, treće strane moraju da realizuju procedure provere predmetne usluge definisane praktičnim pravilima konkretne usluge od poverenja.

1.1.2. Naziv dokumenta

Praktična pravila definišu konkretne detalje implementacije, pravila i procedure rada PKSCA usluge upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata.

Ovaj dokument se identifikuje na sledeći način:

- **Naziv:** Praktična pravila rada za pružanje kvalifikovane usluge upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata
- **Verzija:** 3.1
- **OID:** 1.3.6.1.4.1.31266.10.1.5

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

1.1.2.1. Podržana politika pružanja usluge od poverenja – identifikacija usluge

Kvalifikovana usluga upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata (politika kreiranja elektronskog potpisa/pečata - SCASC policy) je uslaglašena sa zahtevima tehničkih specifikacija ETSI TS 119 431-2 i identifikovana OID-om:

OID: 0.4.0.19431.2.1.2.

itu-t(0) identified-organization(4) etsi(0) CREATION SERVICE-policies(19431) ades (2) policy-identifiers(1) eu-advancedx509 (2)

1.2. Okruženje usluge za udaljeno potpisivanje/pečaćenje

1.2.1. Komponente usluge udaljenog potpisivanja/pečaćenja

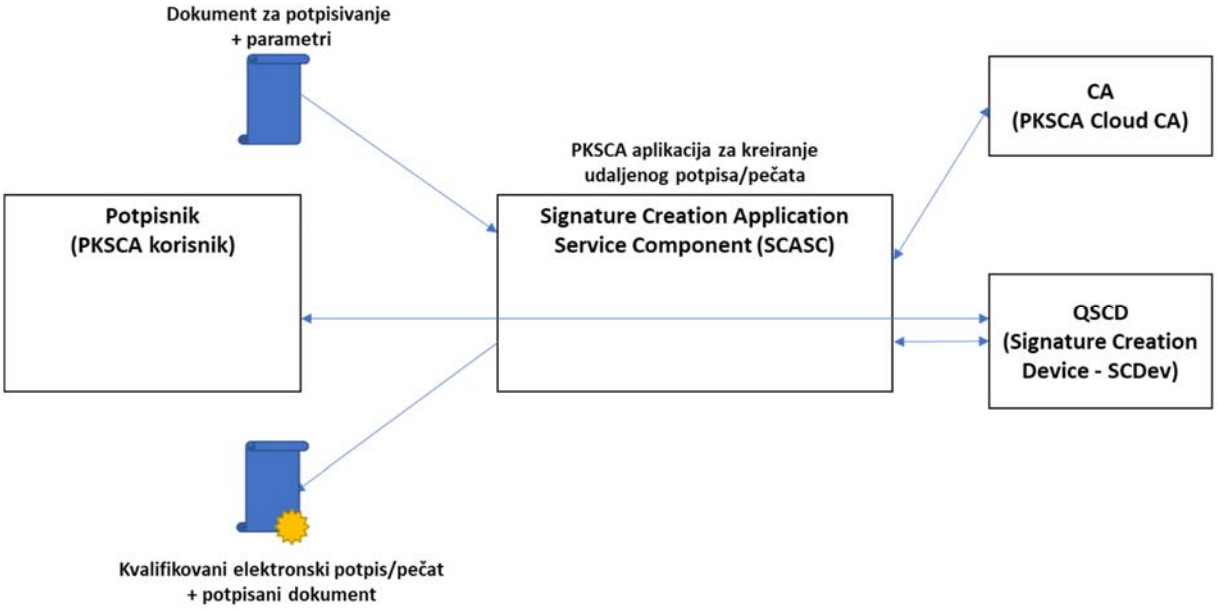
Osnovne komponente kvlifikovane usluge upravljanja kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa/pečata su:

- **CA telo – PKSCA Cloud CA**, kao sertifikacioni autoritet koji generiše korisničke ključeve i izdaje korisničke sertifikate.
- **QSCD**, kao kvalifikovano sredstvo za kreiranje elektronskog potpisa/pečata, koje se sastoji od HSM uređaja i SAM modula (Signature Creation Device – SCDev).
- **Aplikacija za kreiranje udaljenog potpisa**, koja predstavlja softversku komponentu odgovornu za kreiranje kvalifikovanog elektronskog potpisa/pečata (Signature Creation Application Service Component – SCASC). Aplikacija za kreiranje udaljenog potpisa sastoji se od sledećih komponenti:
  - Servis za generisanje ključeva
  - Servis za povezivanje sertifikata
  - Servis za povezivanje sredstava za elektronsku identifikaciju
  - Servis za aktivaciju potpisa
  - Servis za uništenje ključeva
  - Servis za obezbeđivanje sredstava za identifikaciju

  Detaljniji opis funkcionalnosti subkomponenti aplikacije za kreiranje udaljenog potpisa dat je u poglavlju 3.2.1.

1.2.2. Arhitektura usluge za udaljeno potpisivanje

Dijagram na slici 1. prikazuje simplifikovanu arhitekturu PKSCA usluge za upravljanje kvalifikovanim sredstvom za kreiranje elektronskog potpisa/pečata i komponente u procesu udaljenog potpisivanja.



Slika 1. - Arhitektura usluge za za upravljanje kvalifikovanim sredstvom za kreiranje kvalifikovanog elektronskog potpisa/pečata

1.3. Defiicije i skraćenice

1.3.1. Definicije

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

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

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

1.3.2. Skraćenice

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

SAM – Signature Activation Module

SAP – signature Activation Protocol

SCASC – Server Signing Application Service Component

SCDev – Signature Creation Device

SSASP – Server Signing Application Service Provider

1.4. Politike i prakse (procedure)

1.4.1. Organizacija zadužena za administriranje dokumentacije

PKSCA je odgovorno za izradu i administraciju dokumenta Praktična pravila za udaljeno potpisivanje.

1.4.2. Kontakt osoba

Osoba u PKSCA, odgovorna za Praktična pravila za udaljeno potpisivanje je:

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

1.4.3. Primenljivost dokumentacije

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

Praktična pravila su javno dostupna na repozitorijumu PKSCA, koji se nalazi na internet adresi: http://v3.pksca.rs.

Ovaj dokument važi do stupanja na snagu novog dokumenta Praktičnih pravila ili do objave prestanka njegovog važenja.

Nova verzija dokumenta ili objava prestanka važenja biće publikovana na internet stranici PKSCA sa naznačenim danom stupanja na snagu. Stupanjem na snagu nove verzije dokumenta, na sve usluge od poverenja definisane u njemu se od tog dana primenjuju odredbe iz tog dokumenta.

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

Dokument Praktična pravila se revidira po potrebi.

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

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

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

2. UPRAVLJANJE I RADNI POSTUPCI

2.1. Interna organizacija

2.1.1. Pouzdanost organizacije

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

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

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

2.1.2. Razdvajanje dužnosti

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

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

U poverljive uloge PKSCA spadaju:

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

Bezbednosni zahtevi usluga od poverenja uzrokuju razdvajanje sledećih dužnosti:

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

2.2. Ljudski resursi

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.

PKSCA izvršava neophodne aktivnosti u cilju provere biografije, kvalifikacija, kao i neophodnog iskustva u okviru kompetencija neophodnih za specifične poslove. Zaposleni u PKSCA moraju imati potvrdu da nisu zakonski kažnjavani. PKSCA realizuje relevantne provere kandidata za zasnivanje radnog odnosa na bazi statusnih izveštaja izdatih od strane kompetentnih autoriteta, izjava trećih strana ili izjava samih kandidata.

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

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

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

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.

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

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

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

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

2.3. Upravljanje imovinom

2.3.1. Opšti zahtevi

PKSCA obezbeđuje odgovarajuću zaštitu imovine, uključujući i informacionu imovinu, 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, kao i postupci upravljanja i provere sistema su interne prirode i njihovi detalji se ne objavljuju javno.

2.3.2. Rukovanje medijima

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

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.

2.4. Kontrola pristupa

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

Neautorizovan pristup računarima PKSCA nije dozvoljen. PKSCA sistem mogu startovati samo dva ili više ovlašćenih lica sa poverljivim ulogama/dužnostima.

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

Računari koji se koriste u okviru PKSCA čuvaju se unutar specijalne prostorije koja je fizički obezbeđena.

Pristup preko računarske mreže se štiti pomoću specijalnih aplikativnih firewall uređaja - kripto komunikacionih servera.

2.5. Kriptografske mere zaštite

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

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

Korisnički ključevi se mogu se koristiti nakon što je sproveden postupak njihove aktivacije od strane korisnika.

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

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

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

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

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

Hardverske i softverske mehanizme zaštite privatnih ključeva obezbeđuje HSM uređaj. Mehanizmi zaštite privatnih ključeva su minimalno ekvivalentne snage kao i sami privatni

ključevi koji se štite, a po specifikaciji proizvođača HSM-a. Sertifikaciono telo pravi rezervne kopije privatnih ključeva u skladu sa procedurom opisanom u pratećoj dokumentaciji proizvođača HSM, što je definisano internim pravilima rada.

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

2.6. Fizička bezbednost

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

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

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

O svakom pristupu sistemu vodi se evidencija.

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

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

2.7. Bezbednost operacija

U cilju održavanja ispravnog funkcionisanja usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa, odnosno pečata, PKSCA vrši testiranja procesa potpisivanja/pečaćenja, funkcionalne logike, korisničkog interfejsa, bezbednosnih procedura itd. pre puštanja u rad, kao i prilikom svake izmene funkcionalnosti u softveru ili hardveru koji podržava proces udaljenog potpisivanja/pečaćenja.

PKSCA prati raspoloživost kapaciteta, planira održavanje i dalji razvoj sistema usluga od poverenja u skladu sa budućim potrebama, zahtevima standarda i razvojem tehnologije.

Razvojno, testno i produkciono okruženje PKSCA su striktno razdvojeni, posebno se održavaju i ne preklapaju se ni u jednom segmentu.

Informacioni sistem PKSCA je zaštićen od malicioznog softvera. Način zaštite od malicioznog softvera opisan je u Internim pravilima rada PKSCA.

Sve ključne informacije vezane za operacije PKSCA se backup-uju u skladu sa odredbama Politike pružanja kvalifikovanih usluga od poverenja i odgovarajućih praktičnih pravila rada za konkretne usluge od poverenja.

PKSCA vrši prikupljanje evidencionih podataka i audit logova kako je naznačeno u tački 2.10. ovog dokumenta.

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

PKSCA obavlja redovnu procenu rizika vezanu za informacionu imovinu, kao i procenu ranjivosti za prepoznate javne i privatne adrese i penetraciono testiranje. Procena rizika se sprovodi jednom godišnje. Procena ranjivosti sistema za prepoznate javne i privatne adrese PKSCA sprovodi se kvartalno. Penetracioni test sprovodi se jednom godišnje. Svaku novu kritičnu ranjivost PKSCA razmotrai u roku od 48 sati od njenog prepoznavanja i postupa u skladu sa utvrđenim procedurama.

2.8. Bezbednost računarske mreže

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

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

Oprema za zaštitu računarske mreže beleži tok saobraćaja i pokušaje pristupa servisima i javnim internet stranicama PKSCA. Samo ovlašćena lica sa poverljivim ulogama PKSCA imaju

administratorska ovlašćenja za podešavanje i upravljanje opremom za zaštitu računarske mreže. Udaljeno podešavanje opreme za zaštitu računarske mreže nije dozvoljeno.

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

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

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

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

2.9. Upravljanje incidentima

Planom kontinuiteta poslovanja PKSCA je dokument kojim su definisani i regulisani postupci u slučaju nastanka incidenta ili kompromitovanja sistema. Ovaj dokument obuhvata i postupke za oporavak sistema i uspostavu bezbednih uslova za nastavak pružanja usluga od poverenja.

Plan kontinuiteta poslovanja PKSCA revidira se jednom godišnje.

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

Funkcionalnost, ispravnost rada i pravovremeno otklanjanje oštećenja komponenti sistema obezbeđeno je ugovorima o podršci i održavanju sa dobavljačima opreme.

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

2.10. Prikupljanje evidencionih podataka

PKSCA prikuplja evidencione podatke u skladu sa zahtevima specificiranim u poglavlju 7.10 standarda ETSI EN 319 401 V2.2.0 (2017-08) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

PKSCA ove podatke ne čini dostupnima, osim u slučajevima propisanim zakonom ili kada to pismenim putem zahteva sud, upravno ili neki drugi nadležni državni organ.

PKSCA vodi audit logove događaja u PKSCA vezanih za:

- upravljanje životnim ciklusom CA ključeva PKSCA CA-ova,

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

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

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

Audit logovi se čuvaju najmanje 10 godina od prestanka važnosti sertifikata na koji se odnose.

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.

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.

2.11. Plan nastavka poslovanja nakon incidenata

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

2.12. Prekid rada pružaoca usluga od poverenja

PKSCA će, u slučaju planiranog prestanka pružanja usluga od poverenja:

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

U slučaju prestanka pružanja usluga izdavanja kvalifikovanih sertifikata PKSCA će arhivirati, zaštititi i čuvati zapise kako bi ti zapisi bili raspoloživi za pružanje dokaza u sudskim, upravnim i drugim postupcima u skladu sa važećom zakonskom regulativom, ili će sa drugim poslovnim subjektom ugovoriti takvo arhiviranje, zaštitu i čuvanje zapisa.

2.13. Usaglašenost

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

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

Provera usaglašenosti obavlja se u cilju potvrđivanja da PKSCA, za usluge koje pruža, ispunjava zahteve utvrđene Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, Uredbom EU br. 910/2014 i tehničkim specifikacijama ETSI TS 119 431-1 i ETSI TS 119 431-2.

Provere usaglašenosti rada PKSCA mogu biti interne i eksterne.

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

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

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

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.

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

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

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

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

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

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

TEHNIČKI ZAHTEVI ZA USLUGU UDALJENOG POTPISIVANJA

3.1. Interfejsi

PKSCA portal zahteva od klijenta dvofaktorsku autentikaciju, ili autentikaciju korišćenjem kvalifikovanog elektronskog sertifikata. Korisnik može pristupiti usluzi udaljenog potpisivanja tek nakon uspešno izvršenog procesa autentikacije. Na ovaj način se obezbeđuje da su informacije koje se razmenjuju dostupne samo konkretnom autentikovanom klijentu.

Aplikacija za udaljeno potpisivanje (Signature Creation Application Service Component – SCASC) kontaktira servis za udaljeno potpisivanje putem namenskog protokola koji se zasniva na zahtevima standarda ETSI TS 119 432 V1.1.1 (2019-03)Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation.

Komunikacioni kanal između korisnika i sistema za udaljeno potpisivanje obezbeđen je korišćenjem TLS bezbednosnog kanala. Sistem za udaljeno potpisivanje garantuje uspostavljanje bezbednog kanala i očuvanje poverljivosti i integriteta podataka koji se razmenjuju sa korisnikom.

Potpisniku se dokument prezentuje na početku procesa potpisivanja kako bi vizuelno mogao da odabere mesto na kome će stajati potpis. Nakon potpisivanja, potpisani dokument se ne prezentuje potpisniku. PKSCA omogućava potpisniku da download-uje dokument nakon potpisivanja.

3.2. Kreiranje kvalifikovanog elektronskog potpisa/pečata

3.2.1 Opšti zahtevi

1.1.3.1. Generisanje korisničkih ključeva

Asimetrični par ključeva korisnika se generiše na hardverskom bezbednosnom modulu (HSM – Hardware Security Module) i čuva u QSCD uređaju u PKSCA. Generisanje asimetričnog para ključeva i postupci tokom generisanja opisani su u poglavlju 6.1. dokumenta „Praktična pravila rada za pružanje usluge izdavanja kvalifikovanih elektronskih sertifikata u cloud-u“, koji je sastavni deo dokumentacije PKSCA.

Zaštita privatnih ključeva i kontrola hardverskog kriptografskog modula opisani su u poglavlju 6.2. „Praktičnih pravila rada za pružanje usluge izdavanja kvalifikovanih elektronskih sertifikata u cloud-u“.

Korisnički privatni ključevi nikada ne napuštaju QSCD.

Primenjeni kriptografski algoritmi i dužine ključeva opisani su u poglavlju 6.1.5. „Praktičnih pravila rada za pružanje usluge izdavanja kvalifikovanih elektronskih sertifikata u cloud-u“.

1.1.3.2. Povezivanje sa sredstvom za elektronsku identifikaciju

Načini za identifikaciju i autentikaciju korisnika detaljno su opisani u poglavlju 3. dokumenta „Praktična pravila rada za pružanje usluge izdavanja kvalifikovanih elektronskih sertifikata u cloud-u“. Autentikacioni podaci korisnika se generišu tokom instalacije mobilne aplikacije. Autentikacione podatke generiše korisnik.

Podaci za aktivaciju privatnog ključa korisnika se generišu na mobilnom uređaju korisnika, tokom procedure generisanja privatnih ključeva, kako je opisano u tački 3.2.1.5. ovog dokumenta.

1.1.3.3. Povezivanje sa sertifikatima

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

1.1.3.4. Obezbeđivanje sredstva za elektronsku identifikaciju

Autentikacioni podaci se generišu tokom instalacije mobilne aplikacije. Autentikacione podatke generiše korisnik.

1.1.3.5. Aktivacija potpisa/pečata

Aktivacioni podatak za udaljeni elektronski potpis/pečat predstavlja simetrični ključ AES256, koji se generiše na mobilnom uređaju korisnika tokom procedure generisanja ključeva za potpisivanje/pečaćenje. Aktivacioni podatak se čuva na mobilnom uređaju koisnika.

Korisnički privatni ključ se aktivira upotrebom aktivacionih podataka. Ovi aktivacioni podaci se dostavljaju SAM aplikaciji na bezbedan način, kroz protokol (Signature Activation Protocol – SAP) koji je definisan između aplikacije za potpisivanje/pečaćenje i SAM modula.

1.1.3.6. Uništavanje ključeva za potpisivanje

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

- istekao rok važnosti sertifikata korisnika,
- sertifikat korisnika opozvan,
- korisniku istekao ugovor o korišćenju usluge,
- korisnik to zahtevao ili je
- veza između korisnika i njegovog privatnog ključa prestala da postoji.

1.1.3.7. Bekap i oporavak ključeva za potpisivanje

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

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

3.2.2 Proces elektronskog potpisivanja/pečaćenja

PKSCA usluga upravljanja kvalifikovanim sredstvom za kreiranje elektronskih potpisa/pečata podržava izradu osnovnih elektronskih potpisa/pečata (Basic Signatures).

U kontekstu zakonodavstva Republike Srbije i Evropske unije, PKSCA usluga udaljenog potpisivanja podržava sledeće formate elektronskog potpisa i elektronskog pečata:

1. ETSI TS 103 171 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile
2. ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile
3. ETSI TS 103 173 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile

Postupak udaljenog elektronskog potpisivanja/pečaćenja sastoji se od sledećih koraka:

1. Korisnik se prijavljuje na web aplikaciju i selektuje dokument koji želi da potpiše elektronski.
2. Web aplikacija izračunava hash vrednost dokumenta i šalje je aplikaciji za kreiranje elektronskog potpisa/pečata. Sadržaj dokumenta ostaje u korisničkom browser-u, koji se pokreće na njegovom mobilnom uređaju i nikada ne napušta lokalno okruženje.
3. Aplikacija za kreiranje udaljenog elektronskog potpisa zahteva autorizacioni challenge od SAM modula.
4. SAM dostavlja autorizacioni challenge aplikaciji za kreiranje udaljenog elektronskog potpisa.
5. Aplikacija za kreiranje udaljenog elektronskog potpisa dostavlja autorizacioni zahtev korisniku preko Notification manager-a, na aplikaciju koja se izvršava na korisnikovom mobilnom uređaju.
6. Korisnik autorizuje transakciju i mobilna aplikacija šalje potpisan autorizacioni challenge aplikaciji za kreiranje udaljenog elektronskog potpisa.

7. Aplikacija za kreiranje udaljenog elektronskog potpisa prosleđuje potpisani autorizacioni challenge do SAM modula.
8. SAM verifikuje challenge i, ako je ispravan, autorizuje upotrebu korisničkog privatnog ključa za potpisivanje.
9. Aplikacija za kreiranje udaljenog elektronskog potpisa šalje pripremljene podatke za potpisivanje SAM-u.
10. SAM potpisuje pripremeljene podatke i rezultat vraća aplikaciji za kreiranje udaljenog elektronskog potpisa.
11. Aplikacija prima potpisanje podatke i kombinuje ih sa hash vrednošću dokumenta kako bi vratila rezultat potpisivanja web aplikaciji.
12. Web aplikacija pakuje potpisanu hash vrednost sa originalnim sadržajem dokumenta i omogućava da potpisani dokument bude dostupan korisniku.

ISTORIJAT DOKUMENTA

Verzija	Datum	Opis	Autor
1.0	25.10.2019.	Radna verzija	Dušan Berdić
2.0	25.12.2019	Finalna verzija	Dušan Berdić
3.0	23.10.2020	Izmene i dopune	Dušan Berdić
3.1	07.06.2021.	Finalna verzija	Jelena Radić

ODOBRENJE DOKUMENATA

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

PRIVREDNA KOMORA SRBIJE

mr Dušan Berdić

Sertifikaciono telo