Politika i praktična pravila rada

za pružanje kvalifikovane usluge validacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata

OID CPS dokumenta (1.3.6.1.4.1.31266.10.1.6)

- verzija 2.0.-

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

Politika i praktična pravila rada za pružanje kvalifikovane usluge validacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata

1. UVOD

Sertifikaciono telo Privredne komore Srbije (u nastavku: PKSCA), kao registrovani pružalac kvalifikovanih usluga od poverenja, vrši validaciju kvalifikovanih elektronskih potpisa, odnosno 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 validaciji kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata („Službeni glasnik RS", broj 43/19; u daljem tekstu - Pravilnik).

PKSCA pruža kvalifikovanu uslugu validacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata (u nastavku: usluga validacije) u skladu sa standardom ETSI TS 119 441 "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services", uključujući i zahteve drugih standarda na koje se iz pomenutog standarda direktno ili indirektno upućuje, odgovarajućim međunarodnim standardima i preporukama, odnosno drugim standardima, dokumentima i preporukama koje se odnose na pružanje usluge kvalifikovane validacije, 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 kvalifikovane usluge izdavanja kvalifikovanih sertifikata za elektronski potpis na smart karticama;
- ***PKS CA Cloud***, kao podređeno sertifikaciono telo za pružanje kvalifikovane usluge upravljanja kvalifikovanim sredstvom za kreiranje elektronskog potpisa odnosno pečata.
- ***PKS CA TSA,*** kao podređeno sertifikaciono telo za pružanje kvalifikovane usluge izdavanja kvalifikovanih vremenskih žigova.

U okviru ovako definisane hijerarhije, **PKS CA Class1** je sertifikaciono telo koje, osim izdavanja kvalifikovanih elektronskih sertifikata za kvalifikovani elektronski potpis na smart karticama, izdaje i sertifikat za jedinicu validacionog autoriteta (SVU – Signature Validation Unit).

PKSCA ovim dokumentom pod nazivom "Politika i praktična pravila rada za pružanje kvalifikovane usluge validacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata" (u daljem tekstu: Praktična pravila validacije) utvrđuje politiku i praktična pravila pružanja usluge validacije, u skladu sa Zakonom i Politikom pružanja kvalifikovanih usluga od poverenja PKSCA (u daljem tekstu: CP). Praktična pravila validacije 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 validacije 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, a 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 biće predmet 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 validacije dodelilo OID 1.3.6.1.4.1.31266.10.1.6

Struktura Praktičnih pravila validacije je usklađena sa Aneksom A standarda ETSI TS 119 441.

1.1.1. Učesnici

1.1.1.1. Pružalac usluge od poverenja

PKSCA je, kao pružalac kvalifikovanih usluga od poverenja, ujedno i pružalac usluga validacije kvalifikovanog elektronskog potpisa/pečata (Signature Validation Service Provider – SVSP).

Identifikacioni podaci PKSCA su:

PKSCA
Privredna Komora Srbije
Resavska 13-15
11000 Beograd
Srbija
e-mail:
web: http://v3.pksca.rs

1.1.1.2. Korisnici

Korisnici su fizička ili pravna lica, koja sa PKSCA zaključe Ugovor o korišćenju kvalifikovane usluge validacije kvalifikovanog elektronskog potpisa, odnosno 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 validacije kvalifikovanog elektronskog potpisa, odnosno 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 validacije definišu konkretne detalje implementacije, pravila i procedure rada PKSCA usluge validacije kvalifikovanih elektronskih potpisa odnosno kvalifikovanih elektronskih pečata.

Ovaj dokument se identifikuje na sledeći način:

- **Naziv:** Praktična pravila rada za pružanje kvalifikovane usluge validacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata
- **Verzija:** 2.0
- **OID:** 1.3.6.1.4.1.31266.10.1.6
- **Internet adresa na kojoj je dokument objavljen:** http://v3.pksca.rs

1.1.2.1. Podržana politika pružanja kvalifikovane usluge validacije – identifikacija usluge

Politika validacije kvalifikovanih elektronskih potpisa, odnosno pečata, u smislu skupa kriterijuma za proveru elektronskog potpisa ili pečata je identifikovana formalnim registrovanim identifikatorom objekta (OID) 1.3.6.1.4.1. 31266.10.2.3.1.0.5.1.

PKSCA će navedeni OID koristiti u svim izveštajima validacije koje izdaje korisnicima.

Detalji politike validacije dati su u poglavlju 3.1.5. ovih Praktičnih pravila validacije.

1.2. Komponente servisa za validaciju elektronskog potpisa/pečata

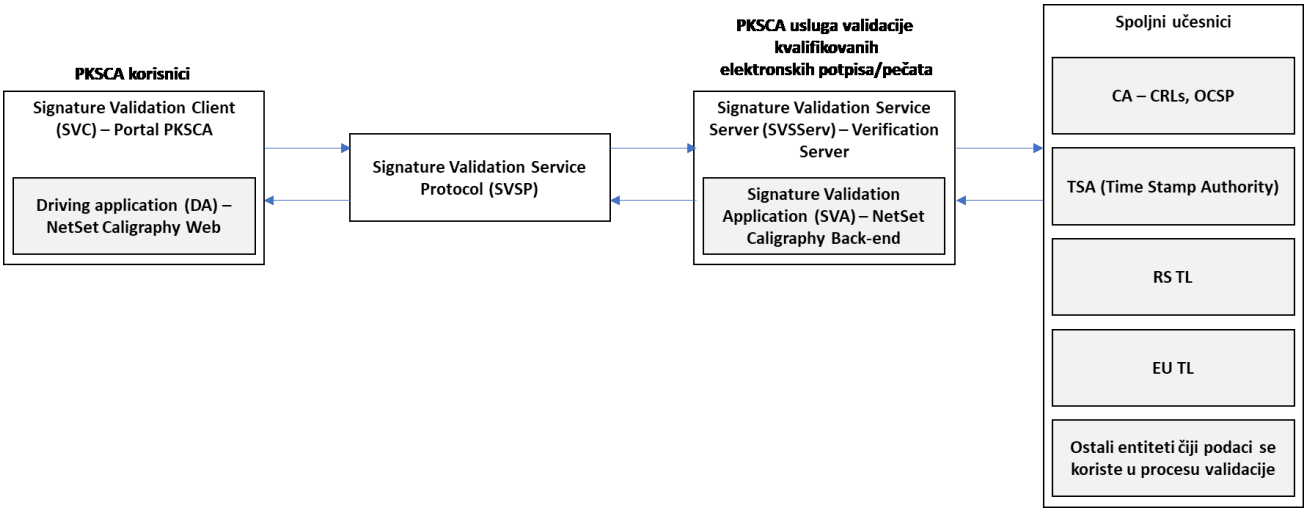
1.2.1. Akteri pružanja usluge validacije

Akteri u pružanju usluge validacije kvalifikovanih elektronskih potpisa/pečata su:

- **Portal PKSCA**, kao softverska komponenta koja obezbeđuje korisnički interfejs sa upravljačkom aplikacijom (Signature Validation Client – SVC).
- **NetSet Calligraphy Web**, kao upravljačka aplikacija koja obezbeđuje fukcionalnost validacije korisniku preko SVC (Driving Application – DA).
- **Protokol za validaciju**, koji predstavlja bezbedan komunikacioni kanal za razmenu informacija korisnika i servera za validaciju (Signature Validation Service Protocol – SVP)
- **Verifikacioni server**, kao komponenta koja implementira protokol validacije na strani pružaoca usluge validacije (Signature Validation Service Server – SVSServ)
- **NetSet Calligraphy Back-end**, kao aplikacija za validaciju, predstavlja softversku komponentu koja je odgovorna za validaciju potpisa/pečata, implementira validacioni algoritam i kreira izveštaj o validaciji (Signature Validation Application – SVA)
- **Eksterni učesnici** – Sertifikacioni autoriteti, time-stamping autoriteti, evropska i srpska lista poverenja, kao i ostali entiteti čiji se podaci koriste u procesu validacije elektronskog potpisa/pečata.

1.2.2. Arhitektura servisa za validaciju

Dijagram na slici 1. prikazuje simplifikovanu arhitekturu PKSCA usluge validacije kvalifikovanih elektronskih potpisa/pečata i učesnike u procesu validacije.



Slika 1. - Arhitektura usluge validacije

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:

Izveštaj validacije - izveštaj validacije je izveštaj koji aplikacija za validaciju isporučuje upravljačkoj aplikaciji i putem nje pouzdajućoj strani da bi se omogućio uvid u razloge iz kojih je proizašao odgovarajući status validacije.

Kriterijum validacije - tehnički kriterijum koji se proverava tokom validacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata.

Podaci za validaciju - podaci koji se koriste za validaciju elektronskog potpisa ili elektronskog pečata (kodovi ili javni kriptografski ključevi).

Politika validacije - Skup tehničkih kriterijuma za validaciju koji se proveravaju od strane aplikacije za validaciju, na osnovu kojih se odlučuje da li je elektronski potpis/pečat ispravan i na osnovu kojih se izrađuje izveštaj validacije.

Status validacije - je krajnji rezultat validacije koji proizvodi aplikacija za validaciju i koji vraća upravljačkoj aplikaciji.

1.3.2. Skraćenice

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

DA – Driving Application – Upravljačka aplikacija

PoE – Proof of Existence – Dokaz postojanja

SVSP - Signature Validation Service Provider – Pružalac usluga validacije kvalifikovanih elektronskih potpisa i kvalifikovanih elektronskih pečata

SVC – Signature Validation Client – Validacioni klijent

SVP – Signature Validation Protocol – Protokol za validaciju

SVA – Signature Validation Application – Aplikacija za validaciju

SVU – Signature Validation Unit – Jedinica validacionog autoriteta

SVSServ – Signature Validation Service Server – Validacioni server

VA – Validation Authority – Validacioni autoritet

1.4. Politike i prakse (procedure)

1.4.1. Organizacija zadužena za administriranje dokumentacije

PKSCA je odgovorno za izradu i administraciju dokumenta Praktična pravila validacije.

1.4.2. Kontakt osoba

Osoba u PKSCA, odgovorna za Praktična pravila validacije 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 validacije 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 validacije 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 validacije 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 validacije se revidira po potrebi, a najmanje jednom u toku kalendarske godine.

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 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 izdavanja kvalifikovanih sertifikata za PKSCA imaju iste obaveze i odgovornosti kao i stalno zaposleni.

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

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

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

Primarni produkcioni sistem PKSCA smešten je u zgradi PKS, u posebnom zaštićenom prostoru izdvojenom za tu namenu, uz primenu više nivoa fizičke i tehničke zaštite koje onemogućavaju neovlašćen fizički pristup sistemu i podacima i time sprečavaju kompromitovanje sistema i usluga. Fizička zaštita zasnovana je na konceptu upotrebe 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 validacije kvalifikovanih elektronskih potpisa, odnosno pečata, PKSCA vrši testiranja procesa validacije, funkcionalne logike, korisničkog interfejsa, bezbednosnih procedura itd. pre puštanja u rad, kao i prilikom svake izmene funkcionalnosti u softveru ili hardveru koji podržava proces validacije.

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.

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 ključeva PKSCA sertifikacionih tela,
- 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 sertifikaciona tela,
- 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 sa zapisima iz tačke 5.4.1. čuvaju se 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 nastojati da 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, Pravilnikom o validaciji kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata, Uredbom EU br. 910/2014 i tehničkim specifikacijama ETSI TS 119 441.

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.

3. DIZAJN SERVISA ZA VALIDACIJU

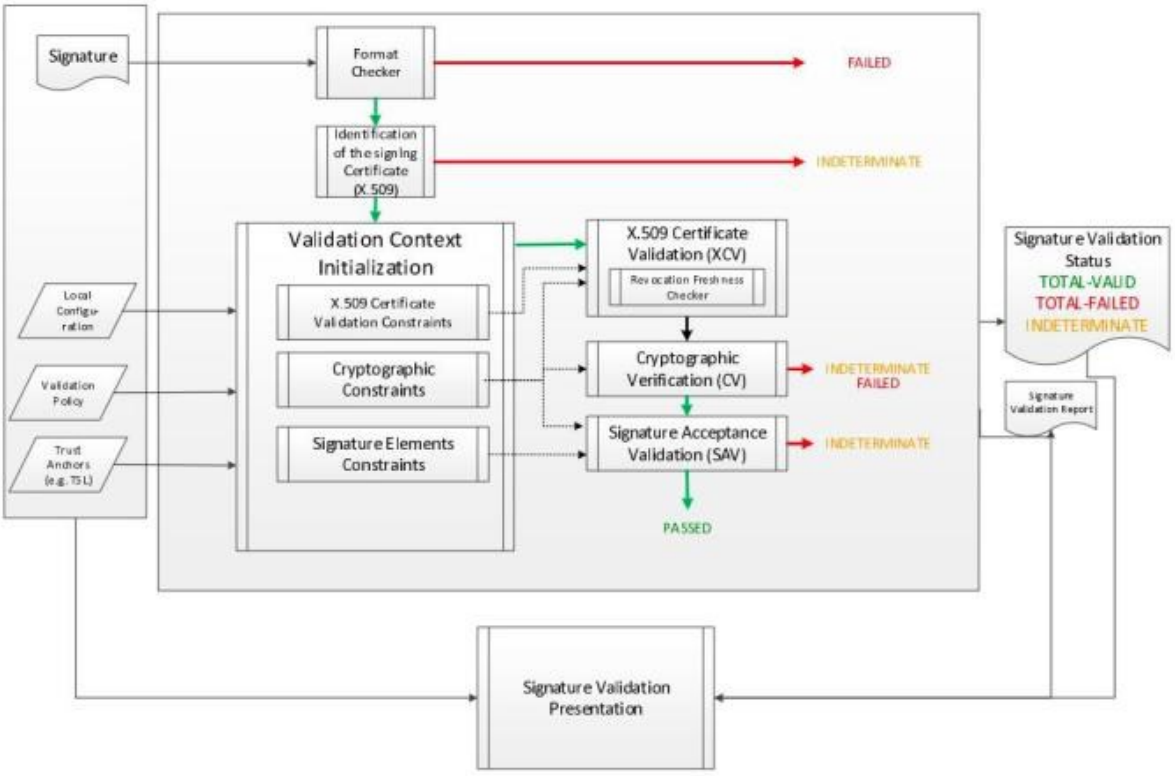
3.1. Zahtevi za proces validacije

PKSCA, kao pružalac usluge validacije kvalifikacionih elektronskih potpisa/pečata, koristi postupak utvrđivanja tehničke ispravnosti kvalifikovanog elektronskog potpisa ili elektronskog pečata koji je u skladu sa standardom ETSI TS 119 102-1 V1.2.1 (2018-08) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

Ovaj dokument u nastavku opisuje način na koji usluga validacije elektronskog potpisa i pečata sprovodi pojedine komponente postupka provere, kao i tehničke kriterijume koji se koriste prilikom procesa validacije elektronskih dokumenata.

3.1.2. Model provere validnosti kvalifikovanog elektronskog potpisa/pečata

Konceptualni model provere validnosti kvalifikovanog elektronskog potpisa/pečata prikazan je na slici 2. i u potpunosti je preuzet iz standara ETSI TS 119 102-1.



Slika 2. - Konceptualni model provere validnosti kvalifikovanog elektronskog potpisa/pečata

Konceptualni model prikazuje da se tokom validacionog procesa proveravaju: format elektronskog potpisa/pečata, sertifikat potpisnika, X.509 kriterijumi za validaciju sertifikata,

kriptografski kriterijumi i kriterijumi vezani za elemente potpisa/pečata. Na osnovu provere ovih kriterijuma aplikacija za validaciju prikazuje rezultat validacije i izdaje izveštaj o validaciji.

PKSCA usluga validacije kvalifikovanog elektronskog potpisa ili pečata istovremeno prihvata samo jednu datoteku za proveru validnosti, koja sadrži elektronske potpise/pečate i datoteke sa potpisanim sadržajem u sebi.

3.1.3. Status validacije i izveštaj o validaciji

PKSCA usluga validacije izdaje sveobuhvatni izveštaj o proveri validnosti kvalifikovanog elektronskog potpisa/pečata na elektronskom dokumentu. Aplikacija za validaciju, na osnovu kriterijuma validacije, detaljno proverava elektronski potpis/pečat i preko upravljačke aplikacije prezentuje izveštaj o validaciji, koji može biti u formi čitljive HTML stranice ili PDF dokumenta.

Izlazni izveštaj procesa provere validnosti potpisa / pečata sadrži:

- listu potpisa/pečata;
- status koji pokazuje rezultate postupka provere potpisa/pečata;
- neispunjeni kriterijumi na osnovu kojih je potpis/pečat nevalidan (TOTAL-FAILED) ili upozorenja koja opisuju zašto se nije mogao utvrditi status potpisa/pečata (INDETERMINATE);
- identifikaciona oznaka politike koju je potpis potvrdio;

Status provere validnosti kvalifikovanog elektronskog potpisa/pečata može imati jednu od tri vrednosti: USPEŠNO, NEODREĐENO i NEUSPEŠNO. Ove vrednosti odgovaraju vrednostima navedenim u standardu ETSI TS 119 102-1: TOTAL-PASSED, INDETERMINATE i TOTAL-FAILED respektivno.

Status validacije USPEŠNO znači da su sve kriptografke provere potpisa, odnosno pečata, kao i sve druge provere u skladu sa propisanim politikama i pravilima za validaciju.

Status validacije NEODREĐENO znači da nisu ispunjeni svi uslovi za status validacije USPEŠNO, s tim da postoji mogućnost da se steknu uslovi za status validacije USPEŠNO na osnovu dodatnih činjenica koje su se u postupku validacije smatrale nepoznatim.

Status validacije NEUSPEŠNO znači da nisu ispunjeni uslovi ni za status validacije USPEŠNO, ni za status validacije NEODREĐENO.

Struktura i semantika osnovnih statusa validacije data je u tabeli 1.

Indikator statusa	Semantika	Podaci izveštaja o proveri validnosti
USPEŠNO	Validacioni proces rezultuje statusom USPEŠNO (TOTAL-	Izlaz iz validacionog procesa su sertifikat za potpisivanje

(TOTAL-PASSED)	PASSED) ukoliko je ispunjeno sledeće: • kriptografka provera potpisa odnosno pečata je bila uspešna; • svi kriterijumi koji se odnose na proveru identiteta potpisnika pozitivno su potvrđeni; • potpis/pečat je pozitivno potvrđen u odnosu na kriterijume validacije.	korišćen u procesu, zajedno sa specifičnim potpisanim atributima, ukoliko su prisutni i razmatranim dokazima validacije.
NEUSPEŠNO (TOTAL-FAILED)	Validacioni proces rezultuje statusom TOTAL-FAILED ukoliko su kriptografske provere potpisa/pečata neuspešne ili može biti dokazano da je generisanje potpisa/pečata nastalo nakon opoziva sertifikata potpisnika ili pečatioca.	Izlaz iz validacionog procesa su dodatne informacije koje objašnjavaju status TOTAL-FAILED za svaki validacioni kriterijum za koji je rezultat provere negativan.
NEODREĐENO (INDETERMINATE)	Dostupne informacije nisu dovoljne da bi provera validnosti potpisa bila u statusu TOTAL-PASSED ili TOTAL-FAILED	Izlaz iz validacionog procesa su dodatne informacije koje objašnjavaju status INDETERMINATE i od pomoći su korisniku da identifikuje nedostajuće podatke neophodne da bi se validacija izvršila uspešno.

Tabela 1. – Struktura i semantika osnovnih statusa validacije

Pored osnovnih statusa, izveštaj o validaciji uključuje i sekundarnu indikaciju sa semantikom prikazanom u tabeli 2.

Osnovna indikacija	Subindikacija	Povezani podaci u validacionom izveštaju	Semantika
TOTAL_FAILED	FORMAT_FAILURE	The validation process shall provide any information	The signature is not conformant to one of the base standards to the extent that the

Osnovna indikacija	Subindikacija	Povezani podaci u validacionom izveštaju	Semantika
		available why parsing of the signature failed.	cryptographic verification building block is unable to process it.
	HASH_FAILURE	The validation process shall provide: An identifier (s) (e.g. an URI or OID) uniquely identifying the element within the signed data object (such as the signature attributes, or the SD) that caused the failure.	The signature validation process results into TOTAL-FAILED because at least one hash of a signed data object(s) that has been included in the signing process does not match the corresponding hash value in the signature.
	SIG_CRYPTO_ FAILURE	The validation process shall output: The signing certificate used in the validation process.	The signature validation process results into TOTAL-FAILED because the signature value in the signature could not be verified using the signer's public key in the signing certificate.
	REVOKED	The validation process shall provide the following:	The signature validation process results into TOTAL-FAILED because: • the signing certificate has been revoked; and

Osnovna indikacija	Subindikacija	Povezani podaci u validacionom izveštaju	Semantika
		• The certificate chain used in the validation process. • The time and, if available, the reason of revocation of the signing certificate.	• there is proof that the signature has been created after the revocation time.
	EXPIRED	The process shall output: The validated certificate chain	The signature validation process results into TOTAL-FAILED because there is proof that the ignature has been created after the expiration date (notAfter) of the signing certificate
	NOT_YET_VALID		The signature validation process results into TOTAL-FAILED because there is proof that the signature was created before the issuance date (notBefore) of the signing certificate.
INDETERMINATE	SIG_CONSTRAINTS_ FAILURE	The validation process shall provide: The set of constraints that	The signature validation process results into INDETERMINATE because one or more

Osnovna indikacija	Subindikacija	Povezani podaci u validacionom izveštaju	Semantika
		have not been met by the signature.	attributes of the signature do not match the validation constraints.
	CHAIN_CONSTRAINTS_ FAILURE	The validation process shall output: • The certificate chain used in the validation process. • The set of constraints that have not been met by the chain.	The signature validation process results into INDETERMINATE because the certificate chain used in the validation process does not match the validation constraints related to the certificate.
	CERTIFICATE_CHAIN_ GENERAL_FAILURE	The process shall output: Additional information regarding the reason	The signature validation process results into INDETERMINATE because the set of certificates available for chain validation produced an error for an unspecified reason.
	CRYPTO_CONSTRAINTS_ FAILURE	The process shall output: • Identification of the material (signature, certificate) that is produced using an algorithm or key size below the required	The signature validation process results into INDETERMINATE because at least one of the algorithms that have been used in material (e.g. the signature value, a certificate...) involved in validating the

Osnovna indikacija	Subindikacija	Povezani podaci u validacionom izveštaju	Semantika
		cryptographic security level. • If known, the time up to which the algorithm or key size were considered secure.	signature, or the size of a key used with such an algorithm, is below the required cryptographic security level, and: • this material was produced after the time up to which this algorithm/key was considered secure (if such a time is known); and • the material is not protected by a sufficiently strong time-stamp applied before the time up to which the algorithm/key was considered secure (if such a time is known).
	POLICY_PROCESSING_ ERROR	The validation process shall provide additional information on the problem.	The signature validation process results into INDETERMINATE because a given formal policy file could not be processed for any reason (e.g. not accessible, not parse-able, digest mismatch, etc.).

Osnovna indikacija	Subindikacija	Povezani podaci u validacionom izveštaju	Semantika
	SIGNATURE_POLICY_ NOT_AVAILABLE		The signature validation process results into INDETERMINATE because the electronic document containing the details of the policy is not available.
	TIMESTAMP_ORDER_ FAILURE	The validation process shall output the list of time-stamps that do no respect the ordering constraints.	The signature validation process results into INDETERMINATE because some constraints on the order of signature time-stamps and/or signed data object(s) time-stamps are not respected.
	NO_SIGNING_ CERTIFICATE_FOUND		The signature validation process results into INDETERMINATE because the signing certificate cannot be identified.
	NO_CERTIFICATE_ CHAIN_FOUND		The signature validation process results into INDETERMINATE because no certificate chain has been found for the identified signing certificate.

Osnovna indikacija	Subindikacija	Povezani podaci u validacionom izveštaju	Semantika
	REVOKED_NO_ POE	The validation process shall provide the following: • The certificate chain used in the validation process. • The time and the reason of revocation of the signing certificate.	The signature validation process results into INDETERMINATE because the signing certificate was revoked at the validation date/time. However, the Signature Validation Algorithm cannot ascertain that the signing time lies before or after the revocation time.
	REVOKED_CA_ NO_POE	The validation process shall provide the following: • The certificate chain which includes the revoked CA certificate. • The time and the reason of revocation of the certificate.	The signature validation process results into INDETERMINATE because at least one certificate chain was found but an intermediate CA certificate is revoked.
	OUT_OF_BOUNDS_ NOT_REVOKED		The signature validation process results into INDETERMINATE because the signing certificate is expired or not yet valid at the

Osnovna indikacija	Subindikacija	Povezani podaci u validacionom izveštaju	Semantika
			validation date/time and the Signature Validation Algorithm cannot ascertain that the signing time lies within the validity interval of the signing certificate. The certificate is known not to be revoked.
	OUT_OF_BOUNDS_ NO_POE		The signature validation process results into INDETERMINATE because the signing certificate is expired or not yet valid at the validation date/time and the Signature Validation Algorithm cannot ascertain that the signing time lies within the validity interval of the signing certificate.
	CRYPTO_CONSTRAINTS_ FAILURE_NO_POE	The process shall output: • Identification of the material (signature, certificate) that is produced using an algorithm or key size below the required	The signature validation process results into INDETERMINATE because at least one of the algorithms that have been used in objects (e.g. the signature value, a certificate, etc.) involved in validating

Osnovna indikacija	Subindikacija	Povezani podaci u validacionom izveštaju	Semantika
		cryptographic security level. If known, the time up to which the algorithm or key size were consider secure.	the signature, or the size of a key used with such an algorithm, is below the required cryptographic security level, and there is no proof that this material was produced before the time up to which this algorithm/key was considered secure.
	NO_POE	The validation process shall identify at least the signed objects for which the POEs are missing. • The validation process should provide additional informatio n on the problem.	The signature validation process results into INDETERMINATE because a proof of existence is missing to ascertain that a signed object has been produced before some compromising event (e.g. broken algorithm).
	TRY_LATER	The validation process shall output the point of time, where the necessary revocation information is expected to become available.	The signature validation process results into INDETERMINATE because not all constraints can be fulfilled using available information. However, it may be possible to do so using additional revocation

Osnovna indikacija	Subindikacija	Povezani podaci u validacionom izveštaju	Semantika
			information that will be available at a later point of time.
	SIGNED_DATA _NOT_FOUND	The process should output when available: The identifier(s) (e.g. an URI) of the signed data that caused the failure.	The signature validation process results into INDETERMINATE because signed data cannot be obtained.

Tabela 2. – Sekundarne indikacije procesa validacije

3.1.4. Proces validacije

PKSCA usluga validacije kvalifikovanih elektronskih potpisa/pečata podržava validaciju za osnovne elektronske potpise/pečate, potpise/pečate sa vremenskim žigom i potpise/pečate za pouzdano elektronsko čuvanje dokumenata.

U kontekstu zakonodavstva Republike Srbije i Evropske unije, PKSCA usluga validacije 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 provere validnosti kvalifikovanog elektronskog potpisa/pečata sprovodi se na sledeći način:

1. Usluga validacije sprovodi postupak validacije za sve elektronske potpise/pečate, nezavisno od njihovog nivoa;
2. Ukoliko je provera odabranim postupkom validacije vratila indikaciju PASSED, usluga dodeljuje statusu validacije vrednost TOTAL-PASSED;
3. Ukoliko je provera odabranim postupkom validacije vratila indikaciju NOT PASSED, usluga dodeljuje statusu validacije vrednost TOTAL-FAILED.
4. U suprotnom, usluga dodeljuje starusu validacije vrednost INDETERMINATE.

Proces validacije kvalifikovanih elektronskih potpisa/pečata na portalu PKSCA sastoji se od sledećih koraka:

1. Provera identiteta klijenta na portalu PKSCA i prijava na upravljačku aplikaciju (DA);
2. Korisnik bira dokument čiji će elektronski potpis/pečat biti validiran. DA računa hash vrednost selektovanog dokumenta i šalje ga aplikaciji za validaciju (SVA);
3. SVA verifikuje kriptografsku strukturu primljenog materijala i lanac sertifikata potpisnika;
4. SVA šalje serijski broj sertifikata potpisnika OCSP servisu, kako bi proverila njegov status;
5. OCSP komponenta vraća rezultat provere koji može biti: Good, Unknown i Revoked;
6. SVA učitava CRL;
7. SVA koristi serijski broj sertifikata da bi u listi povučenih sertifikata proverila da li je sertifikat potpisnika povučen;
8. SVA proverava u pulu sertifikata od poverenja da li se korenskom sertifikatu koji je potpisao sertifikat korisnika može verovati;
9. SVA određuje da li je korenski sertifikat od poverenja;
10. SVA konstruiše izveštaj o validaciji i vraća rezultat validacije DA.
11. DA prezentuje klijentu rezultat validacije i izveštaj o validaciji.

3.1.5. Politika validacije - kriterijumi za validaciju

PKSCA primenjuje politiku validacije kvalifikovanih elektronskih potpisa, odnosno kvalifikovanih elektronskih pečata koja je definisana ETSI politikom validacije označenom OID 0.4.0.19441.1.2 (itu-t(0) identified-organization(4) etsi(0) val-service-policies(19441) policy-identifiers(1) qualified (2)).

Usluga validacije ne prihvata više izvora validacione politike.

Strategija definisana u politici validacije sledi sledeće principe:

- Za isti ulaz, uključujući politiku provere validnosti, usluga validacije potpisa/pečata će vratiti isti izlaz.

- Sistem za proveru validnosti može za proveru potpisa prihvatiti različite elemente kao dokaz postojanja potpisa.

Kriterijumi na osnovu kojih PKSCA usluga validacije vrši proveru validnosti kvalifikovanih potpisa/pečata definisani su u kontrolnim podacima specifičnim za sistem, kao i samom implementacijom.

Svi kriterijumi za proveru u okviru usluge, koji se ne podrazumevaju implementacijom, potiču iz samog sadržaja potpisa (uključeno u atribute potpisa/pečata) ili indirektno, pozivanjem na spoljni dokument, dat u mašinski obradivom obliku. Dodatna kriterijumi mogu biti definisani preko parametara odabranih od strane aplikacije ili korisnika.

Opšti kriterijumi

PKSCA usluga provere validnosti kvalifikovanog elektronskog potpisa/pečata podržava maksimalnu veličinu datoteke dokumenata od 100 MB.

X.509 kriterijumi

PKSCA usluga provrere validosti kvalifikovanog elektronskog potpisa/pečata implementira X.509 kriterijume validacije, koja ukazuju na zahteve provere putanje sertifikata, kako je određeno tehničkim specifikacijama ETSI TS 119 172-1, klauzula A.4.2.1, tabela A.2, red m.

Kriterijum	Vrednost pri validaciji
m)1. X509CertificateValidationConstraints: This set of constraints indicates requirements for use in the certificate path validation process as defined in IETF RFC 5280. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows: (m)1.1. SetOfTrustAnchors: This constraint indicates a set of acceptable trust anchors (TAs) as a constraint for the validation process.	RS TL EU TL
(m)1.2. CertificationPath: This constraint indicates a certification path required to be used by the SVA for validation of the signature. The certificate path is of length 'n' from the trust anchor (TA) down to the certificate used in validating a signed object (e.g. the signer's certificate or a time stamping certificate). This constraint can	None

Kriterijum	Vrednost pri validaciji
include the path to be considered or indicate the need for considering the path provided in the signature if any. • (m)1.3. user-initial-policy-set: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (c) • (m)1.4. initial-policy-mapping-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (e) • (m)1.5. initial-explicit-policy: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (f) • (m)1.6. initial-any-policy-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (g) • (m)1.7. initial-permitted-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (h) • (m)1.8. initial-excluded-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (i) • (m)1.9. path-length-constraints: This constraint indicates restrictions on the number of CA certificates in a certification path. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it) • (m)1.10. policy-constraints: This constraint indicates requirements for certificate policies referenced in the certificates. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it). This should also allow the ability to require a (possible set of) specific certificate policy extension value(s) in end-	

Kriterijum	Vrednost pri validaciji
entity certificates (without requiring such values appearing in certificate of authorities in the certification path).	
(m)2. RevocationConstraints: This set of constraints indicates requirements applicable when verifying the certificate validity status of the certificates during the certificate path validation process. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows: (m)2.1. RevocationCheckingConstraints: This constraint indicates requirements for checking certificate revocation. Such constraints may specify if revocation checking is required or not and if OCSP responses or CRLs have to be used. Semantic for a possible set of requirement values used to express such requirements is defined as follows: • clrCheck: Checks shall be made against current CRLs (or Authority Revocation Lists); • ocspCheck: The revocation status shall be checked using OCSP IETF RFC 6960; • bothCheck: Both OCSP and CRL checks shall be carried out; • eitherCheck: Either OCSP or CRL checks shall be carried out; • noCheck: No check is mandated.	eitherCheck

Kriterijum	Vrednost pri validaciji
(m)2.2. RevocationFreshnessConstraints: This constraint indicates time requirements on revocation information. The constraints may indicate the maximum accepted difference between the issuance date of the revocation status information of a certificate and the time of validation or require the SVA to only accept revocation information issued a certain time after the signature has been created.	None
(m)2.3. RevocationInfoOnExpiredCerts: This constraint mandates the signer's certificate used in validating the signature to be issued by a certification authority that keeps revocation notices for revoked certificates even after they have expired for a period exceeding a given lower bound.	None
(m)3. LoAOnTSPPractices: This constraint indicates the required LoA on the practices implemented by the TSP(s) having issued the certificates to be validated during the certificate path validation process, i.e. the certificates present in the certificate path of the signer's certificate, and optionally those present in all or some of the other certificate chain.	None
EUQualifiedCertificateRequired	Yes
EUQualifiedCertificateSigRequired	Yes
EUQualifiedCertificateSealRequired	Yes
EUQSCDRequired 1	Yes if using QES validation policy, no if using AdES validation policy

Tabela 3. – X.509 kriterijumi validacije

Na osnovu Aneksa C iz ETSI 119 172-1 sledeći kriterijumi ukazuju na zahteve za specifične metapodatke sertifikata čija se semantička primena odnosi na kontekst zakonodavstva EU:

- EUQualifiedCertificateRequired: Ovo ograničenje ukazuje da je potrebno da sertifikat potpisnika, koji se koristi za validaciju potpisa, bude kvalifikovan elektronski sertifikat, kako je definisano u važećem zakonodavstvu EU;
- EUQualifiedCertificateSigRequired: Ovo ograničenje ukazuje na to da je potrebno da sertifikat potpisnika koji se koristi za proveru potpisa bude kvalifikovani sertifikat za elektronski potpis, kako je definisano u važećem zakonodavstvu EU;
- EUQualifiedCertificateSealRequired: Ovo ograničenje ukazuje da je potrebno da sertifikat potpisnika, koji se koristi za proveru elektronskog pečata bude kvalifikovani elektronski sertifikat za elektronski pečat, kako je definisano u važećem zakonodavstvu EU;
- EUQSCDRequired: Ovo ograničenje ukazuje da se sertifikat potpisnika, koji se koristi za proveru elektronskog potpisa, mora biti povezan sa privatnim ključem koji se čuva u QSCD uređaju, kao što je definisano u važećem zakonodavstvu EU;

Kriptografska ograničenja

PKSCA usluga za proveru validnosti kvalifikovanog elektronskog potpisa/pečata implementira kriptografska ograničenja koja ukazuju na zahteve vezane za algoritme i parametre koji se koriste prilikom kreiranja elektronskog potpisa/pečata, ili koji se koriste prilikom provere potpisanog objekta kako je navedeno u ETSI TS 119 172-1, klauzula A.4.2.1, tabela A.2 red p.

Kriterijum	Vrednost pri validaciji
(p)1. CryptographicSuitesConstraints: This constraint indicates requirements on algorithms and parameters used when creating signatures or used when validating signed objects included in the validation or augmenting process (e.g. signature, certificates, CRLs, OCSP responses, time-stamps). They will be typically be represented by a list of entries as in table A.3.	Based on ETSI TS 119 312

Tabela 4. – Kriptografska ograničenja

Kriterijumi vezani za elemente elektronskog potpisa i elektronskog pečata

PKSCA usluga za proveru validnosti kvalifikovanog elektronskog potpisa/pečata podržava kriterijume koji ukazuju na zahteve specificirane u ETSI TS 119 172-1 [ETSI, klauzula A.4.2.1, tabela A.2 red b.

Kriterijum	Vrednost pri validaciji
(b)1. ConstraintOnDTBS: This constraint indicates requirements on the type of the data to be signed by the signer.	None
(b)2. ContentRelatedConstraintsAsPartOfSignatureElements: This set of constraints indicate the required content related information elements under the form of signed or unsigned qualifying properties that are mandated to be present in the signature. This includes: (b)2.1 MandatedSignedQProperties-DataObjectFormat to require a specific format for the content being signed by the signer. (b)2.2 MandatedSignedQProperties-content-hints to require specific information that describes the innermost signed content of a multi-layer message where one content is encapsulated in another for the content being signed by the signer. (b)2.3 MandatedSignedQProperties-content-reference to require the incorporation of information on the way to link request and reply messages in an exchange between two parties, or the way such link has to be done, etc. (b)2.4 MandatedSignedQProperties-content-identifier to require the presence of, and optionally a specific value for, an identifier that can be used later on in the sig	None
(b)3. DOTBSAsAWholeOrInParts: This constraint indicates whether the whole data or only certain part(s) of it have to be signed. Semantic for a possible set of requirement values used to express such requirements is defined as follows: • whole: the whole data has to be signed; • parts: only certain part(s) of the data have to be signed. In this case, additional information should be used to express which parts have to be signed.	None

Tabela 5. – Kriterijumi vezani za elemente kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata

3.2. Protokol za proces validacije

Komunikacioni kanal između korisnika i sistema za proveru validnosti potpisa/pečata prenosi zahteve za proveru kvalifikovanog elektronskog potpisa/pečata u jednom smeru i vraća odgovor, u drugom. PKSCA koristi namenski protokol za uslugu provere validnosti elektronskog potpisa/ pečata koji se zasniva na zahtevima standarda ETSI EN 119 442.

Usluge provere kvalifikovanog elektronskog potpisa/pečata PKSCA dostupne su preko korisničkog interfejsa (PKSCA portal).

3.3. Interfejs

3.3.1. Komunikacioni kanal

Komunikacioni kanal između korisnika i sistema za proveru validnosti kvalifikovanog elektronskog potpisa/pečata obezbeđen je korišćenjem TLS bezbednosnog kanala. Sistem za proveru validnosti potpisa/pečata garantuje uspostavljanje bezbednog kanala i očuvanje poverljivosti i integriteta podataka korisnika.

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

3.3.2. Odnos sa drugim pružaocima usluga od poverenja

Na status verifikacije potpisa i izveštaj o proveri validnosti potpisa/pečata mogu da utiču prakse, politike i sporazumi o usaglašenosti sa drugim pružaocima usluga, koji su van kontrole sistema PKSCA. Ostali pružaoci usluga od poverenja mogu uključivati: autoritete za označavanje tačnog vremena, CRL i OCSP priužaoce usluga i druge pružaoce usluga od poverenja. PKSCA sistem za proveru validnosti potpisa/pečata garantuje status provere validnosti potpisa i izveštaja o proveri validnosti potpisa/pečata samo u vreme stvarne provere potpisa, odnosno pečata.

Komunikacioni kanali između PKSCA sistema za proveru validnosti i drugih TSP-a je izvan je okvira ovog dokumenta.

3.4. Zahtevi za izveštaj o validaciji kvalifikovanog elektronskog potpisa/pečata

PKSCA usluga provere validnosti kvalifikovanog elektronskog pečata/potpisa pruža tri vrste izveštaja o validaciji:

1. Jednostavan izveštaj o validaciji - pruža neophodne informacije u vezi sa identitetom potpisnika i indikacijom statusa validiranog potpisa, uključujući podindikaciju.

2. Detaljan izveštaj o validaciji - pruža izveštaj o svakom kriterijumu validacije koji se obrađuje, uključujući sve kriterijume validacije koji su implicitno primenjeni.
3. Izveštaj o validaciji koji je mašinski čitljiv - pruža detaljan izveštaj o proveri validnosti u formatu koji je mašinski čitljiv.

4. ISTORIJAT DOKUMENTA

Verzija	Datum	Opis	Autor
1.0	23.10.2018	Radna verzija	Dušan Berdić
2.0	07.06.2021.	Radna verzija	Jelena Radić

5. ODOBRENJE DOKUMENATA

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

PRIVREDNA KOMORA SRBIJE

mr Dušan Berdić

Sertifikaciono telo