Pravilnik o postupcima izdavanja sertifikata
(CPS – Certification Practice Statement)

Oznaka dokumenta: PRA_CPS_V1.0
Verzija: 1.1

Autor dokumenta:
Marjan Erceg, Vuk Vujović, Artan Biljali

Vlasnik dokumenta:
Coreit CA PMA

Istorijat izmjena

Verzija	Datum	Broj promjena	Opis promjena
1.0	25.09.2019		
1.1.	11.10.2019	3	1. U odjeljku 1.5.2. dodate su kontakt informacije za korisnike 2. U odjeljku 7.1.2. je dodato mapiranje vrsta sertifikata u skladu sa ETSI EN standardima 3. Dodat je odjeljak 9.17.1. Usklađenost sa međunarodnim standardima

Preispitivanje dokumenta

Datum sljedećeg zakazanog preispitivanja
01.11.2020

Distribucija

Naziv	Naslov
Svi	

Odobrio

Ime	Pozicija	Potpis	Datum
Andrej Minevski	CEO		14.10.2019

SADRŽAJ

1. UVOD

1.1. KRATAK PREGLED

Coreit CA upravlja insfrastrukturom javnih ključeva sa jednim sertifikacionim tijelom (CA) koje izdaje sertifikate za fizička i pravna lica. Coreit posluje kao kvalifikovani davalac usluga sertifikovanja u skladu sa pravnim regulativama Crne Gore.
Ovaj dokument predstavlja Pravilnik o postupcima izdavanja sertifikata (CPS) za Coreit CA. Sadrži opis pravila, procedura i uslova izdavanja, suspendovanja i opoziva sertifikata i opisuje tehničke, proceduralne i kadrovske politike i prakse koje Coreit CA koristi u izdavanju i upravljanju sertifikatima. Numerisanje poglavlja i sekcija je isto kao u RFC 3647.
Dokument definise sledeće kategorije sertifikata koje izdaje Coreit CA:

1. Kvalifikovani setifikat za kvalifikovani elektronski potpis
2. Kvalifikovani sertifikat za kvalifikovani elektronski pečat
3. Kvalifikovani sertifikat za kvalifikovani elektronski potpis za fizičko lice u sklopu pravnog lica
4. Kvalifikovani sertifikat za napredni elektronski pečat i autentifikaciju pravnog lica
5. Sertifikat za Timestamp servis
6. Sertifikat za autentifikaciju fizičkog lica
7. Sertifikat za autentifikaciju fizičkog lica u sklopu pravnog lica

Svaka kategorija sertifikata ima dodijeljenu jedinstvenu politiku koja reguliše kome se može izdati sertifikat za tu kategoriju, koje informacije moraju biti obezbijeđene i druge faktore koji utiču na pouzdanost sertifikata. Ove politike, definisane u ovom dokumentu, biće identifikovane u sertifikatima izdatim u okviru ovog CPS-a time što će sadržati identifikatore objekta (OIDs) u CP ekstenziji sertifikata.

1.2. NAZIV DOKUMENTA I IDENTIFIKACIONI PODACI

Ovaj dokument je Coreit CA Pravilnik o postupcima izdavanja sertifikata od strane sertifikacionog tijela. Takođe, dokument se može kratko nazvati Coreit CA CPS.
Sledeći identifikatori objekata (OIDs) su dodijeljeni kategorijama sertifikata izdatim pod ovim Coreit CA CPS:

Kategorija sertifikata	Identifikacija politike sertifikata (OID)	Kriptografski token	Period važenja
Kvalifikovani sertifikat za kvalifikovani elektronski potpis	1.3.6.1.4.1.53673.1.1.1.1.1.	DA	Jedna (1) do pet (5) godina
Kvalifikovani sertifikat za kvalifikovani elektronski pečat	1.3.6.1.4.1.53673.1.1.2.1.1.	DA	Jedna (1) do pet (5) godina
Kvalifikovani sertifikat za kvalifikovani elektronski potpis za fizičko lice u okviru pravnog lica	1.3.6.1.4.1.53673.1.1.1.2.1.	DA	Jedna (1) do pet (5) godina
Kvalifikovani sertifikat za napredni elektronski pečat i autentifikaciju pravnog lica	1.3.6.1.4.1.53673.1.1.2.2.1.	NE	Jedna (1) do pet (5) godina
Sertifikat za Timestamp servis	1.3.6.1.4.1.53673.1.1.3.1.1.	DA	Pet (5) do deset (10) godina
Sertifikat za autentifikaciju fizičkog lica	1.3.6.1.4.1.53673.1.1.1.3.1.	DA	Jedna (1) do pet (5) godina
Sertifikat za autentifikaciju fizičkog lica u sklopu pravnog lica	1.3.6.1.4.1.53673.1.1.1.4.1.	DA	Jedna (1) do pet (5) godina

Takođe, CA može izdati različite sertifikate koji moraju biti jasno označeni posebnom politikom ili dodatnim identifikatorom objekta u X.509 ekstenizijama. Identifikator objekata treba da ima prefiks 1.3.6.1.4.1.53673. i mora biti jedinstven za ovaj prefiks.

1.3. UČESNICI INFRASTRUKTURE JAVNIH KLJUČEVA

1.3.1. SERTIFIKACIONO TIJELO (CERTIFICATION AUTHORITY)

Coreit CA funkcioniše kao javni TSP i izdaje sertifikate pravnim i fizičkim licima.

Coreit CA koristi primarni CA (root CA) koji je izdao self-signed sertifikat prilikom ceremonije generisanja glavnog ključa i jedan podređeni CA (subCA) za izdavanje sertifikata svim krajnjim entitetima.
Coreit ima osoblje koje je odgovorno za:

- sveobuhvatno funkcionisanje CA
- osoblje koje radi i upravlja sa CA infrastrukturom, CA privatnim kriptografskim ključevima, serverima i softverom (Operations Authority - OA); i
- osoblje zaduženo za identifikaciju i registraciju korisnika (Registration Authority - RA) i koordinaciju sa eksternim RA

1.3.1.1. COREIT CA TIJELO ZA UPRAVLJANJE POLITIKAMA I PRAVILNICIMA (PMA)

Coreit CA PMA (Policu Menagement Authority) je odgovoran za:

- izradu i održavanje Coreit CA CPS-a
- izradu i održavanje Coreit CA javnih dokumenata (Ugovor sa krajnjim korisnicima, ...)
- podnošenje Coreit CA CPS odgovornom tijelu na usvajanje
- Coreit CA registraciju i akreditaciju
- imenovanje OA i RA osoblja
- nadzor i reviziju obavljanja djelatnosti Coreit CA i aktivnosti koje osiguravaju da CA funkcioniše u skladu sa CPS
- nadzor i odobravanje sertifikacionih politika (CP) i CPS-a
- rješavanje sporova između Coreit CA učesnika

1.3.1.2. COREIT CA TIJELO ZA OPERACIJE (OA)

Coreit CA OA (Operations Authority) je odgovorno za:

- generisanje CA para ključeva, sigurno upravljanje CA privatnim ključevima i distribuciju javnih CA ključeva;
- uspostavljanje okruženja i procedura za prihvatanje i obradu zahtijeva za izdavanje sertifikata
- potpisivanje i izdavanje X.509 sertifikata koji povezuju korisnike sa njihovim javnim ključevima kao odgovor na odobrene zahtjeve za izdavanje sertifikata
- pokretanje opoziva sertifikata na zahtjev korisnika ili na sopstvenu inicijativu
- opoziv sertifikata uključujući izdavanje i objavljivanje liste opozvanih sertifikata (CRL) i upravljanje OCSP servisom (Online Certificate Status Protocol)
- funkcionisanje CA u skladu sa nacionalnim zakonima i sa CPS
- opoziv sertifikata OA i RA osoblja

OA članovi su odgovorni za:

- odobravanje i odbijanje zahtjeva za izdavanje sertifikata
- primanje i distribuciju korisničkih aktivacionih kodova dobijenih od strane Coreit CA i pomoć pri aktivaciji korisnika u vremenskom periodu predviđenom za to
- nadgledanje statusa informacija o pretplatniku

Kada je neophodno, ovaj dokument ističe različite korisnike i uloge koji pristupaju CA funkcijama. Kada isticanje ovih razlika nije potrebno, pojam CA se koristi za označavanje CA kao cjelokupnog entiteta uključujući softver i sve njegove funkcionalnosti.

1.3.2. REGISTRACIONA TIJELA (REGISTRATION AUTHORITIES)

Registraciona tijela su odgovorna za provjeru identiteta na osnovu identifikacije "licem u lice" ili prikupljanjem korisničkih informacija kako bi se podržao zahtjev za izdavanje sertifikata i obnova ključa.
Za RA funkcionalnosti za interne sertifikate su zaduženi Coreit CA zaposleni.
RA službenici su odgovorni za:

- Identifikaciju i autentifikaciju pojedinaca ili entiteta koji zahtijevaju sertifikat
- identifikaciju i autentifikaciju pojedinaca ili entiteta koji predaju zahtjev za obnovu sertifikata ili traže novi sertifikat prateći proceduru za obnovu ključa
- prihvatanje ili odbijanje zahtjeva za izdavanje sertifikata
- provjeru i potvrdu identiteta naručioca
- provjeru podataka u zahtjevu za izdavanje sertifikata naručioca, podnošenje zahtjeva za sertifikat i za opoziv sertifikata CA-u

1.3.3. NARUČIOCI I KORISNICI (END USERS AND SUBSCRIBERS)

Coreit CA pretplatnici su pravna i fizička lica (pojedinci). Organizacije, državne institucije i agencije biće tretirane kao pravna lica u ovom dokumentu.
Naručilac je stranka koja zahtijeva Coreit CA sertifikat u ime jednog ili više subjekata. Na primjer, eksterna organizacija koja zahtijeva sertifikat za svoje zaposlene. Vlasnik sertifikata (subject) je entitet identifikovan u sertifikatu kao vlasnik privatnog ključa povezanog sa javnim ključem koji je dat u sertifikatu.
Naručilac snosi krajnju odgovornost za korišćenje privatnog ključa povezanog sa javnim ključem sertifikata, ali vlasnik sertifikata (subject) je identifikovan privatnim ključem. U slučaju da je sertifikat izdat fizičkom licu za sopstvenu upotrebu, onda je naručilac i vlasnik sertifikata (subject) isti entitet.
Pojmovi naručilac i vlasnik sertifikata (subject) sa ovom eksplicitnom razlikom, biće korišćeni u ovom dokumentu gdje god je to smisleno.

1.3.4. TREĆA LICA (RELYING PARTIES)

Treća lica su entiteti uključujući fizička lica (pojedince) i/ili pravna lica (kompanije) koja se oslanjaju na sertifikat i/ili elektronski potpis koji se može provjeriti na osnovu javnog kluča koji se nalazi u sertifikatu vlasnika.
Da bi provjerili validnost sertifikata koji dobiju, treća lica moraju uvijek da provjere Coreit CA CRL ili OCSP prije nego se oslone na informacije u sertifikatu.

1.3.5. OSTALI UČESNICI

Nije primjenjivo.

1.4. UPOTREBA SERTIFIKATA

1.4.1. DOZVOLJENA UPOTREBA SERTIFIKATA

Sertifikati izdati od strane Coreit CA imaju širok spektar primjene u zavisnoti od politike sertifikata. Sertifikate izdate od strane Coreit CA je dozvoljeno koristiti za verifikaciju elektronskog potpisa i/ili pečata, provjeru identiteta mail korisnika, autentifikaciju vlasnika sertifikata, verifikaciju vremenskog pečata (Timestamp).

1.4.2. NEDOZVOLJENA UPOTREBA SERTIFIKATA

Svi sertifikati izdati od strane Coreit CA su namjenjeni korišćenju u skladu sa zakonom.

1.5. UPRAVLJANJE POLITIKAMA I PRAVILNICIMA

1.5.1. TIJELO KOJE UPRAVLJA PRAVILNIKOM

Coreit doo Podgorica upravlja sa Coreit CA.

1.5.2. KONTAKT PODACI

Coreit CA kontakt informacije:
Adresa: Coreit doo Podgorica
Bulevar Džordža Vašingtona 98, The Capital Plaza, Diplomatska kula,
81000 Podgorica, Crna Gora
Email: info@ca.coreit.me
Internet: http://ca.coreit.me

Coreit CA RA kontakt informacije:
Adresa: Coreit doo Podgorica

Bulevar Džordža Vašingtona 98, The Capital Plaza, Diplomatska kula,
81000 Podgorica, Crna Gora
Email: info@ra.coreit.me
Internet: http://ca.coreit.me

Coreit CA kontakt informacije za korisnike:
Adresa: Coreit doo Podgorica
Bulevar Džordža Vašingtona 98, The Capital Plaza, Diplomatska kula,
81000 Podgorica, Crna Gora
Email: info@ca.coreit.me
Internet: http://ca.coreit.me

1.5.3. LICE KOJE UTVRĐUJE USAGLAŠENOST PRAVILNIKA SA POLITIKOM

Nije primjenjivo.

1.5.4. PROCEDURA ZA USVAJANJE PRAVILNIKA

Coreit CA CPS su usvojene od strane Coreit CA PMA.

1.6. DEFINICIJE I SKRAĆENICE

Definicije:

Sertifikat: javni ključ korisnika zajedno sa nekim drugim informacijama, koje se potpisuju sa privatnim ključem sertifikacionog tijela koje ga je izdalo
Cross-sertifikat: sertifikat koji se koristi za uspostavljanje povjerljive veze između dva CA
Politika sertifikata (CP): imenovani skup pravila koji ukazuje na primjenjivost sertifikata na određenu zajednicu i / ili klasu aplikacija sa zajedničkim sigurnosnim zahtjevima
Pravilnik o postupcima izdavanja sertifikata (CPS): Pravilnik o praksama koje sertifikaciono tijelo koristi za izdavanje sertifikata. CPS opisuje opremu, politike i procedure koje su implementirane od strane CA kako bi zadovoljio specifikacije u politikama sertifikata podržane od strane CA.
Sertifikaciono tijelo (CA): tijelo koje kreira i dodjeljuje sertifikate i kome vjeruje jedan ili više korisnika.
Integritet podataka: osiguranje da su podaci ostali nepromijenjeni od samog stvaranja do prijema.
Digitalni potpis: podaci koji se dodaju standardnom skupu podataka i predstavljaju kriptografsku transformaciju istih, a koji omogućavaju primaocu da dokaže izvor i integritet podataka i zaštitu od falsifikovanja.
Elektronski potpis: podaci u elektronskoj formi koji su pridruženi ili logički povezani sa drugim elektronskim dokumentima i služe kao metod za autentifikaciju tih podataka.
Par ključeva za enkripciju: par asimetričnih ključeva sastavljenih od javnog ključa za šifrovanje i odgovarajućegeg privatnog ključa za dešifrovanje. Takođe se naziva i par ključeva poverljivosti.

Aktivacija (inicijalizacija) podataka: aktivacioni kodovi (podaci) koje izdaje CA i koji se koriste jednom tokom procesa inicijalizacije naručioca, za autentifikaciju naručioca i generisanje njihovih sertifikata.
Deponovanje ključa: aranžman u kojem se ključevi potrebni za dešifrovanje šifrovanih podataka čuvaju deponovani od treće strane, tako da ih neko drugi može dobiti za dešifrovanje poruke.
Registraciono tijelo (RA): osoba, organizacija tijelo koje je odgovorno za identifikaciju i autentifikaciju naručioca prije izdavanja sertifikata.
Identifikator objekta (OID): jedinstveni alfanumerički/numerički identifikator registrovan od strane ISO standarda za registraciju i upućuje na određeni objekat ili klasu objekata.
Privatni ključ za dekripciju: pogledaj **par ključeva za enkripciju.**
Privatni ključ za potpis: pogledaj **par ključeva za potpis.**
Javni ključ za enkripciju: pogledaj **par ključeva za enkripciju.**
Tijelo za upravljanje PKI (PMA): tijelo koje je primarno odgovorno za postavljanje, sprovođenje i upravljanje politikama i praksama sertifikata za CA i nadgledanje rada CA.
Infrastruktura javnog ključa (PKI): struktura hardvera, softvera, ljudi, procesa i politika koja koristi tehnologiju digitalnog potpisa kako bi se olakšala povezanost javne komponente asimetričnog javnog ključa sa određenim entitetom.
Verifikacioni ključ za javni potpis: pogledaj **par ključeva za potpis**
Treće lice (Relying party): primaoc sertifikata koji postupa oslanjajući se na taj sertifikat i / ili digitalne potpise provjerene upotrebom tog sertifikata.
Repozitorijum: lokacija gdje su sačuvani CRLs, ARLs i sertifikati kojima pristupaju krajnji entiteti.
Par ključeva za potpis: par asimetričnih ključeva sastavljenih od privatnog ključa za potpisivanje i odgovarajućeg javnog ključa za verifikaciju potpisa
Korisnički sigurnosni uređaj (Kriptografski token): uređaj na kome se nalazi privatni ključ korisnika, koji štiti ključ od kompromitovanja i obavlja funkcije potpisivanja ili dekripcije u ime korisnika.
Subjekat, vlasnik sertifikata: entitet identifikovan u sertifikatu kao vlasnik privatnog ključa koji je povezan sa javnim ključem koji se nalazi u sertifikatu
Naručilac: entitet koji se prijavljuje kod sertifikacionog tijela u ime jednog ili više subjekata.
NAPOMENA: subjekat može biti naručilac koji djeluje u svoje ime.
Ovlašćeni predstavnik: entitet koji nije naručilac CA servisa (npr. naručilac i subjekat su odvojeni entiteti), pod uslovom da je naručilac ovlašćen da djeluje u ime određenog subjekta (npr. ovlašćen je za sve članove identifikovane organizacije).
Lista opozvanih sertifikata (CRL): potpisana lista koja pokazuje skup sertifikata javnih ključeva koje izdavalac sertifikata više ne smatra validnim.
Protokol za online status sertifikata (OCSP): Internet protokol koji se koristi za dobijanje statusa X.509 digitalnog sertifikata
Lista opozvanih sertfikata serifikacionih tijela (ARL): potpisana lista koja predstavlja skup sertifikacionih tijela sertifikata javnog ključa koji se ne smatraju više validnim
Aplikacija sertifikacionog tijela: kriptografski softver koji se koristi za upravljanje ključevima i sertifikatima entiteta, CRL i ARL listama.

Skraćenice:

CA Certification Authority
OA Operations Authority
RARegistration Authority
CSP Certification Service Provider
PDS PKI Disclosure Statement
PKI Public Key Infrastructure
CRL Certificate Revocation List
ARL Authority Revocation List
OCSP Online Certificate Status Provider
OID Object Identifier
PKIX internet X.509 Public Key Infrastructure
SHA-1 Secure Hash Algorithm 1
URI Uniform Resource Identifier
URL Uniform Resource Locator
RDN Relative Distinguished Name
CN Common Name
DN Distinguished Name
PMA Policy Management Authority

2. OBJAVE I ODGOVORNOSTI REPOZITORIJUMA

2.1. REPOZITORIJUMI

Coreit CA objavljuje informacije vezane za upravljanje sertifikata u repozitorijumima na sledećim adresama:
Javna web stranica: http://www.ca.coreit.me

2.2. OBJAVA INFORMACIJA O SERTIFIKATIMA

Coreit CA objavljuje:

- OCSP i listu opozvanih sertifikata (CRL)
- CA sertifikate
- CPS
- Nacrt ugovora sa krajnjim korisnicima
- Izjava o davanju usluga sertifikovanja (PDS)
- Nacrt zahtjeva za izdavanje, opoziv i obnavljanje sertifikata
- Listu registracionih tijela (RA)
- Ostale javne informacije vezane za sertifikate

2.3. OBJAVE INFORMACIJA O SERTIFIKATIMA

CRL se objavljuje odmah nakon što je izdata, kao što je specificirano u Sekciji 4.9.7. Sve informacije se objavljuju odmah nakon što su se promijenile ili postale dostupne Coreit CA.

2.4. KONTROLA PRISTUPA DO REPOZITORIJUMA

Sve javne informacije su dostupne za čitanje bez ograničenja. Repozitorijumi su dodatno zaštićeni od neovlašćenih promjena.

3. IDENTIFIKACIJA I AUTENTIFIKACIJA

3.1. DODJELJIVANJE IMENA

3.1.1. VRSTE IMENA

Atributi CA sertifikata i sertifikata izdatog naručiocu su u formi X.501 jedinstvenog imena (Distinguished Name - DN). DN je upisan u formi X.501 UTF8String ili štampanog stringa i mora biti prisutan u svim izdatim sertifikatima.

3.1.2. POTREBA ZA SMISLENIM IMENIMA

Skup atributa u jedinstvenom imenu upisanim u polje Subject sertifikata, na jedinstven način identifikuje vlasnika sertifikata i ima smislenu vrijednost. Tip atributa serijski broj, kada je prikazan, koristi se za razlikovanje imena u kojima bi polje Subject inače bilo identično.

3.1.3. ANONIMNOST KORISNIKA I UPOTREBA PSEUDONIMA

Nije primjenjivo.

3.1.4. PRAVILA ZA PRIKAZIVANJE RAZNIH FORMI IMENA

Polje Subject je definisano kao X.501 tip imena (x.500 Distinguished Name) u skladu sa RFC 5280. x.500 jedinstveno ime za Coreit CA ima sledeći format:

Za fizicka lica:

Komponenta jedinstvenog imena	Vrijednost
Country (C =)	ISO3155-1 Oznaka države
Given name	Ime potpisinka
Surname	Prezime potpisnika
Common Name (CN=)	Ime + Prezime + tip sertifikata (Autentifikacija ili Potpis)
Serial Number (serialNumber=)	jedinstveni serijski broj

Za fizičko lice povezano sa organizacijom:

Komponente jedinstvenog imena	Vrijednost
Country (C =)	ISO3155-1 oznaka države
Organization (O =)	Registrovani puni ili skraćeni naziv pravnog lica koje je povezano sa korisnikom sertifikata (fizičkim licem)
organizationIdentifier	Registrovani poreski indetifikacioni broj (PIB) pravnog lica u formatu "VATDvoslovna ISO3155-1 oznaka države u kojoj je registrovano sjedište pravnog lica - PIB
Organizational Unit (OU=)	opcionalno
Given name	Ime potpisinka
Surname	Prezime potpisnika
Common Name (CN=)	Ime + Prezime + tip sertifikata (Autentifikacija ili Potpis)
Serial Number (serialNumber=)	jedinstveni serijski broj

Pravno lice:

Komponente jedinstvenog imena	Vrijednost
Country (C =)	ISO Oznaka države
Organization (O =)	Registrovani puni ili skraćeni naziv pravnog lica
organizationIdentifier	Registrovani poreski indetifikacioni broj (PIB) pravnog lica u formatu "VATDvoslovna ISO3155-1 oznaka države u kojoj je registrovano sjedište pravnog lica - PIB
Organizational Unit (OU=)	opcionalno
Common Name (CN=)	Registrovani puni ili skraćeni naziv pravnog lica + tip sertifikata (Pečat ili Pečat/Autentifikacija)
Serial Number (serialNumber=)	jedinstveni serijski broj / Opcionalno

3.1.5. JEDINSTVENOST IMENA

Coreit CA dodjeljuje u polju Subject sertifikata kombinaciju atributa jedinstvenog imena, kao što je definisano u sekciji 3.1.2 i 3.1.4 da osigura nedvosmislenost i jedinstvenost imena.

3.1.6. PREPOZNAVANJE, AUTENTIFIKACIJA I ULOGA ZAŠTITNIH ZNAKOVA

Coreit CA će preduzimati razumne napore za rješavanje sporova koji mogu nastati zbog dodjele imena npr. CA može kontaktirati podnosioca zahtjeva i dogovoriti se da se CN atribut u polju subject promijeni kako bi se DN lako i uočljivo razlikovao od postojećeg DN-a.
Coreit CA po svojoj procjeni može odbiti, promijeniti, ponovo izdati ili opozvati sertifikat u vezi sa bilo kojim DN-om.

3.2. INICIJALNA VALIDACIJA IDENTITETA

3.2.1. NAČIN ZA DOKAZIVANJE POSJEDOVANJA PRIVATNOG KLJUČA

Dokaz o posjedovanju privatnog ključa naručioca je osiguran putem bezbjedne komunikacije između CA aplikacije i PKI klijentske aplikacije koristeći PKCS#10 u skladu sa RSA PKCS#10 Certification Request Syntax standardom.
U ovom slučaju kada su privatni ključ i sertifikat generisani od strane CA, tada je kartica sa ključem i pinom poslata onome ko je zahtijevao sertifikat, što osigurava da naručilac dobije privatni ključ.

3.2.2. PROVJERA IDENTITETA ORGANIZACIJE (PRAVNOG LICA ILI JAVNE USTANOVE)

Organizacija (pravno lice) koja želi da postane Coreit CA naručilac, mora obezbijediti dovoljno dokaza o identitetu sa kojim se predstavlja. Autentifikacija identiteta organizacije može se obaviti na jedan od sledećih načina:

- Sačuvane informacije ako je provjera identiteta organizacije prethodno obavljena od strane Coreit CA
- Kopija zvanične dokumentacije za registraciju koja dokazuje identitet organizacije

Organizacija mora podnijeti zahtjev preko pojedinca (fizičkog lica) koji ima važeće ovlašćenje da djeluje u ime organizacije. Coreit CA će verifikovati identitet fizičkog lica kao što je definisano u sekciji 3.2.3. Provjera identiteta fizičkog lica i njegovo ovlašćenje da djeluje u ime organizacije je definisano u sekciji 3.2.5 Validacija ovlašćenja.

Coreit CA vodi evidenciju o načinu na koji se verifikuje identitet organizacije i pojedinaca ovlašćenih da djeluju u ime organizacije.

3.2.3. PROVJERA IDENTITETA FIZIČKOG LICA

Sva fizička lica koja žele da postanu korisnici Coreit CA, biće verifikovani:

- licem u lice. Fizička lica moraju pokazati neki od ličnih dokumenata koja verifikuju njihov identitet (Lična karta ili pasoš)
- pomoću sertifikata za kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat izdatog od strane Coreit CA
- korišćenjem drugih identifikacionih metoda priznatih na nacionalnom nivou koje pružaju ekvivalentnu sigurnost u pogledu pouzdanosti fizičkog prisustva. Ekvivalentna sigurnost bi trebalo da bude provjerena od strane tijela za ocjenu usklađenosti

Coreit CA vodi evidenciju o načinu na koji je verifikovan identitet pojedinca.

3.2.4. PODACI O KORISNICIMA KOJI SE NE PROVJERAVAJU

Svi identifikacioni atributi opisani u sekciji 3.1.4 su verifikovani u procesu registracije.

3.2.5. VALIDACIJA OVLAŠĆENJA

Pojedinac koji zahtijeva sertifikat u ime organizacije (pravnog lica) mora dostaviti dokaz da je ovlašćeni predstavnik pravnog lica i validnu dokumentaciju na ime organizacije koje će biti upisano u sertifikatu, u skladu sa sekcijom 3.2.2 Provjera identiteta organizacije. Ime korporacije ili organizacije koje bi trebalo biti uključeno u sertifikat, mora biti identično punom ili skraćenom imenu organizacije koje je definisano u dokumentu koji je dostavljen.
Naručioci zahtjeva za sertifikat za sopstvene potrebe, moraju biti identifikovani kao lice čije će ime biti u sertifikatu.

3.2.6. KRITERIJUMI ZA POVEZIVANJE

Procedure i prakse povezanih sertifikacionih tijela moraju biti materijalno ekvivalnetne procedurama i praksi Coreit CA definisanim u politikama sertifikata. Coreit CA PMA definiše detaljne zahtjeve od slučaja do slučaja.

3.3. PROVJERA IDENTITETA KOD ZAHTJEVA ZA OBNOVU SERTIFIKATA

3.3.1. PROVJERA IDENTITETA KOD RUTINSKE OBNOVE SERTIFIKATA

Rutinska obnova se odvija kada se period važenja sertifikata ili privatnog ključa bliži kraju.
Korisnici koji zahtijevaju obnovu sertifikata se autentifikuju:

- kao što je specificirano u sekciji 3.2.2 Provjera identiteta organizacije i 3.2.3 Provjera identiteta fizičkog lica, ili
- koristeći postojeći, jos uvijek validan sertifikat izdat od strane Coreit CA, ako atributi u sertifikatu nijesu mijenjani

3.3.2. PROVJERA IDENTITETA KOD OBNOVE SERTIFIKATA NAKON OPOZIVA

Korisnik koji zahtijeva obnovu nakon opoziva se provjerava kao što je specificirano u sekciji 3.2.2. Provjera identiteta organizacije i 3.2.3. Provjera identiteta fizičkog lica

3.4. IDENTIFIKACIJA I AUTENTIFIKACIJA KOD ZAHTJEVA ZA OPOZIV

Zahtjev za opoziv može obaviti naručilac ili vlasnik sertifikata tako što će pozvati CA ili RA kontakt telefon i identifikovaće se sa tajnim kodom koji je definisan tokom procesa registracije, lično u kancelariji CA registracionog tijela, ili digitalno potpisanim zahtjevom koji se potpisuje privatnim ključem korisnika koji zahtijeva opoziv.
Ovlašćene osobe koje zahtijevaju opoziv potpisanom elektronskom komunikacijom, autentifikuju se na osnovu svog digitalnog potpisa čak i kada se sumnja da je ugrožen privatni ključ za potpis.
Inače, ovlašćeni pojedinci se autentifikuju na osnovu informacija koje se nalaze u korisničkim fajlovima ili kao što je prikazano u sekcijama 3.2.2 Provjera identiteta organizacije i 3.2.3 Provjera identiteta fizičkog lica.

4. ŽIVOTNI CIKLUS UPRAVLJANJA SERTIFIKATIMA

4.1. APLICIRANJE ZA IZDAVANJE SERTIFIKATA

4.1.1. KO MOŽE APLICIRATI ZA IZDAVANJE SERTIFIKATA

Zahtjev za izdavanje sertifikata može podnijeti:

- bilo koje fizičko lice koje ispunjava zahtjeve navedene u formi za registraciju, Coreit CA CPS i relevantnom ugovoru sa korisnikom (End User Agreement)
- bilo koja korporacija, organizacija ili institucija koja ispunjava zahtjeve navedene u formi za registraciju, Coreit CA CPS i relevantnom ugovoru sa korisnikom (End User Agreement).

4.1.2. PROCES OBRADE ZAHTJEVA I ODGOVORNOSTI

Coreit CA izdaje sertifikat jedino nakon provjere identiteta naručioca i uspješnog završetka procesa registracije. Glavni koraci prilikom izdavanja sertifikata su:

- Naručilac podnosi potpisanu registracionu formu i daje validnu dokumentaciju za identifikaciju
- Naručilac prihvata Coreit CA CPS i njegove uslove za potpisivanje ugovora
- Zahtjev za izdavanje sertifikata je prihvaćen i odobren od strane Coreit CA registracionog tijela
- Registraciono tijelo podnosi zahtjev za izdavanje sertifikata Coreit CA OA tijelu
- Coreit CA OA kreira korisnka sa odgovarajućim profilom sertifikata i generiše aktivacione kodove, koji se sastoje od korisničkog ID-a i autorizacionog koda (jednokratna lozinka). Korisniku su potrebni aktivacioni kodovi kako bi zatražio sertifikat od CA.CA administratoru su potrebni aktivacioni kodovi u slučaju kada se sertifikati i ključevi pripremaju na pametnoj kartici (kriptografskom tokenu) od strane Coreit CA
- Ako se aktivacioni kodovi šalju vlasniku sertifikata:
    - korisnički ID se šalje elektronskim putem na mail naručioca koji se nalazi u formi za registraciju
    - Kod za autorizaciju (jednokratna lozinka) je odštampan i zapečaćen u koverti od strane OA. OA dostavlja zapečaćenu kovertu RA. Zapečaćenu kovertu RA šalje naručiocu putem registrovane pošte ili naručilac preuzima kovertu lično.
    - Naručilac koristi aktivacione kodove da zahtijeva sertifikat od CA aplikacije putem internet pretraživača
- Ako su ključevi i sertifikati pripremljeni na pametnoj kartici od strane CA, pametna kartica i pin su dostavljeni u zapečaćenoj koverti RA-u i preuzima ih naručilac lično.

4.2. PROCESUIRANJE ZAHTJEVA ZA IZDAVANJE SERTIFIKATA

4.2.1. POSTUPAK IDENTIFIKACIJE I AUTENTIFIKACIJE

Coreit CA izvršava identifikaciju i autentifikaciju kao što je definisano u sekcijama 3.2.2 Provjera identiteta organizacije i 3.2.3 Provjera identiteta fizičkog lica.

4.2.2. ODOBRAVANJE ILI ODBIJANJE ZAHTJEVA ZA IZDAVANJE SERTIFIKATA

Zahtjev za Coreit CA sertifikat će biti odobren ako su ispunjeni svi sledeći uslovi:

- Naručilac je predao popunjenu formu za registraciju i priložio dokumenta za identifikaciju
- Podnosilac zahtjeva ima odgovarajuće ovlašćenje ako djeluje u ime pravnog lica
- Forma za registraciju zajedno sa dokumentima za identifikaciju i autorizaciju je uspješno provjerena
- Podnosilac zahtjeva je potpisao da je upoznat sa uslovima izdavanja i korišćenja sertifikata navedenim u CPS.

U slučaju da neki od ovih uslova nije ispunjen, ili da postoji opravdana sumnja da naručilac narušava pravila ovog dokumenta, ugovor sa korisnikom ili važeće zakone, Coreit CA registraciono tijelo će odbiti zahtjev za izdavanje sertifikata. Coreit CA zadržava pravo za odbijanje zahtjeva za izdavanje sertifikata bez navođenja razloga.

4.2.3. VRIJEME ZA OBRADU ZAHTJEVA

Inicijalna obrada zahtjeva počinje za vrijeme samog prisustva naručioca u kancelariji Coreit CA registracionog tijela.
Zahtjevi dostavljeni u elektronskoj formi će biti incijalno procesuirani od strane Coreit CA RA u okviru pet radnih dana od prijema zahtjeva.
Maksimalno ukupno vrijeme za kompletnu obradu zahtjeva je 15 radnih dana.

4.3. IZDAVANJE SERTIFIKATA

4.3.1. AKTIVNOSTI CA U FAZI IZDAVANJA SERTIFIKATA

Coreit CA aplikacija će po prijemu zahtjeva za izdavanje sertifikata:

- provjeriti validnost aktivacionih kodova uključenih u zahtjev
- provjeriti da korisnik posjeduje privatni ključ povezan sa javnim ključem uključenim u zahtjev za izdavanje sertifikata, kao što je opisano u sekciji 3.2.1 Način za dokazivanje posjedovanja privatnog kluča;
- verifikuje uskladjenost zahtjeva za izdavanje sertifikata sa PKCS#10 tehničkom specifikacijom

- izdaje zahtijevani sertifkat ako su svi od ovih uslova ispunjeni.

4.3.2. OBAVJEŠTAVANJE KORISNIKA O IZDAVANJU SERTIFIKATA OD STRANE CA

Coreit CA aplikacija će podnosiocu zahtjeva izdati sertifikat odmah, tako da nema potrebe za dodatnim obavještenjima.
U slučaju da CA pripremi ključ i sertifikate na pametnoj kartici, korisnik se obavještava kao dio procesa isporuke.

4.4. PRIHVATANJE SERTIFIKATA

4.4.1. POSTUPAK PRIHVATANJA SERTIFIKATA OD STRANE KORISNIKA

Podnosioc zahtjeva će dobiti sve sertifikate za vrijeme trajanja procesa izdavanja sertifikata. Dodatna potvrda prihvatanja sertifikata nije potrebna.
U slučaju neuspješnog preuzimanja, korisnik mora prijaviti problem Coreit CA-u ili RA-u.

4.4.2. OBJAVLJIVANJE SERTIFIKATA OD STRANE CA

Nije primjenjivo.

4.4.3. OBAVJEŠTAVANJE OSTALIH UČESNIKA O IZDAVANJU SERTIFIKATA

Coreit CA neće obavještavati ostale entitete.

4.5. UPOTREBA PARA KLJUČEVA I SERTIFIKATA

4.5.1. UPOTREBA PARA KLJUČEVA I SERTIFIKATA OD STRANE KORISNIKA

Coreit CA izdaje sertifikate koji mogu podržati više namjena za upotrebu ključa. Podrška je obezbijeđena upotrebom odgovarajućih ekstenzija za namjenu ključa.
Naručilac treba da koristi sertifikat u skladu sa keyUsage i extKeyUsage x.509 ekstenzijama sertifikata i za namjene definisane u sekciji 1.4.1 Dozvoljena upotreba sertifikata.
Naručilac mora čuvati privatni ključ i preduzeti sve mjere opreza kako bi se spriječilo otkrivanje i neovlašćeno korišćenje.
Nakon isteka validnosti sertifikata, dodijeljeni privatni ključ se smatra nevalidnim.

4.5.2. UPOTREBA PARA KLJUČEVA I SERTIFIKATA OD STRANE TREĆIH LICA

Treće lice će se ograničiti u oslanjanju na javni ključ koji se nalazi u sertifikatu koji je izdao Coreit CA za odgovarajuću upotrebu definisanu u sekciji 1.4.1. Dozvoljena upotreba sertifikata. Treće lice je, takođe, odgovorno za:

- poštovanje ograničenja sertifikata i CA odgovornosti kao što je opisano u ovom CPS-u.
- osiguravanje da sertifikat nije opozvan pristupanjem svim on-line raspoloživim listama za opoziv sertifikata CRL ili OCSP
- obavještavanje CA u slučaju sumnje ili poznate zloupotrebe bilo kojeg sertifikata kojeg je izdao CA

4.6. OBNOVA SERTIFIKATA (BEZ GENERISANJA NOVOG KLJUČA)

Obnova sertifikata je proces u kom CA izdaje novi sertifikat istom tijelu i za isti javni ključ. Obnova sertifikata nije dozvoljena i podržana od strane Coreit CA

4.6.1. OKOLNOSTI POD KOJIMA SE MOŽE OBNOVITI SERTIFIKAT

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.6.2. KO MOŽE TRAŽITI OBNOVU

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.6.3. PROCES OBRADE ZAHTJEVA ZA OBNOVU SERTIFIKATA

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.6.4. OBAVJEŠTAVANJE KORISNIKA O IZDAVANJU SERTIFIKATA

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.6.5. POSTUPAK POTVRDE PRIHVATANJA OBNOVLJENOG SERTIFIKATA

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.6.6. OBJAVA OBNOVLJENOG SERTIFIKATA OD STRANE CA

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.6.7. OBAVJEŠTAVANJE O IZDAVANJU OBNOVLJENOG SERTIFIKATA OD STRANE CA DRUGIM LICIMA

Nije podržano kao što je navedeno u 4.6 Obnova sertifikata.

4.7. OBNOVA SERTIFIKATA (UZ GENERISANJE NOVOG KLJUČA)

Obnova sertifikata je proces u kom CA izdaje novi sertifikat korisniku. Novi sertifikat sadrzi iste informacije kao stari sertifikat i novi javni ključ.

4.7.1. OKOLNOSTI POD KOJIMA SE MOŽE OBNOVITI SERTIFIKAT

Obnova sertifikata se vrši:

- nakon opoziva sertifikata
- nakon isticanja sertifikata ili skorog isticanja istog

4.7.2. KO MOŽE TRAŽITI OBNOVU SERTIFIKATA UZ GENERISANJE NOVOG KLJUČA

Obnovu sertifikata može zatražiti naručilac, korisnik sertifikata ili ovlašćeno lice koje je zahtijevalo inicijalno izdavanje sertifikata.

4.7.3. PROCES OBRADE ZAHTJEVA ZA OBNOVU SERTIFIKATA

Obnova sertifikata se izvršava na isti način kao i izdavanje inicijalnog sertifikata.

4.7.4. OBAVJEŠTAVANJE KORISNIKA O IZDAVANJU SERTIFIKATA

Kao što je opisano u sekciji 4.3.2. Obavještavanje korisnika o izdavanju sertifikata od strane CA

4.7.5. POSTUPAK POTVRDE PRIHVATANJA OBNOVLJENOG SERTIFIKATA UZ GENERISANJE NOVOG KLJUČA

Kao što je opisano u sekciji 4.4.1. Postupak prihvatanja sertifikata od strane korisnika.

4.7.6. OBJAVA OBNOVLJENOG SERTIFIKATA UZ GENERISANJE NOVOG KLJUČA OD STRANE CA

Kao što je opisano u sekciji 4.4.2. Objavljivanje sertifikata od strane CA

4.7.7. OBAVJEŠTAVANJE O IZDAVANJU OBNOVLJENOG SERTIFIKATA OD STRANE CA DRUGIM LICIMA

Kao što je opisano u sekciji 4.4.3. Obavještavanje ostalih učesnika o izdavanju sertifikata.

4.8. PROMJENA SERTIFIKATA

Promjena sertifikata je procedura koja omogućava korisnicima da zahtijevaju sertifikat sa izmijenjenim informacijama. Promjena sertifikata zahtijeva obnovu sertifikata i obrađuje se kao inicijalni zahtjev za izdavanje sertifikata.

4.8.1. OKOLNOSTI ZA PROMJENU SERTIFIKATA

Korisnik može zahtijevati promjenu sertifikata kada se informacije poput imena ili prezimena promijene.

4.8.2. KO MOŽE ZAHTIJEVATI PROMJENU SERTIFIKATA

Promjenu sertifikata može zahtijevati naručilac, vlasnik sertifikata ili tijelo koje je zahtijevalo inicijalno izdavanje sertifikata.

4.8.3. PROCESUIRANJE ZAHTJEVA ZA PROMJENU SERTIFIKATA

Promjena sertifikata se obrađuje kao i inicijalno izdavanje sertifikata.

4.8.4. OBAVJEŠTAVANJE KORISNIKA O IZDAVANJU IZMIJENJENOG SERTIFIKATA

Kao što je opisano u sekciji 4.3.2 Obavještavanje korisnika o izdavanju sertifikata od strane CA

4.8.5. POSTUPAK POTVRDE PRIHVATANJA PROMIJENJENOG SERTIFIKATA

Kao što je opisano u sekciji 4.4.1 Postupak prihvatanja sertifikata od strane korisnika.

4.8.6. OBJAVLJIVANJE PROMIJENJENOG SERTIFIKATA OD STRANE CA

Kao što je opisano u sekciji 4.4.2 Objavljivanje sertifikata od strane CA.

4.8.7. OBAVJEŠTAVANJE DRUGIH LICA O PROMJENI SERTIFIKATA OD STRANE CA

Kao što je opisano u sekciji 4.4.3 Obavještavanje ostalih učesnika o izdavanju sertifikata.

4.9. OPOZIV I SUSPENZIJA SERTIFIKATA

4.9.1. OKOLNOSTI ZA OPOZIV SERTIFIKATA

Opoziv sertifikata se zahtijeva:

- ako je to traženo od strane naručioca ili vlasnika sertifikata;
- ako CA utvrdi da je vlasnik sertifikata preminuo, izgubio poslovnu sposobnost, prestao da postoji ili su izmijenjene činjenice koje imaju veliki uticaj na validnost sertifikata
- kada je poznato ili se sumnja da su neke od informacija koje se nalaze u sertifikatu netačne
- kada je kompromitovan privatni ključ koji je dodijeljen sa sertifikatom, ili se sumnja da je kompromitovan
- kada je kompromitovan neki od aktivacionih podataka, kao što su lozinka ili PIN, koji se koriste za zaštitu privatnog ključa ili se sumnja da je kompromitovan
- ako CA utvrdi da sertifikat nije pravilno izdat u skladu sa Coreit CA politikom sertifikata
- ako naručilac ili vlasnik sertifikata krše odredbe definisane Coreit CA politikom sertifkata, ugovorom ili primjenjivim zakonom
- u slučaju da kriptografija koja se koristi više ne osigurava povezivanje između subjekta i javnog ključa

Coreit CA može opozvati Coreit CA sertifkat kada smatra da je to neophodno.

4.9.2. KO MOŽE ZAHTIJEVATI OPOZIV SERTIFIKATA

Opoziv sertifikata može zahtijevati:

- Naručilac ili vlasnik sertifikata
- ovlašćeni predstavnik organizacije koji je zahtijevao izdavanje sertifkata
- Coreit CA RA
- Coreit CA OA
- Coreit CA PMA
- Zakonodavni sud

4.9.3. PROCEDURA OPOZIVA SERTIFIKATA

Opoziv sertifikata može biti podnešen od strane naručioca ili vlasnika sertifkata putem potpisanog zahtjeva za opoziv lično u kancelariji CA registracionog tijela, ili u zahtijevanoj elektronskoj formi potpisanoj privatnim ključem korisnika koji zahtijeva opoziv, poslat email-om na adresu definisanu u sekciji 1.5.2. Kontakt podaci, kao i telefonskim putem ukoliko podnosilac zahtjeva za opoziv saopšti tajni kod za opoziv osoblju RA ili CA.

Zahtjev za opoziv sertifkata je identifikovan kao što je opisano u sekciji 3.4 Identifikacija i autentifikacija kod zahtjeva za opoziv.

4.9.4. PERIOD PREDVIĐEN ZA PODNOŠENJE ZAHTJEVA ZA OPOZIV

Subjekat koji je postao svjestan okolnosti koje zahtijevaju opoziv sertifikata mora zatražiti opoziv što je prije moguće i bez nepotrebnog odlaganja.

4.9.5. VRIJEME ZA KOJE CA MORA PROCESUIRATI ZAHTJEV ZA OPOZIV

U svim slučajevima opoziva sertifkat će biti objavljen u CRL najkasnije jedan radni dan od trenutka kada je Coreit CA ili Coreit CA RA primilo validan zahtjev za opoziv.

4.9.6. OBAVEZA PROVJERE REGISTRA OPOZVANIH SERTIFIKATA OD STRANE TREĆIH LICA

Treća lica su dužna da provjere Coreit CA CRL ili OCSP prije upotrebe bilo kojeg sertifkata izdatog od strane Coreit CA, odnosno uvjeravanja u validnost samog sertifikata. Ukoliko nije moguće utvrditi status sertifikata zbog otkaza sistema ili servisa, nijedan Coreit CA sertifikat ne treba da bude prihvaćen kao validan.
Treća strana će provjeriti CRL ili OCSP odgovor tako što će provjeriti digitalni potpis sa pridruženim Coreit CA sertifkatom i kada ističe.

4.9.7. UČESTALOST IZDAVANJA REGISTRA OPOZVANIH SERTIFIKATA (CRL)

Coreit CA ažurira CRL odmah ili što je prije moguće nakon što je obrađen validni zahtjev za opoziv, ili najmanje jednom u okviru 24 sata sa periodom važenja CRL-a 48 sati.

4.9.8. MAKSIMALNA ZAKAŠNJENJA U OBJAVI REGISTRA OPOZVANIH SERTIFIKATA (CRL)

Nije primjenjivo. (Pogledaj sekciju 4.9.7)

4.9.9. DOSTUPNOST ON-LINE PROVJERE STATUSA OPOZVANIH SERTIFIKATA

OCSP servis obezbjeđuje CA. Lokacija servisa je označena sa URL-om uključenim u svakom izdatom sertifikatu.

4.9.10. OBAVEZA ON-LINE PROVJERE OPOZVANIH SERTIFIKATA

Pogledaj sekciju 4.5.2. Upotreba para ključeva i sertifikata od trećih lica.

4.9.11. OSTALE FORME OBJAVLJIVANJA OPOZVANIH SERTIFIKATA KOJE SU DOSTUPNE

Nije primjenjivo.

4.9.12. POSEBNI ZAHTJEVI U SLUČAJU KOMPROMITOVANJA KLJUČA

Nema posebnih zahtjeva potrebnih u slučaju kompromitovanja privatnog ključa vlasnika sertifikata.

4.9.13. OKOLNOSTI ZA SUSPENZIJU SERTIFIKATA

Nije primjenjivo.

4.9.14. KO MOŽE ZAHTIJEVATI SUSPENZIJU SERTIFIKATA

Nije primjenjivo.

4.9.15. PROCEDURA ZA SUSPENZIJU SERTIFIKATA

Nije primjenjivo.

4.9.16. OGRANIČENJA PERIODA TRAJANJA SUSPENZIJE

Nije primjenjivo.

4.10. SERVISI ZA STATUS SERTIFIKATA

4.10.1. OPERATIVNE KARAKTERISTIKE

Status sertifikata se objavljuje koristeći X.509 listu za opoziv sertifikata (CRL) i OCSP servis. CRL se objavljuje putem internet sajta. Tačna lokacija (http URLs) se objavljuje uz pomoć X.509 CRL Distribution Point ekstenzije. Lokacija OCSP servisa je označena sa URL-om uključenim u svakom izdatom sertifikatu.

4.10.2. RASPOLOŽIVOST SERVISA

Coreit CA garantuje da je status sertifikata raspoloziv 24/7 uz maksimalne neplanirane prekide rada od (10) dana u godini.

4.10.3. OPERATIVNE KARAKTERISTIKE

Nije primjenjivo.

4.11. PREKID DOGOVORA/UGOVORA/SPORAZUMA

Ugovor o korišćenju sertifikata prestaje da važi nakon isteka ili opoziva poslednjeg korisnikovog sertifikata. Coreit CA čuva dokumenta vezana za korisnika, sertifikate i status sertifikata najmanje 10 godina od trenutka isticanja poslednjeg sertifikata.
Institucija koja je zahtijevala sertifikat za svog zaposlenog mora obavijestiti Coreit CA da je radni odnos prestao ili da više ne postoji potreba za sertifikatom.

4.12. DEPONOVANJE (ESCROW) I POVRATAK KLJUČA

Nije primjenjivo.

4.12.1. POLITIKE I PRAKSE ZA DEPONOVANJE (ESCROW) I POVRATAK KLJUČA

Nije primjenjivo.

4.12.2. POLITIKA I PRAKSA ZA UPRAVLJANJE ENKAPSULACIJE I OPORAVKA SESIJE KLJUČA

Nije primjenjivo.

5. OBJEKTI, UPRAVLJANJE I OPERATIVNE KONTROLE

5.1. FIZIČKA ZAŠTITA

5.1.1. LOKACIJA I KONSTRUKCIJA

Coreit CA infrastruktura je smještena na pouzdanoj lokaciji Telenor data centra, na adresi ul. Josipa Broza Tita bb, 81000 Podgorica.
Sistemske komponente i funkcije Coreit CA su smještene u fizički zaštićenom okruženju koje sprečava neautorizovano korišćenje, pristup ili odavanje osjetljivih informacija. Kontrole fizičke sigurnosti implementirane su u skladu sa najboljim praksama. Mjere zaštite uključuju:

- Samostalni pristup je ograničen na ovlašćeno Coreit osoblje uz obaveznu najavu
- Svi ostali pristupi moraju biti pod pratnjom ovlašćenog Coreit osoblja i bilježe se
- Tokom svojih posjeta, osoblje zaduženo za upravljanje i servisiranje se prati uz video nadzor
- Sigurnosne elektronske brave i pristupni sistem
- Nadgledanje 24h / 7 dana u nedelji uz prisustvo stražara na licu mjesta i uz pomoć video nadzora iz centra za nadgledanje zgrade

5.1.2. KONTROLA FIZIČKOG PRISTUPA

Kontrola fizičkog pristupa opremi korisnika vrši se preko odgovarajućih bezbjedonosnih sistema pri čemu se koristi višestruka mehaničko-elektronska kontrola ulaza u objekat i područije data centra. Coreit CA koristi kombinaciju kartice za pristup, pin-a i fizičkog zaključavanja.
Objekat je opremljen sigurnosnom ogradom sa potpuno kontrolisanim pristupom ulazu i opremljen je sistemom video nadzora 24h dnevno, uz stalno prisustvo fizičkog obezbeđenja. Kontrola pristupa prostorijama u Data centru izvršena je u skladu sa unaprijed dodijeljenim pravima pristupa i bezbjedonosnim procedurama koje uključuju autentifikaciju putem čitača kartica instaliranih na svim relevantnim mjestima.
Nadzor svih sigurnosnih sistema u objektu vrši se 24/7 iz Telenorovog centra za bezbijednost, gdje postoji odgovarajući postupak obavještavanja o događajima od intersa.
Stručnjaci tima za tehničku sigurnost konstantno prate i primjenjuju najnovije sigurnosne standarde i proizvode.

5.1.3. NAPAJANJE I KLIMATIZACIJA

Telenor Tier3 Data Centar je direktno povezan na gradsku elektroenergetsku mrežu i napaja se električnom energijom preko dvije nezavisne grane napajanja, svaka kapaciteta 10kV, pri čemu su podzemni elektroenergetski kablovi dovedeni do Data Centra preko različitih trafo stanica kapaciteta 110/10 kV/kV.

Sistemi napajanja električnom energijom projektovani su tako da je moguće održavanje jedne od grana napajanja bez uticaja na funkcionalnost sistema u cjelini.

Dizel generatori obezbjeđuju kontinuirano napajanje Data Centra u trajanju od 72h, prije nego što je neophodna dopuna goriva. Generatori se automatski pokreću nakon detekcije nestanka električnog napajanja. Kapacitet generatora pokriva sva kritična opterećenja cjelokupnog Data Centra za sve vrijeme trajanja prekida napajanja, pri čemu je obezbijeđena N+1 redudantnost sistema. Sistem neprekidnog napajanja – UPS - pokriva prelazni režim od trenutka otkaza strujnog napajanja do pokretanja generatora. UPS sistem je potpuno redudantan i sastoji se iz dva nezavisna UPS podsistema (grana A i grana B) koja podržavaju prelazni režim rada u trajanju od minimalno 30 min pri punom opeterećenju Data Centra.

Potrošnja električne energije mjeri se na ulazu u svaki orman i to preko PDU (Power Distribution Unit) uređaja. Snaga i potrošnja energije za odabrani orman ili grupu ormana nadzire se i kontroliše kroz Centralni PDU sistem za upravljanje.

U cilju obezbjeđenja visoke raspoloživosti sistema za napajanje Telenor sprovodi redovna testiranja sistema električnog napajanja pri punom opterećenju koja podrazumijevaju: minimum jednom mjesečno testno startovanje generatora, kvartalno rutinsko održavanje generatora i godišnji test sistema pri punom opterećenju.

5.1.4. ZAŠTITA OD POPLAVE

Coreit CA osigurava da komponente CA ne budu izložene potencijalnim prijetnjama vezanim za vodu / tečnost.

5.1.5. PREVENCIJA I ZAŠTITA OD POŽARA

Data centar je opremljen modernim detektorima požara koji koriste detektore za rano detektovanje dima (VESDA) koji omogućavaju rano upozerenje na promjene u bilo kom dijelu Data centra.
Data centar je opremljen sa IG-55 protivpožarnim sistemom ("Argonit") koji funkcioniše po principu smanjenja nivoa kiseonika u vazduhu do nivoa koji sprečava dalje širenje požara.

5.1.6. SMJEŠTANJE MEDIJA

Svi mediji koji sadrže Coreit CA informacije, uključujući trake za backup podataka, se čuvaju u sefu otpornom na vatru i u zaštićenom okruženju smještenom u Coreit prostorijama.

5.1.7. ODLAGANJE OTPADA

Papirni dokumenti i magnetni mediji se uništavaju prije odlaganja. CA zadržava sve neupotrebljive hardverske komponente za sigurno odlaganje.

5.1.8. SMJEŠTANJE KOPIJA MEDIJA NA UDALJENOJ LOKACIJI

Coreit CA koristi sigurnosne kontrole za siguran transport i skladištenje svih rezervnih i arhivskih medija van primarne lokacije. Pristup i čitanje rezervnih kopija vrši se jednom godišnje u okviru vježbe kontinuiteta poslovanja.
Operativne sigurnosne kopije (Backups) cjelokupnog CA sistema (konfiguracija sistema, arhivski zapisi, zapisi revizije) snimaju se mjesečno i čuvaju na sigurnom mjestu za skladištenje van primarne lokacije. Operativne sigurnosne kopije mogu se koristiti za oporavak kompletnog CA sistema.
Kontrola fizičkog pristupa na udaljenoj lokaciji je implementirana na sličan način kao u Coreit CA primarnom IT centru.

5.2. PROCEDURALNE KONTROLE

5.2.1. POVJERLJIVE ULOGA OSOBLJA CA

Zavisno od svoje uloge, Coreit CA osoblje može imati nalog na CA operativnom sistemu ili CA aplikaciji ili na oboje. CA aplikacija koju koristi Coreit CA, implementira niz uloga koje dodjeljuje CA osoblju u zavisnoti od njihovih odgovornosti. Prava pristupa na operativnom sistemu CA ograničavaju osoblje na radnje koje su im potrebne u obavljanju njihovih dužnosti.
Različiti nivoi sistemskog i fizičkog pristupa se kontrolišu na osnovu uloga dodijeljenih od strane CA aplikacije i prava pristupa koje ima nalog na sistemu.

Povjerljive uloge su:

Oblast	Uloga	Minimalni broj osoba	Osoba
Upravljanje setifikatima	HSM Administrator	1	D
	HSM Token Owner (User)	2	B,D
	CA Administrator	1	C
	CA Superadmin	1	A
	Crypto Custodian	3	A,B,D
	RA Administrator	1	J
	SCD Administrator	1	I
Upravljanje sistemom	Root CA/ unix root, Issuing CA / unix root	2	A,B
Sigurnost i kontrola	HSM Administration Security Officer (ASO)	1	F
	HSM partition Security Officer (SO)	1	G
	Security Safe Custodian	1	H
	Internal Audit and compliance	1	E

5.2.2. POTREBAN BROJ OSOBA ZA OPERATIVNE POSTUPKE

Za izvršenje sledećih zadataka potrebna su odobrenja dva (2) korisnika:

- HSM inicijalizacija
- Inicijalno generisanje CA sertifikata i ključa
- Backup CA ključa i vraćanje
- Ažuriranje CA ključa i sertifikata
- Unakrsna sertifikacija sa eksternim CA
- Aktivacija CA ključa

Jedna osoba može izvršiti sve ostale zadatke. Sve aktivnosti koje obavljaju pouzdani nosioci uloga se evidentiraju i provjeravaju.

5.2.3. IDENTIFIKACIJA I AUTENTIFIKACIJA ZA OSOBLJA ZA POJEDINE ULOGE

Svaka osoba sa povjerljivom CA ulogom se identifikuje i autentifikuje sa korisičkim imenom i lozinkom ili sa digitalnim sertifikatom. Sistemski CA nalozi i aplikativni CA nalozi su direktno povezani sa pojedincem u čijem su vlasništvu. Nalozi se ne dijele i prava koja su im dodijeljena ograničena su na ona koja su im potrebna da izvršavaju svoje funkcije.

5.2.4. POVJERLJIVE ULOGE KOJE MORAJU IMATI ODVOJENE DUŽNOSTI

Sistem administrator mora imati potrebna prava za instalaciju, konfiguraciju i upravljanje CA računarskim hardverom i softverom. Pri dodjeli korisničkih uloga i fizičkih prava pristupa strogo se poštuje princip segregacije dužnosti tako da jedna osoba ne može koristiti kriptografske materijale za izvršavanje sigurnosnih osjetljivih operacija, već je uvijek potrebno osigurati prisustvo najmanje dvije osobe.

5.3. KONTROLA OSOBLJA

Osoblje Coreit CA imenuje uprava i pismeno ih obavještava o uslovima svog položaja.

5.3.1. KVALIFIKACIJE, ISKUSTVA I PROVJERE

Coreit CA praksa zapošljavanja uzima u obzir kvalifikacije kandidata i zahtjeve svake pozicije, prethodna angažovanja potencijalnih kandidata i broj godina iskistva na sličnim pozicijama, saglasno članu 34 stav 1 tačka 4 Zakona o elektronskoj identifikaciji i elektronskom potpisu.
PKI osoblje sa pouzdanom CA ulogom podvrgnuto je sigurnosnim provjerama prije nego što budu imenovani za člana Coreit CA osoblja.

5.3.2. PROCEDURA POZADINSKIH I BEZBJEDONOSNIH PROVJERA

CA prati provjeru osoblja i provjeru pozadine u skladu sa ISO/IEC 27001.

5.3.3. OBUKE

Svi članovi Coreit CA osoblja su obučeni na odgovarajući način. Za CA osoblje trening obuhvata hardver, softver i CA aplikaciju.
Osoblje CA pruža obuku drugim članovima o CA procesima, postupanjima u kriznim situacijama i slučajevima oporavka od katastrofe. Takođe, pružaju obuku članovima registracionog tijela (RA).

5.3.4. UČESTALOST PONOVNIH OBUKA

Coreit CA zaposleni će redovno a najmanje jednom godišnje pohađati obuke ili seminare radi obnavljanja znanja o aktuelnim bezbjednosnim procedurama i novim bezbjednosnim prijetnjama. Potrebe za obuku Coreit CA osoblja se redovno revidiraju da bi se prilagodili promjenama PKI okruženja.

5.3.5. UČESTALOST I REDOSLJED ROTACIJE ULOGA

Rotacija uloga nije implementirana.

5.3.6. SANKCIONISANJA ZA NEOVLAŠĆENE AKTIVNOSTI

Neovlašćene radnje i kršenja rješavaju se u skladu sa internim disciplinskim postupkom Coreit CA.

5.3.7. KRITERIJUMI ZA OSOBLJE ANGAŽOVANO PO UGOVORU O DJELU

Coreit CA ne zapošljava osoblje pod ugovorom o djelu na bilo kojoj osjetljivoj poziciji. Svi koji su pod ugovorom o djelu na neosjetljivim pozicijama moraju potpisati saglasnost o neotkrivanju podataka.

5.3.8. DOKUMENTACIJA ZA POTREBE OSOBLJA

CA zaposleni imaju pristup CA dokumentaciji, uključujući hardver, softver i dokumentaciju vezanu za aplikaciju, operativnim procedurama, procedurama za bezbijednost, procedurama za kontrolu pristupa i ovom CPS-u.

5.4. PROCEDURA UPRAVLJANJA LOGOVIMA ZA REVIZIJU

5.4.1. VRSTA DOGAĐAJA KOJI SE BILJEŽE

Logovi za potrebe revizije su dostupni za istraživanje u slučaju neautorizovanog pristupa informacijama sistema i za potrebe revizije. Za potrebe revizije, bilježe se sledeći tipovi događaja:

- Logovi koji su vezani za upravljanje životnim ciklusom sertifikata koji uključuje, ali nije ograničen na:
    - Registracija korisnika
    - Izdavanje sertifikata
    - Opoziv sertifikata
    - Izdavanje i objavljivanje CRL-a
- Logovi koji su vezani za administraciju sistema i upravljanje aktivnostima koje uključuju, ali nisu ograničene na:

- Pokretanje i zaustavljanje aplikacije
- Nadzor funkcionisanja sistema (upozorenja, alarmi, prekidi, greške...)
- Promjene u kritičnoj konfiguraciji sistema
- Backup i oporavak podataka

Revizorski zapisi sadrže minimum sledeće zapise:

- Identifikacija korisnika
- Tip događaja
- Vrijeme i datum događaja
- Uspješne i neuspješne događaje
- Ishod događaja
- Identifikacija podataka, komponenti sistema i resursa kojima je pristupljeno.

5.4.2. UČESTALOST PROCESUIRANJA LOGOVA

Skladištenje, zaštita i obrada revizorskih logova vrši se u realnom vremenu uz automatsko upozorenje na pojavu sigurnosnih događaja za sve kritične aktivnosti.
Za manje kritične aktivnosti vrši se periodična provjera.

5.4.3. VRIJEME ČUVANJA LOGOVA

Logovi se zadržavaju i čuvaju u periodu koji je definisan u sekciji 5.5.

5.4.4. ZAŠTITA REVIZIJSKIH LOGOVA

Logovi su adekvatno zaštićeni i vjerodostojni i mogu se predočiti kao dokazni materijal na sudu. Oni obuhvataju sledeće zaštitne mehnizme:

- Svi sistemski satovi i vremena su međusobno usklađeni tako da logovi sadrže zapise sa važećim datumom i vremenom.
- Povjerljivi podaci su isključeni ili maskirani tako da nisu sadržani u logovima.
- Implementirana je kriptografska zaštita integriteta svih kritičnih zapisa kako bi se zaštitili od bilo kakvih izmjena ili brisanja u okviru pojedinog zapisa.
- Administratori sistema ne smiju da mijenjaju ili brišu manje kritične zapise koji nisu obuhvaćeni sistemom za upravljanje revizijskim zapisima.

5.4.5. IZRADA REZERVNIH KOPIJA REVIZIJSKIH LOGOVA

Backup revizijskih logova se vrši automatski kako bi se osigurao kontinuitet poslovanja.
Postupak vraćanja sigurnosnih kopija je poznat, testiran i pouzdan i osigurava vraćanje podataka u razumnom vremenu.
Backup pravi više rezervnih kopija koje se čuvaju na primarnoj i udaljenoj lokaciji.

5.4.6. SISTEM PRIKUPLJANJA LOGOVA

Uspostavljen je sistem za upravljanje logovima i vrši automatsko skladištenje i zaštitu zapisa u realnom vremenu.

5.4.7. OBAVJEŠTAVANJE LICA KOJE JE IZAZVALO DOGAĐAJ

Lice koje je izazvalo događaj nije obaviješteno.

5.4.8. PROCJENA RANJIVOSTI SISTEMA

Coreit CA sprovodi procjene ranjivosti kao dio postupka obrade revizorskih logova.

5.5. ARHIVIRANJE PODATAKA

5.5.1. PODACI KOJI SE ARHIVIRAJU

Coreit CA čuva sledeće tipove podataka:

- Informacije za reviziju specificirane u sekciji 5.4. Procedura upravljanja logovima za reviziju.
- Korisničke zahtjeve i ugovore
- Sertifikate, status opozvanog sertifikata
- Izvještaje o nepodudarnosti i kompromitovanjima

5.5.2. PERIOD ČUVANJA PODATAKA U ARHIVI

Coreit CA čuva revizorske logove najmanje deset (10) godina nakon isteka sertifikata. Status opoziva sertifikata se čuvaju najmanje deset (10) godina nakon isteka sertifikata. Zahtjevi korisnika, ugovori i CA korespodencija se čuvaju minimum deset (10) godina nakon isteka sertifikata.

5.5.3. ZAŠTITA ARHIVE

Pristup informacijama Coreit CA arhive daje se zaposlenima na osnovu potrebe.

5.5.4. PROCEDURA ČUVANJA REZERVNIH KOPIJA ARHIVIRANIH PODATAKA

Arhivirani materijal se čuva van primarne lokacije u sigurnom objektu gdje su fizičke i bezbjedonosne kontrole uporedive sa onima koje su implementirane na primarnoj lokaciji.

5.5.5. POTREBA ZA VREMENSKIM PEČATOM ARHIVIRANIH PODATAKA

Arhivirani podaci se obilježavaju u vrijeme njihovog nastanka koristeći sistemsko vrijeme u kom je događaj zabilježen. Svi sistemi su sinhronizovani sa vremenskim izvorom koji se oslanja na UTC.

5.5.6. SISTEM ARHIVIRANJA (INTERNI ILI EKSTERNI)

Coreit CA koristi interni backup za arhiviranje. Arhivirani podaci su skladišteni na offline medijumu.

5.5.7. PROCEDURA ZA PRISTUP I VERIFIKACIJU ARHIVIRANIH PODATAKA

Pristup sačuvanim podacima je dozvoljen CA predstavniku na osnovu potreba ili u skladu sa važećim zakonom.

5.6. OBNOVA CA KLJUČA

Obnova privatnog ključa će se izvršiti prije isteka sertifikata.. Nakon promjene privatnog ključa, novi javni ključ biće dostupan vlasnicima sertifikata putem javnog repozitorijuma.

5.7. KOMPROMITOVANJE I OPOROVAK SISTEMA OD NEPREDVIĐENIH SITUACIJA

5.7.1. PROCEDURE KOD KOMPROMITOVANJA ILI INCIDENATA

Coreit CA primjenjuje ISO/IEC 27001 procedure kao reakciju na bezbjedonosne incidente i kvarove. Nacionalni nadzorni organ biće obaviješten o incidentu.

5.7.2. GREŠKE U RADU SISTEMA, PROGRAMSKE OPREME ILI OŠTEĆENJA PODATAKA

Coreit CA je implementirao plan za slučaj vanrednih situacija i oporavka od kvara programske opreme koji se odnosi na oporavak funkcionalnosti računarskih resursa, softvera i podataka. Plan za oporavak je definisan u internom aktu ICPS član 2.2.

5.7.3. KOMPROMITOVANJE PRIVATNOG KLJUČA SERTIFIKACIONIOG TIJELA

U slučaju da je privatni ključ za potpisivanje kompromitovan, CA će opozvati sve korisničke sertifikate koji nijesu istekli i sertifikate koji su trenutno u upotrebi i obustaviti izdavanje novih sertifikata upotrebom kompromitovanog ključa. Nacionalni nadzorni organ biće obaviješten o incidentu.

5.7.4. KONTINUITET POSLOVANJA U SLUČAJU PRIRODNE I DRUGE KATASTROFE

Nakon prirodne ili neke druge katastrofe, CA funkcionalnosti i procesi i IT centar će biti ponovo uspostavljeni na rezervnoj lokaciji koristeći sigurnosne kopije podataka koje se svakodnevno uzimaju sa primarne lokacije. Coreit CA će preduzeti sve razumne mjere tako da vrijeme oporavka ne bude duže od deset (10) radnih dana.

5.8. PRESTANAK RADA CA ILI RA

U slučaju dobrovoljnog prekida poslovanja, CA će:

- Obavijestiti Nacionalno nadzorno tijelo i sve trenutne korisnike najmanje devedeset (90) dana prije namjere da se prestane sa radom.
- U dogovoru sa Nacionalnim nadzornim tijelom prenose se sve operacije na drugog pružaoca usluga ili se opozivaju svi validni sertifikati do ili nakon isteka otkaznog roka.
- Osigurati pristup i dostupnost relevantnih CRL-ova i OSCP u periodu od 6 mjeseci nakon opoziva svih sertifikata.
- Osiguraće da sva dokumentacija i arhive budu prebačene na drugog pružaoca usluga ili da budu zadržane najmanje deset (10) godina od poslednjeg dana poslovanja.

6. TEHNIČKO BEZBJEDONOSNE KONTROLE

6.1. GENERISANJE PARA KLJUČEVA I INSTALACIJA

6.1.1. GENERISANJE PARA KLJUČEVA

Coreit CA par ključeva za potpisivanje se kreira u sigurnosnom hardverskom modulu (HSM) za vrijeme inicijalne instalacije CA aplikacije.
Privatni ključ koji se korsiti za kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat, generiše se u hardverskom tokenu koji je u skladu sa QSCD standardima. Privatni ključ koji se koristi za ostale tipove sertifikata, kreira se u softverskom kripto tokenu na korisničkoj strani ili bilo kojem hardverskom tokenu.

6.1.2. DOSTAVLJANJE PRIVATNOG KLJUČA KORISNIKU

Privatni ključevi generisani od strane korisnika i preuzeti koristeći PCKS#10 format, se ne dostavljaju.
Privatni ključevi generisani u QSCD-u od strane CA, dostavljaju se korisnicima.

6.1.3. DOSTAVLJANJE JAVNOG KLJUČA DAVAOCU USLUGE SERTIFIKOVANJA

Javni ključ treba da bude na siguran način isporučen CA aplikaciji kako bi se generisao javni ključ sertifikata. Javni ključ se dostavlja CA aplikaciji u PCKS#10 formatu.

6.1.4. DOSTAVLJANJE JAVNOG KLJUČA DAVAOCA USLUGA SERTIFIKOVANJA TREĆIM LICIMA

Coreit CA javni ključ za verifikaciju potpisa se dostavlja trećim licima u sertifikatu u PKCS#7 ili X.509 formatu.

6.1.5. DUŽINA KLJUČEVA

CA ključevi koji se koriste za potpisivanje sertifikata su RSA ključevi sa minimalnom dužinom od 3072 bita. Korisnički ključevi moraju biti minimalne dužine 2048 bita.

6.1.6. GENERISANJE PARAMETARA JAVNOG KLJUČA I PROVJERA KVALITETA

Coreit CA ne generiše DSA ključeve.

6.1.7. NAMJENA UPOTREBE KLJUČEVA (X.509 v3 upotreba ključa)

Coreit CA je u mogućnosti da izdaje sertifikate koji podržavaju različite slučajeve upotrebe. Ova podrška se ostvaruje uključivanjem odgovarajućih dodataka za korišćenje ključa.
Coreit CA ključ za potpisivanje je jedini dozvoljeni ključ za potpisivanje sertifikata i CRL-ova. CA javni ključ za verifikaciju potpisa sertifikata sadrži keyCertSign i cRLSign bitove.
Korisnički ključevi mogu se koristiti u svrhe zasnovane na keyUsage i extKeyUsage poljima u sertifikatu (takođe pogledati sekciju 7).

Kategorija sertifikata	keyUsage	extKeyUsage
Kvalifikovani sertifikat za kvalifikovani elektronski potpis	nonRepudiation	-
Kvalifikovani sertifikat za kvalifikovani elektronski pečat	nonRepudiation digitalSignature	-
Kvalifikovani sertifikat za kvalifikovani elektronski potpis za fizičko lice u okviru pravnog lica	nonRepudiation	-
Kvalifikovani sertifikat za napredni elektronski pečat i autentifikaciju pravnog lica	nonRepudiation digitalSignature	-
Sertifikat za Timestamp servis	digitalSignature	TimeStamping
Sertifikat za autentifikaciju fizičkog lica	digitalSignature	-
Sertifikat za autentifikaciju fizičkog lica u sklopu pravnog lica	digitalSignature	-

6.2. ZAŠTITA PRIVATNOG KLJUČA I KONTROLE KRIPTOGRAFSKIH MODULA

6.2.1. STANDARDI I KONTROLE KRIPTOGRAFSKIH MODULA

Sve CA operacije za generisanje digitalnih ključeva za potpisivanje i potpisivanje sertifikata vrše se na hardverskom kriptografskom modulu koji zadovoljava sigurnosne standarde FIPS 140-2 Nivoa 3. Privatni ključ koji se koristi za kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat, generiše se i koristi u hardverskom kriptografskom modulu sertifikovanom na osnovu QSCD specifikacije. Privatni ključ vlasnika sertifikata za ostale tipove sertifikata, oslanja se na fizičke i logičke kontrole koje štite računarski sistem vlasnika sertifikata. Odgovornost je vlasnika sertifikata da obezbijedi držanje privatnog ključa u okruženju koje ima dovoljno nivoa fizičke zaštite. U svakom slučaju, preporuka je da vlasnik sertifikata koristi hardverski kriptografski modul (pametna kartica...)

6.2.2. N OD M KONTROLA PRIVATNOG KLJUČA

Kao što je definisano u sekciji 5.2.2 Potreban broj osoba za operativne postupke.

6.2.3. DEPONOVANJE (ESCROW) PRIVATNOG KLJUČA

Coreit CA ne dozvoljava i ne podržava deponovanje privatnog ključa.

6.2.4. SIGURNOSNE KOPIJE PRIVATNOG KLJUČA

Backup CA privatnog ključa se izvršava odmah nakon generisanja. Backup je zaštićen mehanizmom kontrole pristupa i koristeći sigurnosne mehanizme koje omogućava HSM.
Korisnički privatni ključevi za potpisivanje se ne backup-uju od strane Coreit CA.

6.2.5. ARHIVIRANJE PRIVATNOG KLJUČA

Privatni ključevi se ne arhiviraju.

6.2.6. PRENOS PRIVATNOG KLJUČA NA KRIPTOGRAFSKI MODUL

Coreit CA privatni ključ za potpisivanje je generisan u okviru hardverskog sigurnosnog modula (HSM). Privatni ključ za potpisivanje se nikada ne pojavljuje u čitljivom obliku van HSM-a.
Ne postoji zahtjev za prenos korisničkih privatnih ključeva za potpisivanje jer se generišu u okviru kriptografskog modula korisnika.

6.2.7. ČUVANJE PRIVATNOG KLJUČA NA KRIPTOGRAFSKOM MODULU

Coreit CA privatni ključ za potpisivanje se koristi samo na hardverskom sigurnosnom modulu (HSM). CA privatni ključ za potpisivanje može biti sačuvan u enkriptovnoj formi na CA sistemu jedino za potrebe backup-a i oporavka. CA privatni ključ je zaštićen sa hardverskim sigurnosnim modulom (HSM) i jedino se koristi na HSM-u. Master ključ za enkripciju/dekripciju koji se koristi u backup svrhe, zaštićen je pametnim karticama HSM-a i politikom.

6.2.8. NAČIN AKTIVIRANJA PRIVATNOG KLJUČA

Coreit CA privatni ključ za potpisivanje se aktivira tokom startovanja CA aplikacije što zahtijeva HSM lozinku.
Korisnici moraju koristiti PKI klijentsku aplikaciju ili pametne kartice koje aktiviraju privatne ključeve kao dio procesa prijave tokom kojeg se korisnik autentifikuje pomoću lozinke ili PIN-a.

6.2.9. NAČIN DEAKTIVIRANJA PRIVATNOG KLJUČA

Kada se CA aplikacija ugasi, HSM zatvara sesiju i ključevi se deaktiviraju. Korisničke aplikacije moraju deaktivirati privatni ključ kada se korisnik odjavi ili deaktivira (plug-out) kriptografski token.

6.2.10. NAČIN UNIŠTAVANJA PRIVATNOG KLJUČA

Trajno uništavanje CA privatnih ključeva se postiže pozivanjem odgovarajuće HSM operacije brisanja.

6.2.11. REJTING KRIPTOGRAFSKIH MODULA

Pogledaj sekciju 6.2.1 Standardi i kontrole kriptografskih modula.

6.3. OSTALI ASPEKTI UPARAVLJANJA PAROM KLJUČEVA

6.3.1. ARHIVIRANJE JAVNOG KLJUČA

Coreit CA arhivira javne ključeve za verifikaciju potpisa kao što je definisano u sekciji 5.5 Arhiviranje podataka.

6.3.2. ROK VAŽENJA SERTIFIKATA I PERIOD UPOTREBE PARA KLJUČEVA

Periodi korišćenja javnih i privatnih ključeva koje je izdao Coreit CA je sledeći:

- Root CA privatni ključ, javni ključ za verifikaciju potpisa i sertifikat: trideset (30) godina
- Privatni ključ podređenog (Subordinate) CA, javni ključ za verifikaciju potpisa i sertifikat: dvadeset (20) godina
- Privatni ključ krajnjeg entiteta, javni ključ za verifikaciju potpisa i sertifikat: do pet (5) godina

Ove vrijednosti podržavaju specifikaciju svih politika javnog sertifikata. Coreit CA može postaviti kraći period važenja kako bi ispunio posebne zahtjeve aplikacije ili u skladu sa komercijalnim uslovima.

6.4. AKTIVACIJSKI PODACI

6.4.1. GENERISANJE I INSTALACIJA AKTIVACIJSKIH PODATAKA

CA aplikacija (ili RA) generiše aktivacione kodove u softveru i čuva ih u bazi kriptografski zaštićene dok se ne izvrši inicijalizacija korisnika. Brojevi i kodovi su jedinstveni.
Za ključeve koje generišu korisnici lično, svaki korisnik bira svoju lozinku.
Za ključ generisan na QSCD, PIN generiše CA i šalje ga ili predaje korisniku kao dio procesa isporuke kao što je definisano u sekciji 4.1.2 Proces obrade zahtjeva i odgovornosti. Korisnik je obavezan da promijeni lozinku kada prvi put upotrijebi kriptografski token.

6.4.2. ZAŠTITA AKTIVACIJSKIH PODATAKA

Pogledaj sekciju 6.4.1 Generisanje i instalacija aktivacijskih podataka

6.4.3. OSTALI ASPEKTI AKTIVACIJSKIH PODATAKA

Nema odredbi.

6.5. RAČUNARSKE BEZBJEDONOSNE KONTROLE

6.5.1. SPECIFIČNI BEZBJEDONOSNO TEHNIČKI ZAHTJEVI

Coreit CA je implementirao niz tehničkih računarskih bezbijedonosnih kontrola koje koristi CA operativni sistem i CA aplikacija, uključujući:

- Kontrola pristupa CA servisima i PKI ulogama
- Striktna podjela PKI uloga
- Korišćenje pametnih kartica za čuvanje kredencijala CA superadmina
- Enkriptovane sesije između CA aplikacije i korisničke PKI klijentske aplikacije
- Kriptografska zaštita osjetljivih podataka koji se čuvaju u CA (ili RA) bazi
- Revizija sigurnosih događaja

6.5.2. RANGIRANJE NIVOA ZAŠTITE

Operativni sistem hosta i ostali korišćeni proizvodi su gotovi proizvodi dodatno ojačani najboljim IT praksama.

6.6. TEHNIČKE KONTROLE TOKOM UPOTREBE SISTEMA

6.6.1. KONTROLA RAZVOJA SISTEMA

Sve aplikacije i proizvodi koje koristi Coreit CA su komercijalni proizvodi ili *custom* proizvodi napravljeni pod kontrolom i procedurama u skladu sa ISO/IEC 27001 preporukama.

6.6.2. KONTROLA UPRAVLJANJA BEZBJEDNOŠĆU

Coreit CA ima implementirano upravljanje problemima, promjenama i konfiguracijom za sve PKI hardverske i softverske komponente u skladu sa ISO/IEC 27001 preporukama.

6.6.3. KONTROLA BEZBJEDNOSTI TOKOM UPOTREBE SISTEMA

CA testira sve softvere i procedure u kontrolisanim uslovima

6.7. KONTROLA MREŽNE BEZBJEDNOSTI

Coreit CA mreža se sastoji od namjenskog segmenta vezanog za korporativnu TCP/IP mrežu kroz firewall uređaj. Server sa CA aplikacijom je konektovan na taj segment.
Firewall uređaj je iskonfigurisan tako da dozvoljava samo protokole i komande koje su neophodne za pristup CA servisima.

6.8. VREMENSKI PEČAT (TIME-STAMPING)

Datum i vrijeme su dodati svim sistemskim i aplikativnim logovima. Sistemsko vrijeme je sinhronizovano sa više eksternih resursa. Za sinhronizaciju se koristi NTP protokol.

7. SERTIFIKAT, CRL I OCSP PROFILI

7.1. PROFIL SERTIFIKATA

7.1.1. BROJ VERZIJE

Coreit CA izdaje X.509 v3 sertifikate u skladu sa RFC 5280. Koriste se sledeća X.509 osnovna polja:

X.509 ekstenzije	Opis
signature	Potpis sertifikacionog tijela
issuer	Ime sertifikacionog tijela
valid from	Datum aktivacije sertifikata
valid to	Datum isteka sertifikata
subject	Jedinstveno ime korisnika sertifikata
subjectPublicKeyInformation	ID algoritma, ključ
version	X.509 verzija sertifikata, verzija 3
serialNumber	Jedinstveni serijski broj sertifikata

7.1.2. EKSTENZIJE SERTIFIKATA

Koriste se sledeće ekstenzije sertifikata:

X.509 Ekstenzije	Opis
authorityKeyIdentifier	Identifikator javnog ključa CA
subjectKeyIdentifier	Identifikator javnog ključa sertifikata
keyUsage	Kao što je specificirano u sekciji 6.1.7.
extendedKeyUsage	Opcionalno Kao što je specificirano u RFC 5280 u skladu sa specifičnim zahtjevima aplikacije.

privateKeyUsagePeriod	Koristi se samo u sertifikatu za vremenski pečat
certificatePolicies: CertPolicyID CPS URI	Politika sertifikata OID, kao što je specificirano u sekciji 1.2 Naziv dokumenta i identifikacioni podaci
Subject Alternative Name	Alternativno ime korisnika. Može biti i email adresa korisnika.
CRLDistributionPoints	CRL lokacija
basicConstraints	CA=true u CA sertifikatu, CA=false u svim ostalim sertifikatima
Authority Information Access	id-ad-calssuers i id-ad-ocsp u skladu sa RFC 5280
qcStatement	U skladu sa ETSI EN 319 412-5

Oznake vrste sertifikata koje izdaje Coreit CA su mapirani u skladu sa ETSI EN 319 412-5; ETSI EN 319 411-2 (6.6.1) i ETSI EN 319 411-1 na sledeći način:

Kategorija sertifikata	Identifikacija politike sertifikata (OID)	ETSI ekvivalent
Kvalifikovani sertifikat za kvalifikovani elektronski potpis	1.3.6.1.4.1.53673.1.1.1.1.1	ETSI EN 319 411-2 QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD; Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2) Certificates issued under these requirements are aimed to support qualified electronic signatures such as defined in article 3 (12) of the Regulation (EU) No 910/2014 [i.1].

Kvalifikovani sertifikat za kvalifikovani elektronski pečat	1.3.6.1.4.1.53673.1.1.2.1.1	ETSI EN 319 411-2 QCP-l-qscd: certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD; itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3) Certificates issued under these requirements are aimed to support qualified electronic seals such as defined in article 3 (27) of the Regulation (EU) No 910/2014 [i.1].
Kvalifikovani sertifikat za kvalifikovani elektronski potpis za fizičko lice u okviru pravnog lica	1.3.6.1.4.1.53673.1.1.1.2.1	ETSI EN 319 411-2 QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD; Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2) Certificates issued under these requirements are aimed to support qualified electronic signatures such as defined in article 3 (12) of the Regulation (EU) No 910/2014 [i.1].

Kvalifikovani sertifikat za napredni elektronski pečat i autentifikaciju pravnog lica	1.3.6.1.4.1.53673.1.1.2.2.1	ETSI EN 319 411-2 QCP-l: certificate policy for EU qualified certificates issued to legal persons; itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1) Certificates issued under these requirements are aimed to support the advanced electronic seals based on a qualified certificate defined in articles 36 and 37 of the Regulation (EU) No 910/2014 [i.1]. sIDAS: (65) In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers.
Sertifikat za Timestamp servis	1.3.6.1.4.1.53673.1.1.3.1.1	ETSI EN 319 411-1 NCP: Normalized Certificate Policy itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)
Sertifikat za autentifikaciju fizičkog lica	1.3.6.1.4.1.53673.1.1.1.3.1	ETSI EN 319 411-1 NCP: Normalized Certificate Policy itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)

Sertifikat za autentifikaciju fizičkog lica u sklopu pravnog lica	1.3.6.1.4.1.53673.1.1.1.4.1	ETSI EN 319 411-1 NCP: Normalized Certificate Policy itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1) A Normalized Certificate Policy (NCP) which meets general recognized best practice for TSPs issuing certificates used in support of any type of transaction.

7.1.3. IDENTIFIKATORI ALGORITAMSKIH OBJEKATA

Algoritam	Identifikacijska oznaka
RSA Encryption	1.2.840.113549.1.1.1
RSA with SHA-1signature	1.2.840.113549.1.1.5
SHA256 with RSA Encryption	1.2.840.113549.1.1.11

7.1.4. FORME IMENA

Sertifikati koje izdaje Coreit CA sadrže potpuno X.500 jedinstveno ime izdavača i korisnika sertifikata u poljima namijenjenim za izdavača i korisnika. Jedinstvena imena su tesktualna polja u X.501 UTF8 formtu. (Pogledaj sekciju 3.1.4.)

7.1.5. OGRANIČENJA ZA IME

Coreit CA koristi ekstenziju nameConstraints samo u unakrsnim sertifikatima, ako je primjenjivo.

7.1.6. IDENTIFIKATOR OBJEKTA ZA POLITIKU SERTIFIKOVANJA

Svi sertifikati koje je izdao CA sadrže OID politike sertifikata pod kojom se izdao. OID za svaku politiku sertifikata je definsan u sekciji 1.2. Naziv dokumenta i identifikacioni podaci. Mogu biti prisutni dodatni OID-ovi za identifikaciju specifičnih komercijalnih uslova ili ako to zahtijeva posebna aplikacija.

7.1.7. KORIŠĆENJE POLITIKE OGRANIČENJA EKSTENZIJA

Coreit CA koristi ekstenziju policyConstraints samo u unakrsnim sertifikatima, ako je primjenjivo.

7.1.8. SINTAKSA I SEMANTIKA ZA KVALIFIKATORE POLITIKE

Ne koristi se.

7.1.9. PROCESUIRANJE SEMANTIKE ZA KRITIČNE EKSTENZIJE POLITIKE SERTIFIKOVANJA

PKI klijentska aplikacija mora procesuirati ekstenzije označene kao kritične u skladu sa RFC 5280.

7.2. CRL PROFIL

7.2.1. BROJ VERZIJE

CA izdaje CRL u X.509 formatu v2.
Koriste se sledeća osnovna X.509 polja:

X.509 ekstenzija	Opis
Version	V2
Signature	Identifikator algoritma koji se koristi da potpiše CRL
Issuer	CA jedinstveno ime
thisUpdate	Vrijeme izdavanja CRL-a
nextUpdate	Vrijeme izdavanja sledećeg CRL-a
revokedCertificates	Serijski brojevi opozvanih sertifikata

7.2.2. CRL I CRL EKSTENZIJE

X.509 ekstenzije	Opis
CRLNumber	Redni broj CRL-a

reasonCode	Razlog opoziva sertifikata
invalidityDate	Datum kompromitovanja ili sumnje u kompromitovanje privatnog ključa ili datum kada je sertifikat na neki drugi način prestao biti važeći

7.3. OCSP PROFILI

OSCP je definisan u RFC 6960

7.3.1. BROJ VERZIJE

OSCP v1 u skladu sa RFC 6960

7.3.2. OCSP EKSTENZIJE

Ekstenzije u skladu sa RFC 6960 su podržane.

8. REVIZIJA USAGLAŠENOSTI I DRUGE PROCJENE

8.1. UČESTALOST I OKOLNOSTI ZA PROCJENU (REVIZIJU)

Coreit CA tijelo za upravljanje politikama (PMA) je odgovorno za sprovođenje revizija usaglašenosti i za određivanje toga ko ih sprovodi. PMA inicira interni pregled na godišnjoj osnovi.
Eksternu reviziju vrši vladino tijelo prema nacionalnom zakonu koji reguliše elektronsku autentifikaciju i elektronski potpis.

8.2. IDENTITET/KVALIFIKACIJE REVIZORA

Interni revizor će biti iz Coreit doo Podgorica sa odgovarajućim IT znanjem i revizorskim iskustvom.
Interni ili eksterni revizori treba da ispunjavaju sledeće kriterijume:

- Značajno iskustvo u primjeni PKI i kriptografskih tehnologija
- Iskustvo u radu sa CA aplikacijom
- Iskustvo u obavljanju sertifikacionih aktivnosti ili revizija sistema informacionih tehnologija

8.3. REVIZOREVA POVEZANOST SA PREDMETOM PROCJENE (REVIZIJA)

Interni ili eksterni revizor mora biti bez sukoba interesa i nezavistan od CA.

8.4. OBLASTI KOJE POKRIVA PROCJENA (REVIZIJA)

Revizijom se utvrđuje usaglašenost CA servisa sa CPS-om i nacionalnim propisima.

8.5. AKTIVNOSTI KOJE SE PREDUZIMAJU U SLUČAJU NEUSAGLAŠENOSTI

Coreit CA PMA preduzima odgovarajuće mjere za rješavanje nedostataka ili neusklađenosti utvrđenih kao rezultat revizije u dogovorenom vremenskom okviru u zavisnosti od ozbiljnosti rizika koji je uključen.

8.6. OBJAVLJIVANJE REZULTATA PROCJENE (REVIZIJE)

Rezultati revizije se dostavljaju Coreit CA tijelu za upravljanje politikama (PMA).

9. OSTALI POSLOVNI I PRAVNI ASPEKTI

9.1. NAKNADE

9.1.1. NAKNADE ZA IZDAVANJE I OBNOVU SERTIFIKATA

Coreit CA naplaćuje svoje usluge PKI sertifikacije. Cjenovnik je objavljen na CA internet stranici.

9.1.2. NAKNADE ZA PRISTUP SERTIFIKATU

Nije primjenjivo.

9.1.3. NAKNADE ZA OPOZIV ILI PRISTUP INFORMACIJAMA O STATUSU

Pristup informacijama o statusu se ne naplaćuje.

9.1.4. NAKNADE ZA OSTALE USLUGE

Pogledaj sekciju 9.1.1 Naknade za izdavanje i obnovu sertifikata.

9.1.5. POLITIKA REFUNDIRANJA

Podnosioci zahtjeva mogu da otkažu zahtjev za izdavanje sertifikata prije izdavanja aktivacionih kodova bez troškova. Nakon isporuke aktivacionih kodova, izdavanja sertifikata ili isporučivanja uređaja za kreiranje potpisa, naknada se nece vraćati.

9.2. FINANSIJSKA ODGOVORNOST

9.2.1. OSIGURANJE

Coreit CA je definisao politiku osiguranja osnovnog poslovanja u skladu sa Pravilnikom o minimalnom iznosu osiguranja za štetu nastalu pružanjem usluga sertifikacije.

9.2.2. OSTALA SREDSTVA

Nije primjenjivo.

9.2.3. OSIGURANJE ILI GARANCIJE KORISNIKA

Korisnici i treća lica isključivo su odgovorni da obezbijede odgovarajuće osiguranje ili pokriće garancijom u skladu sa korišćenjem sertifikata ili servisa.

9.3. POVJERLJIVOST POSLOVNIH INFORMACIJA

9.3.1. OPSEG POVJERLJIVIH INFORMACIJA

Sve informacije koje je Coreit CA prikupio, generisao, prenio i održavao smatraju se povjerljivim, osim podataka navedenih u sekciji 9.3.2.

9.3.2. INFORMACIJE KOJE NIJESU U OPSEGU POVERLJIVIH INFORMACIJA

Informacije koje su objavljene kao dio Coreit CA sertifikata, CRL-a, Politike sertifikata, uključujući i korisničke sertifikate i druge informacije objavljene u CA javnom repozitorijumu, neće se smatrati povjerljivim.

9.3.3. ODGOVORNOST ZA ZAŠTITU POVJERLJIVIH INFORMACIJA

Coreit CA i RA su odgovorni za zaštitu povjerljivih podataka u skladu sa važećim propisima i Zakonom o zaštiti ličnih podataka.

9.4. PRIVATNOST LIČNIH INFORMACIJA

9.4.1. PLAN PRIVATNOSTI

Bilo koji lični podatak koji daje CA ili RA biće čuvan u skladu sa zahtjevima utvrđenim u Zakonu o zaštiti ličnih podataka. Objavljivanje ovih podataka vršiće se skladu sa Zakonom o zaštiti ličnih podataka ili drugim važećim zakonima.

9.4.2. INFORMACIJE KOJE SE TRETIRAJU KAO LIČNE

Bilo koja informacija o vlasniku sertifikata ili korisniku, a koja nije objavljena u sertifikatu koji je izdao Coreit CA ili CRL-u, smatra se privatnom.

9.4.3. INFORMACIJE KOJE SE NE TRETIRAJU KAO LIČNE

Bilo koja informacija sadržana u Coreit CA sertifikatu, CRL-u, Politici sertifikata/Pravilniku ili druge informacije objavljene u CA javnom repozitorijumu se ne smatraju ličnim.

9.4.4. ODGOVORNOST ZA ZAŠTITU LIČNIH INFORMACIJA

Kako što je utvrđeno u sekciji 9.3.3.

9.4.5. OBAVJEŠTENJE I DAVANJE SAGLASNOSTI ZA KORIŠTENJE LIČNIH INFORMACIJA

Coreit CA koristiće lične informacije isključivo u svrhe za koje je korisnik dao saglasnost tokom postupka registracije.

9.4.6. OTKRIVANJE LIČNIH INFORMACIJA U SKLADU SA SUDSKIM ILI ADMINISTRATIVNOM PROCESOM

Coreit CA će objaviti povjerljive informacije samo zakonodavnim organima u skladu sa važećim zakonodavstvom.

9.4.7. OSTALE OKOLNOSTI KADA SE MOGU OTKRIVATI LIČNE INFORMACIJE

Coreit CA će otkriti privatne podatke samo u okolnostima predviđenim Zakonom o zaštiti ličnih podataka i drugim zakonima, na zahtjev suda ili drugog legitimnog organa vlasti pod uslovom da se zahtjev izdaje na zakonskim osnovama ili ako je korisnik dao pismenu saglasnost.

9.5. PRAVA NA INTELEKTUALNU SVOJINU

Sva prava intelektualne svojine strogo će ostati u posjedu Coreit CA.

9.6. GARANCIJE

9.6.1. GARANCIJE SERTIFIKACIONOG TIJELA

Coreit CA mora izdavati sertifikate, izvršavati ostale procedure vezane za upravljanje sertifikatima, upravljati CA infrastrukturom u skladu sa ovim dokumentom (CPS) i primjenjivim zakonima.
CA je odgovoran za usaglašavanje sa procedurama propisanim u ovoj politici, čak i u slučaju kada pojedinu funkciju sertifikacionog tijela preuzmu pod-ugovorači.
Generalno, Coreit CA obaveze su:

- Da osigura da su podaci o naručiocu i CA-u, koji se nalaze u sertifikatu, tačni
- Da osigura tačnost i integritet informacija objavljenih u javnom repozitorijumu
- Izdavanje sertifikata korisnicima u skladu sa ovom politikom sertifikata
- Opoziv sertifikata koji je izdao CA u skladu sa ovom politikom (CPS)
- Izdavanje i objavljivanje Liste opozvanih sertifikata (CRL) i objavljivnje statusa sertifikata koristeći OCSP servis
- Da osigura da njegovi RA-ovi budu upoznati sa odredbama koje se na njih odnose u ovoj politici sertifikata (CPS)

9.6.2. GARANCIJE REGISTRACIONOG TIJELA

RA je odgovoran za tačnost i potpunost informacija o naručiocima na odobrenim obrascima za prijavu. Detaljnije obaveze RA navedene su u relevantnim djelovima ovog dokumenta (CPS) i ako je primjenjivo, u ugovoru sa eksternim RA.

9.6.3. GARANCIJE KORISNIKA SERTIFIKATA

Prihvatanjem sertifikata koji je izdao Coreit CA, naručilac mora:

- Čuvati privatni ključ za potpisivanje
- Čuvati lozinku i PIN
- Čuvati lozinku za opoziv
- Odmah obavijestiti Coreit CA o bilo kakvoj netačnosti ili promjenama u informacijama sadržanim u sertifikatu
- Koristiti sertifikat u skladu sa zakonskim odredbama i autorizovanim namjenama opisanim u sekciji 1.4. Upotreba sertifikata
- Odmah obavijestiti Coreit CA ukoliko se sumnja ili je detektovano kompromitovanje privatnog ključa
- Odmah obavijestiti Coreit CA o bilo kakvoj zloupotrebi bilo kojeg sertifikata koji je izdao Coreit CA

9.6.4. ODGOVORNOST TREĆIH LICA

Prije oslanjanja na Coreit CA sertifikat, odgovornost trećih lica je da:

- Budu svjesna ograničenja sertifikata i odgovornosti CA kao što je opisano u ovom dokumentu (CPS)
- Ograniče oslanjanja na Coreit CA sertifikate za odgovarajuće potrebe kao što je opisano u sekciji 1.4 Upotreba sertifikata
- Osiguraju da sertifikat nije opozvan pristupajući validnoj i svim drugim važećim listama opozvanih sertifikata (CRLs) ili OCSP
- Odmah obavijeste Coreit CA o bilo kakvoj zloupotrebi bilo kojeg sertifikata izdatog od strane Coreit CA

9.6.5. GARANCIJE OSTALIH UČESNIKA

Bilo koji drugi učesnici obavezni su da koriste sertifikate i ponašaju se u skladu sa ovim dokumentom (CPS) i važećim zakonima.

9.7. IZUZEĆA GARANCIJA

Izuzev garancija izričito navedenih u poglavlju 9.6.1 i ostalim poglavljima ove Politike i u mjeri kojom je to dozvoljeno važećim zakonom (vidi 9.14), CA servis isključuje odgovornost za indirektnu štetu, izgubljen profit, izgubljene, uništene ili nepristupačne podatke, gubitak reputacije ili dobre volje, troškove i potraživanja nastala korišćenjem CA servisa za sertifikaciju i povezanih ključeva.
Coreit CA isključuje svu odgovornost i garancije i ne odgovara za štetu:

- Ako je digitalni sertifikat korišćen nakon isteka
- Ako nije bilo provjere statusa podataka i validnosti sertifikata u registru opozvanih sertifikata (CRL ili OCSP) prilikom korišćenja digitalnog sertifikata
- Ako je digitalni sertifikat korišćen nakon opoziva i objavljivanja u registru opozvanih sertifikata (CRL ili OCSP)
- Ako su podaci u digitalnom sertifikatu na bilo koji način izmijenjeni
- Za upotrebu sertifikata sa netačnim podacima zbog promjena (npr. Elektronska adresa, imena, prezimena ili drugih podataka vlasnika)
- Ako se dogodila zloupotreba, upad u informacioni sistem vlasnika sertifikata ili trećih lica, a samim tim i informacija o sertifikatima od strane neovlašćenih lica
- Ako je vlasnik otkrio privatni ključ ili se sumnja da je to uradio
- Ako se digitalni sertifikat ne koristi u skladu sa ograničenjima koja su utvrđena u ovoj politici ili važećem zakonu (vidjeti 9.14.)
- Ako vlasnik ili treća osoba nisu postupili u skladu sa ovom politikom ili bilo kojim povezanim ugovorom
- Ako je oštećenje prouzrokovano neispravnošću hardvera ili softvera vlasnika ili trećeg lica
- Ako je šteta nastala usled više sile kako je opisano u poglavlju 9.16.5
- Ako je šteta nastala kao rezultat dešavanja van kontrole Coreit CA uključujući raspoloživost ili rad interneta, telekomunikacija ili RA sistema, uključujući opremu i programe

9.8. OGRANIČENJA ODGOVORNOSTI

Coreit CA je dužan da na propisan način izdaje kvalifikovane elektronske sertifikate i odgovoran je za štetu pričinjenu licu koje se pouzdalo u taj sertifikat u skladu sa ovim pravilnikom, propisima iz ove oblasti kao i ugovoru zaključenom između Coreit CA i korisnika. Coreit CA nije odgovoran za bilo kakvu štetu koja je nastala zbog nepridržavanja korisnika sertifikata ili trece strane sa uslovima

definisanim u ovom dokumentu (CPS), zakonskim propisima iz ove oblasti i ugovoru zaključenim između Coreit CA i korisnika.
Coreit CA isključuje svu odgovornost i garancije i ne odgovara za štetu:

- Ako je digitalni sertifikat korišćen nakon isteka
- Ako nije bilo provjere statusa podataka i validnosti sertifikata u registru opozvanih sertifikata (CRL ili OCSP) prilikom korišćenja digitalnog sertifikata
- Ako je digitalni sertifikat korišćen nakon opoziva i objavljivanja u registru opozvanih sertifikata (CRL ili OCSP)
- Ako su podaci u digitalnom sertifikatu na bilo koji način izmijenjeni
- Za upotrebu sertifikata sa netačnim podacima zbog promjena (npr. Elektronska adresa, imena, prezimena ili drugih podataka vlasnika)
- Ako se dogodila zloupotreba, upad u informacioni sistem vlasnika sertifikata ili trećih lica, a samim tim i informacija o sertifikatima od strane neovlašćenih lica
- Ako je vlasnik otkrio privatni ključ ili se sumnja da je to uradio
- Ako se digitalni sertifikat ne koristi u skladu sa ograničenjima koja su utvrđena u ovoj politici ili važećem zakonu (vidjeti 9.14.)
- Ako vlasnik ili treća osoba nisu postupili u skladu sa ovom politikom ili bilo kojim povezanim ugovorom
- Ako je oštećenje prouzrokovano neispravnošću hardvera ili softvera vlasnika ili trećeg lica
- Ako je šteta nastala usled više sile kako je opisano u poglavlju 9.16.5.
- Ako je šteta nastala kao rezultat dešavanja van kontrole Coreit CA uključujući raspoloživost ili rad interneta, telekomunikacija ili RA sistema, uključujući opremu i programe

9.9. OBEŠTEĆENJA

Svaka strana snosi isključivu odgovornost za obeštećenja drugih strana za gubitke ili štetu nastalu kao rezultat neovlašćenog korišćenja sertifikata, neadekvatne upotrebe sertifikata ili nepostupanja u skladu sa ovim dokumentom (CPS), ugovorom i važećim zakonima.

9.10. ROK I PREKID

9.10.1. ROK

Coreit CA politika sertifikata / Pravilnik i drugi dokumenti postaju efektivni pošto ih je odobrio Coreit CA PMA i objavio na internet stranici kao što je opisano u sekciji 2.1 Repozitorijumi

9.10.2. PREKID

Coreit CA CPS nije vremenski ograničena. Trenutna verzija je na snazi do objavljivanja nove verzije.

9.10.3. EFEKTI ZAVRŠETKA I PONOVNOG RADA

Nakon prekida važenja CPS-a kao rezultat postavljanja nove verzije, sertifikat treba da se koristi u skladu sa verzijom CPS-a koja je bila aktivna na datum izdavanja sertifikata. U slučaju da će se okolnosti promijeniti u mjeri u kojoj to nije moguće, Coreit CA će obavijestiti korisnike kao što je opisano u poglavlju 9.12.2. Mehanizmi obavještavanja i vremenski periodi, a treća lica putem internet stranice kao što je definisano u poglavlju 2.1. Repozitorijumi.

9.11. INDIVIDUALNO OBAVJEŠTAVANJE I KOMUNIKACIJA SA UČESNICIMA

Coreit CA distribuira trenutnu verziju ovog CPS-a i trenutnu verziju svih ostalih javnih dokumenata putem svoje internet stranice opisane u poglavlju 2.1 Repozitorijumi.
Takođe, pogledajte poglavlje 9.12.2 Mehanizmi obavještavanja i vremenski periodi.

9.12. IZMJENE

9.12.1. PROCEDURA ZA IZMJENU

Coreit CA osoblje može svoje komentare direktno poslati pismeno ili putem e-maila na adresu navedenu u poglavlju 1.5.2 Kontakt podaci.

9.12.2. MEHANIZMI OBAVJEŠTAVANJA I VREMENSKI PERIODI

Coreit CA tijelo za upravljanje politikama može odlučiti da ne obavještava korisnike i treća lica u slučaju izmjena sa malim ili nikakvim uticajem. Coreit CA tijelo odlučuje o tome da li izmjene imaju bilo kakav uticaj na korisnike i treća lica, na sopstvenu odgovornost.
Sve CPS izmjene biće objavljene kao što je opisano u poglavlju 2. Objave i odgovornosti repozitorijuma. Coreit CA će obavijestiti korisnike o promjenama koje imaju uticaj na njih, putem e-maila i treća lica putem internet stranice.

9.12.3. OKOLNOSTI POD KOJIMA OID MORA BITI PROMIJENJEN

OID za tipove sertifikata će se promijeniti u slučaju da promjene imaju uticaj na korisnike ili treća lica.

9.13. RJEŠAVANJA U SLUČAJU SPORA

Svi sporovi u vezi sa sertifikatima moraju biti proslijeđeni Coreit CA-u na adresu definisanu u sekciji 1.5.2 Kontakt podaci. Spor treba riješiti pregovaranjem ako je moguće. Spor koji nije riješen pregovaranjem, biće riješen na sudu u Podgorici, Crna Gora.

9.14. PRIMJENA ZAKONA

Ovaj CPS i odnosi između CA, RA, korisnika, subjekata (vlasnika sertifikata) i bilo kog trećeg lica podliježu i tumače se u skladu sa nacionalnim zakonima.

9.15. USAGLAŠENOST SA PRIMJENLJIVIM ZAKONIMA

- Zakon o zaštiti podataka o ličnosti
- Zakon o elektronskoj identifikaciji i elektronskom potpisu
- Ostali propisi iz ove oblasti

9.16. RAZNE ODREDBE

9.16.1. CJELOKUPNI UGOVOR

Coreit CA CPS i Coreit CA ugovor obuhvataju sve relevantne elemente koji definišu odnos između Coreit CA i vlasnika sertifikata.

9.16.2. PRENOS PRAVA

Korisnicima ili vlasnicima sertifikata nije dozvoljeno da prava i obaveze koji proističu iz ovog ugovora u cijelosti ili parcijalno prenesu na treća lica po bilo kom osnovu.

9.16.3. KLAUZULA O VALJNOSTI

Nevalidnost jednog ili više djelova ovog dokumeta ne treba da utiču na validnost ostalih odredbi, pod uslovom da nemaju uticaj na materijalne odredbe (povjerenje u sertifikat i upotreba sertifikata).

9.16.4. IZVRŠENJE (NADOKNADE ZA PRAVNOG ZASTUPNIKA I ODRICANJE OD PRAVA)

Nema odredbi.

9.16.5. VIŠA SILA

Višu silu predstavljaju vanredne okolnosti i nepredvidive situacije kao što su prirodne katastrofe, terorizam, nedostatak napajanja ili prekid telekomunikacionih veza, požar, nepredvidivi incidenti kao što su virusi ili napadi sa ciljem onemogućavanja servisa, greške u kriptografskim algoritmima...

9.17. OSTALE ODREDBE

9.17.1. USKLAĐENOST SA MEĐUNARODNIM STANDARDIMA

Coreit doo Podgorica ima uspostavljan sistem menadžmenta u skladu as ISO 9001:2015 i ISO/IEC 27001:2013. Pored navedenih, u u procesu davanja usluga sertifikovanja, poslovanje Coreit CA je usklađeno sa sledećim međunarodnim standardima:

ETSI EN 319 401 General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI EN 319 412-1 Certificate Profiles; Part 1: Overview and common data structures
ETSI EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI EN 319 412-3 Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
ETSI EN 319 412-5 Certificate Profiles; Part 5: QCStatements
ETSI TS 119 312 Cryptographic Suites
ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing ElectronicTime-Stamps
ETSI EN 319 422 Time stamping protocol and electronic time-tamp profiles
RFC 2580 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
RFC 6960 X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP.