Usluga izdavanja kvalifikovanih sertifikata za veb autentikaciju

Praktična pravila pružaoca
usluga od poverenja

(Certificate Practice Statement)

Verzija 1.0

SADRŽAJ

1 Uvod

Ovaj dokument je Izjava o praksi sertifikacije koja se odnosi na izdavanje kvalifikovanog sertifikata za za veb autentikaciju od strane sertifikacionog tela kojim upravlja kompanija Paperless d.o.o (u daljem tekstu: Paperless ili Pružalac usluga od poverenja).

Pružalac usluga od poverenja pruža svoje usluge svojim klijentima sa kojima ima ugovorni odnos.

Ova praktična pravila pružaoca usluga od poverenja opisuju okvir pružanja pomenutih usluga i uključuje detaljne procedure i različita operativna pravila. Pruža preporuke Pouzdanim stranama za verifikaciju elektronske identifikacije i sertifikata kreiranih korišćenjem usluga.

Praktična pravila pružaoca usluga od poverenja usaglašena su sa zahtevima postavljenim od strane eIDAS regulative[1].

Pružalac usluga od poverenja pruža najvažnije informacije klijentima i u obliku Izjave o obaveštenju. Izjava o obaveštenju biće objavljena kako je opisano u poglavlju 2.1.

1.1 Opis

Cilj praktičnih pravila pružaoca usluga od poverenja je da sumiraju sve informacije koje klijenti koji dolaze u kontakt sa Pružaocem usluga od poverenja treba da znaju. To ima za cilj da podstakne klijente i buduće klijente:

- Da se bolje upoznaju sa detaljima i zahtevima usluga koje pruža Pružalac usluga od poverenja, kao i sa praktičnom pozadinom pružanja usluga;
- Da bolje razumeju rad Pružaoca usluga od poverenja i tako lakše odluče da li usluge ispunjavaju ili koji tip usluga zadovoljava njihove individualne potrebe i očekivanja.

Pored toga, cilj ovog dokumenta je podrška korisnicima i trećim licima o statusu sertifikata koje izdaje Pružalac usluga od poverenja da jasno razumeju načine njihovog upravljanja, nivo sigurnosti koji garantuju kao i relevantne tehničke, komercijalne i finansijske garancije sa pravnom odgovornošću koje su s njima povezane.

Sadržaj i format ovog dokumenta usaglašeni su sa zahtevima okvira IETF RFC 3647 [2]. Sastoji se od 9 poglavlja koja sadrže sigurnosne zahteve, procese definisane od strane Pružaoca usluga od poverenja i prakse koje treba slediti tokom pružanja usluga. Da bi se strogo sačuvala struktura koju je odredio IETF RFC 3647, naslovi poglavlja gde nisu definisane odredbe imaju izjavu "Bez odredbe".

[1] Regulativa (EU) Broj 910/2014 Evropskog parlamenta i Saveta od 23. jula 2014. o elektronskoj identifikaciji i uslugama poverenja za elektronske transakcije u internom tržištu i ukidanje Direktive 1999/93/EC

[2] RFC 3647 - https://datatracker.ietf.org/doc/html/rfc3647

1.2 Naziv i identifikacija dokumenta

Ovaj dokument je skup praktičnih pravila pružaoca usluge od poverenja, čiji su glavni podaci za identifikaciju:

Izdavač:	Paperless d.o.o
Naziv dokumenta:	Praktična pravila za uslugu kvalifikovane veb autentikacije
OID:	1.3.6.1.4.1.61124.40.1.1.2
Verzija dokumenta:	1.0
Stupa na snagu od:	01.04.2024.

1.2.1 Polisa sertifikata

Svi sertifikati izdati od strane Paperless d.o.o trebalo bi da ukazuju na Praktična pravila na osnovu koje su izdati.

Prvih sedam brojeva OID-a koji identifikuje Praktična pravila je jedinstveni identifikator Paperless d.o.o, kao što sledi u nastavku: 1.3.6.1.4.1.**61124**

Usluga elektronske veb autentikacije, identifikovana je sufiksom koji prati jedinstveni identifikator pružaoca usluga od poverenja: 1.3.6.1.4.1.61124.**40**

Dalji brojevi unutar OID-a, odnosno sufiksi definisani su na sledeći način:

Sufiks	**Opis**
(1.3.6.1.4.1.61124)	Paperless d.o.o
(20)	Usluga elektronske veb autentikacije
(1)	Dokumentacija
(1)	Javna dokumentacija
(x)	Jedinstveni broj dokumenta

Usluga elektronske autentikacije se pruža u skladu sa ovim Praktičnim pravilima pružaoca usluga od poverenja koja su u skladu sa zahtevima Politike sertifikata u nastavku identifikovanim na sledeći način:

OID	Naziv dokumenta
1.3.6.1.4.1.61124.40.1.1.1	PAPERLESS – POLISA – Kvalifikovana usluga veb autentikacije

1.2.2 Efekat

Opseg subjekta Opseg subjekta

Praktična pravila pružaoca usluga od poverenja odnosi se na pružanje i korišćenje usluga opisanih u poglavlju 1.3.1.

Vremenski opseg

Trenutna verzija praktičnih pravila pružaoca usluga od poverenja važi od datuma stupanja na snagu (definisana u poglavlju 1.2), do povlačenja. Važenje automatski prestaje prestankom usluga ili izdavanjem nove verzije praktičnih pravila pružaoca usluga od poverenja.

Lični opseg

Efekat praktičnih pravila pružaoca usluga od poverenja se odnosi na svakog učesnika navedenog u poglavlju 1.3.

Pružalac usluga poverenja prvenstveno pruža usluge poverenja građanima Republike Srbija i pravnim entitetima registrovanim u Republici Srbiji, ali ne isključuje fizička ili pravna lica iz drugih zemalja sve dok prihvataju sistem pravila koje sledi pružalac usluga poverenja i kontrolu neophodnu za bezbedno i ekonomično pružanje usluga.

Osobe sa invaliditetom

Pružalac usluga poverenja nastoji da obezbedi pristup uslugama koje pruža kompanija najvišim mogućim standardima jednakih mogućnosti.

Kako bi se uspostavile jednake mogućnosti u vezi sa uslugom, pružalac usluga poverenja primenjuje svaku moguću i razumnu meru kako bi svoje usluge učinio dostupnim bez prepreka osobama sa invaliditetom. Posebno je važno obezbediti da osobe sa invaliditetom dobiju usluge prilagođene njihovim posebnim potrebama, istog kvaliteta kao i one za druge klijente.

Pružalac usluga poverenja sarađuje sa klijentima kako bi im garantovao administrativni proces koji je najprikladniji za njihove lične potrebe u okviru određenog okvira utvrđenog Izjavom o opštim pravilima rada pružaoca od poverenja.

Geografski opseg

Ppšta pravila rada pružaoca usluga od poverenja zasnovana na zahtevima Evropske unije uključuje specifične zahteve Republike Srbije za usluge koje funkcionišu u skladu sa Srpskim zakonom u Republici Srbiji.

Usluga pružena prema opštim pravilima rada pružaoca usluga od poverenja dostupna je širom sveta. Validnost sertifikata, liste statusa opoziva sertifikata i OCSP odgovora izdatih prema ovoim opštim pravilma rada pružaoca usluga od poverenja nezavisna je od geografske lokacije sa koje su zatraženi i gde će se koristiti.

Usluga pružena prema opštim pravilma rada pružaoca usluga od poverenja može se koristiti samo kako je opisano u ovim opštim pravilma rada pružaoca usluga od poverenja i u Polisi sertifikata.

1.3 PKI Učesnici (Subjekti)

1.3.1 Pružalac usluga od poverenja

Podaci Podaci o ružaocu usluga od poverenja

Pružalac usluga od poverenja Paperless d.o.o je pružalac usluga od poverenja koji izdaje i upravlja kvalifikovanim elektronskim sertifikatima za za veb autentikaciju i druge usluge.

Podaci o ružaocu usluga od poverenja

Naziv	Paperless d.o.o
Matični broj kompanije	21052019
Sedište	Admirala Vukovića 57
Telefonski broj	+381 11 2920 355
Internet adresa	https://paperless.rs

1.3.2 Registraciona tela

Pružalac usluga od poverenja Paperless d.o.o je ujedno i registraciono telo koje vrši sledeće aktivnosti za potrebe pružanja usluga od poverenja:

- provera identiteta fizičkih lica, pravnih lica, ovlašćenih lica pravnog lica i drugih, relevantnih podataka,
- prijem zahteva za dobijanje sertifikata,
- prijem zahteva za opozivanje/povlačenje sertifikata,
- izdavanje potrebne dokumentacije korisnicima, odnosno budućim korisnicima, kvalifikovanih elektronskih sertifikata,
- prosleđivanje zahteva i ostalih podataka sigurnim putem do pružaoca usluga od poverenja

Paperless d.o.o kao pružalac usluga od poverenja, pored svog registracionog tela može ovlastiti druge pravnog lica u poslovnom i javnom sektoru. Svaku takvu organizaciju pružalac usluga od poverenja Paperless d.o.o ugovorom obavezuje za ispunjavanje strogih bezbednosnih uslova u skladu sa važećim evropskim i nacionalnim propisima te međunarodnim, evropskim i nacionalnim standardima i preporukama, kao i internim pravilima Paperless d.o.o

1.3.3 Naručioci

Usluge koje pruža Pružalac usluga od poverenja klijentima:

- Naručilac
  - Zaključuje ugovor o pružanju usluge sa Pružaocem usluga od poverenja,
  - Prihvata opšte uslove i odredbe,
  - Definiše opseg predmeta,
  - Daje saglasnost za uključivanje organizacionih podataka u sertifikat,
  - Može imenovati organizacione administratore,
  - Odgovoran je za plaćanje naknada koje proizilaze iz korišćenja usluge.

- Subjekt
  - Pružalac usluga od poverenja izdaje sertifikat za subjekta.

- Potpisnik
  - Korisnik elektronske sertifikacije, koji može koristiti veb autentikaciju uz pomoć izdatog sertifikata.
  - Subjekt je Potpisnik.

Naručilac može biti isključivo pravno lice ili državni subjekt.

Usluga	**Izdavalac**	**Naručilac**	**Korisnik**
Sertifikati za pravne subjekte (veb-autentikacija)	Paperless d.o.o	Pravno lice	Fizičko lice
Sertifikati za državne subjekte (veb-autentikacija)	Paperless d.o.o	Državni subjekt	Fizičko lice

1.3.4 Treće Strane

Pouzdana strana nije nužno u ugovornom odnosu sa Pružaocem usluga od poverenja. Praktična pravila pružaoca i ostale navedene polise sadrže preporuke koje se odnose na njen rad.

Pružalac usluga od poverenja održava svoje kontakte sa pouzdanim stranama pretežno putem svoje veb stranice.

1.3.5 Ostali Učesnici

Nezavisni revizor koji vrši reviziju ocenjivanja usaglašenosti.

Nadzorni organ.

1.4 Upotreba Sertifikata

Paperless d.o.o upravlja (izdaje i overava, opoziva, obnavlja, čuva, objavljuje) kvalifikovanim elektronskim sertifikatima za za veb autentikaciju. Sertifikati su namenjeni isključivo pravnim licima i državnim subjektima.

1.4.1 Prikladna Upotreba Sertifikata

Privatni ključevi koji pripadaju sertifikatima krajnjeg korisnika izdatim od strane Pružaoca usluga od poverenja na osnovu ovog dokumenta o opštim pravilima rada pružaoca od poverenja mogu se koristiti samo za za veb autentikaciju ili - ako sertifikat za za veb autentikaciju to omogućava - autentifikaciju klijenta.

1.4.2 Nedozvoljena upotreba sertifikata

Zabranjeno je korišćenje kvalifikovanih elektronskih sertifikata, izdatih u skladu sa ovom politikom, u suprotnosti sa odredbama same politike pružanja usluge, ili važećih propisa, ili izvan opsega dozvoljenog korišćenja, određenog u prethodnom poglavlju.

Kvalifikovani elektronski sertifikati izdati od strane Paperless d.o.o nisu namenjeni daljoj prodaji.

1.5 Upravljanje dokumentima

1.5.1 Pravno lice koje administrira dokument

Podaci o organizaciji koja upravlja ovom Polisom usluge kvalifikovanog sertifikata za veb autentikaciju mogu se pronaći u sledećoj tabeli:

Naziv organizacije:	Paperless d.o.o.
Adresa organizacije:	Admirala Vukovića 57, Beograd
Broj telefona:	+381 11 2920 355
Fax:	+381 11 2920 355
Email adresa:	office@paperless.rs

1.5.2 Kontakt Osoba

Pitanja koja se odnose na ovu Polisu usluge kvalifikovanog sertifikata za za veb autentikaciju mogu se direktno postaviti sledećoj osobi:

Kontakt osoba:	Jovan Gruber
Naziv organizacije:	Paperless d.o.o.
Adresa organizacije:	Admirala Vukovića 57, Beograd
Broj telefona:	+381 11 2920 355
Fax:	+381 11 2920 355

Email adresa:	office@paperless.rs

1.5.3 Odgovorno lice za usklađenost dokumenta

Osoba odgovorna za usklađenost sa trenutnim opštim pravilima rada pružaoca i kvalifikovanom polisom sertifikata za za veb autentikaciju je:

Odgovorna osoba:	Jovan Gruber
Naziv organizacije:	Paperless d.o.o.
Adresa organizacije:	Admirala Vukovića 57, Beograd
Broj telefona:	+381 11 2920 355
Fax:	+381 11 2920 355
Email adresa:	office@paperless.rs

1.5.4 Procedure odobravanja praktičnih pravila

Svaki predlog novog izmenjenog dokumenta se razmatra sa tehnološkog i pravnog aspekta u cilju garantovanja zakonitosti, bezbednosti i kvaliteta. Pružalac usluga od poverenja može izdati ispravke kako je navedeno za svaku odredbu u poglavlju 9.12.1.

1.6 Definicije i Akronimi

1.6.1 Definicije

Data Centar	Objekat dizajniran za smeštaj i rad računarskih sistema i pripadajućih komponenti. Ove komponente obično uključuju telekomunikacione sisteme i veze, redundanto napajanje strujom, skladištenje podataka, klimatizaciju, zaštitu od požara i sigurnosne sisteme.
Subjekat	U slučaju sertifikata za autentifikaciju veb stranice, subjekt je veb server, koji je identifikovan domenskim imenom.
Jedinstveni identifikator subjekta	Jedinstveni identifikator subjekta je globalno jedinstveni identifikator koji dodeljuje Pružalac usluga od poverenja. Ovaj identifikator nalazi se u polju "DN subjekta / serijski broj" sertifikata, u skladu sa zahtevima odjeljka 3.1.1.
Sertifikat za automatizam	Sertifikat u kojem se ime IT uređaja (aplikacija, sistem) koji koristi Subjekat za korišćenje sertifikata beleži među podacima o subjektu.

Usluge poverenja	"Podrazumeva elektronsku uslugu obično pruženu uz nadoknadu koja se sastoji od: • kreiranja, verifikacije i validacije elektronskih potpisa, elektronskih pečata ili vremenskih žigova, elektronskih usluga registrovane dostave i sertifikata povezanih sa tim uslugama, ili • kreiranja, verifikacije i validacije sertifikata za autentifikaciju veb stranica; ili • čuvanja elektronskih potpisa, pečata ili sertifikata povezanih sa tim uslugama;"
Polisa usluga od poverenja	Skup pravila kojima Pružalac usluga od poverenja, pouzdana strana ili druga osoba zahteva uslove za korišćenje usluge poverenja za zajednicu pouzdanih strana i/ili klasu aplikacija sa zajedničkim bezbednosnim zahtevima.
Pružalac usluga od poverenja	Fizičko ili pravno lice koje pruža jednu ili više Usluga od poverenja, bilo kao kvalifikovani ili kao nekvalifikovani Pružalac usluga od poverenja.
Transparentnost sertifikata (CT) Pružalac evidencije (logova)	Pružalac evidencije (logova) Transparentnosti sertifikata (CT), definisan od strane Transparentnosti sertifikata [38], čuva izdate sertifikate i odgovarajuće pretvorene sertifikate.
Elektronski dokument	Elektronski dokument znači svaki sadržaj sačuvan u elektronskom obliku, posebno tekst ili zvuk, vizuelni ili audiovizuelni snimak.
Elektronski vremenski žig	Elektronski vremenski žig predstavlja podatke u elektronskom obliku koji povezuju druge podatke u elektronskom obliku sa određenim vremenom, osiguravajući dokaze da su ti drugi podaci postojali u tom trenutku.
Pretplatnik	Osoba ili organizacija koja potpisuje ugovor o pružanju usluga sa Pružaocem usluga od poverenja radi korišćenja nekih od njegovih usluga.
Predstavnik podnosioca zahteva	Predstavnik podnosioca zahteva je fizičko lice koje je ili Pretplatnik, zaposlen od strane Pretplatnika, ili ovlašćeni agent koji ima izričitu ovlašćenost da predstavlja Pretplatnika i koji ima ovlašćenje u ime Pretplatnika da prizna i saglasi se sa Opštim uslovima i odredbama.

Pre-sertifikat	Digitalno potpisana struktura podataka (PreCert) definisana od strane Transparentnosti sertifikata [38], koja sadrži podatke o subjektu koji će biti prikazani u sertifikatu koji će biti izdat.
Pouzdana strana	Ta komunicirajuća strana koja identifikuje veb server prilikom pristupa veb lokaciji na osnovu njenog sertifikata za za veb autentikaciju, nadalje, ti softverski dobavljači koji proizvode internet pretraživače ili aplikacije u kojima koriste sertifikat za za veb autentikaciju u svom radu.
Suspenzija	Privremena pauza važenja sertifikata pre isteka perioda važenja naznačenog na sertifikatu. Suspenzija sertifikata nije konačna; važenje suspendovanog sertifikata može biti obnovljeno.
Root sertifikat	Takođe poznat kao sertifikat na najvišem nivou. Samopotpisani sertifikat, koji izdaje određena sertifikaciona jedinica za sebe, koji je potpisan sopstvenim privatnim ključem, tako da može biti proveren sopstvenim javnim ključem - naznačenim na sertifikatu.
HSM: Modul za hardversku sigurnost	Hardverski sigurnosni modul (HSM) je uređaj zasnovan na hardveru koji generiše, čuva i štiti kriptografske ključeve i pruža sigurno okruženje za implementaciju kriptografskih funkcija.
Autoritet za sertifikaciju	Pružalac usluga od poverenja, koji identifikuje zahtevaoca unutar okvira sertifikacione usluge, izdaje sertifikate, vodi evidenciju, prima promene podataka vezanih za sertifikat, i objavljuje propise koji pripadaju sertifikatu i informacije o trenutnom stanju (posebno o mogućem opozivu) sertifikata.
Jedinica za sertifikaciju	Jedinica u sistemu Pružaoca usluga od poverenja koja potpisuje sertifikate. Uvek samo jedan skup podataka za kreiranje sertifikata (ključ za potpisivanje, podaci za kreiranje potpisa) pripada jedinici za sertifikaciju. Moguće je da Autoritet za sertifikaciju istovremeno koristi više jedinica za sertifikaciju.
Polisa sertifikata	Polisa sertifikata je polisa Pružaoca usluga od poverenja koja se odnosi na sertifikate izdatih u okviru usluge poverenja.
Specijalista za validaciju	Zaposleni u Sertifikacionoj Agenciji sa pouzdanim ulogom "Registrovani službenik", koji obavlja dužnosti provere informacija navedene u Osnovnim zahtevima CABF-a.
Podnosilac zahteva	To je fizičko lice koje deluje tokom procesa apliciranja za određeni sertifikat.

Dupla kontrola	Dupla kontrola je postupak koji koristi dve ili više odvojenih entiteta (osoba, procesa ili uređaja) koji zajednički deluju kako bi povećali pouzdanost postupka.
Organizacija koja se predstavlja	Organizacija koju predstavlja Administrativni rukovodilac organizacije tokom aktivnosti koje se odnose na sertifikate izdatim datoj organizaciji.
Kompromitovati	Kriptografski ključ se smatra kompromitovanim kada se može pretpostaviti da neovlašćena osoba ima pristup njemu.
Posrednička sertifikaciona jedinica	Jedinica za sertifikaciju čiji je sertifikat izdao drugi sertifikacioni organ.
Kriptografski ključ	Jedinstveni digitalni niz podataka koji kontroliše kriptografsku transformaciju, čije poznavanje je potrebno za enkripciju, dekripciju, kreiranje i verifikaciju elektronskih potpisa i pečata.
Upravljanje ključevima	Proizvodnja kriptografskih ključeva, njihova dostava korisnicima ili algoritamska implementacija, kao i registracija, čuvanje, arhiviranje, opoziv i prestanak korišćenja ključeva koji su usko povezani sa korišćenom metodom bezbednosti.
Privatni ključ	U infrastrukturi javnog ključa, element para ključeva asimetrične kriptografije koji pripada vlasniku para ključeva, a koji Podnosilac zahteva mora strogo čuvati u tajnosti. U slučaju autentifikacije veb servera, veb server će koristiti svoj privatni ključ tokom postupka autentifikacije. Tokom izdavanja sertifikata, Sertifikaciona Agencija koristi privatne ključeve Sertifikacione jedinice za postavljanje elektronskog potpisa ili pečata na sertifikat kako bi ga zaštitila.
Kvalifikovana usluga od poverenja	Usluga od poverenja koja ispunjava primenljive zahteve utvrđene Uredbom eIDAS
Kvalifikovani pružalac usluga od poverenja	Pružalac usluga od poverenja koji pruža jednu ili više kvalifikovanih usluga od poverenja i koji je dobio status kvalifikovanog od strane nadzornog tela.
Kvalifikovani sertifikat za za veb autentikaciju	Označava sertifikat za za veb autentikaciju, koji izdaje Kvalifikovani Pružalac Usluge Poverenja i ispunjava zahteve utvrđene u Prilogu IV eIDAS
Međunarodno prevedeno ime domena	Međunarodno prevedeno ime domena je internet domensko ime koje sadrži barem jednu oznaku koja se prikazuje u softverskim aplikacijama, u celosti ili delimično, u skriptu ili alfabetu specifičnom za određeni jezik, kao što je "ékezet.example.com". Međunarodno prevedena imena domena čuvaju se u Sistemu domenskih imena kao ASCII niske koristeći transkripciju u Punikodu.

Javni ključ	U infrastrukturi javnog ključa, element para ključeva asimetrične kriptografije koji pripada vlasniku para ključeva, a koji bi trebalo da bude javno dostupan. Otkrivanje se obično vrši u obliku sertifikata, koji povezuje ime subjekta sa njegovim javnim ključem. U slučaju autentifikacije veb servera, javni ključ veb servera je potreban za proveru njegove identifikacije. Autentičnost sertifikata može se proveriti pomoću javnog ključa Sertifikacione jedinice.
Infrastruktura javnih ključeva, PKI	Infrastruktura zasnovana na asimetričnoj kriptografiji, uključujući kriptografske algoritme, ključeve, sertifikate, povezane standarde i zakonodavstvo, osnovni institucionalni sistem, različite pružaoce usluga i uređaje.
Otvoreno bankarstvo	Regulisano okruženje za usluge plaćanja van obuhvata EU PSD2 ali koje funkcioniše na osnovu identičnih ili veoma sličnih zahteva.
Registraciona tvrdnja	Podaci i izjava dati unapred radi pripreme aplikacije za sertifikat i ugovora o usluzi Trust Service Providera od strane klijenta, u kojem klijent autorizuje Trust Service Providera za upravljanje podacima.
Registrovano telo	Organizacija koja proverava autentičnost podataka nosioca sertifikata i potvrđuje da je aplikacija za sertifikat autentična, i da ju je podneo ovlašćeno lice.
Neobična operativna situacija	Neobična situacija koja uzrokuje poremećaj u toku rada pružaoca usluga od poverenja, kada nastavak normalnog rada pružaoca usluga od poverenja nije moguć ni privremeno ni trajno.
SCT - Potpisano vremensko obeležje sertifikata	Digitalno potpisani odgovor (vremensko obeležje potpisanog sertifikata) koji šalje pružalac evidencije (logova) Transparentnosti sertifikata tokom objavljivanja sertifikata i odgovarajućeg pretvorenog sertifikata, što dokazuje uključivanje sertifikata i odgovarajućeg pretvorenog sertifikata u datu evidenciju (log).
Organizacija	Pravno lice.
Organizacioni sertifikat	Sertifikat koji sadrži naziv organizacije. U ovom slučaju, naziv organizacije je naznačen u polju "O" (Organization) sertifikata.

Organizacioni administrator	Prirodno lice koje deluje u ime Pretplatnika, i u slučaju posebne autorizacije definitivno za EV sertifikate ima ovlašćenje da izda Zahtev za sertifikat, odobri izdavanje sertifikata, da deluje tokom zahteva, zamene i opoziva sertifikata izdatih Pretplatniku.
Izjava o praksi usluge poverenja	Dokument koji detaljno opisuje procedure ili druge operativne zahteve korišćene u vezi sa pružanjem određenih usluga poverenja od strane Trust Service Provider-a.
Ugovor o pružanju usluge	Ugovor između pružaoca usluga od poverenja i klijenta usluge od poverenja, koji obuhvata uslove za pružanje usluge od poverenja i korišćenje tih usluga.
Sertifikat	Sertifikat za elektronski potpis, sertifikat za elektronski pečat i Sertifikat za autentifikaciju veb stranice, zajedno sa svim elektronskim verifikacijama izdatim unutar okvira usluge od poverenja od strane pružaoca usluge. Obuhvataju podatke o verifikaciji vezane za sertifikat i informacije o upotrebi sertifikata. Ovi elektronski dokumenti su pouzdano zaštićeni od dostupnih tehnologija falsifikovanja kako u trenutku izdavanja, tako i tokom njihovog perioda važenja.
Zahtevač sertifikata	Zahtevač sertifikata je fizičko lice koje je ili Pretplatnik, zaposlen od strane Pretplatnika, ovlašćeni agent koji ima izričitu ovlašćenost da predstavlja Pretplatnika, ili treća strana koja popunjava i podnosi Zahtev za EV sertifikat u ime Pretplatnika.
Odobravatelj sertifikata	Odobravatelj sertifikata je fizičko lice koje je ili Pretplatnik, zaposlen od strane Pretplatnika, ili ovlašćeni agent koji ima izričitu ovlašćenost da predstavlja Pretplatnika i koji može: (i) delovati kao Zahtevač sertifikata i ovlastiti druge zaposlene ili treće strane da deluju kao Zahtevači sertifikata, i (ii) odobriti Zahteve za EV sertifikat koji su podneli drugi Zahtevači sertifikata.
Primena Sertifikata	Podaci i izjave koje je podnosilac zahteva dao Pružaocu usluga od poverenja radi izdavanja sertifikata, u kojima podnosilac zahteva potvrđuje autentičnost podataka koji će biti navedeni u sertifikatu.
Repozitorijum sertifikata	Repozitorijum podataka koji sadrži različite sertifikate. Sertifikaciona Agencija ima Repozitorijum sertifikata u kojem su objavljeni sertifikati, ali sistem koji sadrži sertifikate dostupne aplikaciji na računaru Pouzdane Strane takođe se naziva Repozitorijum sertifikata.

Klijent	Zajednički termin za pretplatnika i svaki povezani termin za aplikanta.
Opoziv	Opoziv je prekid važnosti sertifikata pre isteka perioda važnosti naznačenog na sertifikatu. Opoziv sertifikata je trajan, opozvani sertifikat više ne može biti obnovljen.
Zapisi o statusu opoziva	Unutrašnji zapisi o suspendovanim i opozvanim sertifikatima koji uključuju činjenicu suspendovanja ili opoziva i vreme suspendovanja ili opoziva izraženo u sekundama koje održava Sertifikaciono telo.
Sertifikat za autentifikaciju veb stranice	"Sertifikat za autentifikaciju veb stranice predstavlja potvrdu koja omogućava autentifikaciju veb lokacije i povezuje veb lokaciju sa fizičkim ili pravnim licem kojem je sertifikat izdat." Ime domena veb servera naznačeno je u polju imena sertifikata za autentifikaciju veb stranice.
Zamensko ime domena	String koji počinje sa "*." (U+002A ZVEZDICA, U+002E TAČKA) odmah za kojom sledi Potpuno Kvalifikovano Ime Domena.
Zamenski sertifikat	Sertifikat za autentifikaciju veb stranice koji sadrži barem jedno zamensko ime domena u "Alternativnim imenima subjekta" u sertifikatu.
LDH-oznaka	Niska koja se sastoji od ASCII slova, cifara i crte sa dodatnim ograničenjem da crta ne može da se pojavi na početku ili kraju niske. Kao i sve DNS oznake, njena ukupna dužina ne sme premašiti 63 okteta.
P-oznaka	XN-oznaka koja sadrži validan izlaz algoritma Punikod (kako je definisano u RFC 3492, Sekcija 6.3) počevši od petog položaja i dalje.
XN-oznaka	Klasa oznaka koje počinju sa prefiksom "xn–" (bez obzira na veličinu slova), ali inače se pridržavaju pravila za LDH oznake.
Centar Podataka	Objekat dizajniran za smeštaj i rad računarskih sistema i pripadajućih komponenti. Ove komponente obično uključuju telekomunikacione sisteme i veze, redundanto napajanje strujom, skladištenje podataka, klimatizaciju, zaštitu od požara i sigurnosne sisteme.
Subjekat	Pravno lice čiji su identitet ili atribut verifikovani od strane Pružaoca usluga od poverenja putem sertifikata.

Jedinstveni identifikator subjekta	Globalno jedinstveni identifikator subjekta, dodeljen od strane Pružaoca usluga poverenja. Identifikator se nalazi u polju "DN subjekta / serijski broj" sertifikata, prema zahtevima odeljka 3.1.1.
Sertifikat za automatizam	Sertifikat u kojem se navodi naziv IT uređaja (aplikacije, sistema) koji Subjekat primenjuje za korišćenje. Sertifikat se evidentira među podacima o subjektu.
Kreator pečata	Pravno lice koje kreira elektronski pečat.
Usluge poverenja	"Podrazumeva elektronsku uslugu obično pruženu uz nadoknadu koja se sastoji od: • kreiranja, verifikacije i validacije elektronskih potpisa, elektronskih pečata ili vremenskih žigova, elektronskih usluga registrovane dostave i sertifikata povezanih sa tim uslugama, ili • kreiranja, verifikacije i validacije sertifikata za autentifikaciju veb stranica; ili • čuvanja elektronskih potpisa, pečata ili sertifikata povezanih sa tim uslugama;"
Polisa usluga od poverenja	Skup pravila kojima Pružalac usluga od poverenja, pouzdana strana ili druga osoba zahteva uslove za korišćenje usluge poverenja za zajednicu pouzdanih strana i/ili klasu aplikacija sa zajedničkim bezbednosnim zahtevima.
Pružalac usluga od poverenja	Fizičko ili pravno lice koje pruža jednu ili više Usluga od poverenja, bilo kao kvalifikovani ili kao nekvalifikovani Pružalac usluga od poverenja.
Elektronski pečat	Podaci u elektronskom obliku koji su priloženi ili logički povezani s drugim podacima u elektronskom obliku kako bi se osigurali poreklo i integritet.
Sertifikat za elektronski pečat	Elektronska potvrda koja povezuje podatke o validaciji elektronskog pečata sa pravnom osobom i potvrđuje ime te osobe.
Kvalifikovani sertifikat za elektronski pečat	Sertifikat za elektronski pečat izdat od strane Kvalifikovanog Pružaoca Usluge Poverenja i ispunjava zahteve navedene u Prilogu III eIDAS [1].
Podaci za kreiranje elektronskog pečata	Ovo je jedinstveni podatak koji kreator elektronskog pečata koristi kako bi kreirao elektronski pečat. Obično je to kriptografski privatni ključ.

Uređaj za kreiranje elektronskog pečata	To je konfigurisani softver ili hardver koji se koristi za kreiranje elektronskog pečata.
Elektronski dokument	Elektronski dokument znači svaki sadržaj sačuvan u elektronskom obliku, posebno tekst ili zvuk, vizuelni ili audiovizuelni snimak.
Elektronski vremenski žig	Elektronski vremenski žig predstavlja podatke u elektronskom obliku koji povezuju druge podatke u elektronskom obliku sa određenim vremenom, osiguravajući dokaze da su ti drugi podaci postojali u tom trenutku.
Elektronski pečat za elektronsku upravu	Najmanje elektronski pečat na naprednom nivou može se koristiti od strane organa koji pružaju usluge elektronske uprave, a koji ispunjavaju zahteve Uredbe o elektronskom potpisu [12] 7. § b) i c) tačka.
Pretplatnik	Osoba ili organizacija koja potpisuje ugovor o pružanju usluga sa Pružaocem usluga od poverenja radi korišćenja nekih od njegovih usluga.
Sertifikat za elektronsku poštu	Sertifikat koji se pridržava S/MIME standarda i može se koristiti za enkripciju elektronske pošte i obezbeđivanje integriteta sadržaja u internet baziranim sistemima elektronske pošte.
Pouzdana strana	Primalac elektronskog dokumenta, koji postupa oslanjajući se na elektronski pečat zasnovan na datom sertifikatu.
Validacija	Validacija znači proces provere i potvrde da li je elektronski potpis ili pečat validan.
Lanac validacije	Lanac validacije je niz informacija koji se međusobno povezuju kako bi se potvrdila validnost naprednog ili kvalifikovanog elektronskog potpisa, pečata ili vremenskog žiga na elektronskom dokumentu. Ovaj lanac obično uključuje informacije o sertifikatima, statusu sertifikata, podacima korišćenim za kreiranje potpisa ili pečata, kao i informacije o njihovom opozivu i važenju, omogućavajući potvrdu validnosti potpisa u datom trenutku.
Validacioni podaci	Validacioni podaci su podaci koji se koriste za validaciju elektronskog potpisa ili elektronskog pečata.

Suspenzija	Privremena pauza važenja sertifikata pre isteka perioda važenja naznačenog na sertifikatu. Suspenzija sertifikata nije konačna; važenje suspendovanog sertifikata može biti obnovljeno.
Napredni elektronski pečat	To je napredni elektronski pečat koji ispunjava sledeće zahteve: a) jedinstveno je povezan sa kreatorom pečata; b) sposoban je da identifikuje kreatorom pečata; c) kreiran je korišćenjem podataka za kreiranje elektronskog pečata koje tvorac pečata može, s visokim stepenom pouzdanosti, kontrolisati i koristiti za kreiranje elektronskog pečata; i d) on je povezan sa podacima na koje se odnosi na način koji omogućava otkrivanje bilo kakve naknadne promene u podacima.
Root sertifikat	Root sertifikat, poznat i kao sertifikat najvišeg nivoa, je sertifikat koji se samopotpisuje, tj. izdaje ga određena jedinica za sertifikaciju (Certification Unit) za sebe, potpisan je sopstvenim privatnim ključem, tako da se može proveriti sa sopstvenim javnim ključem - koji je naznačen na sertifikatu.
HSM: Modul za hardversku sigurnost	Hardverski sigurnosni modul (HSM) je uređaj zasnovan na hardveru koji generiše, čuva i štiti kriptografske ključeve i pruža sigurno okruženje za implementaciju kriptografskih funkcija.
Autoritet za sertifikaciju	Pružalac usluga od poverenja, koji identifikuje zahtevaoca u okviru usluge sertifikacije, izdaje sertifikate, vodi evidenciju, prima promene podataka vezane za sertifikate i objavljuje propise koji se odnose na sertifikat i informacije o trenutnom stanju (posebno o mogućem povlačenju) sertifikata.
Jedinica za sertifikaciju	Jedinica u sistemu Pružaoca usluga od poverenja koja potpisuje sertifikate. Uvek samo jedan skup podataka za kreiranje sertifikata (ključ za potpisivanje, podaci za kreiranje potpisa) pripada jedinici za sertifikaciju. Moguće je da Autoritet za sertifikaciju istovremeno koristi više jedinica za sertifikaciju.
Polisa sertifikata	Polisa sertifikata je polisa Pružaoca usluga od poverenja koja se odnosi na sertifikate izdatih u okviru usluge poverenja.
Podnosilac zahteva	To je fizičko lice koje deluje tokom procesa apliciranja za određeni sertifikat.
Dupla kontrola	Dupla kontrola je postupak koji koristi dve ili više odvojenih entiteta (osoba, procesa ili uređaja) koji zajednički deluju kako bi povećali pouzdanost postupka.

Organizacija koja se predstavlja	Organizacija koju predstavlja Administrativni rukovodilac organizacije tokom aktivnosti koje se odnose na sertifikate izdatim datoj organizaciji.
Kompromitovati	Kriptografski ključ se smatra kompromitovanim kada se može pretpostaviti da neovlašćena osoba ima pristup njemu.
Root CA za javnu upravu	Jedinica organizacije definisana je u uredbi o elektronskom potpisu [12] u odjeljku 3. § (2).
Elektronski pečat za javnu upravu	Najmanje napredan nivo elektronskog pečata može se koristiti od strane državnih organa koji pružaju usluge elektronske uprave, koji ispunjava zahteve Uredbe o elektronskom potpisu [12] član 7. a), b) i c) tačka.
Posrednička sertifikaciona jedinica	Jedinica za sertifikaciju čiji je sertifikat izdao drugi sertifikacioni organ.
Kriptografski ključ	Jedinstveni digitalni niz podataka koji kontroliše kriptografsku transformaciju, čije poznavanje je potrebno za enkripciju, dekripciju, kreiranje i verifikaciju elektronskih potpisa i pečata.
Upravljanje ključevima	Proizvodnja kriptografskih ključeva, njihova dostava korisnicima ili algoritamska implementacija, kao i registracija, čuvanje, arhiviranje, opoziv i prestanak korišćenja ključeva koji su usko povezani sa korišćenom metodom bezbednosti.
Heš	Heš funkcija je matematička funkcija koja pretvara numeričku ulaznu vrednost u drugu komprimovanu numeričku vrednost. Ulaz u heš funkciju je proizvoljne dužine, ali je izlaz uvek fiksne dužine. Heš u praksi predstavlja niz bitova fiksne dužine koji jasno zavisi od elektronskog dokumenta iz kojeg je izveden, sa veoma malom verovatnoćom da bi dva različita dokumenta imala isti heš, i praktično je nemoguće na osnovu heša pripremiti dokument koji ima isti heš.
Privatni ključ	U infrastrukturi javnih ključeva, element para ključeva asimetrične kriptografije koji pripada vlasniku para ključeva, a koji Subjekt mora strogo čuvati tajnom. U slučaju elektronskih pečata, kreator elektronskog pečata generiše pečat uz pomoć privatnog ključa. Prilikom izdavanja sertifikata, sertifikaciono telo koristi privatne ključeve sertifikacione jedinice za postavljanje elektronskog potpisa ili pečata na sertifikat kako bi ga zaštitilo.
Kvalifikovana usluga od poverenja	Usluga od poverenja koja ispunjava primenljive zahteve utvrđene Uredbom eIDAS

Kvalifikovani pružalac usluga od poverenja	Pružalac usluga od poverenja koji pruža jednu ili više kvalifikovanih usluga od poverenja i koji je dobio status kvalifikovanog od strane nadzornog tela.
Kvalifikovani elektronski pečat	Napredni elektronski pečat, koji je kreiran pomoću kvalifikovanog uređaja za kreiranje elektronskih pečata, i koji se zasniva na kvalifikovanom sertifikatu za elektronski pečat.
Javni ključ	U infrastrukturi javnih ključeva, javni ključ je element para asimetričnih kriptografskih ključeva koji pripada vlasniku para ključeva i treba da bude javno dostupan. Otkrivanje se obično vrši u obliku sertifikata, koji povezuje ime subjekta sa njegovim javnim ključem. U slučaju elektronskog pečata, javni ključ lica koji kreira pečat potreban je za proveru autentičnosti pečata (ovo je podatak o proveri sertifikata). Autentičnost sertifikata može se proveriti pomoću javnog ključa Sertifikacione jedinice.
Infrastruktura javnih ključeva, PKI	Infrastruktura zasnovana na asimetričnoj kriptografiji, uključujući kriptografske algoritme, ključeve, sertifikate, povezane standarde i zakonodavstvo, osnovni institucionalni sistem, različite pružaoce usluga i uređaje.
Otvoreno bankarstvo	Regulisano okruženje za pružanje usluga plaćanja van opsega EU PSD2, ali koje funkcioniše na osnovu identičnih ili vrlo sličnih zahteva.
Registraciona tvrdnja	Podaci i izjava dati unapred radi pripreme aplikacije za sertifikat i ugovora o usluzi Trust Service Providera od strane klijenta, u kojem klijent autorizuje Trust Service Providera za upravljanje podacima.
Registrovano telo	Organizacija koja proverava autentičnost podataka nosioca sertifikata i potvrđuje da je aplikacija za sertifikat autentična, i da ju je podneo ovlašćeno lice.
Neobična operativna situacija	Neobična situacija koja uzrokuje poremećaj u toku rada pružaoca usluga od poverenja, kada nastavak normalnog rada pružaoca usluga od poverenja nije moguć ni privremeno ni trajno.
Organizacija	Pravno lice.

Organizacioni sertifikat	Organizacioni sertifikat je dokument koji identifikuje organizaciju kao subjekta u vezi sa digitalnim potpisom ili enkripcijom. Ovaj sertifikat može takođe potvrditi da određeno fizičko lice pripada toj organizaciji. U njemu se obično nalazi naziv organizacije u posebnom polju sertifikata. Svaki pečatni sertifikat je organizacioni sertifikat.
Organizacioni administrator	Organizacioni administrator je osoba koja ima odgovornost za upravljanje administrativnim poslovima ili pravilima unutar organizacije. Ova osoba obično ima ovlašćenja za donošenje odluka i implementaciju pravila koja se odnose na organizacione procese, kao i za upravljanje korisnicima i njihovim pravima unutar sistema ili infrastrukture organizacije.
Izjava o praksi usluge poverenja	Dokument koji detaljno opisuje procedure ili druge operativne zahteve korišćene u vezi sa pružanjem određenih usluga poverenja od strane Trust Service Provider-a.
Ugovor o pružanju usluge	Ugovor između pružaoca usluga od poverenja i klijenta usluge od poverenja, koji obuhvata uslove za pružanje usluge od poverenja i korišćenje tih usluga.
Sertifikat	Sertifikat za elektronski potpis, sertifikat za elektronski pečat i Sertifikat za autentifikaciju veb stranice, zajedno sa svim elektronskim verifikacijama izdatim unutar okvira usluge od poverenja od strane pružaoca usluge. Obuhvataju podatke o verifikaciji vezane za sertifikat i informacije o upotrebi sertifikata. Ovi elektronski dokumenti su pouzdano zaštićeni od dostupnih tehnologija falsifikovanja kako u trenutku izdavanja, tako i tokom njihovog perioda važenja.
Primena Sertifikata	Podaci i izjave koje je podnosilac zahteva dao Pružaocu usluga od poverenja radi izdavanja sertifikata, u kojima podnosilac zahteva potvrđuje autentičnost podataka koji će biti navedeni u sertifikatu.
Repozitorijum sertifikata	Repozitorijum podataka koji sadrži različite sertifikate. Sertifikaciono telo ima repozitorijum sertifikata u kojem su prikazani izdati sertifikati, ali sistem koji sadrži sertifikate dostupne aplikaciji na računaru Korisnika i Strane koja se oslanja takođe se naziva repozitorijumom sertifikata.
Usluga daljinskog upravljanja ključevima	Usluga poverenja u kojoj pružalac usluga upravlja privatnim ključevima korisnika pod sigurnim uslovima, obezbeđuje neophodne tehničke i proceduralne uslove kako bi korisnici mogli da obavljaju udaljene operacije ključevima sa svojim privatnim ključevima smeštenim kod pružaoca usluga, kao što su kreiranje elektronskih potpisa ili elektronskih pečata.
Klijent	Zajednički termin za pretplatnika i svaku povezanu denominaciju aplikanata.

Opoziv	Opoziv je prekid važnosti sertifikata pre isteka perioda važnosti naznačenog na sertifikatu. Opoziv sertifikata je trajan, opozvani sertifikat više ne može biti obnovljen.
Zapisi o statusu opoziva	Unutrašnji zapisi o suspendovanim i opozvanim sertifikatima koji uključuju činjenicu suspendovanja ili opoziva i vreme suspendovanja ili opoziva izraženo u sekundama koje održava Sertifikaciono telo.

1.6.2 Akronimi

CA - Sertifikaciono telo (Certification Authority)

CAA - Ovlašćenje sertifikacionog tela (Certification Authority Authorization)

CP - Polisa sertifikata (Certificate Policy)

CPS - Izjava o opštim pravilima rada pružaoca od poverenja (Certification Practice Statement)

CRL - Lista opozvanih sertifikata (Certificate Revocation List)

CSPRNG - Kriptografski siguran generator pseudo-slučajnih brojeva (Cryptographically Secure Pseudo-Random Number Generator)

eIDAS - Elektronska identifikacija, autentifikacija i potpis (electronic Identification, Authentication and Signature)

EVC - Prošireni validacioni sertifikat (Extended Validation Certificate)

EVCP - Proširena polisa validacionog sertifikata (Extended Validation Certificate Policy)

FQDN - Potpuno kvalifikovano ime domena (Fully Qualified Domain Name)

IDN - Međunarodno prevedeno ime domena (Internationalized Domain Name)

LDAP - Protokol za lak pristup direktorijumima (Lightweight Directory Access Protocol)

NMHH - Nacionalni mediji i vlasti za informacione komunikacije (National Media and Infocommunications Authority)

OCSP - Protokol za proveru statusa sertifikata u realnom vremenu (Online Certificate Status Protocol)

OID - Objektni identifikator (Object Identifier)

PKI - Infrastruktura javnog ključa (Public Key Infrastructure)

QCP - Kvalifikovana politika sertifikata (Qualified Certificate Policy)

QGIS - Kvalifikovani izvor informacija vlade (Qualified Government Information Source)

RA - Registraciono telo (Registration Authority)

TSP - Pružalac usluga poverenja (Trust Service Provider)

2 Odgovornosti za objavljivanje i repozitorijuma

2.1 Repozitorijumi

Pružalac usluga od poverenja objavljuje ugovorne uslove i politike elektronski na svom veb sajtu na sledećem linku: https://paperless.rs

Draft verzija novih dokumenata koji će biti uvedeni, dostupni su na veb lokaciji 30 dana pre stupanja na snagu.

Dokumenti koji su na snazi dostupni su na veb sajtu, kao i sve prethodne verzije svih dokumenata.

Aktuelna verzija polisa i ugovornih uslova može se pročitati u kancelariji za korisnike Pružaoca usluga od poverenja.

Nakon zaključenja ugovora, Pružalac usluga od poverenja stavlja na raspolaganje klijentu opšte uslove i odredbe, Izjavu o objavi, Polisu o sertifikatima kvalifikovane elektronske identifikacije i Praktična pravila pružaoca usluga od poverenja u obliku elektronski potpisane PDF datoteke koja se može preuzeti sa njegove internet prezentacije.

Pružalac usluga od poverenja klijentu stavlja na raspolaganje pojedinačni ugovor o uslugama na papiru, autentifikovan ručnim potpisom i pečatom, ili u obliku elektronskog dokumenta u PDF formatu sa kvalifikovanim elektronskim potpisom ili kvalifikovanim elektronskim pečatom.

Pružalac usluga od poverenja obaveštava svoje klijente o promeni opštih uslova i odredbi.

2.2 Objavljivanje informacija o sertifikaciji

Sertifikati pružaoca usluga od poverenja

Sertifikaciono telo će objaviti sertifikate usluga od poverenja koristeći sledeće metode:

- Ime root sertifikata i heš root sertifikata u Izjavi o praksi sertifikacije (videti Poglavlje: 1.3.1.). Informacije o promeni njihovog statusa biće dostupne na veb sajtu sertifikacionog tela.
- Promene statusa posredničkih (intermediate) sertifikata biće objavljene na listama povučenih sertifikata, na veb sajtu i u okviru OCSP usluge u realnom vremenu.
- Za potpisnike odgovora na status sertifikata u realnom vremenu Pružalac usluge poverenja - u skladu sa najboljom međunarodnom praksom - izdaće Sertifikat sa izuzetno kratkim periodom važenja, čime se eliminiše potreba za proverom statusa povučenih sertifikata. Svaki Sertifikat OCSP respondera sadržaće indikaciju ("nocheck"), koja pokazuje da njegov status povlačenja nije potrebno proveravati.

2.3 Vreme ili učestalost objavljivanja

Nove politike se objavljuju najkasnije u roku od 30 dana nakon usvajanja.

Paperless d.o.o obezbeđuje, da se sertifikati objavljuju u centralnom direktorijumu u što krajćem roku nakon njihovog izdavanja.

Registar opozvanih sertifikata se osvežava u najkraćem mogućem roku, nakon opoziva sertifikata u javnom registru. Nakon nekoliko minuta, osvežava se i internet stranica sa listom opozvanih sertifikata.

Javno dostupne informacije i dokumenti (osim gore navedenog) objavljuju se po potrebi.

3 Identifikacija i Autentikacija

3.1 Imenovanje

Jedinstvena imena koje sadrži kvalifikovani elektronski sertifikat nedvosmisleno i jednoznačno definišu korisnika kvalifikovanih elektronskih sertifikata osim ako se, ovim dokumentom ili sadržajem kvalifikovanog elektronskog sertifikata, drugačije zahteva.

3.1.1 Tipovi imena

U skladu sa IETF RFC 5280, svaki kvalifikovani elektronski sertifikat sadrži podatke o korisniku i izdavaocu kvalifikovanog elektronskog sertifikata u obliku jedinstvenog imena. Jedinstveno ime je formirano u skladu sa IETF RFC 5280 i standardom X.501.

Kako je usluga elektronske veb autentikacije namenjena pravnim licima, kao i državnim subjektima, profili sertifikata podeljeni su na sledeći način:

- Profil sertifikata za pravna lica
- Profil sertifikata za državne subjekte

Oznake na sertifikatima pružaoca usluge od poverenja Paperless d.o.o:

Vrsta serfitikata	**Naziv polja**	**Jedinstveno ime**
Kvalifikovani elektronski sertifikat pružaoca usluga od poverenja Paperless d.o.o	Izdavalac engl. Issuer	CN = Paperless Root CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS
Intermediate sertifikati za pravna lica	Izdavalac engl. Issuer	CN = Pravna lica CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS
	Korisnik eng. Subject	**CN = Paperless Veb-Autentikacija** **2.5.4.97 = VATRS-108709130** **2.5.4.97 = MB:RS-21052019** **O = Paperless doo** **C = RS**
Intermediate sertifikati za državne subjekte	Izdavalac engl. Issuer	CN = Paperless GOV CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS
	Korisnik eng. Subject	**CN = Paperless Veb-Autentikacija** **2.5.4.97 = VATRS-108709130** **2.5.4.97 = MB:RS-21052019** **O = Paperless doo** **C = RS**

3.1.1.1 Profil sertifikata za pravna lica

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	V3, vrednost=”2”
Serial Number	CertificateSerialNumber	16 ili 17 okteta, 64 bita entropije
signatureAlgorithm	AlgorithmIdentifier	sha256WithRSAEncryption
signatureValue		Potpis izdavača sertifikata
Issuer	commonName (CN)	Paperless VebAutentikacija
	organizationName (O)	Paperless d.o.o
	countryName (C)	RS
Validity	notBefore	Vreme izdavanja sertifikata
	notAfter	Vreme izdavanja sertifikata +24 meseca
Subject	serialNumber	ID RS, ili ISO kod države prebivališta potpisnika i jedanaestocifreni jedinstveni identifikator, dva broja W i Z koji predstavljaju Paperless interne oznake, Z=48
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	givenName	Ime(na) potpisnika kako je navedeno u identifikacionoj ispravi
	surname (SN)	Prezime(na) potpisnika kako je navedeno u identifikacionoj ispravi
	localityName (L)	Mesto sedišta poslovnog subjekta
	organizationalUnit (OU)	Ovaj atribut opciono može sadržati samo naziv organizacijske jedinice.
	organizationIdentifier	Dvoslovni ISO kod države sedišta poslovnog subjekta zatim jedanaestocifreni broj. Za poslovne subjekte kojima je dodeljen ID u Republici Srbiji: „RS“, ID. Za ostale poslovne subjekte jedanaestocifreni je broj jedinstveni broj kojeg dodeljuje Paperless CA i ne predstavlja ID.
	organizationName (O)	Puni registrovani skraćeni naziv poslovnog subjekta, ili naziv poslovnog subjekta ako skraćeni naziv nije registrovan.
	countryName (C)	RS
	AlgorithmIdentifier	rsaEncryption
subjectPublic KeyInfo	subjectPublicKey	Javni ključ subjekta dužine 2048 bita

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA		Client Authentication, Digital Signature, Key Encipherment, Non Repudiation
certificatePolicies	NE	policyIdentifier	Paperless OID: 1.3.6.1.4.1.61124.40.1.1.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: link cPSuri: link
		policyIdentifier	qcp-natural-qscd (2), OID: 0.4.0.194112.1.2
qCStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-4	OID: 0.4.0.1862.1.4
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 Link od Terms and Conditions ENG Link od Terms and Conditions SRB
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opciono. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: LDAP URL
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak dužine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak dužine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: link
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: link

3.1.1.2 Profil sertifikata za državne subjekte

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	V3, vrednost=”2”

Serial Number	CertificateSerialNumber	16 ili 17 okteta, 64 bita entropije
signatureAlgorithm	AlgorithmIdentifier	sha256WithRSAEncryption
signatureValue		Potpis izdavača sertifikata
Issuer	commonName (CN)	Paperless VebAutentikacija
	organizationName (O)	Paperless d.o.o
	countryName (C)	RS
Validity	notBefore	Vreme izdavanja sertifikata
	notAfter	Vreme izdavanja sertifikata +24 meseca
Subject	serialNumber	ID RS, ili ISO kod države prebivališta potpisnika i jedanaestocifreni jedinstveni identifikator, dva broja W i Z koji predstavljaju Paperless interne oznake, Z=48
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	givenName	Ime(na) potpisnika kako je navedeno u identifikacionoj ispravi
	surname (SN)	Prezime(na) potpisnika kako je navedeno u identifikacionoj ispravi
	localityName (L)	Mesto sedišta DS (Državnog Subjekta)
	organizationalUnit (OU)	Ovaj atribut opciono može sadržati samo naziv organizacijske jedinice DS 2. nivoa.
	organizationalUnit (OU)	Ovaj atribut opciono može sadržati samo naziv organizacijske jedinice DS 1. nivoa.
	organizationIdentifier	Dvoslovni ISO kod za Srbiju zatim ID DS
	organizationName (O)	Puni registrovani skraćeni naziv DS (bez ID-a), ili DS ako skraćeni naziv nije registrovan.
	countryName (C)	RS
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta dužine 2048 bita

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA		Client Authentication, Digital Signature, Key Encipherment, Non Repudiation
certificatePolicies	NE	policyIdentifier	Paperless OID: 1.3.6.1.4.1.61124.40.1.1.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 }

			cPSuri: link
		policyIdentifier	qcp-natural-qscd (2), OID: 0.4.0.194112.1.2
qCStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-4	OID: 0.4.0.1862.1.4
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 Link od Terms and Conditions ENG Link od Terms and Conditions SRB
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opciono. Sadrži E-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: LDAP URL
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak dužine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak dužine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: link
		id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: link

3.1.2 Zahtev da imena budu jedinstvena

Oznaka pravnog lica, koja je u skladu sa odredbama u poglavlju 3.1.1, uključena u jedinstveno ime mora ispunjavati sledeće uslove:

- mora biti jedinstveno registrovano u poslovnom ili drugom službenom registru,
- mora biti jednoznačno povezan sa nosiocem ili pravnim licem,
- maksimalna dužina može biti četrdeset dva (42) karaktera.

Paperless sertifikaciono telo zadržava pravo da odbije firmu, naziv ili šifru privrednog subjekta, ako utvrdi:

- da je neprikladan ili uvredljiv,
- da je zabluda trećim stranama ili već pripada drugom pravnom ili fizičkom licu,
- da je u suprotnosti sa važećim propisima.

3.1.3 Anonimnost ili pseudonimnost Pretplatnika

Pružalac usluge poverenja ne izdaje sertifikate sa pseudonimom.

3.1.4 Pravila za tumačenje različitih oblika imena

U cilju interpretacije identifikatora, preporučuje se da pouzdane strane postupaju prema opisu u ovom dokumentu. Ako pouzdana strana zahteva pomoć u vezi sa interpretacijom identifikatora ili bilo koje druge informacije navedene u Sertifikatu, može direktno kontaktirati Pružaoca usluge od poverenja. U tom slučaju, Pružalac usluge od poverenja ne sme pružiti bilo kakve dodatne informacije o klijentu osim onih navedenih u sertifikatu, osim ako zakon to ne zahteva, već samo pruža informacije radi pomoći u interpretaciji navedenih podataka.

3.1.5 Jedinstvenost imena

Jedinstvena imena su jedinstvena za svaki izdati sertifikat i nedvosmisleno i jedinstveno identifikuju pojedinca u strukturi sertifikata.

Korisnici kvalifikovanih elektronskih sertifikata ne smeju da zahtevaju imena koja pripadaju nekome drugome čime bi se kršila autorska ili druga prava trećih lica.

Postupci za rešavanje sporova koji se odnose na imena

Eventualne sporove rešavaju isključivo oštećena strana i korisnik kvalifikovanog elektronskog sertifikata.

3.1.6 Prepoznavanje, autentifikacija i uloga zaštitnih znakova

Pružalac usluga od poverenja nikada ne uključuje zaštitni znak u izdati sertifikat.

Odgovornost za upotrebu imena ili zaštićenih robnih marki je na strani pravnog lica. Pružalac usluga od poverenja Paperless d.o.o nije u obavezi da proverava i/ili obaveštava korisnika ili pravno lice.

3.2 Početna validacija identiteta

Pružalac usluga od poverenja može koristiti bilo koji komunikacioni kanal unutar granica koje propisuje zakon, radi provere identiteta osobe ili organizacije koja zahteva sertifikat, kao i radi provere autentičnosti pruženih podataka. Pružalac usluga od poverenja može, po vlastitom nahođenju, odbiti izdavanje traženog sertifikata bez posebnog obrazloženja.

3.2.1 Metod za dokazivanje posedovanja privatnog ključa

Posedovanje privatnog ključa koji pripada javnom ključu u sertifikatu garantovano je sigurnosnim procedurama pre i kada se sertifikat prihvati standardom PKCS#10.

Provera vlasništva se obavlja prihvatanjem zahteva za izdavanje sertifikata u formatu PKCS#10.

3.2.2 Provera identifikacije pravnog lica

Podaci o pravnom licu dati su u jedinstvenom imenu.

Za pravnog predstavnika pravnog lica garantuje zakonski zastupnik pravnog lica svojim potpisom na dokumentaciji za izdavanje sertifikata.

Pružalac usluge od poverenja sa odgovarajućim službama i službenim evidencijama proverava ispravnost podataka pravnog lica i identitet odgovornog lica.

Pružalac usluga od poverenja proverava identitet zakonskog zastupnika pravnog lica i podatke o pravnom licu na zvaničnoj veb adresi registrovanih pravnih lica.

3.2.3 Neproverene informacije o pretplatniku

Samo podaci koji su potvrđeni od strane Pružaoca usluga od poverenja mogu biti sadržani u Sertifikatu koji je izdao Pružalac usluga od poverenja.

Pružalac usluge od poverenja proverava tačnost i rad e-pošte naručioca sertifikata.

3.2.4 Provera identiteta zaposlenih za dobijanje sertifikata

Znski zastupnik pravnog lica svojim potpisom na dokumentaciji za dobijanje sertifikata garantuje da želi za pravno lice naručiti odgovarajući sertifikat.

3.2.5 Kriterijumi za Usklađenost

Pružalac usluga poverenja ne sarađuje sa drugim autoritetima za sertifikaciju tokom pružanja usluge.

3.3 Identifikacija i autentifikacija za zahteve za ponovno generisanje ključeva

Re-key je proces kada Pružalac usluge od poverenja izdaje sertifikat subjektu sa zamenjenim javnim ključem. Re-key može biti zatražen samo tokom perioda važenja ugovora o usluzi. U slučaju zahteva za Re-key, Pružalac usluge od poverenja proverava postojanje i proverava važenje tog sertifikata. Pružalac usluge od poverenja prihvata zahteve za re-key u slučaju važećih i nevažećih (suspendovanih, opozvanih ili isteklih) sertifikata.

3.3.1 Identifikacija i autentifikacija za važeći sertifikat

Identifikacija aplikanta će se odvijati kako je opisano u odeljku 3.2.3.

Kada datum isteka novog sertifikata nije kasniji od sertifikata koji se ponovo izdaje, Pružalac usluga od poverenja će ponovo koristiti rezultate i dokaze prikupljene tokom originalnog procesa validacije.

3.3.2 Identifikacija i autentifikacija za nevažeći sertifikat

Pružalac usluge poverenja prihvata zahteve za ponovno generisanje ključeva - samo tokom perioda važenja ugovora o usluzi - u slučaju suspenzije, opoziva ili isteka sertifikata.

Identifikacija aplikanta vrši se kako je opisano u odeljku 3.2.3.

3.4 Identifikacija i autentifikacija u slučaju zahteva za obnovu sertifikata

Obnova sertifikata je proces kada Pružalac usluga od poverenja izdaje sertifikat sa nepromenjenim informacijama o identifikaciji aplikanta, ali za novi period važenja subjektu. Obnova sertifikata može se zatražiti samo tokom perioda važenja ugovora o uslugama i samo za važeće sertifikate.

3.4.1 Identifikacija i autentifikacija u slučaju važećeg sertifikata

Identifikacija subjekta će se odvijati kako je opisano u odjeljku 3.2.3.

U slučaju obnove sertifikata pokrenute od strane Pružaoca usluga od poverenja, Pružalac usluge od poverenja može ponovno koristiti rezultate i dokaze prikupljene tokom originalnog procesa validacije, ukoliko datum isteka novog sertifikata nije kasniji od sertifikata koji se obnavlja.

3.4.2 Identifikacija i autentifikacija u slučaju nevažećeg sertifikata

Nevažeći sertifikat ne može biti obnovljen.

3.5 Identifikacija i autentifikacija za zahteve za izmenu sertifikata

Izmena sertifikata je proces kada pružalac usluga od poverenja izdaje novi sertifikat istom subjektu sa nepromenjenim javnim ključem, ali sa različitim podacima o identifikaciji subjekta.

3.5.1 Identifikacija i autentifikacija u slučaju važećeg sertifikata

Identifikacija aplikanta odvija se prema opisu u sekciji 3.2.3.

Ako modifikovani sertifikat ističe istovremeno kao i originalni sertifikat, tokom postupka, Pružalac usluge od poverenja može koristiti rezultate inspekcija izvršenih pre izdavanja originalnog sertifikata.

3.5.2 Identifikacija i autentifikacija u slučaju nevažećeg sertifikata

Nevažeći sertifikat ne može biti obnovljen.

3.6 Identifikacija i autentifikacija za zahtev za opozivom.

Pružalac usluga od poverenja prima i obrađuje zahteve koji se odnose na suspenziju i opoziv sertifikata, kao i obaveštenja (na primer, vezana za kompromitovanje privatnog ključa ili nepravilnu upotrebu sertifikata) koja se odnose na opoziv sertifikata. Pružalac usluge od poverenja obezbeđuje da se zahtevi prihvataju samo od ovlašćenih strana, pored brze obrade zahteva za suspenziju i opoziv.

U svakom slučaju, Pružalac usluge od poverenja proverava autentičnost podnetog zahteva i pravo lica koje podnosi zahtev.

4 Operativni zahtevi životnog ciklusa sertifikata

Izdavanje novog sertifikata za novog subjekta treba da prethodi slanju registracionog zahteva potrebnog Pružaocu usluge poverenja i potpisivanju ugovora o usluzi sa strane pretplatnika, kao i potpisivanju zahteva za sertifikat sa strane aplikanta.

Zamena sertifikata je proces kada prethodno registrovani (i tokom toga identifikovani) subjekat zahteva novi sertifikat umesto postojećeg (izdatog u skladu sa važećim ugovorom o usluzi).

Zamena sertifikata može se desiti iz sledećih razloga:

- Obnova sertifikata znači traženje sertifikata sa istim podacima kao i u prethodnom od strane Subjekta, pri čemu oba sertifikata budu izdata za isti javni ključ.
  Detalji obnove sertifikata su opisani u odeljku 4.6.
- Modifikacija sertifikata znači traženje modifikacije Sertifikata Subjekta uzimajući u obzir promenu podataka o Subjektu uključenih u sertifikat. Pružalac usluge poverenja prima zahteve za modifikaciju sertifikata tokom perioda važenja sertifikata. Tokom procesa modifikacije sertifikata, novi sertifikat se izdaje za isti javni ključ.
  Detalji modifikacije sertifikata opisani su u odeljku 4.8.
- Re-key znači izdavanje novog sertifikata od strane Pružaoca usluge poverenja za novi javni ključ na zahtev subjekta tokom perioda važenja sertifikata ili nakon isteka.
  Detalji obnove sertifikata su opisani u odeljku 4.7.

Status sertifikata može biti važeći, suspendovan, opozvan ili istekao. Propisi vezani za promene statusa su opisani u odeljku 4.9., a usluga statusa sertifikata opisana je u odeljku 4.10.

Pružalac usluge poverenja pruža održavanje sertifikata samo pod uslovom povezanog ugovora o usluzi. Zahtevi vezani za raskid ugovora o usluzi su opisani u odeljku 4.11.

4.1 Podnošenje zahteva za sertifikat

Za svako novo izdavanje sertifikata, neophodno je podneti zahtev za sertifikat.

Pre nego što podnese prvi Zahtev za sertifikat, Subjekt treba da podnese registracioni zahtev Pružaocu usluge od poverenja, što se može učiniti putem internet prezentacije Pružaoca usluge od poverenja, na primer. Subjekt treba da navede svoje podatke koji će biti naznačeni u sertifikatu i da odredi kakav sertifikat zahteva, kao i da autorizuje Pružaoca usluge od poverenja za upravljanje njihovim ličnim podacima u Registracionom zahtevu.

Pružalac usluge poverenja ne smatra podatke navedene u Registracionom zahtevu autentičnim sve dok ih Subjekt ne potvrdi u Zahtevu za sertifikat.

U slučaju da je zaključenje novog ugovora o usluzi neophodno, Pružalac usluge od poverenja priprema ugovor o usluzi Naručilaca na osnovu informacija navedenih u Registracionom zahtevu. Ugovor o usluzi treba da sadrži vrste sertifikata dostupnih za određene Subjekte u okviru usluga u granicama ugovora.

Novi sertifikat može biti zatražen u okviru prethodno zaključenog ugovora o usluzi. Ako je sertifikat (zamena sertifikata) izdat kao zamena za sertifikat naznačen u ugovoru o usluzi, nije

potrebno menjati ugovor o usluzi. Ako klijent zahteva novi sertifikat pored postojećih, ugovor o usluzi će biti modifikovan.

Pružalac usluge od poverenja informiše Naručioca o uslovima i odredbama korišćenja sertifikata pre zaključenja ugovora. Ako subjekt nije isti kao Naručilac, tada se pomenute informacije daju i subjektu.

Pružalac usluge od poverenja objavljuje dokumenta koja sadrže informacije na razumljiv način, u elektronskom obliku za preuzimanje na svojoj veb sajtu, i na zahtev ih stavlja na raspolaganje u kancelariji za korisnike radi čitanja na licu mesta. U kancelariji za korisnike, klijent ima priliku da pročita dokumenta i konsultuje se.

U Zahtevu za sertifikat, Subjekt mora uključiti najmanje sledeće podatke:

- Podatke koji će biti naznačeni u sertifikatu (na primer, ime, titula, naziv pravnog lica, naziv organizacione jedinice, grad, država, e-mail adresa);
- Llične identifikacione informacije subjekta - u slučaju pravnog lica, predstavnika pravnog lica (puno ime, broj identifikacionog dokumenta, ime majke, datum i vreme rođenja);
- Kontakt podatke subjekta - u slučaju pravnog lica, predstavnika pravnog lica (broj telefona, e-mail adresa);
- Podatke o organizaciji (zvanični naziv, sedište, opcionalno: identifikacioni podaci, naziv odeljenja pravnog lica);
- Podatke Naručilaca (podaci o naplati).

Uz zahtev za sertifikat, Pružalac usluga od poverenja traži i proverava najmanje sledeće dokumente, svedočenja, punomoći i izjave (u slučaju identifikacije kopije na daljinu ovih dokumenata):

- Dokumenti potrebni za identifikaciju subjekta - u slučaju pravnog lica, predstavnika pravnog lica - u skladu sa odeljkom 3.2.3;

- U slučaju zahteva za sertifikat za pravno lice, dokumenti za identifikaciju pravnog lica prema poglavlju 3.2.2;

- Dertifikat ili punomoć dostavlja od strane pravnog lica, kojom se potvrđuje da subjekt ima pravo da predstavlja organizaciju prema poglavlju 3.2.5;

4.1.1 Ko može podneti zahtev za sertifikat

Prijavu za sertifikat mogu podneti samo fizička lica kako bi zatražili sertifikat predstavljene organizacije.

U slučaju predstavnika za organizacioni sertifikat, samo fizička lica mogu podneti prijavu prema sekciji 3.2.5. Prijava za sertifikat podneta od strane bilo koje druge osobe automatski će biti odbijena.

Preduslov za izdavanje sertifikata je važeći ugovor o pružanju usluga (potpisan od strane pretplatnika i Pružaoca usluga od poverenja) koji se odnosi na izdavanje i održavanje sertifikata.

Osoba ovlašćena da predstavlja subjekta može podneti prijavu za sertifikat na sledeće načine:

- Na papiru potpisan ručno na šalteru korisničke usluge Pružaoca usluga od poverenja ili kod mobilnog saradnika za registraciju Pružaoca usluga od poverenja, na prethodno dogovoren datum (u ovom slučaju, lična identifikacija se obavlja tog dana)

- Na papiru potpisan ručno i poslat korisničkoj službi Pružaoca usluga od poverenja (u ovom slučaju, lična identifikacija će se obaviti u drugom terminu)

- U elektronskom obliku sa elektronskim potpisom zasnovanim na ne-pseudonimnom kvalifikovanom Sertifikatu i

  – poslato putem portala za korisnike organizacionog administratora, ili

  – poslato na email adresu office@paperless.rs Pružaoca usluga od poverenja.

Osoba ovlašćena da predstavlja subjekta treba da dostave svoje kontakt informacije prilikom podnošenja registracione aplikacije.

4.1.2 Proces registracije i odgovornosti

Tokom procesa apliciranja, Pružalac usluge od poverenja utvrđuje identitet osobe koja podnosi zahtev za sertifikat (videti Poglavlje 3.2.3).

U slučaju aplikacije za organizacioni sertifikat, Pružalac usluge od poverenja identifikuje organizaciju (videti Poglavlje 3.2.2.) i osigurava da aplikant ima pravo da predstavlja organizaciju (videti Poglavlje 3.2.5.) i da traži sertifikat vezan za organizaciju (videti Poglavlje 3.2.2.).

Pretplatnik određuje koji aplikant ima pravo da zatraži sertifikat u skladu sa polisom sertifikata.

Podnosilac zahteva treba da pruži sve potrebne informacije za sprovođenje procesa identifikacije.

Ako je potrebno, Pružalac usluge od poverenja vrši usklađivanje podataka sa autentičnim vladinim registrima kao što su registar ličnih podataka i adresa ili registar preduzeća. U slučaju baze podataka, ako je to moguće, Pružalac usluge poverenja vrši elektronsko usklađivanje podataka.

Tokom procesa, Pružalac usluge od poverenja određuje jedinstveno ime subjekta i dodeljuje globalno jedinstveni ID (OID) subjektu. To se dešava kako je definisano u odeljku 3.1.

Pružalac usluge poverenja registruje sve potrebne informacije o identitetu aplikanta i organizacije radi pružanja usluge i održavanja kontakta.

Pružalac usluge poverenja od registruje prethodno potpisan ugovor o usluzi od strane pretplatnika koji treba da sadrži izjavu pretplatnika da je svestan svojih obaveza i preuzima obavezu usaglašenosti.

Pružalac usluge poverenja registruje zahtev za sertifikat potpisan od strane podnosioca zahteva koji treba da sadrži sledeće:

- Potvrdu da su podaci navedeni u zahtevu za sertifikat tačni;
- Saglasnost da Pružalac usluge od poverenja beleži i obrađuje podatke navedene u aplikaciji;

- Izjavu da li pristaje na otkrivanje sertifikata;

Pružalac usluga od poverenja čuva navedene zapise tokom vremenskog perioda koji zahteva zakon.

Pružalac usluga od poverenja arhivira ugovore, obrazac zahteva za sertifikat i svako uverenje koje je podnosilac zahteva ili pretplatnik podneo.

Ukoliko identitet osobe ovlašćene da predstavlja subjekta ili identitet organizacije ne može biti potvrđen bez sumnje ili su bilo koji od navedenih podataka u obrascu zahteva za sertifikat netačni, Pružalac usluga od poverenja pruža klijentu mogućnost da ispravi nedostajuće ili netačne podatke i da dostavi nedostajuće potvrde u roku od 3 meseca od podnošenja zahteva za sertifikat, prema svojim unutrašnjim propisima.

4.1.3 Obavljanje funkcija identifikacije i autentifikacije

Pružalac usluge od poverenja identifikuje aplikanta prema odeljku 3.2., i proverava autentičnost zahteva.

Pružalac usluga od poverenja takođe identifikuje organizaciju i proverava njenu sposobnost u skladu sa odeljkom 3.2. Pružalac usluga od poverenja registruje sve informacije koje je organizacija koristila da potvrdi svoj identitet, uključujući registarski broj dokumentacije koja se koristi za potvrdu i slučajna ograničenja vezana za njenu validnost.

Pružalac usluge od poverenja može koristiti originalne autentične dokumente koje poseduje ili autentične elektronske kopije napravljene od njih tokom validacije do perioda važenja naznačenog na dokumentu ili do trenutka kada se dokument ne poništi na neki drugi način.

Pružalac usluga od poverenja može koristiti dokumenta i podatke navedene u odeljku 3.2. kako bi proverio informacije o sertifikatu, ili može ponovo koristiti prethodne validacije same za najviše 3 meseca.

4.1.4 Odobrenje ili odbijanje zahteva za izdavanje sertifikata.

Da bi izbegao bilo kakve sukobe interesa, Pružalac usluge od poverenja osigurava svoju ličnu i operativnu nezavisnost suprotno Pretplatnicima. Ne predstavlja kršenje sukoba interesa ako Pružalac usluge od poverenja izdaje sertifikate za svoje saradnike.

Pružalac usluge od poverenja proverava autentičnost svih informacija date u zahtevu za sertifikat koje će biti navedene na sertifikatu pre izdavanja sertifikata.

Nakon obrade zahteva za sertifikat, Pružalac usluge od poverenja prihvata ili odbacuje zahtev za sertifikat.

Ako identitet fizičkog lica ili organizacije ne može biti potvrđen bez sumnje, ili ako su bilo koji od navedenih podataka u obrascu zahteva za izdavanje sertifikata netačni, a klijent ne ispravi ove nedostatke po zahtevu Pružaoca usluga od poverenja, tada Pružalac usluga od poverenja odbacuje zahtev.

U slučaju odbijanja zahteva za izdavanje sertifikata, Pružalac usluga od poverenja obaveštava aplikanta i pretplatnika o odbijanju, ali Pružalac usluga od poverenja nije obavezan da obrazloži svoju odluku.

4.1.5 Vreme za obradu zahteva za sertifikat

Pružalac usluge poverenja preuzima obradu zahteva za sertifikat u roku od 5 radnih dana ukoliko su dostupni svi potrebni podaci i dokumenti.

4.2 Izdavanje sertifikata

Pružalac usluge od poverenja izdaje sertifikat samo subjektu u slučaju prihvatanja zahteva za sertifikat.

Izdati sertifikat sadrži samo podatke koji su navedeni u zahtevu za sertifikat i koji su verifikovani od strane Pružaoca usluge od poverenja tokom procesa evaluacije.

Pružalac usluge od poverenja trenutno izdaje isključivo cloud sertifikate i proizvodni postupak za sertifikate i za par ključeva sastavljen je od jasno odvojenih delova (ili funkcija), sa njihovim odgovarajuće odvojenim podsistemima:

- razmatranje zahteva za izdavanje sertifikata,
- priprema sertifikata, registracionog i aktivacionog koda,
- dostavljanje registracionog i aktivacionog koda i obaveštenja korisniku,
- generisanje privatnog ključa u HSM-u u cloud-u i izdavanje sertifikata

Registracioni i aktivacioni kod korisniku se dostavljaju putem dva odvojena kanala, jedan putem elektronske pošte, a drugi putem drugog bezbednog kanala (bezbedan internet portal, dostupan pomoću kvalifikovanog sertifikata, lično uručenje putem klasične pošte ili preko posebnog internet mesta, gde se korisnik registruje sa podatkom koji je poznat samo korisniku.

Izuzetno može jedan od navedenih kodova ovlašćeno lice puržaoca usluga od poverenja, korisniku da preda i lično.

4.2.1 Radnje CA tokom izdavanja sertifikata

Izdavanje sertifikata se odvija prema strogo regulisanim i kontrolisanim procesima, detalji su navedeni unutrašnjim propisima i zahtevima Pružaoca usluge od poverenja.

Pružalac usluge od poverenja je razvio svoje interne administrativne procese analizirajući rizike, i primenjuje princip "dvostruke kontrole" prilikom beleženja podataka uključenih u sertifikat i provere autentičnosti podataka.

Izdati sertifikat se u najkraćem mogućem roku dodaje internom repozitorijumu sertifikata Pružaoca usluge od poverenja. Od tog trenutka može biti povučen, a informacije o statusu povlačenja biće dostupne putem OCSP i CRL usluga Pružaoca usluge od poverenja.

Početak perioda važenja sertifikata ne sme biti raniji od stvarnog vremena izdavanja sertifikata.

4.2.2 Obaveštavanje pretplatnika o izdavanju sertifikata.

Opisano u poglavlju 4.3.1.

4.3 Prihvatanje sertifikata

4.3.1 Postupak koji čini prihvatanje sertifikata

Kod sertifikata u cloud-u preuzimanje sertifikata nije potrebno, jer isti prema ovlašćenju korisnika bezbedno čuva pružalac usluga od poverenja. Korisniku se dostavljaju samo kodovi za pristup bezbednom Cloud-u, videti poglavlje 4.3.1.

4.3.2 Objavljivanje sertifikata od strane CA (sertifikacionog tela)

Nakon izdavanja sertifikata, u slučaju prethodne saglasnosti aplikanta, Pružalac usluge od poverenja objavljuje sertifikat u svom javnom repozitorijumu sertifikata.

4.3.3 Obaveštavanje o izdavanju sertifikata od strane Pružaoca usluga od poverenja drugim entitetima

Osoba ovlašćena da predstavlja subjekta se odmah obaveštava od strane Pružaoca usluga od poverenja o izdavanju sertifikata.

4.4 Ključevi i upotreba sertifikata

4.4.1 Upotreba privatnog ključa i sertifikata pretplatnika

Subjekt sme koristiti samo svoj privatni ključ koji odgovara sertifikatu za kreiranje elektronske identifikacije, a svaka druga upotreba je zabranjena.

Privatni ključ koji odgovara isteklom, opozvanom ili suspendovanom sertifikatu ne sme se koristiti.

Subjekt je obavezan da obezbedi adekvatnu zaštitu privatnog ključa i podataka za aktivaciju.

Ograničenja određena u odeljku 1.4. moraju se poštovati tokom upotrebe.

4.4.2 Obaveze i odgovornosti trećih strana

Da bi zadržala nivo sigurnosti garantovan od strane Pružaoca usluge od poverenja, u procesu prihvatanja verifikovanog elektronske identifikacije, pouzdana strana se preporučuje da postupa oprezno, posebno u vezi sa sledećim:

- Treča strana treba da verifikuje validnost i status povlačenja sertifikata;

- Sertifikati za elektronski pečat i odgovarajući javni ključevi treba da se koriste samo za validaciju elektronske identifikacije;
- Verifikacije vezane za sertifikat treba da se obavljaju za celokupni lanac sertifikata sve do pouzdanog root ili intermediate sertifikata;
- Prilikom formiranja lanca sertifikata, treba prihvatiti sertifikat Pružaoca usluge od poverenja kao pouzdanog izdavaoca (oslonac poverenja) koji

    - je naveden u nacionalnoj listi (*Javna lista kvalifikovanih usluga od poverenja prema Zakonu o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju - MTT*) kao pružalac usluga od poverenja ovlašćen da izdaje kvalifikovane korisničke sertifikate,
    - prati ga sertifikat Pružaoca usluge koji je bio važeći u trenutku kreiranja pečata i u trenutku izdavanja korisničkog sertifikata koji se koristi za kreiranje elektronske identifikacije;

- Verifikacija elektronske identifikacije treba da se obavlja pomoću pouzdane aplikacije, koja se pridržava povezanih tehničkih specifikacija, može se otporno konfigurisati i pravilno je postavljena, i radi u okruženju bez virusa;
- Preporučuje se provera da li je sertifikat izdat prema odgovarajućoj Polisi sertifikata;
- Prilikom prihvatanja kvalifikovane elektronske identifikacije, preporučuje se provera da li je sertifikat izdat na osnovu Polise sertifikata koja zahteva uređaj za kreiranje kvalifikovane elektronske identifikacije;
- Ako je naznačeno u sertifikatu, preporučuje se provera najviše vrednosti obaveze preuzete u jednom trenutku (Sertifikaciono telo nije odgovorno za zahteve proizašle iz elektronskih dokumenata izdatih i potpisanih u vezi sa transakcijama većim od tih ograničenja i za štetu koja je na taj način prouzrokovana);
- Pouzdana strana treba da uzme u obzir sve restrikcije naznačene u sertifikatu ili u propisima na koje se sertifikat referiše.

Pružalac usluge od poverenja stavlja na raspolaganje uslugu svojim klijentima i pouzdanim stranama koju mogu koristiti za verifikaciju izdatih sertifikata.

4.5 Obnova sertifikata

Obnova kvalifikovane elektronskog identifikacije je proces u kojem Pružalac usluga od poverenja izdaje novi sertifikat za novi period važenja za isti javni ključ sa nepromenjenim podacima o identitetu subjekta naziva se obnova sertifikata.

Ako subjekt želi da koristi sertifikat nakon isteka, tada mora pokrenuti obnovu sertifikata. Tehnički, obnova sertifikata znači izdavanje novog sertifikata sa istim podacima identifikacije subjekta, ali sa novim periodom važenja. Ostali podaci u sertifikatu mogu se promeniti, poput referenci na CRL, OCSP ili ključa pružaoca korišćenog za potpisivanje sertifikata.

4.5.1 Okolnosti za obnovu sertifikata

Obnova sertifikata dozvoljena je samo kada su ispunjeni svi sledeći uslovi:

- Zahtev za obnovu sertifikata podnet je u roku važenja sertifikata;
- Sertifikat koji se obnavlja nije opozvan;

- Privatni ključ koji odgovara sertifikatu nije ugrožen;
- Informacije o identitetu subjekta navedene u sertifikatu i dalje su validne.

Pružalac usluga od poverenja prihvataće samo aplikaciju za obnovu sertifikata tokom trajanja ugovora o uslugama.

Ako je prethodni sertifikat subjekta povučen, tada novi sertifikat može biti zatražen samo u okviru procesa Re-key (videti sekciju: 4.7.) ili novog zahteva za sertifikat (videti sekciju: 4.1.).

Ako se neki od podataka o subjektu navedenih u sertifikatu promeni, tada se novi sertifikat mora zatražiti u okviru procesa modifikacije sertifikata (videti sekciju 4.8.).

Tokom obnove sertifikata, aplikant se obaveštava da li su se uslovi i odredbe promenili od prethodnog izdavanja sertifikata.

Ako aplikant nije isti kao pretplatnik, tada se navedene informacije takođe pružaju pretplatniku.

Obnova sertifikata se vrši u okviru važećeg ugovora o pružanju usluga, te nije potrebno njegovo modifikovanje.

4.5.2 Ko može zatražiti obnovu

Obnovu sertifikata pokreće osoba u ime klijenta, koja je ovlašćena da podnese zahtev za novi sertifikat istog tipa u trenutku podnošenja zahteva za obnovu.

Podnosilac zahteva treba da navede u aplikaciji za obnovu sertifikata da su podaci o identifikaciji subjekta navedeni u sertifikatu i dalje važeći.

Pružalac usluge od poverenja omogućava sledeće mogućnosti klijentima za podnošenje zahteva za obnovu sertifikata:

- U elektronskom obliku sa elektronskim potpisom ili elektronskim pečatom na osnovu ne anonimnog kvalifikovanog sertifikata subjekta, poslatom na email adresu office@paperless.rs Pružaoca usluge od poverenja.
- Na papiru ručno potpisanom na šalteru za korisnike Pružaoca usluge od poverenja ili kod mobilnog registracionog saradnika Pružaoca usluge od poverenja, na prethodno dogovoren datum (u ovom slučaju, lična identifikacija će se obaviti tokom tog vremena).
- Na papiru ručno potpisanom i poslatom na šalter za korisnike Pružaoca usluge od poverenja (u ovom slučaju, lična identifikacija će se obaviti u drugom terminu).

Pružalac usluga od poverenja ovlašćen je da pokrene obnovu sertifikata ako promene u unutrašnjim ili spoljnim uslovima pružanja usluge to zahtevaju, na primer, ali ne isključivo, u sledećim slučajevima:

- Zbog promena u spoljnim zahtevima, sertifikat više ne može da se koristi u trenutnom obliku;
- Pružalac usluga od poverenja sazna da sertifikat ne ispunjava zahteve navedene u Polisi kvalifikovanog sertifikata za elektronski pečat ili Izjavi o praksi sertifikacije;
- Ako ključ za potpisivanje pružaoca usluge korišćen za izdavanje sertifikata mora biti zamenjen van reda.

4.5.3 Obrada zahteva za obnovu sertifikata

Tokom evaluacije zahteva za obnovu sertifikata, Pružalac usluga od poverenja potvrđuje da:

- Je podneti zahtev za obnovu sertifikata autentičan;
- Podnosilac zahteva za obnovu sertifikata ima odgovarajuće ovlašćenje i autorizaciju;
- Podnosilac zahteva za obnovu sertifikata izjavljuje da su podaci o subjektu koji će biti navedeni u sertifikatu nepromenjeni i tačni;
- Je zahtev za obnovu sertifikata podnet tokom važenja sertifikata;
- Sertifikat koji se obnavlja nije suspendovan ili povučen;
- Na osnovu trenutno dostupnih informacija o kriptografskim algoritmima koji se koriste, oni će i dalje biti primenjivi čak i tokom planiranog važenja sertifikata koji će biti izdat.

4.5.4 Obaveštenje Klijenta o izdavanju novog sertifikata

Pružalac usluga od poverenja obaveštava aplikanta i pretplatnika o izdavanju sertifikata.

4.5.5 Ponašanje koje predstavlja prihvatanje obnovljenog sertifikata

Obnovljeni sertifikat može biti preuzet (skinut) bez ličnog susreta.

Tokom procesa obnove sertifikata, ne dolazi do generisanja ključeva, tako da nema potrebe za predajom ključeva subjektu.

Pružalac usluge od poverenja će direktno poslati izdati sertifikat Pružaocu usluge upravljanja ključem.

Subjekt prihvata sertifikat korišćenjem sertifikata, i nije potrebna posebna izjava.

4.5.6 Objavljivanje obnovljenog sertifikata od strane izdavača sertifikata

Pružalac usluge od poverenja objavljuje obnovljeni sertifikat na isti način kao i originalni sertifikat.

4.5.7 Obaveštavanje drugih entiteta o izdavanju sertifikata

U slučaju organizacionog sertifikata, Pružalac usluge od poverenja bez odlaganja obaveštava kontakt osobe u predstavljenoj organizaciji o izdavanju sertifikata.

4.6 Re-key sertifikat (obnova ključa)

Re-key podrazumeva proces kada Pružalac usluga od poverenja izdaje novi sertifikat za subjekt na način da se javni ključ menja.

Dodatni podaci mogu opcionalno biti promenjeni u novom sertifikatu izdatom tokom procesa Re-ključanja, na primer period važenja, veze CRL i OCSP ili ključ provajdera koji se koristi za potpisivanje sertifikata.

4.6.1 Okolnosti za Re-ključanje Sertifikata

Valjanost prethodnog sertifikata nije potrebna za Re-key, ali Pružalac usluge od poverenja prihvata samo zahteve za Re-key u okviru sporazuma o pružanju usluga.

Tokom procesa Re-key, Pružalac usluge od poverenja obaveštava aplikanta ako su se uslovi i odredbe promenili od prethodnog izdavanja sertifikata. Ako aplikant nije isti kao pretplatnik, tada se navedene informacije takođe daju Pretplatniku.

Re-key sertifikata se vrši u okviru važećeg ugovora o pružanju usluga, te nije potrebno njegovo modifikovanje.

4.6.2 Ko može zatražiti sertifikaciju novog javnog ključa

Re-key sertifikata treba da pokrene osoba koja bi imala pravo da podnese novi zahtev za sertifikat u trenutku podnošenja zahteva za Re-key.

Podnosilac zahteva treba da navede u zahtevu za Re-key sertifikata da li su podaci identifikacije subjekta navedeni u sertifikatu i dalje važeći, ili da pruže nove podatke i izjave o njihovoj validnosti.

Pružalac usluge poverenja omogućava sledeće mogućnosti klijentima za podnošenje zahteva za Re-key sertifikata:

- U elektronskom obliku sa elektronskim potpisom ili elektronskim pečatom na osnovu ne anonimnog kvalifikovanog sertifikata subjekta, poslatom na email adresu office@paperless.rs Pružaoca usluge od poverenja.
- Na papiru ručno potpisanom na šalteru za korisnike Pružaoca usluge poverenja ili kod mobilnog registracionog saradnika Pružaoca usluge od poverenja, na prethodno dogovoren datum (u ovom slučaju, lična identifikacija će se obaviti ovog puta);
- Na papiru ručno potpisanom i poslatom na šalter za korisnike Pružaoca usluge od poverenja (u ovom slučaju, lična identifikacija će se obaviti u drugom terminu).

4.6.3 Obrada zahteva za promenu ključa sertifikata

Tokom procene zahteva za ponovno izdavanje sertifikata, Pružalac usluga od poverenja potvrđuje da:

- Podneti zahtev je autentičan;
- Podnosilac zahteva ima odgovarajuće pravo i ovlašćenje;

- Podaci navedeni u zahtevu su tačni;
- Na osnovu trenutno dostupnih informacija o kriptografskim algoritmima koji se koriste, oni će i dalje biti primenljivi tokom planiranog trajanja sertifikata koji će biti izdat.

Pre obrade zahteva za ponovno izdavanje sertifikata, identitet osobe koja podnosi zahtev za ponovno izdavanje sertifikata mora biti proveren u skladu sa odeljkom 3.3.

4.6.4 Obaveštenje klijenta o izdavanju novog sertifikata.

Pružalac usluga od poverenja obaveštava aplikanta i pretplatnika o izdavanju sertifikata.

4.6.5 Prihvatanje Re-Key sertifikata

Pružalac usluge od poverenja će direktno poslati izdati sertifikat Pružaocu usluge upravljanja ključem.

Novi sertifikat izdat kao deo Re-key-a može biti primljen (skinut) bez potrebe za ličnim susretom.

Subjekt prihvata sertifikat korišćenjem sertifikata, i nije potrebna posebna izjava.

4.6.6 Objavljivanje Re-Key sertifikata

Pružalac usluge od poverenja objavljuje obnovljeni sertifikat na isti način kao i originalni sertifikat.

4.6.7 Obaveštavanje drugih entiteta o izdavanju Re-Key sertifikata

U slučaju organizacionog sertifikata, Pružalac usluge od poverenja bez odlaganja obaveštava kontakt osobu predstavljene organizacije o izdavanju sertifikata.

4.7 Modifikacija sertifikata

Modifikacija sertifikata znači proces kada Pružalac usluge od poverenja izdaje novi sertifikat za subjekta sa promenjenim podacima identiteta subjekta, ali sa neizmenjenim javnim ključem.

Tehnički, modifikacija sertifikata znači izdavanje novog sertifikata. Pružalac usluge od poverenja obavezan je da opozove prethodni sertifikat koji sadrži nevažeće podatke (videti Poglavlje: 4.9.).

Prethodni podaci mogu se promeniti u novom sertifikatu izdatom tokom modifikacije sertifikata, kao što su period važenja, referenca na CRL i OCSP ili ključ Pružaoca usluge od poverenja korišćen za potpisivanje sertifikata.

4.7.1 Okolnosti za modifikaciju sertifikata

Modifikacija sertifikata postaje neophodna u sledećim slučajevima:

- Promena podataka navedenih u sertifikatu subjekta;
- U sistemu izdavanja sertifikata pružaoca usluga od poverenja, menja se bilo koji podatak o izdavaču sertifikata CA naveden u "Subject DN", ili se menja njen javni ključ, što rezultira promenom njegovog sertifikata;
- Profil sertifikata određen od strane pružaoca usluga od poverenja je promenjen.

Zahtevi za modifikaciju sertifikata:

- Zahtev za modifikaciju sertifikata je podnet tokom trajanja važnosti sertifikata;
- Sertifikat koji se modifikuje nije suspendovan ili opozvan;
- Privatni ključ koji odgovara sertifikatu nije kompromitovan.

Pružalac usluge od poverenja prihvata samo aplikacije za modifikaciju sertifikata u okviru ugovora o uslugama.

Ukoliko je prethodni sertifikat subjekta opozvan ili istekao, tada se novi sertifikat može zatražiti u okviru Re-key (videti sekciju: 4.7.) ili nove aplikacije za sertifikat (videti sekciju: 4.1.).

Tokom modifikacije sertifikata, aplikant je obavešten ako su se uslovi promenili od izdavanja prethodnog sertifikata.

Ukoliko aplikant nije isti kao pretplatnik, tada se navedene informacije takođe daju i pretplatniku. Modifikacija sertifikata se vrši u okviru važećeg ugovora o uslugama, nije potrebno njegovo menjanje.

4.7.2 Ko može zahtevati modifikaciju sertifikata

Modifikacija sertifikata treba da bude pokrenuta od strane osobe koja je ovlašćena da podnese novu aplikaciju za sertifikat u trenutku podnošenja zahteva za modifikaciju.

U zahtevu za modifikaciju sertifikata, podnosilac zahteva treba da pruži nove podatke i da izjavi njihovu tačnost.

Pružalac usluge od poverenja inicira modifikaciju sertifikata ukoliko sazna da su se podaci o subjektu navedeni u sertifikatu promenili.

Pružalac usluge od poverenja obezbeđuje sledeće mogućnosti Klijentima za podnošenje zahteva za modifikaciju sertifikata:

- U elektronskom obliku sa elektronskim potpisom ili elektronskim pečatom na osnovu ne anonimnog kvalifikovanog sertifikata subjekta, poslat na mejl adresu Pružaoca usluge od poverenja office@paperless.rs
- Na papiru ručno potpisan u korisničkom servisu Pružaoca usluge od poverenja ili kod mobilnog registracionog saradnika Pružaoca usluge od poverenja, na prethodno dogovoren datum (u ovom slučaju, lična identifikacija će se tada izvršiti)
- Na papiru ručno potpisan i poslat u korisnički servis Pružaoca usluge od poverenja (u ovom slučaju, lična identifikacija će se izvršiti u drugom terminu).

4.7.3 Obrada zahteva za modifikaciju sertifikata

Tokom podnete aplikacije za modifikaciju sertifikata, Pružalac usluga od poverenja će proveriti da li:

- Podneta aplikacija za modifikaciju sertifikata je autentična;
- Podnosilac aplikacije za modifikaciju sertifikata ima odgovarajuće ovlašćenje i autorizaciju;
- Podaci dati u aplikaciji su tačni;
- Aplikacija za modifikaciju sertifikata je podneta tokom važenja sertifikata;
- Na osnovu trenutno dostupnih informacija o kriptografskim algoritmima koji se koriste, oni će i dalje biti primenjivi čak i tokom planiranog važenja sertifikata koji će biti izdat.

Pružalac usluge od poverenja proverava validnost podataka subjekta na isti način kao i tokom početne verifikacije koja se vrši pre izdavanja novog sertifikata.

Pre podnošenja zahteva za modifikaciju sertifikata, podnosilac zahteva treba da bude identifikovan u skladu sa sekcijom 3.5.

4.7.4 Obaveštenje klijenta o izdavanju novog sertifikata

Pružalac usluga od poverenja obaveštava aplikanta i pretplatnika o izdavanju sertifikata.

4.7.5 Ponašanje koje predstavlja prihvatanje izmenjenog sertifikata.

Pružalac usluge od poverenja će takođe direktno poslati izdati sertifikat Pružaocu usluge koji upravlja ključem.

Subjekat prihvata sertifikat njegovim korišćenjem, i nema potrebe za daljim izjavama.

4.7.6 Objavljivanje izmenjenog sertifikata od strane Pružaoca usluga od poverenja

Pružalac usluge od poverenja objavljuje obnovljeni sertifikat na isti način kao i originalni sertifikat.

4.7.7 Objavljivanje izmenjenog sertifikata od strane Pružaoca usluga od poverenja

U slučaju organizacionog sertifikata, administrator organizacije koji je ovlašćen od strane predstavljene organizacije od strane Pružaoca usluge od poverenja, bez odlaganja se obaveštava o izdavanju sertifikata.

4.8 Opoziv i suspenzija sertifikata

Proces kada Pružalac usluga od poverenja prekida važnost sertifikata pre njegovog isteka naziva se opoziv sertifikata. Opoziv sertifikata je trajna i neopoziva promena statusa, opozvani sertifikat više nikada neće biti važeći.

Proces kada Pružalac usluga od poverenja privremeno obustavlja važnost sertifikata pre njegovog isteka naziva se suspenzija sertifikata. Suspenzija sertifikata je privremeno stanje; suspendovani sertifikat može biti opozvan, ili pre njegovog isteka važnosti, povlačenjem suspenzije može ponovo postati važeći. U slučaju povlačenja suspenzije, sertifikat postaje važeći retroaktivno, kao da nije bio suspendovan.

Razlog za povlačenje

Pružalac usluge od poverenja može čuvati informacije o razlogu za povlačenje u registru statusa povlačenja sertifikata, koje može otkriti u uslugama statusa povlačenja sertifikata.

Kada klijent pokrene povlačenje, mogu se navesti sledeći razlozi za povlačenje:

- Kompromitovan ključ (keyCompromise (1))
- Sertifikat više nije potreban (cessationOfOperation (5))
- Pravo korišćenja je opozvano (privilegeWithdrawn (9))

Opcije dostupne u svakoj usluzi povlačenja opisane su u opisu odgovarajuće usluge.

Kada Pružalac usluge od poverenja pokrene povlačenje, mogu se navesti sledeći razlozi za povlačenje:

- Nespecifikovano (unspecified (0), što rezultira time da se ne pruža razlogCode ekstenzija)
- Kompromitovan ključ (keyCompromise (1))
- Modifikacija sertifikata (affiliationChanged (3))
- Obnavljanje sertifikata (superseded (4))
- Pravo korišćenja je opozvano (privilegeWithdrawn (9))

Tokom zahteva za suspendovanje, isti razlozi mogu biti navedeni kao u slučaju povlačenja, ali se sledeći status prikazuje u usluzi statusa povlačenja tokom suspendovanja:

- Suspendovan (certificateHold (6))

Ako klijent zahteva konačno povlačenje suspendovanog sertifikata, može pružiti isti razlog povlačenja kao što je navedeno gore.

Ako Pružalac usluge od poverenja pokrene povlačenje suspendovanog sertifikata, postavlja razlog povlačenja kao što je navedeno tokom zahteva za suspendovanje.

Korišćenje privatnog ključa povučenog sertifikata

Upotreba privatnog ključa koji pripada povučenom ili suspendovanom sertifikatu odmah treba biti eliminisana ili suspendovana.

Ako je moguće, privatni ključ koji pripada povučenom sertifikatu treba odmah uništiti nakon povlačenja.

Regulacije odgovornosti vezane za suspendovanje i povlačenje:

- Ako je Pružalac usluge od poverenja već objavio povučeni status sertifikata, Pružalac usluge od poverenja ne preuzima nikakvu odgovornost ako Pouzdana strana smatra sertifikat važećim.

4.8.1 Okolnosti za opoziv

Razlozi za opoziv sertifikata kod pretplatnika

Sertifikaciono telo opoziva sertifikat krajnjeg korisnika i koristiti odgovarajući razlog u CRL-u u sledećim slučajevima:

- Potpuno usklađeni zahtev za povlačenje podnosi se Pružaocu usluge od poverenja putem veb bazirane usluge povlačenja koju on operiše
  (videti u odeljku 4.9.3)
- Aplikant ili pretplatnik zahteva opoziv sertifikata pismeno (vidi u odeljku 4.9.3)
- Aplikant ili pretplatnik obaveštava sertifikaciono telo da prijava sertifikata nije odobrena i naknadno odobrenje nije dato (privilegeWithdrawn (9))
- Sertifikaciono telo sazna da je privatni ključ koji odgovara javnom ključu u sertifikatu kompromitovan (keyCompromise (1))
- Sertifikaciono telo sazna da javni ključ u sertifikatu ne ispunjava zahteve definisane u odeljku 6.1.5. i 6.1.6 (superseded (4))
- Sertifikaciono telo sazna da je sertifikat zloupotrebljen (privilegeWithdrawn (9))
- Pružalac usluga poverenja sazna da je pretplatnik prekršio jednu ili više svojih materijalnih obaveza prema ugovoru o pružanju usluga ili opštim uslovima
- Sertifikaciono telo sazna za materijalnu promenu informacija sadržanih u sertifikatu
- Modifikacija sertifikata zbog promene podataka koji se odnose na subjekta
- Sertifikaciono telo sazna da sertifikat nije izdat u skladu sa Polisom sertifikata ili Izjavom o praksi izdavanja sertifikata (superseded (4))
- Sertifikaciono telo sazna da su bilo koji od podataka koji se pojavljuju u sertifikatu netačni (privilegeWithdrawn (9))
- Sertifikaciono telo više nije ovlašćeno da izdaje sertifikate, a održavanje nije obezbeđeno za postojeće usluge CRL i OCSP (neodređeno (0))
- Opoziv je potreban prema Polisi sertifikata ili Izjavi o praksi izdavanja sertifikata sertifikacionog tela iz razloga koji inače nisu potrebni da budu navedeni u ovom odeljku (neodređeno (0))
- Sertifikaciono telo je izdalo sertifikat na osnovu dokumenta treće strane i povlači taj dokument pismeno (privilegeWithdrawn (9))
- Format i tehnički sadržaj sertifikata predstavljaju neprihvatljiv rizik za korisnike na koje se oslanjaju (na primer, ako korišćeni kriptografski algoritam ili veličina ključa više nisu bezbedni) (keyCompromise (1))
- Sertifikaciono telo sazna da bi privatni ključ jedinice za izdavanje sertifikata mogao biti kompromitovan (neodređeno (0))
- Sertifikaciono telo sazna da pretplatnik nije ispunio svoje finansijske obaveze prema ugovoru o pružanju usluga (privilegeWithdrawn (9))
- Sertifikaciono telo dobija obaveštenje ili na drugi način saznaje o bilo kojoj okolnosti koja ukazuje na to da upotreba e-adrese u sertifikatu više nije zakonski dozvoljena (privilegeWithdrawn (9))
- Sertifikat je suspendovan i nije vraćen u roku koji je osiguran (videti Poglavlje: 4.9.16.)

- Raskid ugovora o pružanju usluge (privilegeWithdrawn (9))
- Sertifikaciono telo je okončalo svoje aktivnosti (neodređeno (0))
- Nadzorni organ donosi (nešto) u pravno obavezujućoj i izvršnoj odluci (neodređeno (0))
- Zakon nalaže obavezan opoziv (neodređeno (0))

Razlozi za opoziv kod podređenog CA sertifikata

Sertifikaciono telo je obavezno da preduzme akciju povodom opoziva sertifikata za jedinicu posrednog sertifikovanja u sledećim slučajevima:

- Sertifikaciono telo koje upravlja jedinicom posrednog sertifikovanja traži opoziv sertifikata pismeno
- Podređeni CA obaveštava Pružaoca usluga od poverenja da originalni zahtev za sertifikat nije bio ovlašćen i ne daje retroaktivno ovlašćenje
- Sertifikaciono telo sazna da nije isključivi vlasnik privatnog ključa
- Sertifikaciono telo sazna da javni ključ u sertifikatu ne zadovoljava zahteve definisane u odeljku 6.1.5 i 6.1.6
- Sertifikaciono telo sazna da je sertifikat zloupotrebljen
- Sertifikat nije izdat u skladu sa relevantnom polisom sertifikata ili izjavom o praksi izdavanja sertifikata ili rad jedinice posrednog sertifikovanja ne zadovoljava relevantnu polisu sertifikata ili izjavu o praksi izdavanja sertifikata
- Sertifikaciono telo utvrdi da su informacije koje se pojavljuju u sertifikatu netačne ili obmanjujuće
- Izdajući CA ili Podređeni CA prekida operacije iz bilo kog razloga i nije izvršeno dogovoreno da drugo sertifikaciono telo pruži podršku za opoziv sertifikata
- Sertifikaciono telo više nije ovlašćeno da izdaje sertifikate, a održavanje nije obezbeđeno za CRL i OCSP usluge koje se odnose na sertifikate
- Opoziv je potreban prema polisi sertifikata izdajućeg CA-a ili izjavi o praksi izdavanja sertifikata
- Modifikacija sertifikata zbog promene podataka koji se odnose na jedinicu sertifikovanja ili sertifikaciono telo
- Format i tehnički sadržaj sertifikata predstavljaju neprihvatljiv rizik za oslanjajuće strane (na primer, ako korišćeni kriptografski algoritam ili veličina ključa više nisu bezbedni)
- Sertifikaciono telo je okončalo svoje aktivnosti
- Zakon nalaže obavezni opoziv

Razlozi za opoziv sertifikata podređenog CA-a koji ga koristi drugo sertifikaciono telo

Sertifikaciono telo je obavezno da preduzme akciju povodom opoziva sertifikata jedinice posrednog sertifikovanja koju koristi drugo sertifikaciono telo u sledećim slučajevima:

- CA koji upravlja jedinicom posrednog sertifikovanja traži opoziv sertifikata pismeno
- Podređeni CA obaveštava Pružaoca usluga od poverenja da originalni zahtev za sertifikat nije bio ovlašćen i ne daje retroaktivno ovlašćenje
- Izdajuće sertifikaciono telo sazna da operater jedinice posrednog sertifikovanja nije isključivi vlasnik privatnog ključa
- Izdajuće sertifikaciono telo sazna da javni ključ u sertifikatu više ne zadovoljava zahteve definisane u odeljku 6.1.5 i 6.1.6

- Sertifikaciono telo sazna da je sertifikat zloupotrebljen
- Izdajuće sertifikaciono telo sazna da sertifikat nije izdat u skladu sa relevantnom polisom sertifikata i izjavom o praksi izdavanja sertifikata ili rad operatera jedinice posrednog sertifikovanja ne zadovoljava relevantnu polisom sertifikata ili izjavu o praksi izdavanja sertifikata
- Sertifikaciono telo utvrdi da su informacije koje se pojavljuju u sertifikatu netačne ili obmanjujuće
- Izdajući CA ili podređeni CA prekida operacije iz bilo kog razloga i nije izvršeno dogovoreno da drugo sertifikaciono telo pruži podršku za opoziv sertifikata
- Sertifikaciono telo više nije ovlašćeno da izdaje sertifikate, a održavanje CRL i OCSP usluga za postojeće sertifikate nije obezbeđeno
- Opoziv je potreban prema polisi sertifikata izdajućeg CA-a ili izjavi o praksi izdavanja sertifikata
- Modifikacija sertifikata zbog promene podataka koji se odnose na jedinicu sertifikovanja ili drugo sertifikaciono telo
- Ako je sertifikaciono telo izdalo sertifikat na osnovu dokumenta treće strane, a ta treća strana povuče dokument u pismenom obliku
- Format i tehnički sadržaj sertifikata predstavljaju neprihvatljiv rizik za oslanjajuće strane (na primer, ako korišćeni kriptografski algoritam i veličina ključa više nisu bezbedni)
- CA koji upravlja jedinicom za sertifikaciju ili izdavački CA prestao sa aktivnostima
- Zakon nalaže obavezno povlačenje

4.8.2 Ko može zatražiti opoziv

Povlačenje sertifikata može biti zatraženo od strane bilo koga korišćenjem sledećih usluga koje pruža Pružalac usluge od poverenja, ko zna tajnu lozinku za povlačenje i tražene identifikacione podatke:

- Usluga povlačenja putem veba
- U slučaju Email (S/MIME) sertifikata, usluga povlačenja putem SMS-a

Povlačenje sertifikata može biti zatraženo pismenim putem od strane klijenata, tačnije:

- Pretplatnik;
- Kontakt osoba navedena u ugovoru o pružanju usluge; Administrator organizacije imenovan od strane pretplatnika;
- Nadzorni organ koji je izdalo licencu za pružanje platnih usluga za subjekta, ako sertifikat sadrži podatke o subjektu u vezi sa zahtevima otvorenog bankarstva ili Direktive EU o platnim uslugama (PSD2) [2];
  i
- U slučaju usluge upravljanja ključevima na daljinu, pružalac usluge upravljanja ključevima na daljinu;
- Pružalac usluga od poverenja.

Dodatno, pretplatnici, strane koje se oslanjaju na sertifikate, dobavljači aplikativnog softvera i druge treće strane mogu podneti Izveštaje o visokorizičnim problemima sa sertifikatima, obaveštavajući Pružaoca usluge od poverenja o osnovanom razlogu za povlačenje sertifikata, poput prevare, zloupotrebe ili kompromitovanja ključa.

Pružalac usluge poverenja pruža jasne instrukcije o tome kako prijaviti sumnje na kompromitovanje privatnog ključa, zloupotrebu sertifikata ili druge vrste moguće prevare, kompromitovanja, zloupotrebe, neadekvatnog postupanja ili bilo koje druge stvari vezane za sertifikate na veb sajtu pružaoca usluga od poverenja.

4.8.3 Procedura zahteva za opoziv sertifikata

Pružalac usluge od poverenja omogućava sledeće mogućnosti za podnošenje zahteva za povlačenje:

- **Putem Veb-sajta Pružaoca usluge od poverenja 24 sata dnevno**

  Zahtev za povlačenje može se podneti putem sledećeg veb-sajta Pružaoca usluge poverenja: https://paperless.rs

  Prilikom suspendovanja putem veb-sajta Pružaoca usluge poverenja, klijent treba da pruži sledeće informacije:
  - Šifru suspendovanja kao podatak koji potvrđuje autentičnost zahteva za povlačenje,
  - Poslednje tri dela OID-a subjekta u sertifikatu (npr. 2.2.123), ili u slučaju fizičkog lica kao subjekta umesto OID-a datum rođenja subjekta.

  Zahtevi za povlačenje podneti putem veb-sajta Pružaoca usluge od poverenja obrađuju se bez odlaganja od strane informacionog sistema Pružaoca usluge od poverenja, a aplikantu se odmah obaveštava o rezultatu na njegovom veb-veb sajtu.
  U slučaju uspešnog povlačenja, promenjeni status povlačenja odmah se pojavljuje u internom registru statusa povlačenja Pružaoca usluge od poverenja. Unutrašnji procesi Pružaoca usluge od poverenja garantuju da se obrada završava u roku od najviše 5 minuta od pružanja podataka, tako da se promenjeni status povlačenja ažurira od trenutka prijema zahteva unutar tog maksimalnog intervala.
  Prilikom podnošenja zahteva putem veb-sajta Pružaoca usluge od poverenja, razlog povlačenja uvek je:

  - Kompromitovanje ključa (keyCompromise (1))

  Pružalac usluge od poverenja beleži svaki zahtev za suspendovanje. U slučaju uspešnog suspendovanja, Pružalac usluge od poverenja obaveštava subjekta i Naručilaca o činjenici suspendovanja putem e-pošte.

  Pružalac usluge od poverenja garantuje dostupnost usluge suspendovanja samo za zahteve za suspendovanje primljene putem SMS poruke. Ako veb-sajt Pružaoca usluge od poverenja nije dostupan, Pružalac usluge od poverenja preporučuje klijentu da zatraži suspendovanje slanjem SMS poruke.

- **Korišćenjem Korisničkog Portala**

  Zahtev za povlačenje može se podneti 24 sata dnevno korišćenjem Korisničkog Portala kojim operiše Pružalac usluge od poverenja.

  Adresa pristupa Korisničkom Portalu:
  https://vebsite.com

Na interfejsu Korisničkog Portala, Klijent treba da izabere sertifikate koji će biti povučeni, a zatim izaberite razlog povlačenja sa liste ispod:

- Kompromitovanje ključa (keyCompromise (1))
- Prestanak operacije (cessationOfOperation (5))
- Povlačenje privilegija (privilegeWithdrawn (9))

Za autentikaciju zahteva za povlačenje koji treba da bude podnet, dostupne su sledeće opcije:

- **Elektronski pečat**

  Kreiranjem elektronskog pečata na osnovu ne-pseudonimnog kvalifikovanog sertifikata aplikanta na interfejsu Korisničkog Portala.
  Podneti zahtevi za povlačenje obradjuju se od strane Pružaoca usluge od poverenja tokom radnog vremena kako je opisano u poglavlju 4.9.5.
  Korišćenjem ovog metoda, veliki broj sertifikata može biti povučen u jednoj aplikaciji.

- **Unosom Šifre za Suspenziju**

- Klijent unosi šifru suspenzije za Sertifikat koji će biti povučen na interfejsu Korisničkog Portala.
- Zahtevi za povlačenje koji su podneti na ovaj način odmah se obrađuju informacionim sistemom Pružaoca usluge od poverenja i odmah obaveštava podnosioca zahteva o rezultatu na svojoj veb stranici.
- Korišćenjem ovog metoda, ti sertifikati mogu biti povučeni u jednom zahtevu koji imaju istu šifru za suspenziju.

- **Poslat putem Emaila, sa Elektronskim Potpisom ili Elektronskim Pečatom**

  U elektronskom obliku sa elektronskim potpisom ili elektronskim pečatom zasnovanim na ne-pseudonimnom kvalifikovanom sertifikatu poslatom na email adresu Pružaoca usluge od poverenja office@paperless.rs.

  U podnetoj aplikaciji, aplikant mora izabrati razlog povlačenja sa liste ispod:

  - Kompromitovanje ključa (keyCompromise (1))
  - Sertifikat više nije potreban (cessationOfOperation (5))
  - Pravo upotrebe je opozvano (privilegeWithdrawn (9))

- **Na Papiru, Ručno Potpisan**

  Aplikacija potpisana ručno na papiru može se predati lično na Korisničkom servisu Pružaoca usluge od poverenja tokom radnog vremena, ili poslati poštom na adresu Korisničkog servisa Pružaoca usluge od poverenja kako je definisano u poglavlju 1.3.1. U podnetoj aplikaciji, aplikant mora izabrati razlog povlačenja sa liste ispod:

- Kompromitovanje ključa (keyCompromise (1))
- Sertifikat više nije potreban (cessationOfOperation (5))
- Pravo upotrebe je opozvano (privilegeWithdrawn (9))

U slučaju zahteva za opozivom koji je podnet pismeno, Pružalac usluge od poverenja proverava autentičnost zahteva i sposobnost podnosioca tokom evaluacije zahteva.
U slučaju zahteva za opozivom koji je potpisan validnim elektronskim potpisom, nema potrebe za daljom verifikacijom identiteta podnosioca i autentičnosti zahteva.
U slučaju podnošenja zahteva za opozivom na papiru, putem pošte, Pružalac usluge od poverenja proverava ručni potpis na zahtevu. Ako je opoziv zatražio klijent, a ne navede razlog za opoziv, tada Pružalac usluge od poverenja smatra da je razlog za opoziv to što subjekt više ne želi da koristi sertifikat (cessationOfOperation (5)). Ako klijent zatraži opoziv zbog kompromitovanja ključa, Pružalac usluge od poverenja omogućava mogućnost tokom procesa opoziva da se zatraži novi sertifikat u okviru ponovnog izdavanja kako bi se zamenio sertifikat koji treba da bude opozvan.
Pravila za ponovno izdavanje su u sekciji 4.7.
Kada se opoziv zatraži pismeno, Pružalac usluge od poverenja omogućava mogućnost da se opoziv zatraži unapred za kasniji datum navođenjem traženog datuma opoziva.
Zahtev za opoziv mora sadržati podatke koji identifikuju sertifikat. Podnosilac zahteva posebno treba da pruži sledeće informacije:

- Tačno ime subjekta;
- Ako je sertifikat izdat na uređaju za kreiranje kvalifikovanog elektronskog pečata, jedinstveni identifikator uređaja za kreiranje kvalifikovanog elektronskog pečata.
- Jedinstveni identifikator sertifikata;
- Traženi datum opoziva, ako opoziv ne treba da se desi odmah;
- Identifikacioni podaci klijenta.

U slučaju nevažećeg ili nepotpunog zahteva za opoziv, Pružalac usluge od poverenja odbacuje zahtev.
Pružalac usluge od poverenja obaveštava subjekta i pretplatnika putem e-pošte o činjenici i razlogu odbijanja.
U slučaju potpunog i važećeg zahteva, Pružalac usluge od poverenja donosi odluku o prihvatanju zahteva.
U zavisnosti od sadržaja zahteva, Pružalac usluge od poverenja odmah opoziva sertifikat ili postavlja datum opoziva prema zahtevu.
U slučaju uspešnog opoziva, Pružalac usluge od poverenja obaveštava subjekta i pretplatnika o opozivu putem e-pošte.
Dodatne informacije o suspenziji i opozivu mogu se pronaći na početnoj stranici Pružaoca usluge od poverenja na sledećem linku:

https://paperless.rs

- **Izveštaj o visokom prioritetu problema sa sertifikatom**

Pružalac usluge od poverenja održava neprekidnu sposobnost odgovora 24 sata dnevno, 7 dana u nedelji, internim reagovanjem na izveštaj o visokom prioritetu problema sa sertifikatom.
Pružalac usluge od poverenja je obavezan da obradi izveštaje o visokom prioritetu problema sa sertifikatom koji su podneti na srpskom ili engleskom jeziku, a obrada izveštaja o visokom prioritetu problema sa sertifikatom podnetih na drugim jezicima je neizvesna, te Pružalac usluge od poverenja može odbiti takve izveštaje bez suštinskog procesiranja.

Pružalac usluge od poverenja počinje istraživanje izveštaja o problemu sa sertifikatom u roku od 24 sata nakon prijema i odlučuje da li je opoziv adekvatan na osnovu sledećih kriterijuma:

- Priroda navodnog problema,
- Posledice opoziva,
- Broj izveštaja o problemu sa sertifikatom primljenih o određenom sertifikatu ili pretplatniku,
- Subjekt koji podnosi žalbu, i
- Relevantni zakoni.

Pružalac usluge od poverenja dostavlja preliminarni izveštaj o svojim nalazima kako pretplatniku tako i subjektu koji je podneo izveštaj o problemu sa sertifikatom.

Nakon pregleda činjenica i okolnosti, Pružalac usluge od poverenja sarađuje sa pretplatnikom i bilo kojim subjektom koji je prijavio izveštaj o problemu sa sertifikatom ili drugi obavešteni o opozivu kako bi se utvrdilo da li će sertifikat biti opozvan, i ako jeste, datum kada će Pružalac usluge od poverenja opozvati sertifikat.

Period od prijema izveštaja o problemu sa sertifikatom ili obaveštenja o opozivu do objavljenog opoziva ne sme preći vremenski okvir utvrđen u odeljku 4.9.5.

Ako je potrebno, Pružalac usluge od poverenja obaveštava Nacionalnu medijsku i infokomunikacionu agenciju o prijavljenom problemu.

4.8.4 Vreme za izdavanje zahteva za opoziv sertifikata

Pružalac usluga od poverenja ne primenjuje period oprosta tokom ispunjavanja zahteva za opozivom.

4.8.5 Vreme u kojem CA mora da obradi zahtev za opozivom

Pružalac usluge poverenja obrađuje sledeće zahteve za opoziv odmah, 24 sata dnevno:

- Zahtevi za opoziv koji su podneti putem veb-servisa Pružaoca usluge od poverenja.

Pružalac usluge od poverenja obrađuje zahteve za opoziv podnete na bilo koji drugi način u roku od 24 sata od zvaničnog vremena prijema zahteva.

Pružalac usluge od poverenja određuje datum prijema zahteva za opoziv na sledeći način:

- U slučaju zahteva za opoziv poslatih elektronskom poštom na posvećenu adresu e-pošte office@paperless.rs tokom radnog vremena Korisničke službe, zvanično vreme prijema je kada e-pošta stigne na server Pružaoca usluge od poverenja.
- U slučaju zahteva podnetih u Korisničkom portalu tokom radnog vremena Korisničke službe, zvanično vreme prijema je stvarno vreme podnošenja zahteva, zabeleženo od strane servera.

Zahtevi podneti van radnog vremena Korisničke službe smatraju se primljenim na početku narednog radnog vremena Korisničke službe.

- U slučaju podnošenja zahteva lično, vreme prijema je kada službenik Korisničke službe Pružaoca usluge od poverenja primi zahtev.
- U slučaju slanja zahteva poštom, vreme prijema je kada pošiljka stigne Pružaocu usluge od poverenja tokom radnog vremena.

Pružalac usluge od poverenja se obavezuje da ispuni ove zahteve samo za zahteve za opoziv poslate na naznačene adrese navedene u odeljku 1.3.1. U slučaju zahteva za opoziv poslatih na druge adrese - posebno direktno poslate određenim saradnicima Pružaoca usluge od poverenja - ili putem drugih kanala, Pružalac usluge od poverenja ne nudi dostupnost.

Ako klijent želi da opozove svoj sertifikat i opoziv je hitan, ili klijent ne može lično da se pojavi u kancelariji Pružaoca usluge od poverenja, Pružalac usluge od poverenja preporučuje klijentu da suspenduje sertifikat do opoziva koristeći SMS baziranu uslugu suspenzije (videti Poglavlje 4.9.13). Dovoljno je da se kasnije brine o opozivu suspendovanih sertifikata, i Pružalac usluge od poverenja automatski opoziva suspendovane sertifikate nakon isteka vremena za obnovu (videti Poglavlje: 4.9.16.).

4.8.6 Provera opoziva od strane pouzdanih strana

Da bi se održao nivo sigurnosti garantovan od strane Pružaoca usluga od poverenja, pre nego što se informacije navedene u Sertifikatu usvoje i koriste, neophodno je da pouzdane strane postupaju sa odgovarajućom pažnjom. Posebno im se preporučuje da provere sve Sertifikate koji se nalaze u lancu Sertifikata prema relevantnim tehničkim standardima. Verifikacija bi trebalo da obuhvati proveru važenja Sertifikata, zahteve polise i korišćenja ključeva, kao i proveru informacija o opozivu zasnovanih na referentnim CRL ili OCSP podacima.

4.8.7 Frekvencija izdavanja CRL-a

Pružalac usluge od poverenja izdaje novu Listu opozvanih sertifikata za svoje korisničke sertifikate najmanje jednom dnevno. Valjanost ovih Lista opozvanih sertifikata je 25 sati.

Pružalac usluge od poverenja izdaje novu Listu opozvanih sertifikata za svoje sertifikate posredne sertifikacije svakog dana u isto vreme. Valjanost Lista opozvanih sertifikata je 25 sati.

4.8.8 Maksimalno odlaganje za CRL-ove

Najviše 5 minuta prođe između generisanja i objavljivanja Liste opozvanih sertifikata (CRL).

4.8.9 Dostupnost online provere/statusa povlačenja

Pružalac usluge od poverenja pruža online uslugu statusa sertifikata (OCSP).

4.8.10 Online zahtevi za proverom poništenja

Usluga statusa sertifikata putem interneta usklađena je sa zahtevima odeljka 4.10. Sertifikaciono telo pruža OCSP uslugu putem GET metode.

4.8.11 Druge vrste obaveštenja o povlačenju koje su dostupne

Pružalac usluge od poverenja omogućava u svom javnom repozitorijumu sertifikata - sa njihovim statusom - povučene i suspendovane sertifikate. Na taj način, pretraživanjem repozitorijuma sertifikata, klijenti i pouzdane strane mogu lično (bez pomoći aplikacije) da provere status povučenog sertifikata.

4.8.12 Posebni zahtevi za kompromitovan ključ

Svaka zainteresovana strana može podneti izveštaj o kompromitaciji ključa nadležnom sertifikacionom telu ako sazna da je privatni ključ bilo kog sertifikata izdatog od strane tog tela kompromitovan.

Najbrži način za prijavu je na sledećem veb sajtu: https://website.com.

Prilikom prijave, podnosilac izveštaja mora dokazati da je privatni ključ zaista kompromitovan. Izveštaj mora da navede:

- Sam kompromitovani privatni ključ, ili
- PKCS#10 zahtev za sertifikat potpisan kompromitovanim privatnim ključem i sadrži sledeći tekst u polju "CN": "Proof of Key Compromise".

U slučaju kompromitacije privatnog ključa bilo kog sertifikacionog tela, Pružalac usluge od poverenja ulaže svaki razuman napor da obavesti pouzdane strane o incidentu. Objavljuje svaku promenu statusa na sertifikatima na svojoj veb-stranici. U slučaju kompromitovanih sertifikata izdatih od strane Pružaoca usluge od poverenja, Pružalac usluge od poverenja je sposoban da povuče sertifikat krajnjeg korisnika koji pripada kompromitovanom privatnom ključu. Informacija o razlogu povlačenja (reasonCode) u tom slučaju postavlja se na vrednost keyCompromise (1).

4.8.13 Okolnosti za obustavu

Kada je to moguće, Pružalac usluge od poverenja omogućava klijentima mogućnost privremenog suspenzovanja sertifikata.

Pružalac usluge od poverenja ima pravo da suspenduje sertifikat iz sledećih razloga:

- Pretplatnik ne izmiruje obaveze do roka za plaćanje;
- Ako Pružalac usluge od poverenja pretpostavi da podaci navedeni na sertifikatu nisu u skladu sa stvarnošću. Ako Pružalac usluge od poverenja sazna za takve uslove, pokreće suspenziju ili povlačenje sertifikata;
- Ako Pružalac usluge od poverenja pretpostavi da privatni ključ koji pripada sertifikatu nije u posedu Subjekta, a to je potvrđeno značajnim dokazima. Ako Pružalac usluge od poverenja sazna da je uređaj za kreiranje elektronskog pečata u posedu neovlašćene osobe, Pružalac usluge od poverenja suspenduje svaki sertifikat koji sadrži taj ključ;
- Nadzorno telo donese (nešto) u pravno obavezujućoj i izvršnoj odluci.

Pružalac usluge od poverenja ne prihvata zahteve za suspenziju koji se odnose na sertifikate koji nisu važeći, osim ako se ne opravda razlog za odbijanje.

4.8.14 Ko može zatražiti suspenziju

Suspenziju sertifikata može zatražiti ista osoba koja je ovlašćena da pokrene povlačenje sertifikata (videti sekciju: 4.9.2.).

4.8.15 Postupak zahteva za suspenziju sertifikata

Pružalac usluga od poverenja obezbeđuje mogućnost pokretanja suspenzije na sledeće načine:

- **Suspenzija putem Veb stranice Pružaoca usluga od poverenja 24 sata dnevno**

  Zahtev za suspenziju može se podneti putem sledeće veb stranice Pružaoca usluga od poverenja:
  https://paperless.rs

  Prilikom suspenzije putem veb stranice Pružaoca usluga od poverenja, klijent treba da pruži sledeće informacije:

  - Šifru suspenzije kao podatak koji potvrđuje autentičnost zahteva za suspenziju,
  - Poslednje tri cifre OID-a podnosioca u sertifikatu (npr. 2.2.123), ili u slučaju podnosioca fizičkog lica umesto OID-a datum rođenja podnosioca.

  Zahtevi za suspenziju podneti putem veb stranice Pružaoca usluga od poverenja obrađuju se bez odlaganja od strane informacionog sistema Pružaoca usluga od poverenja i on odmah obaveštava podnosioca o rezultatu na svojoj veb stranici.
  U slučaju uspešne suspenzije, promenjeni status suspenzije odmah se pojavljuje u internom registru statusa suspenzije Pružaoca usluga od poverenja. Unutrašnji procesi Pružaoca usluga od poverenja obezbeđuju da se obrada završi najkasnije u roku od 5 minuta od pružanja podataka, tako da se promenjeni status suspenzije ažurira od trenutka prijema zahteva u maksimalnom intervalu.
  Kada se zahtev podnese putem veb stranice Pružaoca usluga od poverenja, razlog suspenzije uvek je:

- kompromitovanje ključa (keyCompromise (1))

Pružalac usluga od poverenja beleži svaki zahtev za suspenziju. U slučaju uspešne suspenzije, Pružalac usluga od poverenja obaveštava podnosioca i pretplatnika o činjenici suspenzije putem e-pošte.
Pružalac usluga od poverenja garantuje dostupnost usluge suspenzije samo za zahteve za suspenziju primljene putem SMS poruka. Ako veb stranica Pružaoca usluga od poverenja nije dostupna, Pružalac usluga od poverenja preporučuje klijentu da zatraži suspenziju slanjem SMS poruke.

- **Korišćenjem Korisničkog Portala**

  Zahtev za povlačenje može se podneti 24 sata dnevno korišćenjem Korisničkog Portala kojim operiše Pružalac usluge od poverenja.

  Adresa pristupa Korisničkom Portalu:
  https://vebsite.com

  Na interfejsu Korisničkog Portala, Klijent treba da izabere sertifikate koji će biti povučeni, a zatim izaberite razlog povlačenja sa liste ispod:

  - Kompromitovanje ključa (keyCompromise (1))
  - Prestanak operacije (cessationOfOperation (5))
  - Povlačenje privilegija (privilegeWithdrawn (9))

  Za autentikaciju zahteva za povlačenje koji treba da bude podnet, dostupne su sledeće opcije:

  - **Elektronski pečat**

    Kreiranjem elektronskog pečata na osnovu ne-pseudonimnog kvalifikovanog sertifikata aplikanta na interfejsu Korisničkog Portala.
    Podneti zahtevi za povlačenje obradjuju se od strane Pružaoca usluge od poverenja tokom radnog vremena kako je opisano u poglavlju 4.9.5.
    Korišćenjem ovog metoda, veliki broj sertifikata može biti povučen u jednoj aplikaciji.

- **Suspenzija na isti način kao podnošenje zahteva za opoziv**

  Pružalac usluga od poverenja omogućava podnošenje zahteva za suspenziju na isti način kao zahteva za opoziv, u skladu sa zahtevima sekcije 4.9.3. Iz aplikacije za suspenziju, Pružalac usluga od poverenja mora biti u mogućnosti da utvrdi tačno koji sertifikat podnosilac zahteva traži da se suspenduje i iz kojih razloga. Član osoblja za registraciju šalje obaveštenje putem e-pošte podnosiocu zahteva i pretplatniku.
  Prilikom suspenzije, razlog suspenzije mora biti naveden. Ako klijent zatraži suspenziju, a ne navede razlog, Pružalac usluga od poverenja pretpostavlja da je razlog kompromitovanje privatnog ključa (keyCompromise (1)).
  Ako klijent zatraži suspenziju zbog kompromitovanja ključa, Pružalac usluga od poverenja pruža mogućnost Klijentu tokom procesa suspenzije da naznači da će, ukoliko sertifikat ne bude vraćen u roku (i tako postane opozvan), biti zatražen novi sertifikat u okviru Re-key. Pravila za Re-key nalaze se u sekciji 4.7.

4.8.16 Ograničenja na period suspenzije

Ako je suspenzija sertifikata zahtevana od strane klijenta, klijent može zatražiti ponovno aktiviranje sertifikata u roku od 5 radnih dana nakon suspenzije. Ako ponovno aktiviranje sertifikata nije zatraženo u ovom intervalu, Pružalac usluga od poverenja opoziva sertifikat.

Zahtev za ponovno aktiviranje sertifikata može se podneti samo Pružaocu usluga od poverenja:

- Lično u korisničkom servisu Pružaoca usluga od poverenja;
- U elektronskom obliku sa elektronskim potpisom zasnovanim na nepseudonimnom kvalifikovanom sertifikatu.

U slučaju uspešnog ponovnog aktiviranja sertifikata, Pružalac usluga od poverenja obaveštava podnosioca zahteva i pretplatnika putem e-pošte o tome.

4.9 Usluge statusa sertifikata

Pružalac usluga od poverenja omogućuje sledeće mogućnosti za upit o statusu opoziva sertifikata:

- OCSP – online usluga upita o statusu opoziva sertifikata,
- CRL – Liste opozvanih sertifikata.

Pružalac usluga od poverenja održava interni registar statusa opoziva, koji sadrži informacije o trenutnom statusu opoziva svih sertifikata izdatih od strane Pružaoca usluga od poverenja, uključujući važeće, opozvane i suspendovane statuse.

U slučaju suspendovanja, ponovnog aktiviranja i opoziva, novi status sertifikata - vidi Poglavlje: 4.9. - odmah se pojavljuje u evidenciji opoziva Pružaoca usluga od poverenja nakon uspešnog završetka procesa.

Registar statusa opoziva takođe sadrži informacije o statusu opoziva isteklih sertifikata, koje će biti dostupne do datuma isteka izdavačkog CA.

Pružalac usluga od poverenja generiše listu opozvanih sertifikata na osnovu aktuelnih informacija dobijenih iz registra statusa opoziva, tako da će svaka promena u statusima opoziva biti objavljena u prvoj listi opozvanih sertifikata izdatih nakon date promene.

OCSP odgovori izdati od strane OCSP Pružaoca usluga od poverenja uvek se zasnivaju na informacijama o statusu opoziva dobijenih iz rRegistra statusa opoziva u trenutku koji je naznačen u OCSP odgovoru.

OCSP odgovor izdat od strane Pružaoca usluga od poverenja može sadržavati informacije "dobro" statusa samo za sertifikate koji su izdati od strane određene sertifikacione jedinice i koji se čuvaju u repozitorijumu sertifikata Pružaoca usluga od poverenja (pozitivni OCSP).

4.9.1 Operativne karakteristike

Svaka sertifikaciona jedinica Pružaoca usluga od poverenja izdaje Listu opozvanih sertifikata sa sledećom učestalošću:

- Svaka korenska sertifikaciona jedinica Pružaoca usluga od poverenja izdaje CRL najviše jednom u roku od 24 sata.
- Produktivne (podređene) sertifikacione jedinice koje se koriste u okviru sistema Pružaoca usluga od poverenja izdaju CRL u roku od 60 minuta nakon promene statusa opoziva bilo kog sertifikata izdate od strane određene sertifikacione jedinice, ali najmanje jednom u roku od 24 sata.

Period važenja Liste opozvanih sertifikata je 25 sati.

Svevremenski trenutno važeće Liste opozvanih sertifikata za određene sertifikate mogu se pronaći na sledećoj adresi:

https://vebsite.com

Datum stupanja na snagu Liste opozvanih sertifikata ("thisUpdate") označava i vreme kada je sertifikaciona jedinica sastavljena i počela da potpisuje Listu opozvanih sertifikata. Nakon toga, u slučaju dugih Lista opozvanih sertifikata, objavljivanje Liste opozvanih sertifikata može trajati 1 ili 2 minuta. Pojava sledeće Liste opozvanih sertifikata ("nextUpdate") označava najkasnije sledeće vreme, od kojeg je lista javno dostupna. Prema tome, vremenski interval između datuma kada Lista opozvanih sertifikata stupa na snagu i datuma objavljivanja sledeće Liste opozvanih sertifikata može biti duži od navedenih vremenskih intervala, ali to ne utiče na vremenski interval između pojave CRL-a koji iznosi najviše 24 sata.

Imajući u vidu da se među pruženim uslugama, važnost sertifikata može odrediti najbrže i najlakše putem OCSP-a, sertifikacioni autoritet preporučuje upotrebu OCSP-a svojim klijentima.

Online Certificate Status Protocol (OCSP)

Pružalac usluga od poverenja takođe objavljuje status opoziva sertifikata putem OCSP servisa.

Pružalac usluga od poverenja pruža OCSP servis u skladu sa IETF RFC 6960 principom "autorizovanog odgovarača", tako da svaka sertifikaciona jedinica posebno sertifikuje OCSP odgovarača, koji pruža informacije o statusu opoziva sertifikata izdatih od strane sertifikacione jedinice.

Pružalac usluga od poverenja pruža OCSP usluge na dva različita načina, a ispod su prikazane karakteristike ova dva pristupa.

OCSP Servis Pružen Klijentima

- Koriste ovu verziju OCSP servisa samo oni klijenti koji imaju važeći ugovor o održavanju tog sertifikata. Pružalac usluga od poverenja može identifikovati klijenta putem sertifikata ili putem para korisničkog imena i lozinke pri upitu.
- Ova verzija OCSP servisa je dostupna za sve sertifikate, odgovori uvek sadrže trenutne informacije navedene u registru Pružaoca usluga od poverenja.
- Izdati OCSP odgovor uvek se pravi u trenutku upita. Vrednosti vremena "thisUpdate" i "producedAt" u OCSP odgovoru se podudaraju sa vremenom upita.
- "nextUpdate" naznačen u odgovoru ili nije popunjen ili sadrži vremensku vrednost koja nije kasnija od vremena isteka sertifikata odgovarača.
- Pomoću OCSP servisa koji je dostupan klijentima uvek se može prikupiti dokaz koji kasnije potvrđuje prema trećim stranama status opoziva sertifikata navedenog u registru Pružaoca usluga od poverenja za datum upita.

Javni i Besplatni OCSP Servis

- Ova verzija OCSP servisa je javno i besplatno dostupna, svaka Pouzdana strana može da je koristi isto kao i Liste opozvanih sertifikata. Nema potrebe za autentifikacijom prilikom upita.
- Ova verzija OCSP servisa može se dostići putem URL-ova navedenih na sertifikatima na podrazumevanom HTTP portu (port 80).
- U slučaju Email (S/MIME) sertifikata, OCSP servis ispunjava zahtev IETF RFC 5019 [35] da podrži PKI okruženja velikog obima koja zahtevaju laganu rešenje kako bi se minimizirala propusnost komunikacije i obrada na klijentskoj strani.
- Na osnovu IETF RFC 6960 "Response Pre-production" procesa, izdati OCSP odgovor može biti kreiran pre upita i ne mora nužno sadržati element nonce. Vremenske vrednosti "thisUpdate" i "producedAt" su identične, ali one mogu prethoditi vremenu upita.
- U slučaju Email (S/MIME) sertifikata, "nextUpdate" koji je naznačen u odgovoru uvek je popunjen i sadrži vremensku vrednost koja nije kasnija od vremena isteka sertifikata odgovarača.
- U slučaju drugih sertifikata, "nextUpdate" koji je naznačen u odgovoru ili nije popunjen ili sadrži vremensku vrednost koja nije kasnija od vremena isteka sertifikata odgovarača.
- Vrednost "thisUpdate" naznačena u izdatom OCSP odgovoru nikada nije starija od 24 sata, jer Pružalac usluga od poverenja kreira novi OCSP odgovor barem svakih 24 sata.
- U slučaju Email (S/MIME) sertifikata, razlika u vremenu između "nextUpdate" i "thisUpdate" vrednosti u izdatom OCSP odgovoru nikada nije manja od 8 sati.
- Razlika u vremenu između "nextUpdate" i "thisUpdate" vrednosti u izdatom OCSP odgovoru nikada nije veća od 10 dana.
- OCSP odgovori uvek sadrže trenutne informacije navedene u registru opoziva Pružaoca usluga od poverenja u vremenu "thisUpdate" OCSP odgovora, ali ako je vreme "thisUpdate" OCSP odgovora ranije od vremena za koje se vrši provera - što je ili ranije ili se poklapa sa vremenom upita - tada OCSP odgovor nije jasan dokaz trećoj strani u vezi sa statusom opoziva sertifikata.

Zbog navedenih razlika između pomenute dve verzije OCSP servisa, javni i besplatni servis može se smatrati ekvivalentnim servisu koji se pruža klijentima u sledećim slučajevima:

- Ako nema potrebe za čuvanjem OCSP odgovora, već se koristi za brzo, odmah odlučivanje. U ovom slučaju, prihvatljivo je da OCSP odgovor ne potvrđuje jasno validnost sertifikata trećim stranama u određenom trenutku naknadno.
- Ako je vremenski razmak između vremena OCSP upita i vremena, u kom se vrši provera, veći od razlike između vrednosti "nextUpdate" i "thisUpdate" u sačuvanom OCSP odgovoru (koji može biti najviše period važenja sertifikata odgovarača korišćen za potpisivanje OCSP odgovora). U ovom slučaju, OCSP odgovori koje pruža javni i besplatni servis mogu se prihvatiti kao jasan dokaz za treću stranu, jer je polje thisUpdate u njima garantovano kasnije od vremena, u kom se vrši provera.
- Ako strana koja vrši proveru ne upita OCSP odgovor direktno (već, na primer, koristi OCSP odgovor priložen uz arhivsku potpis), tada nije potrebno proveriti izvorne izvore OCSP odgovora. Dovoljno je verifikovati samo da je vrednost "thisUpdate" u OCSP odgovoru kasnija od vremena, u kom se vrši provera.

Pružalac usluga od poverenja osigurava navedene dve verzije OCSP servisa sa istom dostupnošću.

4.9.2 Dostupnost usluge

Pružalac usluga od poverenja garantuje dostupnost repozitorijuma sertifikata i uslove i odredbe vezane za sertifikate izdatih od strane Pružaoca usluga od poverenja u najmanje 99,9% godišnje, a trajanje prekida ne sme biti duže od 3 sata.

Pružalac usluga od poverenja garantuje dostupnost informacija o statusu opoziva i uslugu upravljanja opozivom u najmanje 99,9% godišnje, a trajanje prekida ne sme biti duže od najviše 3 sata u bilo kom trenutku.

Vreme odziva usluge statusa opoziva u slučaju normalnog funkcionisanja je manje od 10 sekundi.

4.9.3 Opcionalne karakteristike

Pružalac usluga od poverenja pruža različite usluge (CRL i dva tipa OCSP) prema opisima u ovoj sekciji, u okviru kojih klijenti i strane kojima se oslanjaju mogu proveriti status opoziva sertifikata izdatih od strane Pružaoca usluga od poverenja. Pored toga, Pružalac usluga od poverenja omogućava pristup svojem javnom Repozitorijumu sertifikata - sa naznačenim statusima - opozvanih i suspendovanih sertifikata, tako da klijenti i strane kojima se oslanjaju mogu (bez pomoći aplikacije) proveriti status opoziva sertifikata dok pretražuju repozitorijum sertifikata.

4.10 Kraj pretplate

Pružalac usluga od poverenja povući će sertifikate krajnjih korisnika u slučaju raskida ugovora zaključenog sa pretplatnikom.

5 Ovlašćenja, Upravljanje i Operativne Kontrole

Pružalac usluga od poverenja primenjuje fizičke, proceduralne i personalne mere bezbednosti koje su u skladu sa priznatim standardima, zajedno sa administrativnim i upravljačkim procedurama koje ih sprovode.

Pružalac usluga od poverenja vodi evidenciju o jedinicama sistema i resursima koji se odnose na pružanje usluga, i sprovodiće procenu rizika na osnovu njih. Koristi zaštitne mere proporcionalne rizicima povezanim sa pojedinačnim elementima.

Pružalac usluga od poverenja prati potrebe kapaciteta i osigurati da su dostupne odgovarajuće procesorske snage i skladištenje za pružanje usluga.

5.1 Fizičke kontrole

Pružalac usluga od poverenja treba da vodi računa o tome da se fizički pristup kritičnim uslugama kontroliše i da se fizički rizik po imovinu koja se odnosi na kritične usluge svede na minimum.

Svrha fizičkih mera opreza je sprečavanje neovlašćenog pristupa, oštećenja i neovlašćenog pristupa informacijama Pružaoca usluga od poverenja i fizičkim zonama.

Usluge koje obrađuju kritične i osetljive informacije treba da budu implementirane na bezbednim lokacijama.

Primenjena zaštita treba da bude proporcionalna identifikovanim pretnjama analize rizika koju je Pružalac usluga od poverenja sproveo.

Da bi pružio adekvatnu bezbednost:

- Pružalac usluga od poverenja implementira snažno zaštićene usluge u svojoj zaštićenoj računarskoj sali. Ova računarska sala je posebno dizajnirana i izgrađena u tu svrhu, uz uniformno sprovođenje različitih aspekata zaštite (raspored i struktura lokacije, fizički pristup (kontrola pristupa i nadzor), napajanje, klimatizacija, zaštita od curenja vode i poplava, prevencija i zaštita od požara, skladištenje medija itd.).
- Kancelarija Korisničke podrške Pružaoca usluga od poverenja je dizajnirana da može da ispuni zahteve za registracione usluge po realnim troškovima.
- Pružalac usluga od poverenja konstruisao je svoje pokretne registracione jedinice tako da odgovaraju zahtevima postavljenim na registracionu uslugu.
- Pružalac usluga poverenja implementira svaku ključnu uslugu i svaki neophodan alat u zasebnoj sigurnosnoj zoni. Svi uređaji potrebni za to smešteni su u zaštićenoj računarskoj sali - koja čini deo sigurnosne zone.

5.1.1 Lokacija i konstrukcija

IT sistem Pružaoca usluga poverenja smešten je i operiše unutar adekvatno obezbeđenog Data centra sa fizičkom i logičkom zaštitom koja sprečava neovlašćen pristup. Defanzivna rešenja - kao što su čuvari, sigurnosne brave, sistemi za detekciju upada, video nadzor, sistem kontrole pristupa - primenjuju se tokom lociranja i uspostavljanja Data centra koji se grade jedno na drugom i suzavni, i zajedno pružaju moćan sistem zaštite za IT sisteme koji učestvuju u pružanju usluga, i za čuvanje poverljivih podataka koje čuva pružalac.

5.1.2 Fizički pristup

Pružalac usluga od poverenja treba da zaštiti uređaje i opremu koji učestvuju u pružanju usluge od neovlašćenog fizičkog pristupa kako bi se sprečilo manipulisanje uređajima.

Pružalac usluga od poverenja treba da obezbedi da:

- Svaki ulazak u Data centar bude evidentiran;
- Ulazak u Data centar može se desiti samo nakon istovremene identifikacije dva ovlašćena člana osoblja sa pouzdanim ulogama - i barem jedan od članova osoblja mora biti sistemski administrator;
- Osobe bez nezavisne autorizacije mogu boraviti u Data centru samo u opravdanim slučajevima, za vreme potrebno za izvršenje zadatka i u pratnji osoblja sa odgovarajućim ovlašćenjima;
- Evidencija ulaska mora se kontinuirano arhivirati.

Aktivacioni podaci (šifre, PIN kodovi) uređaja ne smeju biti otvoreno skladišteni čak ni u Data centru.

U prisustvu neovlašćenih osoba:

- Medijski nosači podataka koji sadrže osetljive informacije treba da budu van domašaja;
- Terminali na kojima je neko prijavljen ne smeju ostati bez nadzora;
- Ne bi trebalo obavljati radne procese tokom kojih bi mogle biti otkrivene poverljive informacije.

Pri napuštanju prostorije sa računarima, administrator treba da proveri da li:

- Su svi uređaji u Data centru u adekvatnom bezbednom operativnom stanju;
- Nijedan terminal nije ostavljen prijavljen;
- Su fizički skladišni uređaji pravilno zaključani;
- Sistemi, uređaji za fizičku zaštitu funkcionišu ispravno;
- Je alarmni sistem aktiviran.

Treba imenovati odgovorne osobe za redovne procene fizičke bezbednosti.

Rezultati pregleda treba da budu zabeleženi u odgovarajućim evidencijama.

5.1.3 Napajanje i klimatizacija

Pružalac usluga od poverenja primenjuje neometanu jedinicu za napajanje u Data centru koja:

- ima adekvatan kapacitet da osigura napajanje za IT sisteme Data centra i prateće sisteme;
- štiti IT opremu od fluktuacija napona u spoljnoj mreži, prekida napajanja, prenapona i slično;
- u slučaju trajnog prekida napajanja ima svoju opremu za generisanje energije koja može obezbediti potrebnu energiju tokom bilo kog perioda.

Spoljni vazduh ne sme direktno ulaziti u Data centar. Čistoća vazduha u Data centru obezbeđuje se adekvatnim sistemom filtera koji detektuje različite kontaminante iz vazduha (prašinu, zagađivače i korozivne materijale, toksične ili zapaljive supstance).

Ventilacioni sistem treba obezbediti neophodnu količinu svežeg vazduha sa odgovarajućim filtriranjem za bezbedne radne uslove operatera.

Vlažnost treba smanjiti na nivo potreban za IT sisteme.

Pružalac usluga poverenja od koristi sisteme za hlađenje sa odgovarajućim performansama kako bi obezbedio potrebnu radnu temperaturu i sprečio pregrevanje IT uređaja.

5.1.4 Izloženost vodi

Data centar Pružaoca usluga od poverenja adekvatno je zaštićen od prodora vode i poplava. Ukupna površina sigurnosne zone je slobodna od sanitarnih prostorija, nema nikakvih odvoda niti vodovodnih cevi u blizini.

Celokupno područje zone bezbednosti od vode nadgleda sistem za detekciju upada.

U zaštićenoj računarskoj sobi sigurnost je dodatno pojačana upotrebom podignutog poda.

5.1.5 Prevencija i zaštita od požara

U Data centru Pružaoca usluga od poverenja funkcioniše sistem zaštite od požara odobren od nadležne vatrogasne brigade. Detektori dima i požara automatski obaveštavaju vatrogasnu brigadu.

U računarskoj sobi instaliran je automatski sistem gašenja požara na bazi vodene pare, koji nije opasan po ljudski život i ne oštećuje IT opremu.

U svakoj prostoriji nalazi se određena vrsta i količina ručnih aparata za gašenje požara u skladu sa relevantnim propisima, postavljeni na vidljivim mestima.

5.1.6 Skladište za medije

Pružalac usluga od poverenja štiti svoje medije za skladištenje od neovlašćenog pristupa i slučajnih oštećenja. Sva revizijska i arhivska podataka se stvaraju u duplikatu. Dva primerka se čuvaju fizički odvojeno jedan od drugog u protivpožarnim sefovima, na lokacijama udaljenim jedna od druge u prostoriji za operatere u data centru koji se koristi za poverene usluge.

Skladišni mediji su zaštićeni od štetnih uticaja okoline kao što su niske ili visoke temperature, prljavština, vlaga, sunčeva svetlost, jaka magnetska polja i jaka radijacija.

5.1.7 Odlaganje otpada

Pružalac usluga od poverenja obezbeđuje postupak odlaganja viška imovine i medija koji je u skladu sa ekološkim standardima.

Pružalac usluga od poverenja ne koristi elektronske skladišne medije koji sadrže informacije klasifikovane kao poverljive čak ni za skladištenje podataka koji nisu poverljivi nakon brisanja njihovog sadržaja, i uređaji poput toga ne smeju biti izneti van prostorija Pružaoca usluga od poverenja.

Pružalac usluga od poverenja fizički uništava - prema pravilima odlaganja - neispravne iz drugih razloga neupotrebljive, redundantne skladišne medije koji sadrže poverljive klasifikovane informacije:

- seče papirne dokumente u mašini za uništavanje papira;
- rasklapa tvrde diskove i uništava kritične komponente;
- uništava optičke diskove pomoću odgovarajuće mašine za uništavanje.

5.1.8 Rezervne kopije podataka van objekta (Off-Site Backup)

Pružalac usluga od poverenja nedeljno pravi sigurnosne kopije pomoću kojih bi ceo servis mogao biti obnovljen u slučaju fatalne greške. Sigurnosne kopije - uključujući barem poslednju potpunu kopiju - čuvaju se na eksternoj lokaciji čija je fizička i operativna zaštita identična primarnoj lokaciji. Obezbeđen je siguran prenos podataka između primarne i rezervne lokacije.

Na osnovu nasumično odabranih podataka iz sigurnosnih kopija, godišnje se vrši test obnove. Glavne okolnosti i rezultati testa obnove se beleže u izveštaju o reviziji.

5.2 Proceduralne mere

Pružalac usluga od poverenja brine se da njegovi sistemi budu bezbedno operativni, u skladu sa pravilima i sa minimalnim rizikom od grešaka. Proceduralne mere imaju za cilj da dopune, ali istovremeno i da pojačaju efikasnost fizičkih zaštita, kao i onih koje se odnose na osoblje, putem imenovanja i izolacije pouzdanih uloga, dokumentovanja odgovornosti različitih uloga, kao i specificiranja broja osoblja i izuzeća neophodnih za različite zadatke.

Interni sistem upravljanja Pružaoca usluga od poverenja osigurava da njegovo poslovanje bude u skladu sa zakonskim, kao i internim propisima. U svom sistemu odgovorna osoba će biti jasno dodeljena za svaku datu sistemsku jedinicu i proces.

Osobe odgovorne za određeni element ili proces sistema su jednoznačno dodeljene svakoj sistemskoj jedinici i svakom procesu u sistemu Pružaoca usluga od poverenja. Razvojne i operativne zadatke strogo se razdvajaju u sistemu Pružaoca usluga od poverenja. Revizorska aktivnost nezavisnog revizora sistema i internog revizora Pružaoca usluga od poverenja obezbeđuje odgovarajuće funkcionisanje sistema.

5.2.1 Pouzdane uloge

Pružalac usluga od poverenja definiše sledeće pouzdane uloge, sa sledećim odgovornostima:

Menadžer sa opštom odgovornošću za IT sistem provajdera;

Osoba odgovorna za IT sistem.

Bezbednosni službenik

Stariji bezbednosni saradnik, osoba koja ima opštu odgovornost za bezbednost usluge.

Administrator sistema

Administrator infrastrukture. Osoba zadužena za instalaciju, konfiguraciju i održavanje sistema Pružaoca usluga od poverenja. Odgovorna je za pouzdan i kontinuiran rad dodeljenih sistemskih jedinica, praćenje razvoja tehnologije i otkrivanje te predlaganje rešenja za razvoj ranjivosti svake komponente sistema.

Operater

Operater sistema, pojedinac koji obavlja kontinuiranu operaciju IT sistema, kao i njegovu sigurnosnu kopiju i obnavljanje.

Nezavisni sistemski auditor

Pojedinac koji vrši reviziju zabeleženih, kao i arhiviranih podataka Pružaoca usluga od poverenja, odgovoran je za proveru sprovođenja kontrolnih mera koje Pružalac usluga implementira u cilju obezbeđenja operacija u skladu sa propisima, kao i za kontinuiranu reviziju i praćenje postojećih procedura.

Registracioni službenik

Pojedinac odgovoran za odobravanje proizvodnje, izdavanja, opoziva i suspenzije krajnjih korisničkih sertifikata.

Za dodelu pouzdanih uloga, menadžer odgovoran za bezbednost Pružaoca usluga od poverenja formalno imenuje zaposlene Pružaoca usluga od poverenja. Pouzdane uloge mogu obavljati samo osobe koje su u radnom odnosu sa Pružaocem usluga od poverenja. Pouzdane uloge ne smeju se držati u kontekstu ugovora o komisiji. Vode se ažurni podaci o pouzdanim ulogama i u slučaju bilo kakve promene, Nacionalna medijska i informatička agencija odmah se obaveštava.

5.2.2 Broj osoba potrebnih po zadatku

Bezbednosni i operativni propisi Pružaoca usluga od poverenja definišu da sledeći zadaci mogu biti obavljeni samo u zaštićenom okruženju, uz istovremeno prisustvo dva zaposlena koji obavljaju pouzdane uloge:

- Generisanje para ključeva usluge Pružaoca usluga od poverenja;
- Izrada sigurnosne kopije privatnog ključa Pružaoca usluga;
- Aktiviranje privatnog ključa Pružaoca usluga;
- Uništavanje privatnog ključa Pružaoca usluga.

Najmanje jedna od osoba koje obavljaju navedene postupke treba da bude sistem administrator, dok druga osoba ne sme biti nezavisni revizor sistema.

Tokom sprovođenja navedenih operacija, neovlašćena lica ne smeju biti prisutna u prostoriji.

5.2.3 Identifikacija i autentikacija za svaku ulogu

Korisnici koji upravljaju IT sistemom Pružaoca usluga od poverenja imaju jedinstvene podatke za identifikaciju, omogućavajući sigurnu identifikaciju i autentifikaciju korisnika.

Korisnici mogu pristupiti samo IT sistemima koji su kritični sa aspekta pružanja usluge sertifikacije nakon identifikacije i autentifikacije.

Podaci za identifikaciju i autentifikaciju odmah se opozivaju u slučaju prestanka korisničkih prava.

Svaki korisnik IT sistema i svaki akter u administrativnom procesu identifikuje se individualno.

Za verifikaciju fizičkog pristupa, Pružalac usluga od poverenja koristi sistem kontrole pristupa zasnovan na RFID kartici, dok za logičku kontrolu pristupa koristi VPN sertifikate izdatih na Sigurnom uređaju za kreiranje potpisa. Pre uspešne autorizacije, ni jedan sigurnosno kritičan zadatak ne može biti izvršen. Svaki zaposleni Pružaoca usluga od poverenja ima tačno toliko prava pristupa koliko je apsolutno neophodno za dodeljenu ulogu.

5.2.4 Funkcije koje zahtevaju razdvajanje zaduženja

Zaposleni Pružaoca usluga od poverenja mogu istovremeno obavljati više poverenih uloga, ali Pružalac usluga od poverenja je dužan da obezbedi sledeće:

- Sigurnosni službenik i službenik za registraciju ne smeju obavljati ulogu nezavisnog sistemskog revizora;
- Administrator sistema ne sme obavljati ulogu sigurnosnog službenika i nezavisnog sistemskog revizora;
- Menadžer sa ukupnom odgovornošću za IT sistem ne sme obavljati ulogu sigurnosnog službenika i nezavisnog sistemskog revizora.

Pored pomenutog, Pružalac usluga od poverenja teži potpunoj separaciji pouzdanih uloga.

5.3 Kontrole osoblja

Pružalac usluga od poverenja vodi računa da njegova polisa osoblja, kao i prakse koje se primenjuju na zapošljavanje članova osoblja, pojačavaju i podržavaju pouzdanost operacija Pružaoca usluga od poverenja. Cilj mera koje se odnose na osoblje je smanjenje rizika od ljudskih grešaka, krađe, prevare i zloupotrebe.

Pružalac usluga od poverenja obraća pažnju na bezbednost osoblja već tokom procesa zapošljavanja, uključujući zaključivanje ugovora i njihovu validaciju tokom zapošljavanja. Aplikanti bi trebalo da poseduju važeći izvod iz krivičnog dosijea u vreme podnošenja zahteva. Svaki zaposleni u poverenim ulogama i eksterni saradnici koji dolaze u kontakt sa uslugama Pružaoca usluga od poverenja potpisuju ugovor o poverljivosti.

U isto vreme, Pružalac usluga od poverenja obezbeđuje svojim zaposlenima sticanje i dalje razvijanje opšteg i specijalizovanog profesionalnog znanja neophodnog za obavljanje različitih poslova.

5.3.1 Kvalifikacije, iskustvo i zahtevi za odobrenje

Kao uslov za zapošljavanje, Pružalac usluga od poverenja zahteva najmanje srednje obrazovanje, ali nastavlja da vodi računa da zaposleni dobiju odgovarajuću obuku. Neposredno nakon zapošljavanja, Pružalac usluga od poverenja obezbeđuje obuku za svoje nove zaposlene, tokom koje stiču potrebno znanje za obavljanje posla. Službenik za registraciju može biti samo zaposleni koji je završio obuku tokom koje je stekao sposobnost prepoznavanja ličnih dokumenata prihvatljivih za Pružaoca usluga od poverenja (lična karta,

pasoš i vozačka dozvola). Pružalac usluga od poverenja obično podržava profesionalni razvoj zaposlenih, ali takođe očekuje da zaposleni samostalno razvijaju svoje veštine u svojim oblastima. Neki zaposleni Pružaoca usluga od poverenja imaju ulogu da detektuju i prikupljaju tehničke i poslovne inovacije i organizuju, te dele ovo znanje sa svojim kolegama.

Poverene uloge mogu obavljati samo osobe koje nemaju spoljni uticaj i poseduju neophodno stručno znanje validirano od strane Pružaoca usluga od poverenja. Svi zaposleni u poverenim ulogama moraju biti oslobođeni sukoba interesa koji bi mogli ugroziti nepristrasnost operacija Pružaoca usluga od poverenja.

Menadžer sa ukupnom odgovornošću za IT sistem može biti samo osoba koja ima:

- Specijalizovanu diplomu (diploma sa matematikom, fizikom ili diplomirani inženjerski fakultet iz tehničkog polja nauke);
- Najmanje tri godine stručnog iskustva u radu vezanom za informacionu bezbednost.

5.3.2 Procedure provere prošlosti

Pružalac usluga od poverenja može zaposliti samo osobe za poverene ili vodeće uloge koje:

- Imaju čist dosije i nema pokrenutih postupaka protiv njih koji bi mogli uticati na njihovu nekažnjivost.
- Nisu podložne profesionalnim diskvalifikacijama koje zabranjuju obavljanje usluga povezanih sa elektronskim potpisima.

Prilikom imenovanja, zaposlenik Pružaoca usluga od poverenja sa vodećom ulogom mora priložiti izjavu, a zaposlenik sa poverenom ulogom mora dostaviti potvrdu o nekažnjavanju koja nije starija od 3 meseca kako bi opravdao čist krivični dosije.

Pružalac usluga pd poverenja će proveriti autentičnost relevantnih informacija date u CV-u aplikanta tokom procesa zapošljavanja, kao što su prethodno zaposlenje, profesionalne reference i najrelevantnije obrazovne kvalifikacije.

5.3.3 Zahtevi za obuku

Pružalac usluga od poverenja će obučavati novo zaposlene, tokom kojeg će steći:

- Osnovna znanja o PKI (infrastrukturi javnih ključeva);
- Specifičnosti i način rukovanja IT sistemom Pružaoca usluga od poverenja;
- Neophodna posebna znanja za obavljanje njihovog opsega aktivnosti;
- Procese i procedure definisane u javnim i unutrašnjim propisima Pružaoca usluga od poverenja;
- Pravne posledice pojedinačnih aktivnosti;
- Primenjive IT sigurnosne propise u obimu neophodnom za specifičan opseg aktivnosti;
- Pravila za zaštitu podataka.

Pružalac usluga od poverenja će obučavati zaposlene koji su zaduženi za registraciju o opasnostima i rizicima povezanim sa proverom podataka koji treba da budu navedeni na sertifikatu.

Zaposleni zaduženi za registraciju polažu i prolaze ispit o poznavanju relevantnih zahteva i procedura za proveru podataka pre njihovog imenovanja, a ova činjenica se dokumentuje od strane Pružaoca usluga od poverenja.

Samo zaposleni koji su prošli obuku će dobiti pristup proizvodnom IT sistemu Pružaoca usluga od poverenja.

5.3.4 Učestalost i zahtevi ponovne obuke

Pružalac usluga od poverenja će se pobrinuti da zaposleni neprekidno imaju neophodna znanja, pa će po potrebi biti održavane dalje ili ponovljene vrste obuke.

Dalja obuka se održava ako dođe do promene u procesima ili IT sistemu Pružaoca usluga od poverenja.

Obuka materijala se ažurira najmanje svakih 12 meseci i sadržaće nove pretnje i aktuelne prakse sigurnosti.

Obuka je biti adekvatno dokumentovana, iz čega će biti jasno određen program i obim učesničkih zaposlenih.

5.3.5 Frekvencija i redosled rotacije poslova

Pružalac usluga od poverenja ne primenjuje obaveznu rotaciju između pojedinačnih radnih rasporeda.

5.3.6 Sankcije za neovlašćenje radnje

Pružalac usluga od poverenja reguliše mogućnosti sankcionisanja zaposlenih u radnom ugovoru u slučaju propusta, grešaka, slučajnih ili namernih šteta. Ako zaposleni – usled nemara ili namere – prekrši svoje obaveze, protiv njega može biti preduzeta sankcija od strane Pružaoca usluga od poverenja, koju određuje uzimajući u obzir prekršaj i posledice. Sankcije mogu uključivati disciplinski postupak, otkaz, opoziv imenovanja, krivičnu odgovornost. Prilikom imenovanja svaki zaposleni na poverenju kao deo radne dokumentacije:

- Dobija pismene informacije o pravnim obavezama, pravima, standardima za upravljanje sertifikatima i upravljanju ličnim podacima,
- Dobija opis posla koji obuhvata odgovarajuće bezbednosne zadatke,
- Potpisuje ugovor o poverljivosti u kojem su navedene posledice koje proizlaze iz neusklađenosti sa bezbednosnim merama (krivične sankcije).

Sve ovo uključuje radno zakonodavstvo ili krivične posledice koje sankcionišu različite prekršaje radnih obaveza ili kršenje zakona.

5.3.7 Zahtevi za nezavisne kontraktore

Pružalac usluga od poverenja dodeljuje samo pouzdane uloge svojim zaposlenima. Pružalac usluga od poverenja bira osobe zaposlene ugovorom o angažovanju ili podugovaračem da

obavljaju druge zadatke, birane po mogućstvu sa liste prethodno kvalifikovanih dobavljača. Pružalac usluga od poverenja zaključuje pisani ugovor pre početka rada sa dobavljačima.

Svaka ugovorna strana - pre početka aktivnog rada - potpisuje izjavu o poverljivosti kojom se saglašava da poslovni/korporativni tajni kasnije naučeni neće biti otkriveni neovlašćenim osobama, i neće biti iskorišćeni na bilo koji drugi način. Izjava o poverljivosti obuhvata sankcije u slučaju kršenja. Spoljni zaposleni zaposleni po ugovoru se očekuje da imaju odgovarajuće tehničke veštine, i Pružalac usluga od poverenja ne organizuje obuke za njih.

5.3.8 Dokumentacija dostavljena osoblju

Pružalac usluga od poverenja kontinuirano obezbeđuje zaposlenima dostupnost aktuelne dokumentacije i propisa neophodnih za obavljanje njihovih uloga. Svaki zaposleni u pouzdanoj ulozi dobija sledeće dokumente u pisanom obliku:

- Organizacione bezbednosne propise Pružaoca usluga od poverenja,
- Sporazum o poverljivosti koji treba potpisati,
- Lični opis posla,
- Obrazovni materijal povodom planirane ili posebne obuke za određeni oblik obrazovanja.

Svi zaposleni se pismeno obaveštavaju o svim promenama u organizacionim bezbednosnim propisima.

5.4 Postupci vođenja evidencije o reviziji

Da bi održao sigurno IT okruženje, Pružalac usluga od poverenja će implementirati i održavati sistem za beleženje događaja i kontrolu koji pokriva celokupni IT sistem.

5.4.1 Vrste zabeleženih događaja

Pružalac usluga od poverenja beleži svaki događaj vezan za bezbednost koji može pružiti informacije o događajima, promenama u IT sistemu ili u njegovom fizičkom okruženju prema opšte prihvaćenoj praksi informacione bezbednosti. Za svaki unos u evidenciji, čuva sledeće podatke:

- Vreme događaja;
- Vrsta događaja;
- Identifikacija korisnika ili sistema koji/što je pokrenuo događaj;
- Uspeh ili neuspeh proverenog događaja.

Svi novi zapisi o reviziji dodaju se u zapise o reviziji. Ranije sačuvani zapisi o reviziji ne mogu biti izmenjeni ili obrisani.

Svi važni evidencijski zapisi dostupni su nezavisnim sistemskim revizorima, koji ispituju usaglašenost rada Pružaoca usluga od poverenja.

Pružalac usluga od poverenja beleži sledeće događaje barem:

- UNUTRAŠNJI SAT

  - Sinhronizacija unutrašnjeg sata sa UTC vremenom, uključujući i operativne ponovne kalibracije;
  - Gubitak sinhronizacije;

- LOGOVANJE:
  - Gašenje, ponovno pokretanje sistema za beleženje događaja ili nekih od njegovih komponenti;
  - Izmena bilo kog parametra postavki za beleženje, na primer frekvencije, praga upozorenja i događaja koji se prate;
  - Izmena ili brisanje sačuvanih podataka o beleženju;
  - Aktivnosti izvršene usled neispravnosti sistema za beleženje.

- PRIJAVLJIVANJE:
  - Uspešne prijave, neuspeli pokušaji prijavljivanja za poverene uloge;
  - U slučaju autentikacije zasnovane na lozinkama:
    - Promena broja dozvoljenih neuspelih pokušaja;
    - Dostizanje limita dozvoljenog broja neuspelih pokušaja prijave u slučaju korisničke prijave;
    - Ponovni prijem korisnika blokiranog zbog neuspelih pokušaja prijave;
  - Promena tehnike autentikacije (na primer, iz autentikacije zasnovane na lozinkama u autentikaciju zasnovanu na PKI-ju).

- UPRAVLJANJE KLJUČEVIMA:
  - Svi događaji za ceo životni ciklus servisnih ključeva (generisanje ključeva, čuvanje, učitavanje, uništavanje itd.);

- UPRAVLJANJE SERIFIKATIMA:
  - Svaki događaj vezan za izdavanje i promenu statusa sertifikata provajdera.
  - Svaki zahtev uključujući izdavanje sertifikata, ponovno ključiranje, obnavljanje ključa, suspenziju i opoziv;
  - Događaji vezani za obradu zahteva;
  - Sve kontrole aktivnosti koje su sprovedene u vezi sa izdavanjem Sertifikata, uključujući vreme telefonskih razgovora vezanih za verifikaciju, telefonski broj, ime osobe koja je pozvana i prikupljene informacije, beleže se.
  - Odobravanje ili odbijanje aplikacija za sertifikat;
  - Izdavanje sertifikata ili promena statusa.

- PROTOKOLI PODATAKA:
  - Svaka vrsta bezbednosno kritičnih podataka ručno unesenih u sistem;
  - Bezbednosno relevantni podaci, primljene poruke od sistema;

- KONFIGURACIJA CA:
  - Reparametrizacija, bilo koja promena postavki bilo kog komponenta, CA;
  - Prijem, brisanje korisnika;
  - Promena korisničkih uloga, prava;
  - Promena profila sertifikata;
  - Promena profila CRL-a;
  - Generisanje nove liste CRL-a;
  - Generisanje OCSP odgovora;

- Generisanje vremenskog žiga;
- Prekoračenje potrebnog praga tačnosti vremena.

- MODUL ZA BEZBEDNOST HARDVERA:
  - Instalacija modula za bezbednost hardvera;
  - Uklanjanje modula za bezbednost hardvera;
  - Odlaganje, uništavanje modula za bezbednost hardvera;
  - Isporuka modula za bezbednost hardvera;
  - Brisanje (resetovanje) hardverskog modula za bezbednost;
  - Učitavanje ključeva, sertifikata na hardverski modul za bezbednost.

- ZMENE U KONFIGURACIJI:
  - Hardvera;
  - Softvera;
  - Operativnog sistema;
  - Zakrpa;
  - Instalacija, ažuriranje i uklanjanje softvera na sistemu za sertifikaciju;

- FIZIČKI PRISTUP, BEZBEDNOST LOKACIJE:
  - Ulazak i izlazak osoba iz zone bezbednosti u kojoj se nalaze komponente sistema koje se koriste za pružanje usluga od poverenja;
  - Pristup komponenti sistema koje se koriste za pružanje usluge poverenja;
  - Poznato ili sumnjičavo kršenje fizičke bezbednosti;
  - Saobraćaj na firewall-u ili ruteru.

- OPERACIONE ANOMALIJE:
  - Pad sistema, kvar hardvera;
  - Greške u softveru;
  - Greška u validaciji integriteta softvera;
  - Netačne ili pogrešno adresirane poruke;
  - Mrežni napadi, pokušaji napada;
  - Kvar opreme;
  - Kvar električne energije;
  - Greška u UPS-u (Neprekidnom Napajanju);
  - Greška u pristupu osnovnoj mrežnoj usluzi;
  - Kršenje Izjave o Praksi Sertifikacije;
  - Brisanje sata operativnog sistema.

- OSTALI DOGAĐAJI:
  - Imenovanje osobe za bezbednosnu ulogu;
  - Instalacija operativnog sistema;
  - Instalacija PKI aplikacije;
  - Pokretanje sistema;
  - Pokušaj ulaska u PKI aplikaciju;
  - Promena lozinke, pokušaj postavljanja;
  - Čuvanje unutrašnje baze podataka i obnova iz sigurnosne kopije;
  - Operacije nad datotekama (na primer, kreiranje, preimenovanje, premeštanje);
  - Pristup bazi podataka.

5.4.2 Učestalost procesa evidencije revizije

Nezavisni sistemski revizori Pružaoca usluga od poverenja evaluiraju generisane dnevničke datoteke svakog radnog dana.

Tokom evaluacije, osigurava se autentičnost i integritet pregledanih dnevnika, proveravaju se poruke o greškama u dnevnicima i, ako je potrebno, dokumentuju se razlike i preduzimaju mere za otklanjanje uzroka odstupanja.

Za evaluaciju IT sistema, Pružalac usluga od poverenja koristi i automatizovane evaluacione alate koji se koriste za praćenje rezultirajućih dnevnih unosa prema unapred postavljenim kriterijumima i, gde je potrebno, obaveštavaju operativno osoblje.

Obaveštenja dobijena od automatizovanih evaluacionih alata obrađuju se i evaluiraju od strane stručnjaka za IT operacije u roku od 24 sata.

Činjenica istraživanja, rezultati istraživanja i preduzete mere radi otklanjanja nedostataka dokumentovani su na odgovarajući način.

5.4.3 Period zadržavanja evidencije revizije

Pre nego što se izbrišu iz online sistema, dnevnici se arhiviraju i Pružalac usluga od poverenja obezbeđuje njihovo sigurno čuvanje u trajanju definisanom u odeljku 5.5.2, ali najmanje 10 godina od datuma njihovog nastanka.

Tokom tog perioda, Pružalac usluga od poverenja osigurava čitljivost arhiviranih podataka i održava softverske i hardverske alate neophodne za to.

5.4.4 Zaštita evidencije revizije

Pružalac usluga od poverenja će zaštititi kreirane evidencije tokom potrebnog vremena čuvanja. Tokom celog vremena čuvanja, sledeće osobine podataka iz evidencija će biti obezbeđene:

- Zaštita od neovlašćenog otkrivanja: samo ovlašćene osobe - pre svega nezavisni sistemski revizori - će imati pristup evidencijama;
- Dostupnost: ovlašćenim osobama će biti omogućen pristup evidencijama;
- Integritet: bilo kakva izmena podataka, brisanje u evidencijama i promena redosleda unosa, itd. će biti sprečeni.

Pružalac usluga od poverenja obezbeđuje dnevničke zapise sa kvalifikovanim vremenskim žigovima, i oni se čuvaju na način koji isključuje neprekidan unos i brisanje unosa iz dnevnika.

Dnevnički fajlovi su zaštićeni od slučajne i zlonamerne štete putem rezervnih kopija. U slučaju dnevnih zapisa koji sadrže lične podatke, Pružalac usluga od poverenja se brine za poverljivo čuvanje podataka. Pravo pristupa dnevnim zapisima imaju samo osobe koje to apsolutno potrebno za svoj rad. Pružalac usluga od poverenja proverava pristupe na bezbedan način. Dnevničke datoteke se čuvaju u sigurnom okruženju. Pružalac usluga od poverenja čuva kopije datoteka na drugom operativnom mestu.

5.4.5 Procedure za rezervne kopije evidencije revizije

Dnevničke datoteke se kreiraju od kontinuirano generisanih dnevničkih unosa tokom rada u svakom sistemu.

Dnevničke datoteke se arhiviraju u dva primerka nakon evaluacije i fizički se čuvaju odvojeno jedna od druge, na odvojenim lokacijama, tokom potrebnog perioda.

Tačan proces izrade rezervnih kopija definiše se u propisima o rezervnim kopijama Pružaoca usluga od poverenja.

5.4.6 Sistem za prikupljanje revizije (interno vs. eksterno)

Svaka aplikacija automatski prikuplja i šalje zapise u sistem za evidentiranje.

Funkcije evidentiranja automatski se pokreću u trenutku pokretanja sistema i kontinuirano se izvršavaju tokom čitavog perioda rada sistema.

U slučaju bilo kakvih anomalija u automatskom ispitivaču i sistemima evidentiranja, rad povezanih područja obustavlja Pružalac usluga od poverenja sve dok se incident ne reši.

5.4.7 Obaveštavanje subjekta koji je izazvao događaj

Osobe, organizacije i aplikacije koje su uzrokovale događaj greške neće uvek biti obaveštene, ali ako je potrebno, Pružalac usluga od poverenja ih uključuje u istraživanje događaja.

Klijenti koji su pogođeni pokretanjem događaja imaju dužnost da sarađuju sa Pružaocem usluga od poverenja kako bi istražili događaj.

5.4.8 Procena ranjivosti

Pored svakodnevnog procesuiranja unosa dnevnika, stručnjaci Pružaoca usluga od poverenja prate javno dostupne informacije o mogućim ranjivostima i novim zakrpama za softver. Oni analiziraju informacije, klasifikuju ranjivost i, ako je potrebno, obaveštavaju menadžment o rezultatu i predlažu plan akcije za povećanje sigurnosti sistema.

Svaki značajan događaj koji ukazuje na značajne nedostatke otkriven ili u slučaju spoljnje pretnje u roku od 48 sati od otkrića, ali najmanje jednom godišnje, stručnjaci Pružaoca usluga od poverenja sprovode sveobuhvatnu analizu ranjivosti koristeći mapiranje potencijalnih internih i eksternih pretnji koje mogu rezultirati neovlašćenim pristupom i mogu uticati na proces izdavanja sertifikata ili dozvoliti modifikaciju podataka koji se čuvaju u sertifikatu.

Na osnovu rezultata analize, Pružalac usluga od poverenja:

- Kreira i sprovodi plan za ublažavanje ranjivosti; ili
- Dokumentuje faktičku osnovu za odluku da se prihvati preostali rizik i da ranjivost ne zahteva sanaciju.

Nove verzije softvera i softverske zakrpe prvo se instaliraju na testnom sistemu Pružaoca usluga od poverenja, a tek nakon uspešno završenog testa se instaliraju na živi sistem koji se koristi za pružanje usluga.

Nove softverske zakrpe se ne instaliraju na živi sistem ako uvode dodatne ranjivosti ili nestabilnosti koje prevazilaze koristi od njihove primene. Razlozi za neprimenu bilo kakvih sigurnosnih zakrpi se dokumentuju.

5.5 Arhiviranje zapisa

5.5.1 Vrste arhiviranih zapisa

Pružalac usluga od poverenja mora biti spreman za pravilno, bezbedno dugoročno arhiviranje elektronskih i papirnih dokumenata.

Pružalac usluga od poverenja će arhivirati sledeće vrste informacija:

- Svaki dokument vezan za akreditaciju Pružaoca usluga od poverenja;
- Sve izdate verzije Polisa sertifikata;
- Sve izdate verzije Izjava o praksi sertifikacije;
- Sve izdate verzije opštih uslova i odredbi;
- Ugovori vezani za rad Pružaoca usluga od poverenja;
- Sve informacije vezane za registraciju, uključujući:
    - Svaki dokument dostavljen uz zahtev za sertifikat;
    - Identifikacioni podaci dokumenta dostavljeni tokom lične identifikacije;
    - Ugovore o usluzi;
    - Ostala odricanja korisnika usluga;
    - ID administratora koji je ocenjivao zahtev za registraciju;
    - Uslovi i rezultati pregleda zahteva;
- Sve informacije vezane za sertifikat tokom celog životnog ciklusa;
- Svaki elektronski i papirni log zapis.

5.5.2 Period čuvanja arhive

Pružalac usluga od poverenja je obavezan da čuva arhivirane podatke tokom sledećih vremenskih perioda:

- Polisu sertifikata najmanje 10 godina od datuma povlačenja;
- Izjava o praksi sertifikacije najmanje 10 godina od datuma povlačenja;
- Opšti uslovi i odredbe najmanje 10 godina od datuma povlačenja;
- U slučaju video identifikacije, sva komunikacija snimljena tokom identifikacije najmanje 10 godina od datuma snimanja;
- Svi elektronski i/ili papirni podaci koji se odnose na sertifikate najmanje:
    - 10 godina nakon isteka važnosti sertifikata;
- Svi ostali dokumenti koji se arhiviraju najmanje 10 godina od datuma njihovog nastanka.

5.5.3 Zaštita arhive

Pružalac usluga od poverenja obavezan je da čuva sve arhivirane podatke u dva primerka na lokacijama fizički udaljenim jedna od druge. Autentična papirna ili elektronska kopija može se napraviti u skladu sa primenjivim zakonom iz jedine dostupne autentične papirne kopije.

Svaka od dve lokacije mora ispuniti zahteve za bezbednost arhiviranja i druge zahteve.

Tokom čuvanja arhiviranih podataka, mora se osigurati da:

- Njihov integritet bude očuvan;
- Budu zaštićeni od neovlašćenog pristupa;
- Budu dostupni;
- Sačuvaju autentičnost.

Arhivirani elektronski podaci moraju biti opremljeni barem naprednim elektronskim potpisom ili pečatom i kvalifikovanim vremenskim pečatom.

5.5.4 Procedure za sigurnosne kopije arhive

Pružalac usluga od poverenja pravi autentičnu elektronsku kopiju originalnih papirnih dokumenata u skladu sa relevantnim zakonodavstvom.

Elektronske kopije čuvaju se prema istim pravilima kao i ostali zaštićeni elektronski dokumenti.

Nakon arhiviranja autentičnih elektronskih kopija, Pružalac usluga od poverenja može uništiti originalne papirne dokumente.

5.5.5 Zahtevi za vremensko obeležavanje zapisa

Svaki elektronski zapis u dnevniku opremljen je vremenskom oznakom, na kojoj je označeno vreme koje pruža sistem, precizno do najmanje sekunde.

Vrednost vremena dolazi od unutrašnjeg sata Pružaoca usluga od poverenja koji je sinhronizovan sa dva odvojena Stratum-1 UTC vremenska izvora:

- Jedan precizni izvor vremena koristi satelitski GNSS (GPS i Galileo) sistem;
- Drugi precizni izvor vremena baziran je na usluzi dugačkih talasa vremenskog signala (DCF77).

Da bi se obezbedila tačnost, Pružalac usluga od poverenja sinhronizuje svoje interno vreme sa navedenim Stratum-1 izvorima sa tačnošću od 0.1 sekunde, i vrši ovu sinhronizaciju najmanje 4 puta dnevno.

Na ovaj način Pružalac usluga od poverenja garantuje da odstupanje vremena navedenog u vremenskim oznakama od UTC vremenske osnove iznosi najviše 1 sekundu.

Pružalac usluga od poverenja obezbeđuje dnevne log fajlove sa kvalifikovanom vremenskom oznakom.

Tokom čuvanja arhiviranih podataka, ako je potrebno (na primer, istek promene algoritma originalne vremenske oznake), osigurava se autentičnost podataka.

5.5.6 Sistem za prikupljanje arhiva (interno ili eksterno)

Zapisnici se generišu u zaštićenom računarskom sistemu Pružaoca usluga od poverenja, i samo log fajlovi koji su elektronski potpisani i zaštićeni kvalifikovanim vremenskim oznakama mogu da napuste sistem.

Jedna originalna kopija dokumenata kreiranih tokom pružanja usluge čuva se i štiti od strane Pružaoca usluga od poverenja u unutrašnjem skladištu podataka koje on operiše.

5.5.7 Procedure za dobijanje i proveru informacija iz arhive

Pružalac usluga od poverenja može ručno ili automatski kreirati zapisnike. U slučaju automatskog sistema za evidentiranje, sertifikovani zapisnici se generišu svakodnevno.

Arhivirane datoteke moraju biti zaštićene od neovlašćenog pristupa.

Kontrolisani pristup arhiviranim podacima biće dostupan ovlašćenim osobama:

- Klijenti imaju pravo da vide podatke koji se odnose na njih;
- U slučaju pravnog spora radi obezbeđivanja dokaza, neophodni podaci će biti dostavljeni.

5.6 Promena ključa CA

Pružalac usluga poverenja osigurava da korišćene sertifikacione jedinice neprekidno poseduju važeći ključ i sertifikat za svoj rad. Za tu svrhu, dovoljno vremena pre isteka njihovih sertifikata i isteka ključeva povezanih sa njima, generiše novi par ključeva za sertifikacione jedinice i pravovremeno obaveštava svoje klijente. Novi provajderski ključ se generiše i upravlja prema ovom pravilniku.

Ako Pružalac usluga od poverenja promeni bilo koji od ključeva sertifikata izdavača sertifikata krajnjih korisnika, mora se pridržavati sledećih zahteva:

- Moraju se otkriti pogođeni sertifikati i javni ključevi u skladu sa zahtevima definisanim u odeljku 2.2;
- Nakon ponovnog ključanja sertifikata krajnjih korisnika, sertifikati koji se izdaju mogu se potpisati samo novim ključevima pružaoca;
- Čuvanje starrih sertifikata i javnih ključeva, i stavljanje na raspolaganje verifikaciju pečata sve dok svi Sertifikati sa starim ključevima ne isteknu.

5.7 Kompromis i oporavak od katastrofe

U slučaju katastrofe, pružalac usluga poverenja preduzima sve potrebne mere kako bi se minimalizovala šteta nastala nedostatkom usluge, i što je brže moguće obnavlja usluge.

Na osnovu procene incidenta koji se dogodio, preduzeće neophodne izmene, korektivne mere kako bi se sprečilo buduće pojavljivanje incidenta. Nakon rešavanja problema, događaj će biti prijavljen Nacionalnoj medijskoj i telekomunikacionoj agenciji, kao nadležnom organu.

5.7.1 Postupci za obradu incidenata i kompromitacije

Pružalac usluga od poverenja ima plan kontinuiteta poslovanja.

Pružalac usluga od poverenja je uspostavio i održava potpuno funkcionalni sistem rezervnih kopija, koji se nalazi na sigurnoj udaljenosti od primarne lokacije, geografski na drugom mestu i nezavisno je sposoban da obezbedi pun opseg usluga.

Pružalac usluga od poverenja godišnje testira prelazak na rezervni sistem i pregleda svoje planove kontinuiteta poslovanja.

Pružalac usluga od poverenja je unapredio sigurnosne alate i sisteme kako bi se minimizirali softverski i hardverski kvarovi i oštećenja podataka. Obezbeđuje se mogućnost oporavka usluga putem osnovnih ugovora i sopstvenih alata za rezervne kopije pružaoca usluga poverenja.

Pružalac usluga od poverenja je konstruisao svoj IT sistem koji pruža poverene usluge tako da u slučaju ispadanja bilo kog uređaja može nastaviti pružanje svojih poverenih usluga. Ako više jedinica pružaoca usluga poverenja zakaže, Pružalac usluga od poverenja je u mogućnosti da pokrene svoj rezervni sistem u roku od najviše 3 sata, koji je sposoban da pruži usluge vezane za neprekidno operativne usluge - objavljivanje skladišta sertifikata, upravljanje opozivom, objavljivanje informacija o statusu opoziva - Pružaoca usluga od poverenja za svoje klijente.

Interna pravila Pružaoca usluga od poverenja detaljno definišu zadatke vezane za upravljanje sigurnosnim incidentima. Svako odstupanje od normalnog poslovanja se evidentira u internom sistemu upravljanja zadacima nakon otkrivanja. Po otkrivanju odstupanja, Pružalac usluga od poverenja odmah započinje istraživanje odstupanja, eliminiše otkriveno odstupanje što je pre moguće i, ako je potrebno, preduzima preventivne mere kako bi sprečio ponovno pojavljivanje odstupanja.

U svim slučajevima, Pružalac usluga od poverenja klasifikuje svako odstupanje koje može uticati na dostupnost, integritet ili poverljivost usluga kao sigurnosni incident i prioritizuje ga (npr. prekid usluge).

Pružalac usluga poverenja zvanično obaveštava Nacionalnu medijsku i infokomunikacionu agenciju o prekidima usluge i sigurnosnim incidentima koji se smatraju ozbiljnim u roku od 24 sata od nastanka incidenta.

U slučaju sigurnosnog incidenta, Pružalac Usluga Poverenja kreira izveštaj o incidentu u sistemu Mozilla Bugzilla u skladu sa zahtevima programa za poverene korenske sertifikate. U tom izveštaju detaljno opisuje okolnosti sigurnosnog incidenta, osnovne uzroke, pogođene Sertifikate, hitne mere preduzete radi otklanjanja incidenta i dugoročne mere kako bi se sprečili dalji incidenti.

5.7.2 Resursi za računanje, softver i/ili podaci su oštećeni

IT sistemi Pružaoca usluga od poverenja izgrađeni su od pouzdanih hardverskih i softverskih komponenti. Kritične funkcije su implementirane korišćenjem redundantnih sistemskih elemenata tako da u slučaju kvara nekog od elemenata mogu nastaviti sa radom.

Pružalac usluga od poverenja pravi punu dnevnu rezervnu kopiju svojih baza podataka i generisanih log događaja.

Pružalac usluga od poverenja pravi punu rezervnu kopiju sistema onoliko često koliko je potrebno da bi mogao da obnovi punu uslugu u slučaju katastrofe.

Plan kontinuiteta poslovanja Pružaoca usluga od poverenja uključuje precizne zahteve za zadatke koji treba da se obave u slučaju kvara kritičnih sistema.

Nakon što se problem reši i integritet bude obnovljen, Pružalac usluga od poverenja ponovo pokreće svoje usluge što je pre moguće.

Tokom obnove usluga, sistemi za informacije o statusu sertifikata imaju prioritet.

5.7.3 Procedure u slučaju kompromitovanja privatnog ključa subjekta

Plan kontinuiteta poslovanja Pružaoca usluga poverenja ima plan akcija u slučaju kompromitacije privatnih ključeva pružaoca. Plan akcija otkriva okolnosti kompromitacije, pored opoziva javnog ključa pružaoca i pratećeg sertifikata, organizuje obaveštavanje svih zainteresovanih strana, preduzima neophodne korake protiv ponovne kompromitacije i, ako je potrebno, obezbeđuje novi ključ za jedinicu usluge i korisnike koji su pogođeni kompromitacijom. Pružalac usluga poverenja odmah prestaje da koristi taj određeni ključ u slučaju kompromitacije ključa jedinice za sertifikaciju.

U slučaju da je još jedna sertifikaciona autoriteta takođe izdala sertifikat za datu jedinicu za sertifikaciju - zakonom, ugovorom ili sporazumom između CA na osnovu - i nad nadležnošću prekriženo ovu jedinicu za sertifikaciju Pružaoca usluga poverenja, Pružalac usluga poverenja odmah obaveštava tu drugu sertifikacionu vlast o kompromitaciji ključa i pokreće opoziv sertifikata koji pripada ključu u pitanju.

Pružalac usluga poverenja objavljuje obaveštenje o opozivu javnog ključa pružaoca u skladu sa odeljkom 1.3.1.

5.7.4 Poslovne kontinuitetske mogućnosti nakon katastrofe

Zadaci koji se moraju izvršiti u slučaju otkaza usluge zbog prirodne ili druge katastrofe definisani su u planu kontinuiteta poslovanja Pružaoca usluga od poverenja.

U slučaju katastrofe, propisi stupaju na snagu, kontrola štete i obnavljanje usluga počinje.

Sekundarno mesto za pružanje usluga je udaljeno toliko daleko od primarnog mesta da verovatna katastrofa ne može istovremeno zahvatiti oba mesta.

Pružalac usluga od poverenja je obavezan da što pre obavesti pogođene korisnike u slučaju katastrofe.

Nakon obnove usluga, Pružalac usluga od poverenja što pre obnavlja svoje uređaje oštećene tokom katastrofe i originalni nivo bezbednosti usluge.

5.8 Prekid rada CA ili RA

U slučaju planiranog prestanka pružanja usluge, Pružalac usluga od poverenja obaveštava krajnje korisnike i Nacionalnu medijsku i infokomunikacionu agenciju najmanje 60 dana pre prestanka usluge.

Prestanak pružanja usluge sertifikacije i usluge statusa sertifikata

U isto vreme sa obaveštenjem o prestanku usluge, Pružalac usluga od poverenja zaustavlja sledeće usluge:

- registracija,
- kreiranje sertifikata,
- izdavanje sertifikata,
- obnavljanje sertifikata,
- modifikacija sertifikata,
- ponovna izrada ključeva.

Pružalac usluga od poverenja najmanje 20 dana pre planiranog prestanka, ali najmanje 14 dana nakon obaveštenja klijenata:

- opoziva sve važeće sertifikate krajnjih korisnika;
- zaustavlja obradu zahteva za opoziv i suspenziju;
- prekida redovno izdavanje liste opozvanih sertifikata;
- izdaje završnu listu opozvanih sertifikata, u kojoj je vrednost polja "nextUpdate" "99991231235959Z".

U isto vreme sa prestankom, Pružalac usluga od poverenja zaustavlja i sledeće usluge:

- objavljivanje sertifikata,
- objavljivanje statusa opoziva sertifikata,
- OCSP uslugu,
- tehničku podršku,
- pružanje informacija.

Pre planiranog prestanka, Pružalac usluga od poverenja pregovara o preuzimanju svojih usluga sa drugim Pružaocem usluga poverenja čija je ocena identična njegovoj. U skladu sa odeljkom 9.3, predaće svoje zapise, uključujući poverljive korisničke podatke, takvom Pružaocu usluga od poverenja ili Nacionalnoj medijskoj i infokomunikacionoj agenciji, zavisno od ishoda pregovora ili će završiti bez predaje.

Pružalac usluga od poverenja preduzima mere u vezi sa opozivom sertifikata provajdera (i uništavanjem privatnih ključeva) tokom 60-dnevnog perioda - u zavisnosti od ishoda pregovora.

Pružalac usluga od poverenja obaveštava Nacionalnu medijsku i infokomunikacionu agenciju o konačnom ishodu pregovora. Pružalac usluga od poverenja obaveštava svoje klijente putem elektronske pošte, a oslanjajuće strane putem objave na svom veb-sajtu.

Pružalac usluga od poverenja će objaviti obaveštenje o prestanku aktivnih korenskih jedinica sertifikacije najmanje 5 dana pre prestanka u skladu sa poglavljem 2.1.

Pružalac usluga od poverenja uništava privatne ključeve prestalih korenskih jedinica sertifikacije u roku od 5 radnih dana nakon prestanka na dokumentovan način.

Po prestanku usluge, Pružalac usluga od poverenja pravi punu sigurnosnu kopiju svojih podataka koji se nalaze u svom IT sistemu, zaštićenom kvalifikovanim vremenskim pečatom.

Pružalac usluga od poverenja omogućava ovlašćenim oslanjajućim stranama mogućnost tumačenja podataka koji se pojavljuju u njegovim opozvanim zapisima sertifikata ako je to neophodno.

Da bi omogućio prenos svojih podataka drugom Pružaocu usluga od poverenja, Pružalac usluga od poverenja smešta podatke na medijima i u formatu koji novi Pružalac od usluga poverenja može da prihvati ili omogućava novom Pružaocu usluga od poverenja da obradi podatke u originalnom formatu, i predaje odgovarajuće alate, dokumentaciju i know-how za to.

6 Tehničke bezbednosne kontrole

Pružalac usluga od poverenja koristi sisteme sastavljene od pouzdane i bezbedne tehnički ocenjene opreme za pružanje svojih usluga. Tokom čitavog životnog ciklusa, Pružalac usluga od poverenja upravlja privatnim kriptografskim ključevima unutar Modula hardverske sigurnosti koji poseduje odgovarajuću sertifikaciju.

Svi uključeni - Pružalac usluga od poverenja, dobavljači sistema i izvođači - imaju značajno iskustvo u implementaciji sistema zasnovanih na PKI tehnologiji i uslugama poverenja, koristeći međunarodno priznate tehnologije.

Pružalac usluga od poverenja neprekidno prati potrebe za kapacitetom i procenjuje očekivane buduće potrebe za kapacitetom, omogućavajući proširenje ograničenih kapaciteta ako je potrebno kako bi se osigurala neophodna obrada i neprekidna dostupnost skladišta.

6.1 Generisanje i instalacija parova ključeva

Pružalac usluga od poverenja se pobrinuti da generisanje i upravljanje svim privatnim ključevima koje generiše - za sebe i za neke od svojih odeljenja (na primer, repozitorijum za sertifikate, autoritet za registraciju) - bude bezbedno i da se pridržava važećih regulatornih zahteva i industrijskih standarda.

6.1.1 Generisanje parova ključeva

Pružalac usluga od poverenja koristiti samo algoritme generisanja ključeva za generisanje parova ključeva koji ispunjavaju zahteve utvrđene u sledećim normativima:

- ETSI TS 119 312 [24];

Generisanje parova ključeva od strane Pružaoca usluga

Pružalac usluga od poverenja prilikom generisanja svog para ključeva treba da obezbedi:

- Proizvodnja ključnog para provajdera se vrši na osnovu skripte za generisanje ključa.
- U slučaju generisanja ključnog para za CA, Kvalifikovani revizor svedoči procesu generisanja ključnog para CA ili Pružalac usluga od poverenja beleži video snimak celog procesa generisanja ključnog para CA.
- Ako se ključni par CA generiše za korenski (root) CA ili podređeni CA kojim upravlja druga organizacija, kvalifikovani revizor će svedočiti procesu generisanja ključa. Kvalifikovani revizor izdaje izveštaj koji potvrđuje da je CA sledio svoju ceremoniju ključa tokom procesa generisanja ključnog para i kontrolisao integritet i poverljivost ključnog para.
- Generisanje ključnog para se vrši (vidi odeljak 5.1), sa najmanje dva ovlašćena lica u isto vreme pod principom deljenog znanja, isključujući prisustvo neovlašćenih osoba.
- Kreiranje ključnog para provajdera se vrši na uređaju koji:
  - Ispunjava zahteve ISO/IEC 19790 [29], ili
  - Ispunjava zahteve FIPS 140-2 [41] nivoa 3 ili više, ili
  - Ispunjava zahteve FIPS 140-3 [42] nivoa 3 ili više, ili
  - Ispunjava zahteve CEN 419 221-5 [26], ili

  - Je pouzdan sistem koji je evaluiran u skladu sa ISO/IEC 15408 [28] ili jednakim bezbednosnim kriterijumima vrednim na nivou 4 ili više garantnog nivoa. Ocena treba da se zasniva na dizajnu bezbednosnog sistema ili na bezbednosnim dodelama koje ispunjavaju zahteve ovog dokumenta.

- Napravljeni su detaljni log zapisi o procesu generisanja ključa.
- Pružalac usluga od poverenja preduzima neophodne mere kako bi se osiguralo da je privatni ključ generisan i zaštićen u skladu sa propisanim procesima tokom generisanja ključa.
- U slučaju generisanja ključnih parova za korenski i posrednički sertifikat Pružaoca usluga, Pružalac usluga od poverenja treba da napravi zapis o generisanju ključa koji demonstrira da je proces sproveden u skladu sa unapred određenim radnim tokom koji osigurava poverljivost i integritet generisanih ključeva.
  Zapis treba da bude potpisan od strane:
  - U slučaju generisanja ključnog para korenske jedinice za sertifikaciju Pružaoca usluga, ovlašćeni službenik Pružaoca usluga od poverenja zadužen za upravljanje ključevima i pouzdana osoba nezavisna od operacija Pružaoca usluga od poverenja, kao svedok (npr. kvalifikovani revizor), koji proverava da li zapis odgovara izvršenom procesu;
  - U slučaju generisanja ključnog para posredničke jedinice za sertifikaciju Pružaoca usluga, ovlašćeni službenik Pružaoca usluga od poverenja zadužen za upravljanje ključevima koji proverava da li zapis odgovara izvršenom procesu.

Generisanje ključnih parova infrastrukture od strane Pružaoca usluga

U slučaju generisanja ključeva infrastrukture korišćenih u vlastitim IT sistemima, Pružalac usluga od poverenja treba obezbeđuje:

- Generisanje infrastrukturnog ključa Pružaoca usluga vrši se u fizički zaštićenom okruženju (videti odeljak 5.1) od strane ovlašćene osobe u ulozi poverenja (videti odeljak 5.2.1), isključujući prisustvo drugih neovlašćenih osoba;
- Generisanje ključeva potpuno se pridržava uputstava u korisničkoj dokumentaciji uređaja.

Ključevi korisnika

Pružalac usluga od poverenja nikada ne generiše parove ključeva za softverske sertifikate krajnjih korisnika.

U slučaju ključnog para generisanog od strane aplikanta:

- Proizvodnja ključeva vrši se u adekvatno sigurnom okruženju koje je pod nadzorom aplikanta;
- Aplikant osigurava odgovarajuću zaštitu generisanog privatnog ključa;
- Pružalac usluga od poverenja osigurava da je generisani ključni par u skladu sa zahtevima definisanim u odeljcima 6.1.5 i 6.1.6, i da javni ključ nije jedan od poznatih slabih ključnih parova.

Prilikom obrade zahteva za sertifikat, Pružalac usluga od poverenja proverava ključni par i odbija zahtev za sertifikat ako su ispunjeni jedan ili više sledećih uslova:

- Ključni par ne ispunjava zahteve utvrđene u odeljcima 6.1.5 i/ili 6.1.6;

- Postoji jasan dokaz da je specifična metoda korišćena za generisanje privatnog ključa bila nesavršena;
- Pružalac usluga od poverenja je svestan demonstrirane ili dokazane metode koja izlaže privatni ključ aplikanta kompromitaciji;
- Pružalac usluga od poverenja je prethodno obavešten da je privatni ključ aplikanta kompromitovan, kao što je navedeno u odeljku 4.9.1;
- Pružalac usluga od poverenja je svestan demonstrirane ili dokazane metode za lako izračunavanje privatnog ključa aplikanta na osnovu javnog ključa (kao što je Debian slab ključ, videti https://wiki.debian.org/SSLkeys).

6.1.2 Isporuka privatnog ključa Pretplatniku

Pružalac usluga od poverenja nikada ne generiše parove ključeva za sertifikate krajnjih korisnika.

6.1.3 Isporuka javnog ključa izdavaču sertifikata

Kada ključni par generiše aplikant, moraju se poštovati sledeće odredbe:

- Javni ključ će biti poslat Pružaocu usluga od poverenja na način da ga je moguće nedvosmisleno dodeliti aplikantu;
- Proces podnošenja zahteva za sertifikaciju mora dokazati da aplikant zaista poseduje privatni ključ koji odgovara javnom ključu.

Kada korisnik generiše ključeve koje je napravio aplikant, aplikant šalje Pružaocu usluga od poverenja PKCS#10 formatiranu aplikaciju za sertifikat koju potpisuje privatnim ključem koji pripada javnom ključu koji će biti naznačen na sertifikatu. PKCS#10 formatirana aplikacija za sertifikat sadrži javni ključ koji je generisao aplikant i podatke o Subjektu koji će biti naznačeni na sertifikatu, tako da su oba zahteva ispunjena.

6.1.4 Dostava javnog ključa CA provajdera pouzdanim stranama

Pružalac usluga od poverenja objavljuje informacije o statusu povezanim sa sertifikatima Pružaoca usluga od poverenja za Pouzdane strane na sledeće načine:

- Pružalac usluga od poverenja objavljuje potpunu hijerarhiju sertifikata pružaoca koja sadrži svaki koren i posredni sertifikat pružaoca od kojih je svaki trenutni sertifikat pružaoca dostupan za preuzimanje (vidi tačku o sertifikatima pružaoca na adresi https://vebsite.com).
- Naziv korenskih i posrednih jedinica sertifikacije i heš korenskih sertifikata nalazi se u sekciji 1.3.1 Izjave o opštim pravilima rada pružaoca od poverenja.
- Sertifikati posrednih jedinica sertifikacije objavljeni su na listi sertifikovanih srpskih Pružalaca usluga od poverenja [53], koju održava i objavljuje Nacionalna medijska i informatička agencija u okviru evropskih zajedničkih propisa [52]. Lista sadrži svaki sertifikat pružaoca (čak i one koji su istekli i povučeni).
- Za odgovore signera na zahtev za status sertifikata putem mreže, Pružalac usluga od poverenja - u skladu s najboljom međunarodnom praksom - izdaje sertifikate sa veoma

kratkim periodima važenja, čime se eliminiše potreba za proverom statusa povlačenja sertifikata.
- Trenutni status sertifikata kontinuirano je dostupan na veb stranici Pružaoca usluga od poverenja na adresi https:/vebsite.com.

Pružalac usluga od poverenja objavljuje za Pouzdane strane informacije o statusu povezane sa sertifikatom jedinica sertifikacije kojima upravlja, kao i jedinica koje učestvuju u usluzi za status sertifikata putem mreže na sledeće načine:

- Informacije o statusu sertifikata korenskih jedinica sertifikacije dostupne su na veb stranici Pružaoca usluga od poverenja.
- Informacije o promeni statusa sertifikata posrednih (ne korenskih) jedinica sertifikacije objavljuju se na Listi povučenih sertifikata, na veb stranici i unutar okvira usluge za odgovor na zahtev za status sertifikata putem mreže.
- Za potpisnike odgovora na zahtev za status sertifikata putem mreže, Pružalac usluga od poverenja - u skladu s najboljim međunarodnim praksama - izdaje sertifikat sa veoma kratkim periodom važenja kako bi se eliminisala potreba za proverom statusa povlačenja sertifikata. Pružalac usluga od poverenja garantuje da u slučaju kompromitacije ključa ili drugog problema neće biti izdat novi sertifikat za stari privatni ključ koji je potpisivao OCSP odgovore. Pružalac usluga od poverenja izdaje sertifikate OCSP odgovora za nove, sigurne privatne ključeve.

Što se tiče metoda otkrivanja informacija o statusu, pogledajte i Odeljak 4.10.

6.1.5 Veličine ključeva

Pružalac usluga od poverenja sme koristiti samo kriptografske algoritme i minimalne veličine ključeva koje su u skladu sa zahtevima navedenim u sledećim standardima:

- ETSI TS 119 312 [24];
- Preporuka osnovnih zahteva CABF-a;
- Trenutno važeća algoritamska regulativa Nacionalne medijske i infokomunikacijske vlasti izdata u skladu sa ovlašćenjem Zakona CCXXII iz 2015. godine, član 92. stav (1) b).

Sertifikaciono telo koristi ključeve barem od 2048 bita RSA ili barem od 256 bita ECC u svakom trenutno aktivnom korenskom i posrednom sertifikatu pružaoca, pa čak i u sertifikatima jedinica vremenskog pečata i OCSP odgovorima.

Sertifikaciono telo izdaje sertifikate krajnjih korisnika samo za ključeve od barem 2048 bita RSA ili barem 256 bita ECC.

Pružalac usluga od poverenja podržava samo sledeće dužine RSA ključeva:

- RSA-2048 (2048 bita)
- RSA-3072 (3072 bita)
- RSA-4096 (4096 bita)

Pružalac usluga od poverenja podržava samo sledeće ECC krive:

- ECC NIST P-256 (256 bita)
- ECC NIST P-384 (384 bita)

- ECC NIST P-521 (521 bit)

ECC ključ uvek predstavlja validnu tačku na podržanoj eliptičnoj krivoj.

6.1.6 Generisanje parametara javnog ključa i provera kvaliteta

Pružalac usluga od poverenja generiše ključeve prema opisu u odeljku 6.1.1.

Provera usklađenosti parametara

Sertifikacioni organ proverava usklađenost ključeva svakog pružaoca usluga i krajnjeg korisnika pre izdavanja sertifikata prema sledećim parametrima:

1. Za RSA ključeve
   - Dužina RSA ključa je unutar podržanih vrednosti.
   - RSA eksponent je neparan.
   - Vrednost RSA eksponenta je najmanje "(2 na eksponentu 16) + 1" i najviše "(2 na eksponentu 256) - 1".
   - Modulus je neparan, nije prost broj i nema delilac manji od 752.

2. Za ECC ključeve
   - Ključ je validna tačka na podržanoj krivoj (ECC Rutina potpune provere javnog ključa kako je definisano u odeljku 5.6.2.3.3 NIST Posebnog izdanja 800-56A Revizija 3 [49]).

6.1.7 Namene korišćenja ključa (prema polju namena ključa X.509 v3)

Privatni ključ korenske sertifikacione jedinice Pružaoca usluga od poverenja može se koristiti samo u sledeće svrhe:

- Izdavanje samo potpisanog sertifikata korenske sertifikacione jedinice,
- Potpisivanje sertifikata međusobnih sertifikacionih jedinica,
- Potpisivanje sertifikata OCSP,
- Potpisivanje CRL lista.

Privatni ključevi međusobnih sertifikacionih jedinica Pružaoca usluga od poverenja - kao i privatni ključ izdat međusobnoj sertifikacionoj jedinici drugih organizacija - mogu se koristiti samo u sledeće svrhe:

- Potpisivanje sertifikata međusobnih sertifikacionih jedinica,
- Potpisivanje sertifikata krajnjih korisnika,
- Potpisivanje sertifikata jedinice za vremensko žigosanje,
- Potpisivanje sertifikata OCSP,
- Potpisivanje CRL lista.

Pružalac usluga od poverenja treba da uključi "Korišćenje ključa" ekstenziju u sertifikate krajnjih korisnika koja definišu oblast korišćenja sertifikata i u aplikacijama kompatibilnim sa X.509v3. Zahtevi postavljeni za vrednost polja nalaze se u odeljku 7.1.2.

Privatni ključ aplikanta koji pripada njegovom sertifikatu sme se koristiti samo za autentifikaciju veb servera ili - ukoliko sertifikat za autentifikaciju veb sajtova to omogućava - autentifikaciju klijenata, i svaka druga upotreba nije dozvoljena.

6.2 Zaštita privatnog ključa i inženjerske kontrole kriptografskog modula

Pružalac usluga od poverenja obezbeđuje sigurno upravljanje privatnim ključevima koje poseduje i sprečava otkrivanje, kopiranje, brisanje, modifikaciju i neovlašćeno korišćenje privatnih ključeva. Pružalac usluga od poverenja može čuvati privatne ključeve samo onoliko dugo koliko je to definitivno neophodno za pružanje usluge.

Pružalac usluga od poverenja čuva i koristi privatne ključeve Root CA fizički izolovane od normalnih operacija tako da samo određeno ovlašćeno osoblje ima pristup ključevima za upotrebu.

Privatni ključevi Pružaoca usluga od poverenja koji se koriste za izdavanje sertifikata organizacije za sertifikaciju čuvaju se na fizički bezbednom mestu, u bezbednom modulu za hardversku sigurnost.

Pružalac usluga od poverenja briše privatne ključeve za potpisivanje koji su smešteni na modulima za hardversku sigurnost koji su van funkcije, kako je definisano u uputstvu uređaja, tako da je praktično nemoguće vratiti ključeve.

Povereni pružalac usluge ne generiše parove ključeva za aplikanta, čime se eliminiše potreba da se obezbedi čuvanje privatnih ključeva krajnjeg korisnika.

6.2.1 Standardi i kontrole kriptografskog modula

Sistemi Pružaoca usluga od poverenja koji izdaju sertifikate, potpisuju OCSP i CRL treba da čuvaju privatne ključeve u takvim sigurnosnim hardverskim uređajima koji su u skladu sa sledećim:

- Zahteve ISO/IEC 19790 [29], ili
- Zahteve FIPS 140-2 [41] nivoa 3 ili višeg, ili
- Zahteve FIPS 140-3 [42] nivoa 3 ili višeg, ili
- Zahteve CEN 419 221-5 [26], ili
- Pouzdane sisteme koji su ocenjeni na nivou garancije 4 ili višeg prema ISO/IEC 15408 [28] ili ekvivalentnim kriterijumima bezbednosti. Procena može biti zasnovana na odgovarajućem planu bezbednosnog sistema koji ispunjava zahteve ovog dokumenta, ili na bezbednosnim odredbama.

Pružalac usluga od poverenja čuva privatne ključeve pružaoca izvan modula za hardversku sigurnost samo u enkriptovanom obliku. Za kodiranje se koriste samo algoritmi i parametri ključa koji odgovaraju stvarnoj algoritamskoj odluci Nacionalne medijske i informatičke agencije koja je izdata prema Zakonu CCXXII iz 2015. godine [8] 92. § (1) b) i koji se očekuje da mogu da izdrže kriptografske napade tokom celog životnog veka ključeva.

Privatni ključevi pružaoca usluga od poverenja se čuvaju na fizički bezbednom mestu čak i u enkriptovanom obliku, u sefu podatkovnog centra, gde su dostupni samo ovlašćenim osobama.

U slučaju oslabljivanja kriptografskih algoritama i parametara ključa, Pružalac usluga od poverenja uništava kodirane ključeve ili ih ponovo kodira koristeći algoritme i parametre ključa koji obezbeđuju veću zaštitu.

6.2.2 Kontrola privatnog ključa (N od M) višestruka osoba

Pružalac usluga od poverenja primenjuje "n od m" prilikom aktivacije funkcija upravljanja ključevima povezanih sa privatnim ključem. Parametri su određeni tako da je istovremeno prisustvo najmanje dva zaposlenika sa pouzdanim ulogama potrebno za kritične operacije koje se izvode sa njegovim privatnim ključevima pružaoca.

6.2.3 Čuvanje privatnog ključa

Pružalac usluga od poverenja ne čuva kopije svojih privatnih ključeva pružaoca usluga ili krajnjih korisnika.

6.2.4 Rezervna kopija privatnog ključa

Pružalac usluga od poverenja pravi sigurnosne kopije svojih privatnih ključeva pružaoca pre nego što stavi privatni ključ pružaoca u upotrebu, kako je opisano u odeljku 6.2.1, u zaštićenom okruženju, u istovremenom prisustvu najmanje dve osobe sa pouzdanim ulogama, uz isključenje drugih osoba. Tokom bekapovanja, privatni ključ napušta modul u enkriptovanom obliku, i ovaj enkriptovani ključ može biti učitan u drugi modul. Bekapovanje i vraćanje se mogu obaviti samo putem mehanizama zaštite opisanih u odeljku 6.2.2.

Pružalac usluga od poverenja čuva rezervne kopije u dupliciranoj formi, pri čemu se najmanje jedna kopija čuva na drugom mestu od lokacije pružaoca usluga.

Isti strogi bezbednosni standardi primenjuju se na upravljanje i očuvanje rezervnih kopija kao i na rad proizvodnog sistema.

Pružalac usluga od poverenja ne pravi nikakve kopije privatnih ključeva krajnjih korisnika.

6.2.5 Arhiviranje privatnog ključa

Pružalac usluga od poverenja ne arhivira svoje privatne ključeve niti privatne ključeve krajnjih korisnika.

6.2.6 Transfer privatnog ključa u ili iz kriptografskog modula

Svi privatni ključevi pružaoca usluga od poverenja moraju biti kreirani u kriptografskom modulu koji ispunjava zahteve.

Privatni ključevi ne smeju postojati u otvorenom obliku izvan hardverskog sigurnosnog modula.

Pružalac usluga od poverenja može izvesti privatni ključ iz hardverskog sigurnosnog modula samo u svrhu pravljenja sigurne kopije.

Izvoz i učitavanje privatnih ključeva pružaoca usluga se vrši prema odredbama odeljka 6.2.2.

6.2.7 Čuvanje privatnog ključa na kriptografskom modulu

Pružalac usluga od poverenja treba da čuva privatne ključeve koji se koriste za pružanje usluge u skladu sa trenutnim Polisama sertifikacije u hardverskom sigurnosnom modulu.

Nema ograničavajućeg uslova koji se odnosi na oblik skladištenja u hardverskom sigurnosnom modulu.

6.2.8 Način aktiviranja privatnog ključa

Pružalac usluga od poverenja čuva svoje privatne ključeve pružaoca u sigurnom hardverskom modulu za bezbednost i poštuje uputstva za korisnike i zahteve navedene u dokumentima za sertifikaciju.

Hardverski sigurnosni modul može biti aktiviran samo odgovarajućim operaterskim karticama, i privatni ključevi unutar hardverskog sigurnosnog modula ne mogu biti korišćeni pre aktiviranja modula.

Pružalac usluga od poverenja čuva operaterske kartice u sigurnom okruženju i pristup njima mogu imati samo ovlašćeni zaposlenici Pružaoca usluga od poverenja.

Pružalac usluga od poverenja obezbeđuje da se potpisi mogu kreirati samo pomoću privatnog ključa korenskog sertifikata u slučaju komandi izdatih direktno od strane ovlašćenog poverenja koji je zapravo ovlašćen da to učini.

U slučaju oslabljivanja kriptografskih algoritama i parametara ključeva, Povereni pružalac usluge uništava kodirane ključeve ili ih ponovo kodira koristeći algoritam i parametre ključeva koji obezbeđuju veću zaštitu.

6.2.9 Način deaktivacije privatnog ključa

Privatni ključevi Pružaoca usluga od poverenja

Privatni ključ koji koristi Pružalac usluga od poverenja, a upravlja ga kriptografskim uređajima, postaje deaktiviran ako (na redovan ili nepravilan način) uređaj bude izuzet iz aktivnog statusa. To se može desiti u sledećim slučajevima:

- Korisnik deaktivira ključ,
- Napajanje uređaja je prekinuto (isključeno ili problem sa napajanjem),
- Uređaj pređe u stanje greške.

Privatni ključ deaktiviran na ovaj način ne može se koristiti sve dok modul ponovo ne bude u aktivnom stanju.

Privatni ključevi krajnjih korisnika

Aplikant je odgovoran za pravilnu upotrebu privatnih ključeva.

6.2.10 Metod uništavanja privatnog ključa

Privatni ključevi pružaoca usluga poverenja

Odbačeni, istekli ili kompromitovani privatni ključevi Pružaoca usluga od poverenja uništavaju se na način koji čini dalju upotrebu privatnih ključeva nemogućom.

Pružalac usluga od poverenja uništava privatne ključeve pružaoca usluga koji su smešteni u sigurnom hardverskom sigurnosnom modulu organizacije za sertifikaciju prema procedurama i zahtevima definisanim u uputstvu za korisnike i u dokumentima za sertifikaciju korišćenog hardverskog sigurnosnog modula, u istovremenom prisustvu dva zaposlenika Pružaoca usluga od poverenja (administratora infrastrukture i bezbednosnog službenika), uz isključenje drugih osoba.

Pružalac usluga od poverenja uništava svaku rezervnu kopiju privatnog ključa na dokumentovan način, tako da njegovo vraćanje i korišćenje postane nemoguće.

Privatni ključevi krajnjeg korisnika

Preporučuje se da odbačeni privatni ključevi za autentifikaciju veb sajtova krajnjih korisnika budu uništeni.

6.2.11 Ocena kriptografskog modula

Prema zahtevima odeljka 6.2.1, svaki privatni ključ provajdera Pružaoca usluga od poverenja treba da bude smešten u kriptografskom modulu koji:

- Ima sertifikat u skladu sa ISO/IEC 19790 [29], ili
- Ima sertifikat u skladu sa FIPS 140-2 Nivoom 3 [41], ili
- Ima sertifikat u skladu sa FIPS 140-3 Nivoom 3 [42], ili
- Ima sertifikat sa najmanje EAL-4 nivoom po zajedničkim kriterijumima [43] koji potvrđuje usklađenost sa zahtevima CEN 419 221-5 [26], ili
- Ima sertifikat izdat u te svrhe od strane nezavisnog tela za sertifikaciju ovlašćenog za evaluaciju proizvoda elektronskog potpisa, registrovanog kod Nacionalne medijske i informatičke agencije ili u nekoj članici Evropske unije.

6.3 Drugi aspekti upravljanja parovima ključeva

6.3.1 Arhiviranje javnog ključa

Pružalac usluga od poverenja arhivira svaki izdati sertifikat tokom deset godina nakon isteka perioda važenja ili do okončanja nastale dispute vezane za sertifikat.

Tokom istog perioda, Pružalac usluga od poverenja čuva uređaje pomoću kojih se može utvrditi sadržaj sertifikata.

6.3.2 Operativni periodi sertifikata i periodi upotrebe parova ključeva

Ključevi i sertifikati korenskih jedinica sertifikacije

Period važenja sertifikata korenske jedinice sertifikacije Pružaoca usluga od poverenja i privatnih ključeva koji im pripadaju ne sme biti duži od vremena do kojeg se mogu sigurno koristiti korišćeni kriptografski algoritmi prema algoritamskoj odluci Nacionalne medijske i informatičke agencije.

Period važenja sertifikata korenske jedinice sertifikacije Pružaoca usluga od poverenja i privatnih ključeva je kako sledi:

- Ključ korenske jedinice sertifikacije " " bio je važeći do 2017-04-06.
- Ključ korenske jedinice sertifikacije " " bio je važeći do 2017-04-26.
- Ključ korenske jedinice sertifikacije " " važi do 2029-12-30.
  Zbog planiranog ukidanja korišćenja 2048-bitnih RSA ključeva - do 31.12.2025. prema trenutno važećim kriptografskim zahtevima - cela hijerarhija će biti zatvorena prema planu.
- Ključ korenske jedinice sertifikacije " " važi do 2042-08-22.
- Period važenja root sertifikata kreiranih posle 15. septembra 2023. godine treba da bude:
  - Minimalno 2.922 dana (oko 8 godina).
  - Maksimalno 9.132 dana (oko 25 godina).

Ključevi i sertifikati posrednih jedinica sertifikacije

Period važenja sertifikata posrednih jedinica sertifikacije Pružaoca usluga od poverenja i privatnih ključeva koji im pripadaju:

- Ne sme biti duži od vremena do kog se kriptografski algoritmi mogu sigurno koristiti prema algoritamskoj odluci Nacionalne medijske i infokomunikacione agencije;
- Ne sme biti duži od perioda važenja sertifikata korenskog ili posrednog provajdera koji je izdao sertifikat posrednog provajdera.

Privatni ključevi posrednih (ne korenskih) jedinica sertifikacije Pružaoca usluga od poverenja važe do isteka vremena važenja sertifikata koji im pripadaju.

Sertifikati krajnjih korisnika

Period važenja sertifikata za krajnje korisnike izdatih od strane Pružaoca usluga od poverenja je:

- Maksimalno 398 dana (oko 13 meseci) od datuma izdavanja.
- Ne sme biti duži od datuma do kog se kriptografski algoritmi mogu sigurno koristiti prema algoritamskoj odluci Nacionalne medijske i infokomunikacione agencije;
- Ne sme biti duži od datuma isteka sertifikata provajdera koji je izdao sertifikat.

Uzimajući u obzir navedene aspekte, Pružalac usluga od poverenja izdaje sertifikate krajnjih korisnika sa sledećim podrazumevanim periodima važenja:

- 365 dana (=12 meseci) od datuma izdavanja.

Ukoliko Pružalac usluga od poverenja odstupi od navedenih vrednosti, obavestiće Klijente unapred.

Tokom obnove sertifikata i modifikacije sertifikata, Pružalac usluga od poverenja može izdati novi sertifikat za isti privatni ključ krajnjeg korisnika.

Ako Nacionalna medijska i infokomunikaciona agencija donese novu uredbu o algoritmima, prema kojoj korišćeni kriptografski algoritam ili parametar ključa nije bezbedan do planiranog perioda upotrebe, to utiče na period važenja kako ključeva pružaoca usluga tako i krajnjih korisnika. Ukoliko se ovo dogodi, Pružalac usluga od poverenja opoziva pripadajuće sertifikate.

6.4 Aktivacioni podaci

6.4.1 Generisanje i instalacija aktivacionih podataka

Privatni ključevi Pružaoca usluga od poverenja moraju biti zaštićeni u skladu sa procedurama i zahtevima definisanim u uputstvu za korisnika korišćenog modula za hardversku sigurnost i dokumentima o sertifikaciji.

U slučaju korišćenja aktivacionih podataka zasnovanih na lozinkama, lozinke moraju biti dovoljno složene kako bi se obezbedio potreban nivo zaštite.

Pružalac usluga od poverenja nikada ne generiše privatne ključeve bazirane na softveru za sertifikate krajnjih korisnika.

Kreiranje i instalacija aktivacionih podataka za privatne ključeve koje je kreirao aplikant je obaveza aplikanta.

6.4.2 Zaštita aktivacionih podataka

Zaposlenici Pružaoca usluga od poverenja upravljaju uređajima za aktivaciju privatnih ključeva i aktivacionim podacima na siguran način, štiteći ih korišćenjem tehničkih i organizacionih mera, pri čemu se lozinke čuvaju samo u enkriptovanom obliku.

Zaštita aktivacionih podataka privatnih ključeva kreiranih od strane aplikanta je dužnost i odgovornost samog aplikanta.

6.4.3 Drugi aspekti aktivacionih podataka

Nema odredbe.

6.5 Kontrole računarske bezbednosti

6.5.1 Specifični tehnički zahtevi za računarsku bezbednost

Tokom konfiguracije i operacije IT sistema Pružaoca usluga od poverenja, obezbeđuje se usaglašenost sa sledećim zahtevima:

- Identitet korisnika se proverava korišćenjem kontrola multifaktorske autentifikacije putem VPN sertifikata koji su sačuvani na kartici pre nego što se omogući pristup sistemu ili aplikaciji;
- Korisnicima se dodeljuju uloge i obezbeđuje se da svi korisnici imaju samo dozvole koje odgovaraju njihovim ulogama;
- Za svaku transakciju se kreira evidencija u dnevniku (log-u), a dnevnički zapisi se arhiviraju;
- Za procese od ključnog značaja za bezbednost, obezbeđeno je da su interni mrežni domeni Pružaoca usluga od poverenja dovoljno zaštićeni od neovlašćenog pristupa;
- Primenjuju se odgovarajuće procedure radi osiguranja oporavka usluge nakon gubitka ključa ili kvara sistema.

6.5.2 Ocena računarske bezbednosti

Paperless ističe važnost iskustva korisnika. Kako bi održala visok nivo usluga, Paperless već od 23. januara 2002. godine funkcioniše po sistemu kontrole kvaliteta u skladu sa standardom ISO 9001. Usaglašenost sa ovim standardom je potvrđena od strane Lloyd's Register Quality Assurance.

Paperless pridaje visok prioritet bezbednosti sistema koje koristi, te stoga već od 19. maja 2003. godine funkcioniše po sistemu upravljanja informacionom bezbednošću koji je usklađen sa standardom ISO/IEC 27001 (ranije poznat kao BS 7799) u svojim glavnim oblastima delatnosti. Usaglašenost sa ovim standardom je potvrđena od strane Lloyd's Register Quality Assurance.

Obuhvat sistema kontrole kvaliteta i sistema upravljanja informacionom bezbednošću pokriva usluge poverenja koje pruža Paperless.

Paperless ima dvostruku procenu rizika koja obuhvata, osim rizika u informacionim tehnologijama, celu organizaciju uključujući i poslovne rizike. Procena rizika se ažurira najmanje jednom godišnje.

Na osnovu rezultata procene rizika, Pružalac usluga

- sprovodi nove mere kako bi eliminisao ranjivosti, ili/ili
- prihvata identifikovane preostale rizike navodeći razlog odluke.

6.6 Tehničke kontrole životnog ciklusa

6.6.1 Kontrole razvoja sistema

Pružalac usluga od poverenja sme koristiti samo aplikacije i uređaje u svom produkcijskom IT sistemu koji:

- Su komercijalni softver, dizajniran i razvijen dokumentovanom metodologijom dizajna, ili;
- Su prilagođena hardverska i softverska rešenja razvijena od strane Pružaoca usluga od poverenja tokom kojih su korišćene strukturirane metode razvoja i kontrolisano okruženje razvoja, ili;

- Su prilagođena hardverska i softverska rešenja razvijena od strane pouzdane strane za Pružaoca usluga od poverenja tokom kojih su korišćene strukturirane metode razvoja i kontrolisano okruženje razvoja, ili;
- Su softver otvorenog koda koji se pridržava sigurnosnih zahteva i čija adekvatnost je obezbeđena verifikacijom softvera i strukturiranim razvojem i upravljanjem životnim ciklusom.

Nabavka IT alata se vrši na način koji isključuje promene hardverskih i softverskih komponenti koristeći pouzdane, redovno kvalifikovane dobavljače.

Hardverske i softverske komponente koje se primenjuju za pružanje usluga ne koriste se u druge svrhe od strane Pružaoca usluga od poverenja.

Pružalac usluga od poverenja sprečava zlonamerni softver da uđe u uređaje koji se koriste za pružanje usluga sertifikacije uz odgovarajuće bezbednosne mere.

Hardverske i softverske komponente se redovno proveravaju na zlonamerni softver pre prve upotrebe, i naknadno.

Pružalac usluga od poverenja postupa sa istom pažnjom prilikom nabavke ažuriranja programa kao i prilikom nabavke prve verzije.

Pružalac usluga od poverenja zapošljava pouzdan, adekvatno obučen kadar tokom instaliranja softvera i hardvera.

Pružalac usluga od poverenja instalira samo softvere na svoju IT opremu za pružanje usluga koji su neophodni za svrhe pružanja usluga.

Pružalac usluga od poverenja ima sistem kontrole verzija gde je svaka promena u IT sistemu dokumentovana.

Pružalac usluga od poverenja koristi automatski sistem nadgledanja kako bi zabeležio sve neovlaštene promene, koji beleži sve promene u svakom fajlu i u slučaju promena u praćenim fajlovima generiše unos u dnevnik ili šalje upozorenje operaterima sistema.

6.6.2 Kontrole upravljanja sigurnošću

Pružalac usluga od poverenja mora implementirati procese za dokumentovanje, upravljanje, proveru, praćenje i održavanje sistema koji se koriste u usluzi, uključujući njihovu modifikaciju i dalji razvoj. Sistem za kontrolu verzija mora detektovati svaku vrstu neovlašćenih promena, unosa podataka koji utiču na sistem, firewall-a, rutera, programa i drugih komponenti korišćenih u usluzi.

Pri instaliranju programa koji se koristi u usluzi, Pružalac usluga od poverenja mora osigurati da je instalirana odgovarajuća verzija programa i da je slobodna od svake neovlašćene modifikacije.

Pružalac usluga od poverenja redovno mora proveravati integritet softvera u svom sistemu koji se koristi u usluzi.

Svaki Hardverski sigurnosni modul koji koristi Pružalac usluga od poverenja je proveren, testiran i evaluiran. Pružalac usluga od poverenja proverava integritet modula:

- Nakon nabavke uređaja tokom preuzimanja,
- Neposredno pre prve upotrebe,

- Redovno tokom rada.

Pružalac usluga od poverenja trajno ili privremeno briše privatne ključeve pružaoca iz hardverskih sigurnosnih modula koji su povučeni iz upotrebe.

Pružalac usluga od poverenja čuva nekorišćene hardverske sigurnosne module na fizički zaštićenoj lokaciji.

6.6.3 Kontrole sigurnosti tokom životnog ciklusa

Pružalac usluga od poverenja mora obezbediti zaštitu korišćenih modula za hardversku sigurnost tokom celog njihovog životnog ciklusa.

Tokom operacije IT opreme i sistema koji se koriste za pružanje usluga, Pružalac usluga od poverenja uzima u obzir bezbednosne aspekte koji se odnose na životni ciklus opreme, prema kojem:

- Koristi adekvatno sertifikovane Hardverske sigurnosne module u svojim sistemima;
- Nakon prijema hardverskih sigurnosnih modula, obezbeđuje da kontrola kvaliteta garantuje zaštitu hardverskih sigurnosnih modula od manipulacija tokom transporta;
- Čuva hardverske sigurnosne module na sigurnom mestu i obezbeđuje zaštitu od manipulacija tokom skladištenja;
- Neprekidno se pridržava zahteva postavljenih u sigurnosnom cilju hardverskih sigurnosnih modula, uputstvima za upotrebu i izveštaju o sertifikaciji tokom operacije;
- Briše privatne ključeve sa svojih van upotrebe izbačenih hardverskih sigurnosnih modula na način da postane praktično nemoguće vratiti ključeve;
- Rukuje i odlučuje o van upotrebe izbačenim hardverskim sigurnosnim modulima u skladu sa zahtevima njihovog sigurnosnog cilja, uputstvima za upotrebu i izveštaju o sertifikaciji.

6.7 Kontrole sigurnosti mreže

Pružalac usluga od poverenja prati najbolje prakse industrije za osiguravanje svojih mreža. On se pridržava Zahteva za sigurnost mreže i sistema sertifikata CA/B foruma.

Pružalac usluga od poverenja strogo kontroliše konfiguraciju svojih IT sistema, dokumentujući svaku promenu, uključujući i najmanju modifikaciju, razvoj i ažuriranje softvera.

Pružalac usluga od poverenja implementira odgovarajuće procedure za otkrivanje bilo kakve promene hardvera ili softvera, instalaciju sistema i održavanje na IT sistemu.

Pružalac usluga od poverenja proverava autentičnost i integritet svake softverske komponente prilikom njihovog prvog učitavanja.

Pružalac usluga od poverenja primenjuje odgovarajuće mere zaštite mreže, na primer:

- deli svoj IT sistem na dobro odvojene sigurnosne zone;
- razdvaja posvećenu mrežu za administraciju IT sistema i operativnu mrežu Pružaoca usluga od poverenja;
- razdvaja proizvodne sisteme za usluge Pružaoca usluga od poverenja od sistema korišćenih u razvoju i testiranju;
- uspostavlja komunikaciju između različitih pouzdanih sistema samo putem pouzdanih kanala koji su logički odvojeni od drugih komunikacionih kanala i obezbeđuju

pouzdanu identifikaciju njihovih krajnjih tačaka i zaštitu podataka kanala od izmene ili otkrivanja;
- operiše IT sisteme koji se koriste za živu operativnu mrežu u sigurnim mrežnim zonama;
- ograničava pristup i komunikaciju između zona na one neophodne za rad usluge;
- onemogućava nekorišćene protokole i korisničke naloge;
- onemogućava nekorišćene mrežne portove i servise;
- Pokreće samo mrežne aplikacije koje su bezuslovno neophodne za pravilan rad IT sistema;
- redovno pregleda uspostavljena pravila.

Pružalac usluga od poverenja sprovodi ili vrši skeniranje ranjivosti javnih i privatnih IP adresa:

- u roku od jedne nedelje od dobijanja zahteva od strane CA/Browser Foruma;
- nakon bilo kakvih promena u sistemu ili mreži koje CA odredi kao značajne;
- najmanje svaka tri (3) meseca.

Pružalac usluga od poverenja proverava usklađenost konfiguracije lokalnih komponenti mreže (npr. rutera) sa zahtevima navedenim od strane Pružaoca usluga od poverenja najmanje svaka tri meseca.

Pružalac usluga od poverenja naručuje testiranje penetracije od spoljnog nezavisnog stručnjaka koji ima potrebne veštine, alate, stručnost i etički kodeks kako bi pružio pouzdan izveštaj jednom godišnje i u slučaju značajne promene u IT mreži.

6.8 Vremensko označavanje

Za zaštitu integriteta log datoteka i drugih elektronskih datoteka koje treba arhivirati, Pružalac usluga od poverenja koristi kvalifikovane elektronske vremenske žigove.

7 Profili sertifikata, CRL-a i OCSP-a

7.1 Profil sertifikata

Sertifikati za krajnje korisnike izdati od strane Pružaoca usluga od poverenja i svi root i intermediate sertifikati provajdera koji se nalaze u sertifikacionom lancu koji se koristi za izdavanje sertifikata moraju se pridržavati sledećih preporuka i zahteva:

- ITU X.509
- IETF RFC 3739
- IETF RFC 5280
- IETF RFC 6818
- ETSI EN 319 412-1
- ETSI EN 319 412-2
- ETSI EN 319 412-5

Osnovna polja root i intermediate sertifikata:

Paperless ROOT CA	
Nazivi Polja	Vrednost (i značenje)
Version	V3
Serial Number	DODATI
Signature algorithm	Sha256RSA
Signature	DODATI
Issuer	CN = Paperless Root CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS
Validity	Valid from: DODATI Valid to: DODATI
Subject	CN = Paperless Root CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS
Subject Public Key Algorithm	rsaEncryption (OID)

Paperless Pravna lica CA	
Nazivi Polja	Vrednost (i značenje)
Version	V3
Serial Number	DODATI
Signature algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature	DODATI
Issuer	CN = Paperless Root CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS

Validity	Valid from: DODATI Valid to: DODATI
Subject	CN = Paperless Pravna lica CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS
Subject Public Key Algorithm	rsaEncryption (OID)

Paperless GOV CA	
Nazivi Polja	Vrednost (i značenje)
Version	V3
Serial Number	DODATI
Signature algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature	DODATI
Issuer	CN = Paperless Root CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS
Validity	Valid from: DODATI Valid to: DODATI
Subject	CN = GOV CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS
Subject Public Key Algorithm	rsaEncryption (OID)

7.1.1Broj verzije

Paperless d.o.o pružalac usluga od poverenja izdaje elektronske sertifikate u formatu X.509 tako da su svi sertifikati verzije 3.

7.1.2 Ekstenzije sertifikata

Ekstenzije root i intermediate sertifikata:

Paperless ROOT CA	
Nazivi Polja	Vrednost (i značenje)
Certificate Policies	Certificate Policy: • Policy Identifier=All issuance policies [1,1] Policy Qualifier Info: • Policy Qualifier Id=CPS • Qualifier: LINK
Authority Key Identifier	KeyID=DODATI
Subject Key Identifier	DODATI
Basic Constraints	Subject Type=CA

	Path Length Constraint=None
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing

Paperless Pravna lica CA	
Nazivi Polja	Vrednost (i značenje)
Certificate Policies	Certificate Policy: • Policy Identifier=All issuance policies [1,1] Policy Qualifier Info: • Policy Qualifier Id=CPS • Qualifier: LINK
Authority Key Identifier	KeyID=DODATI
Subject Key Identifier	DODATI
Basic Constraints	Subject Type=CA Path Length Constraint=None
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing

Paperless GOV CA	
Nazivi Polja	Vrednost (i značenje)
Certificate Policies	Certificate Policy: • Policy Identifier=All issuance policies [1,1] Policy Qualifier Info: • Policy Qualifier Id=CPS • Qualifier: LINK
Authority Key Identifier	KeyID=DODATI
Subject Key Identifier	DODATI
Basic Constraints	Subject Type=CA Path Length Constraint=None
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing

7.1.3 Identifikatori objekata algoritma

Oznaka kriptografskog algoritma koji je korišćen za overu sertifikata. Sledeći kriptografski algoritmi su korišćeni od strane sertifikacionog tela za overu korisničkih sertifikata:

- "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
- "sha384WithRSAEncryption" (1.2.840.113549.1.1.12)
- "sha512WithRSAEncryption" (1.2.840.113549.1.1.13)
- "ecdsaWithSHA256" (1.2.840.10045.4.3.2)
- "ecdsaWithSHA384" (1.2.840.10045.4.3.3)
- "ecdsaWithSHA512" (1.2.840.10045.4.3.4)

7.1.4 Oblici imena

Pogledati poglavlje 3.1.1.

7.1.5 Ograničenja imena

Pružalac usluga od poverenja ne koristi ograničenja imena sa upotrebom polja "nameConstraints".

7.1.6 Identifikator objekta polise sertifikata

Pogledati poglavlje 7.1.2.

7.1.7 Korišćenje Polise o Ograničenjima Ekstenzija

Nema odredbe.

7.1.8 Sintaksa i semantika kvalifikatora polise

U sertifikatima, koje izdaje pružalac usluga od poverenja, upisuje se specifičan podatak policyQualifiers, koji je u skladu sa standardima IETF RFC i ETSI.

7.1.9 Semantika obrade za kritičko proširenje polise sertifikata

Nema odredbe.

7.2 CRL Profil

Registar opozvanih kvalifikovanih elektronskih sertifikata (CRL) izdaje pružalac usluga od poverenja:

- Registar opozvanih intermediate/podređenih sertifikata
  CN= Paperless ROOT CA
  O = Paperless d.o.o
  C = RS
- Registar opozvanih sertifikata za elektronski potpis pravnih lica
  CN= Paperless Pravna lica CA
  O = Paperless d.o.o
  C = RS
- Registar opozvanih sertifikata za elektronski potpis fizičkih lica
  CN= Paperless Fizicka lica CA
  O = Paperless d.o.o
  C = RS

Osnovna polja CRL profila:

Paperless ROOT CA	
Nazivi Polja	Vrednost (i značenje)

Version	V2
Serial number	DODATI
Signature Algorithm	Sha256RSA
Signature	Potpis Paperless ROOT CA
Issuer	CN = Paperless ROOT CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS
thisUpdate	Effective date: <vreme izdavanja prema GMT>
nextUpdate	Next Update: <vreme izdavanja sledeće CRL prema GMT>
revokedCertificate	Serial Number: <identifikaciona oznaka (serijski broj) opozvanog kvalifikovanog elektronskog kvalifikovanih elektronskih sertifikata> Revocation Date: <vreme opoziva prema GMT>

Paperless Fizicka lica CA	
Nazivi Polja	Vrednost (i značenje)
Version	V2
Serial number	DODATI
Signature Algorithm	Sha256RSA
Signature	Potpis Paperless ROOT CA
Issuer	CN = Paperless ROOT CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS
thisUpdate	Effective date: <vreme izdavanja prema GMT>
nextUpdate	Next Update: <vreme izdavanja sledeće CRL prema GMT>
revokedCertificate	Serial Number: <identifikaciona oznaka (serijski broj) opozvanog kvalifikovanog elektronskog kvalifikovanih elektronskih sertifikata> Revocation Date: <vreme opoziva prema GMT>

Paperless Pravna lica CA	
Nazivi Polja	Vrednost (i značenje)
Version	V2
Serial number	DODATI
Signature Algorithm	Sha256RSA
Signature	Potpis Paperless ROOT CA
Issuer	CN = Paperless ROOT CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019

	O = Paperless doo C = RS
thisUpdate	Effective date: <vreme izdavanja prema GMT>
nextUpdate	Next Update: <vreme izdavanja sledeće CRL prema GMT>
revokedCertificate	Serial Number: <identifikaciona oznaka (serijski broj) opozvanog kvalifikovanog elektronskog kvalifikovanih elektronskih sertifikata> Revocation Date: <vreme opoziva prema GMT>

Paperless GOV CA	
Nazivi Polja	Vrednost (i značenje)
Version	V2
Serial number	DODATI
Signature Algorithm	Sha256RSA
Signature	Potpis Paperless ROOT CA
Issuer	CN = Paperless ROOT CA 2.5.4.97 = VATRS-108709130 2.5.4.97 = MB:RS-21052019 O = Paperless doo C = RS
thisUpdate	Effective date: <vreme izdavanja prema GMT>
nextUpdate	Next Update: <vreme izdavanja sledeće CRL prema GMT>
revokedCertificate	Serial Number: <identifikaciona oznaka (serijski broj) opozvanog kvalifikovanog elektronskog kvalifikovanih elektronskih sertifikata> Revocation Date: <vreme opoziva prema GMT>

7.2.1 Broj verzije

Registar opozvanih kvalifikovanih elektronskih sertifikata odgovara preporuci ITU-T X.509 i ISO/IEC 9594-8:2014. Registar opozvanih kvalifikovanih elektronskih sertifikata dostupan je putem HTTP protokola.

7.2.2 CRL Ekstenzije

Ekstenzijež CRL profila:

Paperless ROOT CA	
Nazivi Polja	Vrednost (i značenje)
Authority Key Identifier	KeyID=DODATI

CRL number	Redni broj izdatog registra opozvanih kvalifikovanih elektronskih sertifikata

Paperless Pravna lica CA	
Nazivi Polja	Vrednost (i značenje)
Authority Key Identifier	KeyID=DODATI
CRL number	Redni broj izdatog registra opozvanih kvalifikovanih elektronskih sertifikata

Paperless GOV CA	
Nazivi Polja	Vrednost (i značenje)
Authority Key Identifier	KeyID=DODATI
CRL number	Redni broj izdatog registra opozvanih kvalifikovanih elektronskih sertifikata

7.3 OSCP Profil

OCSP (Online Certificate Status Protocol) se koristi za proveru statusa opoziva X.509 elektronskog sertifikata.

Ova usluga je implementirana u skladu sa IETF RFC 6960.

Osnovna polja		
Polje	**Atribut**	**Vrednost**
Version	Version	V3, vrednost=”2”
Serial Number	CertificateSerialNumber	16 ili 17 okteta, 64 bita entropije
signatureAlgorithm	AlgorithmIdentifier	sha256WithRSAEncryption
signatureValue		Potpis izdavača sertifikata
Issuer	commonName (CN)	Paperless d.o.o
	organizationName (O)	Paperless - Veb-Autentikacija
	countryName (C)	RS
Validity	notBefore	Vreme izdavanja sertifikata
	notAfter	Vreme izdavanja sertifikata + 12 meseci
Subject	commonName (CN)	Paperless d.o.o 2024 OCSP
	organizationName (O)	Paperless - Veb-Autentikacija
	countryName (C)	RS
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption

	subjectPublicKey	Javni ključ subjekta dužine 2048 bita

Ekstenzije			
Polje	**Kritično**	**Atribut**	**Vrednost**
KeyUsage	DA		Client Authentication, Digital Signature, Key Encipherment, Non Repudiation
extKeyUsage	NE	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak dužine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak dužine 160 bita
BasicConstraints	DA		cA=FALSE pathLenConstraint=None

7.3.1 Broj verzije

Pružalac usluga od poverenja podržava zahteve i odgovore za online proveru statusa sertifikata u skladu sa "v1" verzijom prema standardu IETF RFC 6960. Podrazumevana vrednost polja (Version) je "v1", pa ovo polje nije uključeno u OCSP odgovor.

7.3.2 OCSP ekstenzije

OCSP poruke (zahtevi/odgovori) za stalnu proveru statusa sertifikata podržavaju ekstenziju Nonce, koja nije označena kao kritična.

8 Revizija usklađenosti i druga procenjivanja

U okviru pružaoca usluga od poverenja postoji jedinica za unutrašnju kontrolu i usklađenost koju čine stručnjaci sa odgovarajućim tehnološkim i pravnim znanjima, a koji ne vrše zadatke vezane za upravljanje kvalifikovanim elektronskim sertifikatima.

Sistem evidentičar nadzire rad Paperless d.o.o U slučaju otkrivenih nedostataka definiše odgovarajuće mere za uklanjanje tih nedostataka, koje je pružalac usluga od poverenja dužno da sprovede, i nadzire sprovođenje definisanih mera.

Sistem evidentičar vrše nadzor rada pružaoca usluga od poverenja najmanje jedanput u godini.

8.1 Učestalost ili okolnosti procene

Pružalac usluge od poverenja godišnje sprovodi procenu usaglašenosti svog IT sistema koji obavlja pružanje usluga.

8.2 Identitet/Kvalifikacije procenitelja

Pružalac usluga od poverenja može sprovoditi interne revizije uz pomoć svojih zaposlenih koji obavljaju ulogu nezavisnih revizora sistema.

Spoljni revizor ima odgovarajuća tehnološka i pravna znanja

8.3 Odnos procenitelja prema procenjenom subjektu

Spoljni revizor može biti samo osoba koja:

- Je nezavisna od vlasnika, menadžmenta i operacija pregledanog pružaoca usluga od poverenja;
- Je nezavisna od pregledane organizacije, odnosno ni ona sama ni njeni bliski rođaci nemaju zaposlenje niti poslovni odnos sa pružaocem usluga od poverenja.
- Naknada nije zavisna od rezultata aktivnosti sprovedenih tokom revizije.

8.4 Teme obuhvaćene procenom

Pregled bi trebalo da obuhvati sledeće oblasti:

- Usaglašenost sa važećim zakonodavstvom;
- Usaglašenost sa tehničkim standardima;
- Usaglašenost sa Polisom sertifikata i Izjavom o praksi sertifikacije;
- Adekvatnost primenjenih procesa;
- Dokumentacija;
- Fizička bezbednost;
- Adekvatnost osoblja;
- IT bezbednost;
- Usaglašenost sa pravilima o zaštiti podataka.

Ako Pružalac usluga od poverenja izda podređeni sertifikat za sertifikacionu jedinicu druge organizacije, tada se navedena područja takođe pregledaju i u tim spoljnim organizacijama.

8.5 Akcije preduzete kao rezultat nedostataka

Nezavisni revizor treba da sumira rezultate pregleda u detaljnom izveštaju o pregledu koji obuhvata testirane komponente sistema, procese i sadrži dokaze korištene u pregledu i izjave revizora. Nesuglasice otkrivene tokom pregleda i rokovi za njihovo ispravljanje trebalo bi da budu zabeleženi u posebnoj poglavlju izveštaja.

Nezavisni revizor može da zabeleži, na osnovu njihove ozbiljnosti, razlike i nesuglasice otkrivene tokom pregleda:

- Predloge za izmene koje se opciono mogu uzeti u obzir;
- Derogacije koje obavezno treba izbeći.

8.6 Objava rezultata

Rezultati sprovođenja nadzora čuvaju se u okviru pružaoca usluga od poverenja.

9 Ostale poslovne i pravne stvari

9.1 Naknade

Pružalac usluga od poverenja objavljuje cene i tarife na svojoj veb lokaciji i čini ih dostupnim za čitanje putem svoje korisničke službe.

Dostupnost cenovnika:

- https://paperless.rs

Pružalac usluga od poverenja može jednostrano promeniti cenovnik. Pružalac usluga od poverenja objavljuje svaku izmenu cenovnika 30 dana pre stupanja na snagu.

Promene koje su povoljne za klijenta mogu stupiti na snagu sa kraćim rokom od 30 dana.

Izmene neće uticati na cenu usluga plaćenih unapred.

Odredbe vezane za plaćanje i refundiranje taksi sadržane su u ugovoru o pružanju usluga i njegovim prilozima - posebno u Opštim uslovima i odredbama.

9.1.1 Naknade za izdavanje ili obnavljanje sertifikata

Videti Poglavlje 9.1.

9.1.2 Naknade za pristup sertifikatu

Pružalac usluga od poverenja mora omogućiti besplatan online pristup svom repozitorijumu sertifikata za strane koji se oslanjaju na te sertifikate.

9.1.3 Naknade za pristup informacijama o povlačenju ili statusu

Pružalac usluga od poverenja pruža besplatnu uslugu CRL i OCSP putem interneta za strane osobe na statusu svih krajnjih korisničkih i posredničkih sertifikata koje je izdao.

9.1.4 Naknade za ostale usluge

Videti Poglavlje 9.1.

9.1.5 Politika povraćaja novca

Videti Poglavlje 9.1.

9.2 Finansijska odgovornost

Da bi olakšao poverenje, Pružalac usluga od poverenja mora da se pridržava finansijskih i odgovornih zahteva navedenih u nastavku.

9.2.1 Pokriće osiguranja

Pružalac usluga od poverenja ima dovoljno finansijskih resursa za svoje odgovornosti vezane za pružanje usluga i za pokrivanje troškova povezanih sa njegovim prestankom.

9.2.2 Druga sredstva

Nema odredbi.

9.3 Poverljivost poslovnih informacija

Pružalac usluga od poverenja upravlja podacima klijenata u skladu sa zakonskim propisima. Pružalac usluga ima regulativu o obradi podataka (videti Poglavlje 9.4), koja se posebno bavi obradom ličnih podataka.

Podnošenjem zahteva za izdavanje sertifikata i potpisivanjem ugovora o pružanju usluga, klijenti daju saglasnost Pružaocu usluga da zadržava i obrađuje njihove lične podatke (na način koji je u skladu sa propisima o obradi podataka). Takva saglasnost se odnosi na prosleđivanje informacija koje su navedene zakonom i unete u evidencije trećim licima u slučaju prestanka usluga Pružaoca usluga; takođe na prosleđivanje takvih informacija podizvođačima Pružaoca usluga – isključivo u svrhu obavljanja zadataka vezanih za pružanje usluga.

Aplikanti će dati izjavu da li pristaju na otkrivanje sertifikata na obrascu zahteva za sertifikat koji je povezan sa ugovorom o pružanju usluga.

Pružalac usluga od poverenja koristi podatke klijenata isključivo u vezi sa pružanjem svojih usluga.

Pružalac usluga od poverenja otkriva podatke o subjektima koji se pojavljuju u sertifikatu zajedno sa sertifikatom.

Pružalac usluga od poverenja čuva njihove podatke koji nisu uneti u sertifikat na bezbedan način, u svrhu pružanja dokaza o identitetu subjekata predstavljenih organizacija i obaveza vezanih za pružanje raznih podataka.

Pružalac usluga od poverenja zadržava podatke o kojima saznaje u skladu sa zakonskim zahtevima i za određeni period. Tokom zadržavanja podataka, Pružalac usluga od poverenja vodi računa o netaknutosti, poverljivosti i bezbednom čuvanju informacija. Pristup informacijama dozvoljen je samo pojedincima čiji zadaci to opravdavaju.

Pružalac usluga od poverenja obezbeđuje poverljivost i netaknutost informacija koje nisu javne tokom prosleđivanja podataka klijenata.

9.3.1 Opseg poverljivih informacija

Pružalac usluga od poverenja smatra kao poverljive:

- Sve podatke klijenata, osim onih koji se smatraju informacijama koje nisu poverljive prema sekciji 9.3.2;
- Pored podataka klijenata:
    - Privatne ključeve i aktivacione kodove,

- Zahteve za sertifikatima i Ugovore o pružanju usluga,
- Podatke o transakcijama i logove,
- Ne javne propise,
- Sve podatke čije bi javno otkrivanje imalo štetan uticaj na bezbednost usluge..

9.3.2 Informacije koje nisu obuhvaćene opsegom poverljivih informacija

Pružalac usluga od poverenja smatra sve podatke javnim koji se mogu dobiti iz javnog izvora, ili za čije je otkrivanje pretplatnik dao pismeni pristanak unapred.

Pružalac usluga od poverenja tretira sve podatke koje navede u sertifikatu kao ne-poverljive informacije. Takvi podaci se pojavljuju u formularu zahteva za sertifikat koji je povezan sa ugovorom o pružanju usluga na jasno označen način.

Pružalac usluga od poverenja upravlja statusom opoziva i suspenzije sertifikata za krajnje korisnike i posredne sertifikate kao javne informacije i čini ih dostupnim bez ograničenja Pouzdanih strana objavljivanjem Liste opozvanih sertifikata (CRL) i pružanjem online protokola za proveru statusa sertifikata (OCSP) usluge. Otkrivene informacije sadrže serijski broj sertifikata, vreme opoziva i opciono razlog opoziva. Za više informacija, pogledajte sekciju 7.2. i 7.3.

9.3.3 Odgovornost za zaštitu poverljivih informacija

Pružalac usluga od poverenja odgovoran je za zaštitu poverljivih podataka koje upravlja.

Pružalac usluga od poverenja obavezuje svoje zaposlene, podizvođače, povezane partnere da štite sve poverljive podatke potpisivanjem izjave o poverljivosti ili ugovora.

Pružalac usluga od poverenja obrađuje poverljive informacije koje dobije u skladu sa odredbama Zakona CXII od 2011. o pravu na slobodan pristup informacijama, i samo ih otkriva licima/organizacijama u sledećim slučajevima:

- **Pružanje informacija nadležnim organima**

  U svrhu istraživanja ili sprečavanja krivičnih dela počinjenih korišćenjem pouzdanih usluga koje pruža, kao i u slučaju interesa za nacionalnu bezbednost, Pružalac usluga od poverenja - ako su ispunjeni zakonski kriterijumi koji se odnose na zahteve za podacima - otkriva relevantne informacije o identitetu i informacije koje je proverio Pružalac usluga od poverenja nadležnim istražnim organima i službama nacionalne bezbednosti besplatno.
  Pružalac usluga od poverenja beleži činjenicu prenosa podataka, ali ne obaveštava uključene klijente o tome.

- **Pružanje informacija u okviru pravnih sporova**

  U toku pravnih postupaka i vanparničnih radnji po opštem pravu, Pružalac usluga od poverenja može dostaviti - u slučaju potvrđenog pogođenosti - informacije o identitetu subjekta i informacije proverene od strane Pružaoca usluga od poverenja, protivnoj strani ili njenom zastupniku, kao i može ih otkriti istražujućem sudu.

Pružalac usluga od poverenja beleži činjenicu prenosa podataka i obaveštava pogođene klijente o tome.

- **Otkrivanje na zahtev vlasnika**

  Na lični zahtev klijenta ili na osnovu njegove zvanične autorizacije, u pisanom obliku, Pružalac usluga od poverenja otkriva poverljive informacije o korisniku koje se odnose na klijenta trećim stranama.

- **Različite okolnosti koje dovode do otkrivanja informacija**

- Po završetku svoje aktivnosti, Pružalac usluga od poverenja je obavezan da preda svoje zapise koji su predmet obaveza pristupa zajedno sa poverljivim podacima korisnika pouzdanom pružaocu usluga koji ga preuzima.

9.4 Privatnost ličnih informacija

Pružalac usluga od poverenja mora voditi računa o zaštiti ličnih podataka kojima upravlja.

Pružalac usluga od poverenja mora:

- Čuvati,
- Po isteku obaveze čuvanja - osim ako klijent drugačije ne naznači - izbrisati iz baze podataka klijenata registrovane lične podatke i informacije o Klijentu u skladu sa zakonskim zahtevima.

Pružalac usluga od poverenja čuva podatke o identifikaciji, podatke o Subjektu koji se pojavljuje u Sertifikatu, podatke o Pretplatniku povezane sa kontakt podacima i podatke povezane sa pružanjem usluge u svojim zapisima.

Pružalac usluga od poverenja prenosi podatke klijenata trećim stranama samo u slučajevima kada je to propisano zakonskim propisom ili ako je klijent dao svoj pristanak za to pismeno.

9.4.1 Plan privatnosti

Pružalac usluga od poverenja ima Politiku privatnosti i dokument obaveštenje o privatnosti, koji sadrže detaljna pravila o postupanju sa ličnim podacima.

9.4.2 Informacije koje se tretiraju kao privatne

Pružalac usluga od poverenja dužan je da zaštiti sve lične podatke koji se odnose na ispitanika ili sadrže zaključke o ispitaniku koji nisu javno dostupni iz sertifikata ili drugih javnih izvora podataka.

9.4.3 Informacije koje se ne smatraju privatnim

Pružalac usluga od poverenja može otkriti podatke o subjektima navedenim u sertifikatu na osnovu pismenog pristanka aplikanta.

Pružalac usluga od poverenja može navesti jedinstveni identifikator pružaoca dodeljen subjektu u sertifikatu.

9.4.4 Odgovornost za zaštitu privatnih informacija

Pružalac usluga od poverenja mora bezbedno čuvati i zaštititi lične podatke koji se odnose na izdavanje sertifikata, a koji nisu navedeni u sertifikatu. Podaci moraju biti zaštićeni odgovarajućim merama, posebno od neovlašćenog pristupa, izmene i otkrivanja.

9.4.5 Obaveštenje i saglasnost za korišćenje privatnih informacija

Pružalac usluga od poverenja sme otkriti samo lične podatke navedene u sertifikatima uz pismenu saglasnost klijenta.

9.4.6 Otkrivanje u skladu sa sudskim ili administrativnim postupkom

U slučajevima definisanim relevantnim zakonodavstvom, Pružalac usluga od poverenja može otkriti sačuvane lične podatke o klijentu bez obaveštavanja klijenta.

9.4.7 Drugi slučajevi otkrivanja informacija

Nema odredbi.

9.5 Prava intelektualne svojine

Tokom svog poslovanja, Pružalac usluga od poverenja ne sme ugroziti nikakva intelektualna prava trećih lica.

Vlasnik privatnog i javnog ključa koje Pružalac usluga od poverenja izdaje klijentima je pretplatnik, dok je puni korisnik aplikant bez obzira na fizički medijum koji sadrži i štiti ključeve.

Vlasnik Sertifikata koji Pružalac usluga od poverenja izdaje svojim klijentima je Pružalac usluga od poverenja, a puni korisnik je aplikant.

Pružalac usluga od poverenja može objaviti, reprodukovati, opozvati i upravljati izdatim sertifikatima krajnjih korisnika, sa javnim ključem sadržanim u njima na način opisan u uslovima i odredbama.

Informacije o statusu opoziva sertifikata su vlasništvo Pružaoca usluga od poverenja, a objavljuju se kako je definisano u sekcijama 7.2. i 7.3.

Jedinstveni identifikator pružaoca koji Pružalac usluga od poverenja izdaje klijentima je vlasništvo Pružalca usluga od poverenja, a objavljuje se kao deo sertifikata od strane Pružaoca usluga od poverenja u repozitorijumu sertifikata.

Imenovani subjekat i klijent imaju pravo na korišćenje identifikacije u sertifikatu (koja identifikuje subjekat sertifikata).

Ovaj praktični dokument o sertifikaciji je isključivo vlasništvo Pružaoca usluga od poverenja. Klijenti i ostale zainteresovane strane imaju pravo samo na korišćenje dokumenta u skladu sa

zahtevima ovog Praktičnog dokumenta o sertifikaciji, a svaka druga upotreba u komercijalne ili druge svrhe strogo je zabranjena.

Ovaj Praktični dokument o sertifikaciji može se slobodno distribuirati u neizmenjenom obliku, u punoj dužini i uz navođenje porekla.

Pravila primene softvera predviđenog za korišćenje usluge od strane Pružaoca usluga od poverenja dostupna su u opisu softvera i uključena su u korisnički priručnik naveden u opisu.

9.6 Izjave i garancije

9.6.1 Izjave i garancije proizvođača sertifikata

Odgovornost sertifikacionog organa

Odgovornost Pružaoca usluga od poverenja definisana je u Praktičnom dokumentu o sertifikaciji, pripadajućim Politikama sertifikacije, i ugovoru o pružanju usluge sa Klijentom i njegovim prilozima.

- Pružalac usluga od poverenja preuzima odgovornost za poštovanje procedura opisanih u Sertifikacionim polisama koje podržava;
- Pružalac usluga od poverenja preuzima odgovornost kao svoju za štetu koja je nastala tokom pružanja usluge od strane njegovih podizvođača;
- Pružalac usluga od poverenja snosi odgovornost u skladu sa pravilima odgovornosti za kršenje ugovora u Građanskom zakoniku Republike Srbije u odnosu na Klijente koji su u ugovornom odnosu.
- Pružalac usluga od poverenja odgovoran je prema pravilima uzrokovane štete van ugovora u Građanskom zakoniku Republike Srbije [6] u odnosu na treće strane (poput poverenika) koje nisu u ugovornom odnosu sa njim.
- Pružalac usluga od poverenja će isplatiti naknadu za štetu sa ograničenjima navedenim u svojim propisima i ugovorima o pružanju usluga zaključenim sa klijentima za dokazane štete koje nastanu u okviru njegove odgovornosti (videti Poglavlje Ograničenje odgovornosti 9.8.).
- Ako važeći zahtev nekoliko ovlašćenih strana u vezi sa događajem osiguranja premašuje iznos definisan za događaj osiguranja u osiguranju od odgovornosti za štetu, tada se nadoknada zahteva vrši u relativnom odnosu prema iznosu utvrđenom u ugovoru o odgovornosti.

Pružalac usluga od poverenja nije odgovoran:

- Za aktivnosti Subjekta vezane za privatni ključ;
- Za aktivnosti provere i korišćenja sertifikata od strane Pouzdanih strana;
- Za propise izdate od strane Pouzdanih strana ili drugih.

Obaveze Sertifikacionog organa

Pružalac usluga poverenja mora ispuniti zahteve definisane u sekciji (2) člana 24. eIDAS uredbe.

Osnovna obaveza Pružaoca usluga poverenja je da pruži uslugu u skladu sa Polisom sertifikacije, ovim praktičnim izveštajem o sertifikaciji, Opštim uslovima i odredbama, kao i internim propisima korporativne i bezbednosne prirode. Ove osnovne obaveze su sledeće:

- Ustanoviti pravni, regulatorni, materijalni, ugovorni, itd. okvir koji je odgovarajući za pružanje usluge;
- Pružiti visok standard i sigurne usluge u skladu sa primenjivim propisima;
- Neprekidno operisati i auditovati organizacije koje su povezane sa uslugama (sertifikaciono telo, korisnička podrška itd.);
- Poštovati procedure propisane propisima i izbeći ili eliminisati bilo kakvo potencijalno neispravno funkcionisanje;
- Osigurati usluge svakom aplikantu koji prihvata uslove i odredbe navedene u propisima;
- Održavati javne i vlasničke zapise, kao i činiti ih kontinuirano dostupnim svima putem interneta.

Obaveze sertifikacione organizacije

Pružalac usluga od poverenja ima zadatak da uspostavi i upravlja sertifikacionim jedinicama (videti Poglavlje: 1.3.1), kao i jedinicama neophodnim za online uslugu statusa sertifikata, da se brine o repozitorijumu sertifikata i informacijama o statusu povlačenja, upravlja i čini dostupnim pametne kartice, kao i da upravlja propisima.

Interna, operativna pravila Pružaoca usluga od poverenja specificiraju kako će se operativno upravljati sertifikacionom organizacijom. Sertifikati izdati od strane sertifikacionih jedinica (za članove osoblja za registraciju, osoblje na dužnosti, itd.) upravljaju se u skladu sa odredbama operativnih propisa. Ova izjava obuhvata samo odredbe u vezi sa javnim pružaocima i korisničkim sertifikatima.

Zadaci koji se obavljaju u okviru upravljanja propisima:

- Specifikacija, odobrenje i održavanje vrsta sertifikata koje se koriste;
- Priprema javnih propisa usluga i internih (ne javno dostupnih) odredbi, njihovo usklađivanje sa pravnim propisima i internim (ne javno dostupnim) propisima, kao i sprovođenje svih ažuriranja;
- Zapisivanje primedbi koje se odnose na propise koji se primenjuju na usluge, i ocenjivanje preporuka.

Autoritet za izdavanje sertifikata sertifikata elektronske identifikacije odgovoran je:

- Za autentičnost i tačnost izdatih sertifikata;
- Za propise koje je izdao i za njihovu usklađenost i saglasnost sa zakonskim propisima;
- Za usklađenost ključnih parova koje je generisao, i za odnos između privatnog i javnog ključa i sertifikata;
- Za odnos aktivacionog koda uređaja za kreiranje elektronske identifikacije i ključeva postavljenih na uređaj;
- Generalno, za poštovanje svojih obaveza.

9.6.2 Izjave i garancije registracionog autoriteta

Korisnička podrška ima zadatak da predstavlja Pružaoca usluga od poverenja krajnjim korisnicima u vezi sa uslugama. Obavlja sledeće zadatke u okviru toga:

- Učestvuje u prodaji usluga;
- Vrši registraciju subjekata;
- Prima zahteve koji se odnose na različite operacije sa sertifikatima (suspendovanje, opoziv, ponovno uvođenje, zamena sertifikata);

- Prima i obrađuje podneske za izmenu podataka;
- Učestvuje u objavljivanju statusa opoziva;
- Nudi aktivnost pružanja informacija klijentima i Pouzdanim stranama u vezi sa svojim aktivnostima vezanim za usluge koje pruža Pružalac usluga od poverenja.

Registrovani autoritet je odgovoran:

- Za utvrđivanje ličnog identiteta osobe koja je ovlašćena da predstavlja aplikanta;
- Za autentičnost zabeleženih podataka o registraciji;
- Za pružanje informacija onima koji koriste usluge o sadržaju i dostupnosti Polise o sertifikatima i Izjave o praksi izdavanja sertifikacije, kao i uslova korišćenja usluge pre zaključivanja ugovora o uslugama;
- Uopšteno, da u potpunosti ispuni svoje obaveze.

9.6.3 Izjave i garancije pretplatnika

Odgovornost Pretplatnika

Odgovornost pretplatnika određena je ugovorom o pružanju usluga i njegovim prilozima (uključujući uslove i odredbe).

Obaveze pretplatnika

Odgovornost Pretplatnika je da postupa u skladu s ugovornim uslovima i propisima Pružaoca usluga od poverenja prilikom korišćenja usluge, uključujući zahtevanje i primenu sertifikata i privatnih ključeva.

Obaveze Pretplatnika određuju se ovom Izjavom o praksi sertifikacije, ugovorom o pružanju usluga, Opštim uslovima poslovanja, kao i odgovarajućom Polisom sertifikata.

Kada pretplatnik bude obavešten o bilo kakvoj stvarnoj ili sumnjičavoj zloupotrebi ili kompromitu ključa privatnosti koji je povezan sa javnim ključem uključenim u sertifikat koji pripada pretplatniku, pretplatnik je dužan da:

- Odmah prijavi ovu činjenicu Pružaocu usluga od poverenja,
- Odmah zatraži opoziv ili suspendovanje Sertifikata,
- Odmah prestane da koristi Sertifikat i povezani ključ privatnosti.

Prava Pretplatnika

- Pretplatnici imaju pravo da koriste usluge u skladu sa ovom Izjavom o praksi sertifikacije.
- Pretplatnici imaju pravo da odrede koje subjekte treba da bude dozvoljeno da primaju sertifikate, pismeno, i pretplatnici imaju pravo da zatraže suspendovanje i opoziv takvih sertifikata.
- Pretplatnici imaju pravo da zatraže suspendovanje i opoziv sertifikata.
- Pretplatnici imaju pravo da imenuju organizacione administratore.

Odgovornost aplikanta je:

- Autentičnost, tačnost i validnost pruženih podataka tokom registracije;
- Provera podataka navedenih u sertifikatu;

- Da odmah obavesti o promenama svojih podataka;
- Korišćenje svog elektronskog uređaja za kreiranje elektronske identifikacije, privatnog ključa i sertifikata u skladu sa propisima;
- Sigurno upravlja svojim privatnim ključem i aktivacionim kodom;
- Odmah obavesti Pružaoca usluga od poverenja u slučaju spora;
- Uopšteno poštuje svoje obaveze.

Obaveze aplikanta su:

- Pažljivo pročita Izjavu o praksi izdavanja sertifikacije pre korišćenja usluge;
- Potpuno obezbediti podatke koje zahteva Pružalac usluga od poverenja potrebne za korišćenje usluge, i obezbediti tačne podatke;
- Ukoliko aplikant postane svestan činjenice da su se neophodni podaci koje je obezbedio za korišćenje usluge - posebno podaci navedeni u sertifikatu - promenili, dužan je odmah:
    - Obavestiti Pružaoca usluga od poverenja pismeno,
    - Zatražiti suspenziju ili opoziv sertifikata i
    - Prekinuti upotrebu sertifikata.
- Odmah prekinuti korišćenje privatnog ključa koji pripada sertifikatu, ako aplikant postane svestan da je sertifikat subjekta opozvan, ili da je izdavačka CA ugrožena;
- Koristiti uslugu isključivo u svrhe koje su dozvoljene ili nisu zabranjene zakonskim propisima, u skladu sa citiranim propisima i dokumentima;
- Osigurati da neovlašćena lica nemaju pristup podacima i alatima (lozinkama, tajnim kodovima, uređajima za kreiranje identifikacije) neophodnim za korišćenje usluge;
- Obavestiti Pružaoca usluga od poverenja pismeno i bez odlaganja u slučaju pokretanja pravnog spora u vezi sa bilo kojim od elektronskih identiteta ili sertifikatima povezanim sa uslugom;
- Sarađivati sa Pružaocem usluga od poverenja kako bi potvrdili podatke neophodne za izdavanje sertifikata i učiniti sve što je u njihovoj moći da omoguće što brži završetak takve verifikacije;
- Odgovoriti na zahteve Pružaoca usluga od poverenja u roku određenom od strane Pružaoca usluga od poverenja u slučaju kompromitovanja ključa ili sumnje na nezakonitu upotrebu;
- Priznati da Pretplatnici imaju pravo da zatraže opoziv i/ili suspenziju sertifikata;
- Priznati da Pružalac usluga od poverenja izdaje sertifikate na način naveden u Izjavi o praksi sertifikacije, nakon završetka opisanih koraka verifikacije;
- Priznati da Pružalac usluga od poverenja prikazuje samo podatke koji odgovaraju stvarnosti u izdatim sertifikatima. Prema tome, Pružalac usluga od poverenja potvrđuje podatke koji se unose u sertifikate prema Izjavi o praksi sertifikacije;
- Priznati i prihvatiti da Pružalac usluga od poverenja ima pravo da suspenduje i/ili opozove izdati sertifikat odmah ako
    - Postane svestan da podaci navedeni u sertifikatu ne odgovaraju stvarnosti ili privatni ključ nije u isključivom posedovanju ili korišćenju aplikanta i u ovom slučaju, aplikant je dužan da prekine upotrebu sertifikata;
    - Pretplatnik prekrši uslove ugovora o pružanju usluga ili Opšte uslove i odredbe;
    - Je opoziv neophodan prema Polisi sertifikacije ili Izjavi o praksi sertifikacije Pružaoca usluga od poverenja;
    - Pružalac usluga od poverenja postane svestan da je sertifikat korišćen za nezakonitu aktivnost
    - Pretplatnik ne izmiri naknade za usluge do roka.

Prava aplikanta:

- Aplikanti imaju pravo da podnesu zahtev za sertifikate u skladu sa Izjavom o praksi izdavanja sertifikata.
- Ukoliko je to dozvoljeno odgovarajućom Polisom o sertifikatima, aplikanti imaju pravo da zatraže suspenziju i opoziv svojih sertifikata, u skladu sa ovom Izjavom o praksi sertifikacije.

9.6.4 Izjave i garancije pouzdanih strana

Pouzdane strane odlučuju na osnovu svoje diskrecije i/ili svojih polisa o načinu prihvatanja i korišćenja sertifikata. Prilikom provere validnosti radi održavanja nivoa sigurnosti garantovanog od strane Pružaoca usluga od poverenja, neophodno je da Pouzdane strane deluju sa oprezom, pa se posebno preporučuje da:

- Poštuju zahteve, propise definisane u trenutnoj Polisi sertifikata i odgovarajućoj Izjavi o praksi izdavanja sertifikata;
- Koriste pouzdano IT okruženje i aplikacije;
- Provere status opoziva sertifikata na osnovu trenutnog CRL-a ili OCSP odgovora;
- Uzmu u obzir svako ograničenje u vezi sa korišćenjem sertifikata koje je uključeno u sertifikat, u Izjavi o praksi izdavanja sertifikata i u odgovarajućoj Polisi sertifikata.

9.6.5 Izjave i garancije ostalih učesnika

Nema odredbi.

9.7 Odricanje od odgovornosti

Pružalac usluga od poverenja isključuje svoju odgovornost ukoliko:

- Aplikanti ne prate zahteve koji se odnose na upravljanje privatnim ključem;
- Nije u mogućnosti da pruži informacije ili ispuni obaveze komunikacije zbog problema na internetu, ili njegovom delu;
- Šteta proističe iz ranjivosti ili greške kriptografskih algoritama prihvaćenih od strane Nacionalne medijske i infokomunikacione vlasti.

9.8 Ograničenja odgovornosti

- Pružalac usluga od poverenja nije odgovoran za štetu koja nastaje iz propusta Pouzdanih strana da postupi kako je preporučeno prema važećim zakonskim propisima i regulativama Pružaoca usluga od poverenja u procesu validacije i korišćenja sertifikata, kao i iz propusta da postupi kako se očekuje u određenoj situaciji.
- Pružalac usluga od poverenja je odgovoran samo za ugovorne i van ugovorne štete povezane sa svojim uslugama u odnosu na treće strane, u vezi sa dokazivim štetama koje se javljaju isključivo zbog očiglednog kršenja svojih obaveza.
- Pružalac usluga od poverenja nije odgovoran za štetu koja proizlazi iz njegove nemogućnosti da ispuni svoje obaveze u vezi sa pružanjem informacija i drugih komunikacijskih obaveza zbog operativnog kvara Interneta ili njegovog komponenti usled nekog spoljašnjeg incidenta van njegove kontrole.

- Ako Pružalac usluga od poverenja vrši upoređivanje podataka sa autentičnom bazom podataka pre izdavanja sertifikata za subjekta, oslanja se na podatke dobijene iz autentične baze podataka. Pružalac usluga od poverenja neće preuzeti odgovornost za štetu koja proizilazi iz netačnosti informacija koje pružaju takve autentične baze podataka.
- Pružalac usluga od poverenja preuzima odgovornost samo za pružanje usluga u skladu sa odredbama ovog dokumenta o praksi izdavanja sertifikata, kao i dokumenata na koje se ovde referiše (Polise sertifikata, standardi, preporuke), kao i sa svojim internim propisima.

Administrativni procesi

Pružalac usluga od poverenja beleži svoje aktivnosti, štiti integritet i autentičnost unosa u dnevniku, i čuva (arhivira) podatke dnevnika dugoročno u interesu omogućavanja utvrđivanja, dokumentovanja i dokazivanja finansijske odgovornosti, njegove svojinske odgovornosti za štetu koju prouzrokuje, kao i odštete štete koju trpi.

Finansijska odgovornost

Pružalac usluga od poverenja ima odgovarajući depozit prema relevantnim zakonskim zahtevima za svoju finansijsku odgovornost i za garantovanje troškova povezanih sa njegovim prestankom i pouzdanosti.
Pružalac usluga od poverenja ima osiguranje odgovornosti prema zakonskim propisima koja su neophodna kako bi se obezbedila pouzdanost.

Ograničenje finansijske odgovornosti
Pružalac usluga od poverenja ne ograničava najviši nivo obaveze koju preuzima istovremeno.
U vezi sa uslugama pruženim kao kvalifikovani provajder, Pružalac usluga od poverenja definiše tarifne planove, koji se razlikuju po finansijskoj odgovornosti Pružaoca usluga od poverenja kako je navedeno u nastavku.

Tip Sertifikata	Ograničenje odgovornosti Pružaoca usluga
Osnovni	
Bronze	
Silver	
Gold	
Platinum	

Ako važeći zahtev više ovlašćenih strana u vezi sa događajem osiguranja premaši iznos definisan za događaj osiguranja u osiguranju od odgovornosti za štetu, tada se isplata zahteva vrši u relativnom odnosu prema iznosu određenom u ugovoru o odgovornosti.

9.9 Obeštećenja

9.9.1 Obeštećenja od strane Pružaoca usluga od poverenja

Detaljna pravila nadoknada Pružaoca usluga od poverenja navedena su u ovoj regulativi (videti Poglavlje: 9.8.), ugovoru o pružanju usluga i u ugovorima zaključenim sa klijentima.

9.9.2 Obeštećenja od strane pretplatnika

Pretplatnik i subjekat su odgovorni za štetu koju nanose Pružaocu usluga od poverenja usled nepoštovanja svojih obaveza i relevantnih preporuka.

9.9.3 Obeštećenja od strane pouzdanih strana

Pogledati Poglavlje 9.8.

9.10 Rok i Raskid

9.10.1 Rok

Datum stupanja na snagu određene Izjave o praksi izdavanja sertifikata naveden je na naslovnoj strani dokumenta.

9.10.2 Raskid

Praktična pravila pružaoca važi bez vremenskog ograničenja sve do povlačenja ili izdavanja novije verzije Izjave o praksi izdavanja sertifikata.

Poglavlje 9. Izjave o praksi izdavanja sertifikata ostaje na snazi čak i nakon prestanka važenja Izjave o praksi izdavanja sertifikata (bez obzira na način na koji prestaje važenje) u vezi sa svim sertifikatima koje Pružalac usluga od poverenja bude izdao dok je Praktična pravila pružaoca bila na snazi.

9.10.3 Efekat raskida i opstanak

U slučaju povlačenja Izjave o praksi izdavanja sertifikata, Pružalac usluga od poverenja objavljuje detaljna pravila o povlačenju, kao i prava i obaveze koje nastavljaju da važe nakon povlačenja na svojoj veb stranici.

Pružalac usluga od poverenja garantuje da u slučaju povlačenja Izjave o praksi izdavanja sertifikata, zahtevi za zaštitu poverljivih podataka ostaju na snazi.

9.11 Individualna obaveštenja i komunikacija sa učesnicima

ružalac usluga od poverenja održava korisničku podršku kako bi bio u kontaktu sa svojim klijentima. Klijenti mogu davati svoje pravne izjave Pružaocu usluga od poverenja isključivo

pismeno, i u izvršenom obliku. Izvršenje u ime pravnog lica važi samo uz sertifikaciju takvog prava zastupanja.

9.12 Izmene

Pružalac usluga od poverenja zadržava pravo da promeni Izjavu o praksi izdavanja sertifikata na kontrolisan način u slučaju promene normativnih propisa, sigurnosnih zahteva, tržišnih uslova ili drugih okolnosti.

9.12.1 Postupak za izmenu

Pružalac usluga od poverenja samo otkriva one svoje postupke u svojim javno dostupnim propisima čije poznavanje ne ugrožava sigurnost usluga. Pružalac usluga od poverenja ima niz internih sigurnosnih i drugih propisa, kao i operativne odredbe koje tretira kao poverljive (ova Praktična pravila pružaoca pominje nekoliko takvih). Postupci opisani u odeljku 8.4. kontrolišu ove dokumente takođe.

Tim odgovoran za održavanje propisa i dokumentacije funkcioniše unutar pravnog lica Pružaoca usluga od poverenja. Ovaj tim prikuplja zahteve za promene, sprovodi modifikacije i ispunjava sve unutrašnje i spoljašnje obaveze vezane za dostupnost informacija.

Tim proizvodi interne, neobjavljene radne kopije propisa dok prikuplja promene, i ove kopije prolaze internu proveru pre nego što budu objavljene. Pružalac usluga od poverenja se trudi da izdaje nove propise samo u najmanje mogućim intervalima.

Pružalac usluga od poverenja godišnje pregleda Izjavu o praksi izdavanja sertifikata ili u slučaju izuzetnog zahteva za promenom s prioritetom i vrši potrebne izmene. Dokument će dobiti novi broj verzije čak i nakon najmanje promene - ili u slučaju godišnjeg pregleda čak i ako ne dođe do promena u dokumentu - i uzimajući u obzir vreme potrebno za proces odobravanja, planirani datum stupanja na snagu će takođe biti određen.

Pružalac usluga od poverenja će prihvatiti primedbe u vezi sa novim propisima objavljenim 14 dana pre njihovog stupanja na snagu, na sledeću e-poštu: office@paperless.rs

U slučaju primedbi koje zahtevaju suštinske promene, dokument će biti izmenjen.

Pružalac usluga od poverenja će zatvoriti i objaviti verziju propisa kako je izmenjena sa primedbama 7 dana pre njenog stupanja na snagu.

9.12.2 Mehanizam i period obaveštavanja

Pružalac usluga od poverenja obaveštava Pouzdane strane o izdanjima nove verzije dokumenata kako je opisano u odeljku 9.12.1.

9.12.3 Okolnosti pod kojima se OID mora promeniti

Pružalac usluga od poverenja izdaje novu verziju sa novim brojem verzije čak i u slučaju najmanje promene Izjave o praksi izdavanja sertifikata, pri čemu se ili glavni broj verzije ili pod verzija menja u zavisnosti od obima promene.

U verzijama 1.x i 2.x, broj verzije Izjave o praksi izdavanja sertifikata pojavljivao se u oznakama "2" na kraju OID-a identifikatora dokumenta, tako da dve Izjave o praksi izdavanja

sertifikata sa različitim sadržajem - koje su stupile na snagu - nisu mogle imati isti OID identifikator.

Počevši od verzije 3.1 Izjave o praksi izdavanja sertifikata, broj verzije ne pojavljuje se na kraju OID-a, pa OID identifikator Izjave o praksi izdavanja sertifikata ima istu vrednost u svim objavljenim verzijama. Pojedinačna Praktična pravila pružaoca može se identifikovati korišćenjem OID-a dokumenta i broja verzije zajedno.

9.13 Odredbe za rešavanje sporova

Sve pritužbe korisnika kvalifikovanog elektronskog sertifikata rešavaju poverenici za unutrašnju kontrolu i zakonsku regulativu. Moguće sporove između korisnika kvalifikovanog elektronskog sertifikata ili trećeg lica i Paperless d.o.o rešava nadležni sud.

9.14 Važeće zakonodavstvo

Ovaj dokument je izrađen u potpunosti u skladu sa odgovarajućom zakonskom regulativom Republike Srbije, i to pre svega sa Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i drugim uslugama od poverenja u elektronskom poslovanju i odgovarajućim podzakonskim aktima.

9.15 Usklađenost sa primenjivim zakonima

Nadzor nad usklađenošću operativnog rada pružaoca usluga od poverenja sa važećim zakonodavstvom i propisima sprovodi nadležna služba ili akreditovani organ.

Akreditovani organ za ocenjivanje usaglašenosti za Paperless d.o.o sprovode reviziju usaglašenosti najmanje na svaka 24 meseca. Svrha revizije je da potvrdi da li je pružalac usluge od poverenja ispunjava zakonske uslove.

Interne provere usaglašenosti rada sprovode ovlašćena lica u okviru Paperless d.o.o

9.16 Različite odredbe

9.16.1 Ceo sporazum

Nema odredbe.

9.16.2 Dodeljivanje

Pružaoci koji posluju prema ovom Izveštaju o praksi izdavanja sertifikata mogu svoja prava i obaveze preneti trećoj strani samo uz prethodni pismeni pristanak Pružaoca usluga od poverenja.

9.16.3 Razdvojivost

Ukoliko neke od odredbi ove Izveštaju o praksi izdavanja sertifikata postanu nevažeće iz bilo kog razloga, preostale odredbe će ostati na snazi nepromenjene.

9.16.4 Izvršenje (advokatski troškovi i odricanje od prava)

Pružalac usluga od poverenja ima pravo da zahteva nadoknadu štete i troškove advokata za nadoknadu štete, gubitke, troškove prouzrokovane od strane svojih partnera. Ako u određenom slučaju Pružalac usluga od poverenja ne koristi svoje pravo na nadoknadu štete, to ne znači da u sličnim slučajevima u budućnosti ili u slučaju kršenja drugih odredbi ovog Izveštaja o praksi izdavanja sertifikata, odustaje od potraživanja za nadoknadu štete.

9.16.5 Viša sila

Pružalac usluga od poverenja nije odgovoran za neispravno ili kašnjenje u izvršenju zahteva navedenih u Polisi o sertifikatu i Izjavi o praksi izdavanja sertifikata ako je razlog za neuspeh ili kašnjenje bio uslov koji je van kontrole Pružaoca usluga od poverenja.

9.17 Ostale odredbe

Nema odredbi.