



POLITIKA CERTIFIKACIJE ZA INFORMATIČKE RESURSE

- verzija 0.2 -

Radna verzija dokumenta

Standardni SSL certifikat za server
OID Politike (1.3.6.1.4.1.19124.10.1.1.2.3.1.1)

Standardni certifikat za agenta zaštite
OID Politike (1.3.6.1.4.1.19124.10.1.1.2.3.1.1)

Standardni certifikat za e-mail agenta zaštite
OID Politike (1.3.6.1.4.1.19124.10.1.1.2.3.1.1)

e-mon d.o.o.
Bul. Sv. Petra Cetinjskog 3
81000 Podgorica

SADRŽAJ

1. UVOD	4
1.1 Pregled	5
1.2 Identifikacija	5
1.3 Okruženje i primjenljivost politike	5
1.3.1 e-mon CA	5
1.3.2 e-mon CA i partneri	6
1.3.3 e-mon CA i Registraciona tijela	6
1.3.4 Korisnici	7
1.3.5 Treće strane	7
1.3.6 Odgovarajuće korišćenje certifikata	8
1.3.7 Definicije	8
1.3.8 Kontaktni detalji	11
2. OPŠTE ODREDBE	12
2.1 Obaveze	12
2.1.1 e-mon CA obaveze	12
2.1.2 e-mon RA obaveze	13
2.1.3 e-mon LRA obaveze	13
2.1.4 Korisničke obaveze	13
2.1.5 Obaveze trećih strana	15
2.1.6 Obaveze vezane za repozitorijum	15
2.2 Odgovornost	15
2.3 Finansijska odgovornost	16
2.4 Interpretacija i sprovođenje	17
2.4.1 Zakon koji se poštuje	17
2.4.2 Procedure rješavanja sporova	17
2.5 Cijene	17
2.6 Objavljivanje i repozitorijumi	17
2.7 Provjera saglasnosti rada u skladu sa ovom politikom	18
2.8 Politika zaštite informacija	18
2.9 Prava intelektualnog vlasništva	19
3. IDENTIFIKACIJA I AUTENTIKACIJA KORISNIKA	20
3.1 Inicijalna registracija	20
3.2 Rutinsko obnavljanje ključeva	21
3.3 Obnavljanje ključeva nakon povlačenja	21
3.4 Zahtjev za povlačenje certifikata	21
4. OPERATIVNI ZAHTJEVI	23
4.1 Aplikacija za dobijanje certifikata	23
4.2 Izdavanje certifikata	23
4.3 Prihvatanje certifikata	24
4.4 Povlačenje certifikata	24
4.5 Procedure bezbjednosnih provjera/auditing	25
4.6 Arhiviranje zapisa	25
4.7 Izmjena ključeva	26
4.8 Kompromitacija i oporavak u slučaju katastrofa	26
4.9 Završetak rada CA ili RA	26

5. FIZIČKE, PROCEDURALNE I KADROVSKE BEZBJEDNOSNE KONTROLE	28
5.1 Fizičke bezbjednosne kontrole	28
5.2 Proceduralne kontrole.....	28
5.3 Kadrovske bezbjednosne kontrole.....	29
5.3.1 Kvalifikacija i iskustvo	29
5.3.2 Procedura provjere biografije	29
5.3.3 Zahtjevi za obučenošću	29
5.3.4 Ponovna obuka	29
5.3.5 Rotacija poslova	29
5.3.6 Kaznene mere u odnosu na zaposlene	29
5.3.7 Kontrole nezavisnih ugovarača	29
5.3.8 Dokumentacija za inicijalnu obuku i ponvnu obuku	30
6. TEHNIČKE BEZBJEDNOSNE KONTROLE	31
6.1 Generisanje i instalacija asimetričnog para ključeva.....	31
6.1.1 Proces generisanja privatnog ključa e-mon CA	31
6.1.2 Generisanje ključa e-mon CA	31
6.1.3 Uređaji za generisanje ključeva e-mon CA	31
6.1.4 Čuvanje privatnog ključa e-mon CA.....	32
6.1.5 Distribucija privatnog ključa e-mon CA	33
6.1.6 Uništavanje privatnog ključa e-mon CA	33
6.2 Zaštita privatnog ključa	33
6.3 Neki aspekti upravljanja parom ključeva	34
6.4 Aktivacioni podaci.....	34
6.5 Bezbjednosne kontrole računara.....	34
6.6 Bezbjednosne kontrole životnog ciklusa	34
6.7 Mrežno bezbjednosne kontrole.....	34
6.8 Kontrole inženjeringa kriptografskih modula.....	34
7. PROFILI CERTIFIKATA I CRL LISTE	35
7.1 Profil certifikata.....	36
7.2 Profil CRL liste.....	37
8. ADMINISTRIRANJE POLITIKE	38

1. UVOD

Certifikaciono tijelo izdaje kvalifikovane elektronske certifikate tako što formira elektronski potpis certifikata na osnovu svog privatnog ključa i asimetričnog kriptografskog algoritma. U tako formiranom elektronskom certifikatu, sertifikaciono tijelo se identifikuje kao izdavač kvalifikovanog elektronskog certifikata, u skladu sa Zakonom o elektronskom potpisu.

Certifikaciono tijelo prije početka rada utvrđuje Opšta pravila pružanja usluge certifikacije koja korisnicima obezbjeđuju dovoljno informacija na osnovu kojih se mogu odlučiti o prihvatanju usluga i o obimu usluga. Certifikaciono tijelo ugrađuje pomenuta Opšta pravila u dva osnovna dokumenta koji su dostupni javnosti:

1. Politika certifikacije (Certificate Policy) i
2. Praktična pravila pružanja usluge Certifikacije (Certification Practices Statement) (u daljem tekstu: Praktična pravila).

Pomenuta dokumenta se zasnivaju na sljedećim principima, i to:

1. Politika certifikacije definiše predmet rada sertifikacionog tijela dok Praktična pravila definišu procese i način njihovog korišćenja pri formiranju i upravljanju elektronskim certifikatima. Politika certifikacije definiše zahtjeve poslovanja sertifikacionog tijela dok Praktična pravila definišu operativne procedure u cilju ispunjenja tih zahtjeva. Praktična pravila definišu način na koji sertifikaciono tijelo ispunjava tehničke, organizacione i proceduralne zahtjeve poslovanja koji su identifikovani u Politici certifikacije.
2. Politika certifikacije i Praktična pravila su javni dokumenti.
3. Politika certifikacije je manje specifičan i detaljan dokument u odnosu na Praktična pravila koja predstavljaju mnogo detaljniji opis načina poslovanja, kao i poslovne i operativne procedure koje sertifikaciono tijelo primenjuje u izdavanju i upravljanju kvalifikovanim elektronskim certifikatima.
4. Politika certifikacije se definiše nezavisno od specifičnog operativnog okruženja sertifikacionog tijela, dok Praktična pravila daju detaljan opis organizacione strukture, operativnih procedura, kao i fizičko i računarsko okruženje sertifikacionog tijela.

Ovaj materijal predstavlja Politiku certifikacije (u daljem tekstu CP – Certificate Policy) e-mon Certifikacionog tijela (u daljem tekstu e-mon CA) za potrebe informatičkih resursa pravnih i fizičkih lica u Crnoj Gori.

e-mon CA izdaje sljedeće vrste certifikata za informatičke resurse pravnih i fizička lica:

- Standardni SSL certifikat za server,
- Standardni certifikat za agenta zaštite,
- Standardni certifikat za e-mail agenta zaštite.

Ova CP je u saglasnosti sa formalnim zahtjevima navedenim u dokumentu IETF RFC 2527 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, u odnosu na format i sadržaj. Međutim, ni na koji način se ne garantuje puna kompatibilnost ovog dokumenta sa RFC 2527 dokumentom.

e-mon C primjenjuje periodične evaluacije u cilju osiguravanja saglasnosti sa zahtjevima iz akreditacionih šema koje su navedene u Poglavlju 8 ove CP.

1.1 Pregled

Ova CP je namijenjena stvaranju uslova za pružanje certifikacionih usluga od strane e-mon CA, Podgorica. Ova CP se može primijeniti na sva certifikaciona tijela koja se baziraju na Pexim CA tehnologiji.

1.2 Identifikacija

Identifikacioni podaci e-mon CA su:

e-mon d.o.o.
e-mon CA
Bul. Sv. Petra Cetinjskog 3
81000 Podgorica
Crna Gora
www.emonca.com

Jedinstveno ime: **OU=e-mon CA, O=e-mon, C=CG.**

Certifikati koji se izdaju u okviru ove Politike imaju sljedeće oznake:

- **Standardni SSL certifikat za server**
OID Politike (1.3.6.1.4.1.19124.10.1.1.2.3.1.1)
- **Standardni certifikat za agenta zaštite**
OID Politike (1.3.6.1.4.1.19124.10.1.1.2.3.1.1)
- **Standardni certifikat za e-mail agenta zaštite**
OID Politike (1.3.6.1.4.1.19124.10.1.1.2.3.1.1)

1.3 Okruženje i primjenljivost politike

Svrha ove CP je da, prije svega, opiše odgovornosti i prava CA (izdavač certifikata), RA (identifikator korisnika), i korisnika (korisnik – vlasnik certifikata). Kao dio ove CP, opisane su procedure koje e-mon CA sprovodi u procesu izdavanja certifikata.

1.3.1 e-mon CA

Certifikaciono tijelo je organizacija koja izdaje elektronske certifikate. e-mon CA Podgorica je CA. e-mon CA je odgovorna za izdavanje ove politike u cilju izdavanja

određenih tipova elektronskih certifikata e-mon CA je takođe i autoritet koje izdaje odgovarajuće politike. U tom smislu, ova CP, kao i pridruženi dokument e-mon CA CPS (Certificate Practice Statement), predstavljaju odgovarajuće politike i pravila koja se primjenjuju pri izdavanju e-mon CA elektronskih certifikata.

U cilju objavljivanja trećim stranama informacija koje se odnose na opozvane certifikate, neophodno je da se izvrši odgovarajuća publikacija liste povučenih certifikata (CRL – Certificate Revocation List). e-mon CA objavljuje takvu listu.

1.3.2 e-mon CA i partneri

e-mon CA je hijerarhijski CA sistem koji podržava jedan ili više nivoa podređenih CA, uključujući CA za svaku banku u sistemu elektronskog bankarstva, kao i za bilo koje CA za koje e-mon CA pruža outsourcing certifikacione usluge. Naime, e-mon CA podržava implementaciju certifikacionih servisa i drugim CA, kao trećim stranama, u skladu sa odgovarajućim dogovorenim uslovima. U okviru datog certifikacionog okruženja, takva CA predstavljaju podređena CA u okviru e-mon CA hijerarhije. Međutim, ova tijela moraju da pružaju nivo servisa koji je ekvivalentan nivou koje e-mon CA obezbjeđuje. U tom smislu, sprovodi se odgovarajuća procedura akreditacije, kontrole i primjene odgovarajućih procedura u kojima e-mon CA provjerava sposobnost datog CA treće strane da izdaje elektronske certifikate u skladu sa ovom CP.

U okviru e-mon CA PKI hijerarhije, certifikaciono tijelo – treća strana niže hijerarhije izdaje elektronske certifikate na bazi sljedećih odnosa sa e-mon CA:

- Kao e-mon CA partner,
- e-mon CA je provjerilo i analiziralo praktična pravila i procedure rada datog certifikacionog tijela (uključujući Politiku certifikacije i/ili CPS – Certificate Practice Statement),
- Direktno vrši aktivnosti u okviru e-mon CA hijerarhije.

Ova CP se primjenjuje na upravljanje cjelokupnom hijerarhijom e-mon CA i odnosi se na sve entitete koji koriste e-mon CA certifikacione usluge. Određena ograničenja primjenljivosti ove CP se mogu pojaviti kao rezultat odgovarajućih legalnih ili ugovornih obaveza.

1.3.3 e-mon CA i Registraciona tijela

e-mon CA pristupa svojim korisnicima putem mreže registracionih tijela (centralno RA i LRA). Ova registraciona tijela mogu biti:

- e-mon CA, kao centralno RA, za banke i treće strane za koje e-mon CA pruža outsourcing usluge registracionog tijela.
- Banke kao LRA za potrebe servisnog centra za elektronsko bankarstvo kao i za druge potrebe izdavanja certifikata,
- Treće strane kao LRA kojima e-mon CA pruža outsourcing usluge certifikacionog tijela.

Ova tijela interaktivno komuniciraju i sa korisnicima i sa e-mon CA u cilju isporuke certifikacionih usluga krajnjim korisnicima. e-mon CA registraciona tijela:

- Prihvataju, analiziraju, potvrđuju ili odbijaju registraciju odgovarajućih zahtjeva za certifikatima (aplikacije za certifikate).
- Registruju korisnike za korišćenje e-mon CA certifikacionih usluga.
- Sprovode sve korake u proceduri identifikacije korisnika kao što je definisano od strane e-mon CA i u skladu sa tipom certifikata koji se izdaje.
- Koriste službene i ovjerene dokumente u cilju provjere korisnikove aplikacije.
- Nakon potvrde aplikacije korisnika, obavještavaju na odgovarajući način e-mon CA u cilju izdavanja certifikata.
- Iniciraju proces povlačenja i zahtijevaju povlačenje certifikata od strane e-mon CA.

e-mon CA registraciona tijela djeluju lokalno u okviru njihovog sopstvenog konteksta geografskog ili poslovnog partnerstva koje je potvrđeno i autorizovano od strane e-mon CA. e-mon CA registraciona tijela djeluju u skladu sa praksom, procedurama i osnovnim dokumentima rada e-mon CA. Ne postoji ograničenje na broj registracionih tijela koja mogu biti pridružena e-mon CA. e-mon CA obezbjeđuje svojim registracionim tijelima neophodnu tehnologiju i know-how u cilju dobijanja visokog nivoa obučenosti u skladu sa e-mon CA akreditacionim zahtjevima.

1.3.4 Korisnici

Korisnici e-mon CA usluga su pravna i fizička lica koja koriste certifikacione usluge za potrebe svojih informatičkih resursa. Korisnici su strane koje:

- Apliciraju za dobijanje certifikata,
- Identifikovani su u certifikatu,
- Posjeduju privatni ključ koji odgovara javnom ključu koji je naveden u korisnikovom certifikatu.

1.3.5 Treće strane

Treće strane su entiteti, kao na primjer fizička lica (pojedinci i/ili pravna lica (kompanije)), koja prihvataju certifikate i verifikuju elektronski potpis korisnika na bazi javnog ključa koji se nalazi u korisnikovom certifikatu.

U cilju provjere validnosti primijenjenog elektronskog certifikata, treće strane moraju uvek da provjere status povučenosti datog certifikata u okviru e-mon CA CRL liste prije nego što prihvate informacije koje su navedene u certifikatu.

1.3.6 Odgovarajuće korišćenje certifikata

e-mon CA certifikati se mogu koristiti za većinu transakcija elektronskog poslovanja i elektronske trgovine, kao i u transakcijama mobilne trgovine koje se baziraju na upotrebi elektronskih certifikata. U takve transakcije spadaju:

- Transakcije elektronskog bankarstva,
- Bankarske transakcije građana - home banking,
- Elektronska pošta,
- Elektronski ugovori,
- Pristup bezbjednim web sajtovima (SSL autentikacija) i drugim on-line sadržajima,
- Elektronsko potpisivanje dokumenata u elektronskom obliku,
- Šifrovanje i dešifrovanje dokumenata u elektronskom obliku, itd.

1.3.7 Definicije

Ovaj dokument koristi sljedeće definicije:

Aktivacioni podaci – Vrijednosti podataka, koji nijesu ključevi, koji su zahtijevani u cilju rada kriptografskih modula koji moraju biti zaštićeni (kao na primjer PIN, passphrase, ili manuelno razmjenjivanje ključeva).

CA certifikat – Certifikat za jedno CA (za jedan javni ključ CA sa odgovarajućim podacima) izdat (digitalno potpisan) od strane drugog CA ili samopotpisan.

Politika certifikacije – Imenovan skup pravila koji indicira primjenljivost certifikata na određeno okruženje i/ili na klasu aplikacija sa zajedničkim bezbjednosnim zahtjevima. Na primjer, određena politika certifikacije može indicirati primjenljivost odgovarajućeg tipa certifikata za autentikaciju transakcija razmjene elektronskih podataka za trgovanje robom u okviru datog opsega cijena.

Put certifikata – Uređena sekvenca certifikata koja se, zajedno sa javnim ključem inicijalnog objekta u putu, procesira u cilju provjere istog u posljednjem objektu na putu.

Certification Practice Statement (CPS) – Javna izjava o praktičnim pravilima i procedurama koje certifikaciono tijelo primjenjuje u proceduri izdavanja certifikata.

Certifikaciono tijelo – izdavač certifikata (issuing CA) – U kontekstu određenog certifikata, certifikaciono tijelo – izdavač certifikata je ono CA koje je izdalo (digitalno potpisalo) certifikat.

Kvalifikator politike – Informacija koja zavisi od politike i koja je pridružena identifikatoru politike certifikacije u okviru X.509 certifikata.

Registraciono tijelo (RA) – Entitet koji je odgovoran za identifikaciju i autentikaciju korisnika/vlasnika certifikata ali koje ne izdaje i ne potpisuje certifikat (tj. RA vrši odgovarajuće poslove (identifikaciju korisnika) i u tom smislu je delegirano od CA). Često se i termin LRA (Local Registration Authority) koristi u istom kontekstu.

Treća strana – Primalac certifikata koji provjerava dati certifikat i/ili provjerava digitalni potpis dobijenog elektronskog dokumenta primjenom javnog ključa potpisnika iz certifikata. Treća strana može biti takođe korisnik certifikata izdatog od strane istog certifikacionog tijela ali i ne mora.

Skup pravila – Kolekcija praktičnih pravila i/ili stavova u politikama u cilju korišćenja za izražavanje definicija u politici certifikacije ili CPS.

Certifikaciono tijelo – subjekt (subjekt CA) – U kontekstu određenog CA certifikata, subjekt CA je ono CA čiji javni ključ je certifikovan u okviru datog certifikata.

Elektronski dokument – Dokument u elektronskom obliku koji se koristi u pravnom prometu, upravnim, sudskim i drugim postupcima, a uključuje sve oblike pisanog i drugog teksta, podatke, slike, crteže, karte, zvuk, muziku, govor, računarske baze podataka i sl.

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

Napredni elektronski potpis – Elektronski potpis kojim se pouzdano garantuje identitet potpisnika i integritet elektronskih dokumenata.

Potpisnik – Lice koje posjeduje sredstva za izradu elektronskog potpisa kojim se potpisuje u svoje ime ili u ime fizičkog ili pravnog lica koje predstavlja.

Podaci za izradu elektronskog potpisa – Jedinstveni podaci, kao što su kodovi ili privatni kriptografski ključevi, koje potpisnik koristi za izradu elektronskog potpisa.

Sredstva za izradu elektronskog potpisa – Odgovarajuća računarska oprema ili računarski program koje potpisnik koristi pri izradi elektronskog potpisa, uz korišćenje podataka za izradu elektronskog potpisa.

Podaci za provjeru elektronskog potpisa – Podaci kao što su kodovi ili javni kriptografski ključevi koji se koriste za provjeru elektronskog potpisa.

Sredstva za provjeru elektronskog potpisa – Odgovarajuća računarska oprema ili program koji se koriste za provjeru elektronskog potpisa.

Elektronski certifikat – Potvrda u elektronskom obliku koja povezuje podatke za provjeru elektronskog potpisa sa nekim licem i potvrđuje identitet tog lica.

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

Aplikacija za certifikat - Zahtjev poslat od strane korisnika koji zahtijeva certifikat (aplikant) ka Certifikacionom tijelu u cilju izdavanja elektronskog certifikata.

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

Autentikacija – Proces koji se koristi u cilju potvrđivanja identiteta lica ili u cilju dokazivanja integriteta odgovarajuće specifične informacije putem njihovog postavljanja u ispravan kontekst i verifikacijom takvog odnosa.

Autorizacija – Procedura dodjeljivanja prava i određivanja koja prava u datom informacionom sistemu dati korisnik ima.

Isticanje certifikata – Kraj perioda validnosti elektronskog certifikata.

Ekstenzije u certifikatu – Dodatna polja u certifikatu, pored osnovnih, koja daju bliže informacije o vlasniku (korisniku) i izdavaču (CA) certifikata, kao i o procesu certifikacije.

Hijerarhija certifikata – Sekvenca certifikata bazirana na nivoima koja ima jedan root CA certifikat i subordinate/intermediate entitete, kao što su drugi CA i korisnici.

Upravljanje certifikatima – Aktivnosti pridružene upravljanju certifikatima uključuju čuvanje, isporuku, objavljivanje i povlačenje certifikata.

Lista povučenih certifikata (CRL – Certificate Revocation List) – Lista izdata i elektronski potpisana od strane CA koja uključuje povučene certifikate, kao i razloge njihovog povlačenja. Takva lista se mora koristiti od strane trećih strana uvijek kada treba provjeriti validnost certifikata i/ili verifikaciju elektronskog potpisa.

Serijski broj certifikata – Sekvencijalni broj koji jedinstveno identifikuje certifikat u domenu datog CA.

Zahtjev za dobijanje certifikata (CSR – Certificate Service Request) – Standardna forma (po PKCS#10 preporuci) koja se koristi za slanje zahtjeva za dobijanjem certifikata.

Certifikacija – Proces izdavanja elektronskog certifikata.

Asimetrični par ključeva (key pair) – Privatni ključ i javni ključ, kao matematički par datom privatnom ključu za potrebe rada asimetričnog kriptografskog algoritma, kao što je na primjer RSA algoritam.

Privatni ključ – Matematički kod koji se koristi kao ključ za kreiranje elektronskog potpisa i, u kombinaciji sa javnim ključem, za raspakivanje digitalne envelope - dešifrovanje simetričnog ključa kojim je šifrovan dokument za datog korisnika primjenom asimetričnog kriptografskog algoritma.

Javni ključ – Matematički kod koji može biti javno objavljen i koji se koristi za verifikaciju elektronskog potpisa, kreiranog pomoću odgovarajućeg privatnog ključa koji je matematički par sa datim javnim ključem, kao i za šifrovanje podataka za korisnika koji posjeduje odgovarajući privatni ključ.

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

Repozitorijum – Baza podataka i/ili direktorijum na kome su publikovani osnovni dokumenti rada CA, kao i eventualne druge informacije koje se odnose na pružanje certifikacionih usluga od strane datog CA (kao na primjer publikacija svih izdatih certifikata, itd.).

Povlačenje certifikata – Permanentno ukidanje validnosti datog certifikata i njegovo smještanje na CRL listu.

Dijeljena tajna – Dio kriptografske tajne koja je podijeljena na unapred definisan broj fizičkih tokena, kao na primjer smart kartica.

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

Korisnički ugovor – Ugovor između korisnika i CA u cilju obezbjeđenja certifikacionih usluga.

1.3.8 Kontaktne detalji

e-mon CA Podgorica ima registrovane kancelarije u:

e-mon d.o.o.
e-mon CA
Bul. Sv. Petra Cetinjskog 3
81000 Podgorica
Crna Gora
www.emonca.com

2. OPŠTE ODREDBE

2.1 Obaveze

e-mon CA garantuje da će sprovoditi sve procedure definiisane u ovoj CP. e-mon CA koristi korisnički ugovor, ovu CP i CPS u cilju sprovođenja legalnih uslova korišćenja e-mon CA sertifikata od strane korisnika i trećih strana.

Učesnici u čitavoj PKI infrastrukturi koji imaju odgovarajuće obaveze uključuju CA, RA, korisnike, treće strane i druge učesnike.

2.1.1 e-mon CA obaveze

Do nivoa specificiranog u odgovarajućim poglavljima ove CP, e-mon CA garantuje:

- Saglasnost sa ovom CP i svim njenim dodacima u vrijeme kada se publikuju.
- Obezbjediavanje infrastrukture i certifikacionih usluga, uključujući uspostavu i održavanje e-mon CA repozitorijuma i odgovarajućeg web sajta u cilju pružanja certifikacionih usluga.
- Obezbjediavanje sigurnih mehanizama koji uključuju mehanizme generisanja ključa, zaštite ključa, kao i procedure dijeljenja tajni u skladu sa svojom sopstvenom PKI infrastrukturom.
- Obezbjediavanje promptnog obavještanja u slučaju kompromitacije njegovog sopstvenog privatnog ključa.
- Obezbjediavanje i validacija aplikacionih procedura za različite tipove sertifikata koje su javno raspoložive.
- Izdavanje elektronskih sertifikata u skladu sa ovom CP i ispunjavanje njegovih obaveza.
- Obavještanje korisnika putem e-mail poruka da su certifikati generisani za njih i kako korisnici mogu da preuzmu certifikate.
- Obavještanje aplikanta ako e-mon CA nije sposobno da validuje korisničku aplikaciju za dobijanje sertifikata u skladu sa ovom CP.
- Nakon prijema zahtjeva od strane RA koje radi u okviru e-mon CA mreže promptno izdaje e-mon CA sertifikat u skladu sa ovom CP.
- Povlačenje sertifikata koji su izdati u skladu sa ovom CP nakon prijema validnog zahtjeva za povlačenje sertifikata od strane autorizovanog lica koje može da zahtijeva povlačenje.
- Objavljivanje izdatih sertifikata u skladu sa ovom CP.
- Obezbjediavanje podrške korisnicima i trećim stranama kao što je opisano u ovoj CP.
- Obezbjediavanje isticanja i obnavljanja sertifikata u skladu sa ovom CP.
- Regularno objavljivanje CRL liste u skladu sa ovom CP.

- Obavještanje trećih strana o statusu povučenosti certifikata putem publikovanja CRL lista na e-mon CA repozitorijumu.
- Dostavljanja kopije ove CP i ostalih primjenjivih politika po zahtjevu.

e-mon CA potvrđuje da ono nema drugih obaveza po ovoj CP.

2.1.2 e-mon RA obaveze

e-mon RA se obavezuje na:

- Prijem aplikacija za izdavanje e-mon CA certifikata u skladu sa ovom CP.
- Izvršavanje svih aktivnosti na verifikaciji i provjeri autentičnosti aplikanata u skladu sa opisom e-mon CA procedura i ove CP.
- Dostavljanje zahtjeva aplikanata e-mon CA u potpisanoj poruci (zahtjev za izdavanjem certifikata).
- Zapisivanje svih aktivnosti u žurnalu događaja.
- Prijem, verifikaciju i prosleđivanje ka e-mon CA svih zahtjeva za povlačenjem e-mon CA izdatih certifikata u skladu sa e-mon CA procedurama i ovom CP.
- Verifikaciju pouzdanosti i autentičnosti informacija dostavljenih od strane korisnika u vrijeme obnavljanja certifikata u skladu sa ovom CP.

2.1.3 e-mon LRA obaveze

e-mon LRA se obavezuje na:

- Prijem aplikacija za izdavanje e-mon CA certifikata u skladu sa ovom CP.
- Izvršavanje svih aktivnosti na verifikaciji i provjeri autentičnosti aplikanata u skladu sa opisom e-mon CA procedura i ove CP.
- Dostavljanje zahtjeva aplikanata e-mon CA u potpisanoj poruci (zahtjev za izdavanjem certifikata).
- Zapisivanje svih aktivnosti u žurnalu događaja.
- Prijem, verifikaciju i prosleđivanje ka e-mon CA svih zahtjeva za povlačenjem e-mon CA izdatih certifikata u skladu sa e-mon CA procedurama i ovom CP.
- Verifikaciju pouzdanosti i autentičnosti informacija dostavljenih od strane korisnika u vrijeme obnavljanja certifikata u skladu sa ovom CP.

2.1.4 Korisničke obaveze

Sem ako nije drugačije definisano u ovoj CP, korisnici su odgovorni za:

- Imanje odgovarajućih znanja i, ako je neophodno, pohađanje odgovarajuće obuke za korišćenje elektronskih certifikata i certifikacionih usluga.
- Bezbjedno generisanje njihovog asimetričnog para ključeva i, ukoliko ih generišu sami, korišćenjem bezbjednih sistema.

- Obezbeđivanje korektnih i preciznih informacija u njihovoj komunikaciji sa e-mon RA i CA.
- Osiguranje da javni ključ dostavljen do e-mon CA na certifikaciju odgovara privatnom ključu koji će se koristiti.
- Osiguranje ispravnosti javnog ključa dostavljenog do e-mon CA na certifikaciju.
- Generisanje novog asimetričnog para ključeva koji će se koristiti sa pridruženim certifikatom koji se zahtijeva od strane e-mon CA.
- Upoznavanje, razumevanje i saglasnost sa svim stavovima i uslovima u ovoj CP i drugim pridruženim politikama koje su objavljene na e-mon CA repozitorijumu, uključujući CPS.
- Uzdržavanje od narušavanja integriteta i proizvodnja e-mon CA izdatog certifikata neispravnim.
- Korišćenje e-mon CA certifikata samo za legalne i autorizovane svrhe u skladu sa ovom CP.
- Obavješćavanje e-mon CA ili e-mon RA o bilo kojim promjenama informacija koje su ranije dostavljene.
- Prekid korišćenja e-mon CA izdatog certifikata ukoliko je bilo koja informacija u certifikatu postala nevalidna.
- Prekid korišćenja e-mon CA izdatog certifikata ukoliko sam certifikat postane nevalidan.
- Odstranjivanje serverskog certifikata koji je nevalidan iz bilo koje aplikacije i/ili bilo kog uređaja gde je bio instaliran.
- Korišćenje samo jednog certifikata za elektronski potpis u datom trenutku.
- Uzdržanje od korišćenja svog privatnog ključa koji odgovara javnom ključu koji je certifikovan od strane e-mon CA izdatog certifikata pod istim imenom za potrebe izdavanja drugih certifikata.
- Razumno korišćenje e-mon CA izdatog certifikata pod različitim okolnostima.
- Sprečavanje kompromitacije, gubljenja, objavljivanja, modifikacije ili bilo kog drugog neautorizovanog korišćenja svog privatnog ključa.
- Korišćenje bezbjednih uređaja i proizvoda koji obezbjeđuju odgovarajuću zaštitu njihovih privatnih ključeva.
- Za bilo koje aktivnosti i propuste partnera ili agenata u smislu generisanja, zadržavanja, odlaganja, ili uništavanja bilo kog privatnog ključa.
- Uzdržavanje od dostavljanja do e-mon CA ili bilo kog e-mon CA direktorijuma bilo kakvog materijala koji sadrži stavove koji ugrožavaju bilo koji zakon ili bilo koje pravo bilo koje strane.
- Zahtijevanje povlačenja certifikata u slučaju događaja koji materijalno utiče na integritet e-mon CA izdatog certifikata.
- Na odgovarajući način nadzire rad agenata ili partnera koji su aplicirali za korišćenje e-mon CA u ime korisnika.

- Kontrolisanje podataka koje agenti dostavljaju do e-mon CA i obavještanje e-mon CA o bilo kojim pogrešnim tumačenjima i propustima načinjenim od strane agenta.

2.1.5 Obaveze trećih strana

Strana koja se oslanja na e-mon CA izdati certifikat je obavezna da:

- Ima odgovarajuća znanja o korišćenju elektronskih certifikata i drugih tehnologija vezanih za usluge certifikacije.
- Primi obavještenje u vezi e-mon CA CP i pridruženih uslova koji važe za treće strane.
- Verifikuje e-mon CA izdati certifikat primjenom između ostalog i CRL liste (e-mon CA CRL) i u skladu sa procedurom validacije certifikacionog puta.
- Vjeruje u e-mon CA izdati certifikat samo ukoliko se sve informacije koje se odnose na takav certifikat mogu verifikovati da su korektne i ažurne.
- Razumno osloni i pouzda na e-mon CA izdati certifikat u skladu sa odgovarajućim okolnostima.

2.1.6 Obaveze vezane za repozitorijum

Strane u komunikaciji (uključujući korisnike i treće strane) koje pristupaju e-mon CA repozitorijumu i web sajtu u potpunosti su saglasne sa odredbama ove CP, kao i bilo kojim drugim uslovima korišćenja koje je e-mon CA mogao učiniti dostupnim. Strane u komunikaciji demonstriraju prihvatanje uslova korišćenja navedenih u ovoj CP dostavljanjem upita vezanih za status elektronskih certifikata ili bilo kojim drugim načinom koji pokazuje korišćenje ili oslanjanje na obezbijedene informacije ili usluge. e-mon CA repozitorijum uključuje ili sadrži:

- Mogućnost pretrage u cilju pronalaženja izdatog elektronskog certifikata.
- Verifikaciju statusa elektronskog potpisa koji je kreiran korišćenjem privatnog ključa koji odgovara javnom ključu koji je uključen u certifikat.
- Informacije publikovane na e-mon CA web sajtu (ova CP, CPS, korisnički ugovor, itd.).
- Bilo koje druge usluge koje e-mon CA može reklamirati ili obezbijediti putem svog web sajta.

e-mon CA čini sve u svojoj moći u cilju osiguranja da strane koje pristupaju njegovom repozitorijumu dobijaju pouzdane, ažurne i tačne informacije. e-mon CA, međutim, ne može prihvatiti bilo kakvu odgovornost koja je van ograničenja definisanih u ovoj CP.

2.2 Odgovornost

e-mon CA ne prihvata bilo kakvu drugu odgovornost osim one koja je eksplicitno opisana u ovom dokumentu. e-mon CA ne može da prihvati odgovornost za bilo kakve konsekvence prouzrokovanim ovom CP, certifikatima izdatim u skladu sa ovom CP,

certifikatima izdatim od strane e-mon CA uopšte, aktivnostima izvršenih korišćenjem ovih certifikata, kao i za korišćenje ovih certifikata od strane organizacija i/ili pojedinaca, ili od bilo čega drugog što nije eksplicitno opisano u ovom dokumentu.

Ni u kom slučaju (izuzev zloupotrebe ili namjere) e-mon CA nije odgovorno za:

- Bilo kakav gubitak profita.
- Bilo kakav gubitak podataka.
- Bilo koju indirektnu, slučajnu ili kaznenu štetu koja je prouzrokovana ili je vezana za korišćenje, isporuku, licencu, performance ili neperformanse certifikata ili elektronskih potpisa.
- Bilo koju transakciju ili uslugu ponuđenu ili u okviru obuhvata ove CP.
- Bilo koju drugu štetu izuzev onih koje potiču od opravdanog oslanjanja na verifikovane informacije koje se nalaze u izdatom certifikatu.
- Bilo koju odgovornost koja se pojavila u slučaju greške u verifikovanim informacijama koja je rezultat greške, zloupotrebe ili namjere aplikanta.

2.3 Finansijska odgovornost

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

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

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

- Bilo kojeg lažnog ili pogrešno prezentovanog podatka dostavljenog od strane korisnika ili njihovih agenata.
- Bilo kojeg propusta korisnika da dostavi materijalnu činjenicu da je pogrešna prezentacija ili propust učinjen iz nemarnosti ili sa namjerom da se prevari e-mon CA, ili bilo koje lice koje prima i odnosi se prema dobijenom certifikatu.
- Neobezbjedivanja odgovarajuće zaštite korisnikovog privatnog ključa. Korišćenja bezbjednog sistema kako je zahtijevano, ili neizvršenja odgovarajućih preventivnih mera neophodnih da se sprieči kompromitacija, gubitak, objavljivanje, modifikacija ili neautorizovano korišćenje korisnikovog privatnog ključa ili napada na integritet e-mon CA Root privatnog ključa.
- Kršenja bilo kojih zakona koji su primjenljivi, uključujući one koji se odnose na zaštitu intelektualnih prava, viruse, pristup računarskim sistemima, itd.

2.4 Interpretacija i sprovođenje

Ovo poglavlje sadrži sve primjenljive odredbe koje se odnose na interpretaciju i sprovođenje ove politike certifikacije, obrađujući teme kao što su:

- Zakon koji se poštuje,
- Procedure za rešavanje sporova.

2.4.1 Zakon koji se poštuje

Ova CP je izdata u potpunosti u skladu sa odgovarajućom zakonskom regulativom države Crne Gore. Sve pravne stvari koje se odnose na e-mon CA i/ili koji se odnose na certifikate izdate od strane e-mon CA će biti procesuirani od strane odgovarajućeg suda u Crnoj Gori.

2.4.2 Procedure rješavanja sporova

e-mon CA se referiše na arbitražu u cilju rješavanja svih sporova koji se odnose na ovu CP. Ako se spor ne riješi u okviru deset (10) dana nakon inicijalnog obavještenja shodno pravilima CP, strane u sporu dostavljaju spor na arbitražu. Arbitraža se sastoji od 3 arbitra, svaka strana predlaže po jednog, dok trećeg predlažu zajedno obje strane u sporu. Mjesto za arbitražu je Podgorica, Crna Gora, a arbitri određuju sve pridružene troškove. Za sve sporove koji se odnose na tehnologiju, kao i sporove koji se odnose na samu CP, strane u sporu prihvataju arbitražno tijelo koje će biti izabrano od strane vlade Crne Gore.

2.5 Cijene

e-mon CA naplaćuje korisniku korišćenje e-mon CA izdatih certifikata. e-mon CA zadržava prava da mijenja cijene svojih certifikata.

Objavljivanje cijena certifikata i drugih certifikacionih usluga se vrši putem web sajta e-mon CA, partnera e-mon CA (banke i treća lica) ili putem odgovarajućeg ugovora tamo gdje je to primjenljivo.

2.6 Objavljivanje i repozitorijumi

e-mon CA publikuje informacije u vezi elektronskih certifikata koje izdaje na on-line repozitorijumu. e-mon CA zadržava pravo da publikuje statusne informacije o certifikatima i na repozitorijumu neke treće strane.

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

Participanti u certifikacionim uslugama su obaviješteni da će e-mon CA možda publikovati informacije koje su oni dostavili na javno pristupačnim direktorijumima uz pridružene statusne informacije o elektronskim certifikatima.

Iz razloga njihove osjetljivosti, e-mon CA se uzdržava od publikacije internih pravila rada koji se odnose na izvjesne podkomponente i elemente koji uključuju izvjesne bezbjednosne kontrole, procedure koje se odnose na registraciona tela, root signing proceduru, itd.

e-mon CA publikuje statusne informacije o digitalnim certifikatima u određenim intervalima, kako je to naznačeno u njegovom CPS dokumentu.

e-mon CA održava raspoloživim pristup do svog javnog repozitorijuma trećim stranama sa svrhom validacije samog e-mon CA certifikata. e-mon CA može ograničiti ili zabraniti pristup određenim njegovim uslugama, kao što su publikovanje statusnih informacija o bazama podataka treće strane, pristup određenim privatnim direktorijumima, itd.

Dok je pristup e-mon CA repozitorijumu i direktorijumima besplatan, e-mon CA zadržava pravo da naplaćuje usluge za određena specifična korišćenja ove i drugih politika.

2.7 Provjera saglasnosti rada u skladu sa ovom politikom

e-mon CA prihvata periodični audit/provjeru saglasnosti svojih politika, uključujući ovu CP. Rad e-mon CA je takođe u saglasnosti sa najvažnijim međunarodnim i Evropskim standardima u ovoj oblasti, kao i sa Evropskom direktivom 99/93 o elektronskim potpisima. U domenu izdavanja elektronskih serifikata, e-mon CA radi u okviru ograničenja definisanim u okviru Zakona o elektronskom potpisu države Crne Gore.

e-mon CA prihvata pod određenim uslovima i provjeru/auditing internih procedura i pravila rada koja nisu javno dostupna. e-mon CA evaluira rezultate ovakvih provjera prije nego što ih implementira.

2.8 Politika zaštite informacija

e-mon CA se pridržava pravila zaštite privatnosti personalnih podataka i pravila povjerljivosti kako je opisano u CPS dokumentu.

e-mon CA ne objavljuje niti se od njega zahtijeva da objavljuje bilo koju povjerljivu informaciju bez autentikovanog i potvrđenog zahtjeva od strane:

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

e-mon CA može naplatiti odgovarajuću administrativnu cijenu za obradu ovakvih objavljivanja.

Strane koje zahtijevaju i dobijaju povjerljive informacije imaju dozvolu za to na osnovu pretpostavke da će oni te informacije koristiti za zahtijevane svrhe, da će ih osigurati od kompromitacije, i da će se uzdržavati od njihovog korišćenja i objavljivanja trećim stranama.

e-mon CA i njegovi partneri čine raspoloživom specifičnu politiku privatnosti u cilju zaštite personalnih podataka aplikanta koji zahtijeva izdavanje certifikata od strane e-mon CA ili njegovog partnera putem njihovih web sajtova i/ili CP ili CPS dokumenata.

2.9 Prava intelektualnog vlasništva

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

3. IDENTIFIKACIJA I AUTENTIKACIJA KORISNIKA

e-mon CA održava dokumentovana praktična pravila i procedure u cilju autentikacije identiteta i/ili drugih atributa aplikantata/krajnjih korisnika e-mon CA certifikata što se izvršava pre izdavanja certifikata.

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

e-mon CA autentikuje zahtjeve strana koje žele da povuku certifikate u skladu sa ovom politikom.

e-mon CA održava odgovarajuće procedure u cilju određivanja praktičnih pravila za dodjeljivanje imena, uključujući i prepoznavanje trademark prava u izvjesnim imenima.

U cilju identifikacije korisnika, e-mon CA sprovodi odgovarajuća pravila dodjeljivanja imena i identifikacije koja uključuje tipove imena pridruženih subjektu, kao na primer X.500 distinguished imena.

Kada aplicira za e-mon CA certifikat, ime aplikanta mora biti u potpunosti sa odgovarajućim značenjem sem ako to nije eksplicitno dozvoljeno u relevantnom proizvodnom opisu i u e-mon CA CPS dokumentu. e-mon CA izdaje certifikate aplikantima koji dostavljaju dokumentovane aplikacije koje sadrže ime koje se može verifikovati.

Izvjesni tipovi certifikata, kao što su certifikati izdati u skladu sa Evropskom direktivom 99/93 mogu, međutim, biti izdati i uz korišćenje pseudonima koji je povezan sa prvim imenom koje e-mon CA čuva u svojoj arhivi.

e-mon CA ne izdaje anonimne certifikate korisnicima.

Imena pridružena korisnicima certifikata su jedinstvena u domenu e-mon CA pošto se uvek koriste zajedno sa serijskim brojem certifikata.

e-mon CA ne prihvata trademark oznake, logo ili drugi grafički ili tekstualni material koji je zaštićen od kopiranja a uključen je u njegove certifikate.

3.1 Inicijalna registracija

U cilju realizacije procedure identifikacije i autentikacije za inicijalnu korisnikovu registraciju za svaki tip subjekta (CA, RA, korisnik, ili drugi participant) e-mon CA sprovodi sljedeće korake:

- Korisnik identifikovan u polju subjekta mora dokazati posjedovanje asimetričnog privatnog ključa koji odgovara javnom ključu koji treba da bude certifikovan od strane e-mon CA. Takav odnos može biti dokazan na primjer

putem elektronskog potpisa u zahtjevu za izdavanjem certifikata (samopotpisani zahtjev).

- Zahtjevi e-mon CA u smislu identifikacije i autentikacije organizacija koje su aplicirale za e-mon CA izdate certifikate, uključuju ali nisu ograničene na konsultovanje određenih baza podataka treće strane koje jednoznačno identifikuju organizaciju ili provjerom dokumenata o udruživanju date organizacije.
- Organizacije koje apliciraju za e-mon CA certifikate uključuju ali nisu ograničene na druge CA (treće strane), RA, korisnike pravna lica (u slučaju da su certifikati izdati samim organizacijama ili informatičkim resursima kontrolisanim od strane te organizacije), ili drugi kompanijski participanti.

U cilju identifikacije i autentikacije za individualnu korisničku organizaciju koja aplicira za e-mon CA certifikat (CA, RA, korisnik (u slučaju certifikata izdatih organizacijama ili informatičkim resursima kontrolisanim od strane organizacije) ili drugi participanti), e-mon CA može primijeniti korake koji uključuju ali nisu ograničeni na:

- Kontrolisanje dokumenata kao što su identifikacione kartice, pasoš, vozačka dozvola,
- Autentikacijom identiteta organizacije ili pojedinca koja se bazira na dostavljenoj dokumentaciji.
- U slučaju određenih klasa certifikata, zahtjev je da se pojedinac fizički pojavi u e-mon RA u odgovarajućoj fazi prijave nego što se certifikat izda.
- Primjenjujući dodatne zahtjeve za organizaciju aplikanta kao što su potpisani autorizacioni dokumenti (ovlašćenja) ili neka druga identifikaciona oznaka organizacije.

Kada e-mon CA uključuje informaciju koja indicira određeni autoritet kao što su specifična prava, ovlašćenja, ili dozvole uključujući dozvolu da realizuje odgovarajuće aktivnosti u ime date organizacije da dobije certifikat, e-mon CA može zahtijevati specijalnu pismenu dozvolu od strane date organizacije.

3.2 Rutinsko obnavljanje ključeva

Poglavlje nije primjenljivo.

3.3 Obnavljanje ključeva nakon povlačenja

Poglavlje nije primjenljivo.

3.4 Zahtjev za povlačenje certifikata

U cilju sprovođenja procedura identifikacije i autentikacije za potrebe zahtjeva za povlačenje certifikata za odgovarajuće tipove subjekata (CA, RA, korisnik i drugi



participanti), e-mon CA zahtijeva korišćenje on-line autentikacionog mehanizma (autentikacija putem digitalnog certifikata, putem PIN broja, putem autorizacionog koda, itd.) i zahtjevi se upućuju odgovarajućem e-mon RA. e-mon RA sprovodi takve zahtjeve do e-mon CA u cilju realizacije procedure povlačenja serifikata.

4. OPERATIVNI ZAHTJEVI

Za sva certifikaciona tijela, subordinate/intermediate (subject) certifikaciona tijela, registraciona tijela, korisnike ili druge participante postoji stalna obaveza da informišu e-mon CA o svim promjenama u informacijama koje su objavljene u certifikatu za čitav period operativnog rada takvog certifikata. Određene druge obaveze se takođe mogu dodatno primijeniti.

4.1 Aplikacija za dobijanje certifikata

Aplikanti za dobijanje certifikata imaju odgovornost da obezbijede pouzdane informacije u njihovim aplikacijama za dobijanje certifikata.

Što se tiče aplikacije za izdavanje korisnikovog certifikata, e-mon CA zahtijeva da aplikant korisnik bude njegov pravni predstavnik koji će podnijeti aplikaciju za certifikat.

Korisnici sprovode enrolment process sa e-mon CA ili njegovim partnerom koji zahtijeva:

- Popunjavanje aplikacione forme.
- Generisanje asimetričnog para ključeva.
- Isporuku generisanog javnog ključa, koji odgovara privatnom ključu iz asimetričnog para ključeva, do e-mon CA na certifikaciju.
- Demonstriranje e-mon CA certifikacionom tijelu da aplikant posjeduje privatni ključ koji odgovara javnom ključu koji je dostavio do e-mon CA.
- Prihvatanje korisničkog ugovora.

Nakon prijema aplikacije datog korisnika, e-mon CA ili RA vrše definisanu identifikacionu i autentikacionu proceduru u cilju validacije aplikacije za izdavanje certifikata.

Nakon toga, e-mon CA ili RA ili potvrđuju ili odbijaju aplikaciju za izdavanje certifikata. Takvo potvrđivanje ili odbijanje ne mora neophodno da bude obrazloženo aplikantu ili bilo kojoj drugoj strani.

e-mon CA mora da izvrši aktivnosti i procesira aplikaciju za izdavanje certifikata u okviru vremenskog perioda od sedam (7) radnih dana.

4.2 Izdavanje certifikata

Nakon dostavljanja aplikacije za izdavanje certifikata ili zahtjeva za obnavljanje certifikata e-mon RA potvrđuje ili odbija dostavljene informacije.

Nakon potvrđivanja dostavljenih informacija u aplikaciji za izdavanje certifikata, e-mon RA potvrđuje ili odbija aplikaciju za izdavanje certifikata.

Nakon potvrđivanja aplikacije za izdavanje certifikata, e-mon RA nakon toga šalje zahtjev za izdavanje certifikata do e-mon CA.

4.3 Prihvatanje certifikata

Izdati e-mon CA certifikat se smatra prihvaćenim od strane korisnika ukoliko se bilo koji od dole navedenih uslova ispuni:

- Potvrda prijema poslata elektronskm poštom,
- Korišćenje standardne on-line forme gde je to moguće primijeniti,
- Korišćenje certifikata prvi put,
- Petnaest (15) dana nakon izdavanja.

Bilo koja primjedba na prihvatanje izdatog certifikata mora biti eksplicitno dostavljena do e-mon CA, kao certifikacionom tijelu – izdavaču. Potvrda odbijanja koja uključuje sva polja u certifikatu koja sadrže pogrešne informacije mora takođe biti dostavljena.

4.4 Povlačenje certifikata

Nakon odgovarajućeg zahtjeva od strane e-mon RA, e-mon CA vrši povlačenje izdatog elektronskog certifikata u sljedećim slučajevima:

- Desio se gubitak, krađa, modifikacija, neautorizovano objavljivanje ili neka druga kompromitacija privatnog ključa subjekta certifikata.
- Subjekt certifikata je narušio materijalne obaveze koje su definisane ovom CP ili u CPS dokumentu.
- Izvršenje odgovarajućih obaveza lica koja su navedena u ovoj CP kasni ili je sprečeno usled prirodne katastrofe, računarskog ili komunikacionog otkaza, ili usled drugog uzroka koji izlaze van kontrole datog lica, i kao rezultat, informacije o drugom licu su materijalno ugrožene ili kompromitovane.
- Desila se promjena određenih informacija koje se sadrže u certifikatu datog lica.

Korisnik mora u bilo koje vrijeme, ako se desi neki od gore pomenutih događaja, da kontaktira e-mon RA u cilju zahtjeva za povlačenjem. Pomenuti kontakt može biti on-line ili puten nekih nedigitalnih kanala. e-mon CA povlači certifikat promptno nakon verifikacije identiteta strane koja je zahtijevala povlačenje i potvrdom da je zahtjev podnet u skladu sa procedurom zahtijevanom u ovoj CP, kao i u CPS dokumentu. Verifikacija identiteta može biti izvršena na osnovu informacionih elemenata koji su sadržani u identifikacionim podacima koje je korisnik dostavio do e-mon RA. Nakon ispunjenja pomenutih uslova, e-mon CA izvršava promptnu aktivnost u cilju povlačenja certifikata.

Treće strane moraju koristiti on-line resurse koje e-mon CA čini raspoloživim putem repozitorijuma u cilju provjere statusa certifikata na koje oni žele da se oslone. e-mon CA CRL se često ažurira pri čemu se svako ažuriranje dešava jednom dnevno.

Treće strane moraju biti u saglasnosti sa e-mon CA politikom a posebno da obavezama trećih strana publikovanim u ovoj CP ili CPS dokumentu.

Nakon povlačenja certifikata, period operativnog rada datog certifikata se istovremeno smatra završenim.

U cilju nesmanjenja kapaciteta korisnika elektronskih certifikata da vrše elektronski potpis, aproksimativno trideset (30) dana pre isticanja validnosti elektronskog certifikata, e-mon CA čini razumne napore da obavijesti korisnike putem elektronske pošte ili na neki drugi način, u vezi bliskog isticanja njihovog elektronskog certifikata.

4.5 Procedure bezbjednosnih provjera/auditing

Procedure audit logovanja uključuju logovanje događaja i auditing sistema, implementirane za svrhu održavanja bezbjednog okruženja. U tom smislu, e-mon CA implementira sljedeće kontrole:

- e-mon CA zapisuje događaje koji uključuju ali nisu ograničeni na operacije vezane za životni ciklus certifikata, pokušaje pristupa sistemu, kao i zahtjeve poslate sistemu.
- e-mon CA čuva audit logove u realnom vremenu, koji se kasnije procesiraju i arhiviraju na sedmičnom nivou. U slučaju alarma ili incidentnog događaja, administrator mreže se obavještava.
- Audit logovi se mogu videti od samo strane autorizovanog osoblja, uključujući Oficira bezbjednosti.
- e-mon CA implementira procedure backup-a audit logova.

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

e-mon CA ralizuje s vremena na vrijeme procjenu ranjivosti sistema.

4.6 Arhiviranje zapisa

Zahtjevi za čuvanjem zapisa se primjenjuju kako na e-mon CA tako i na RA. Opšte politike čuvanja zapisa e-mon CA uključuju sljedeće:

- Tipove zapisa – e-mon CA čuva na bezbjedan način zapise o e-mon CA izdatim elektronskim certifikatima, audit podacima, informacije o aplikacijama za izdavanje certifikata, kao i dokumentaciju o samim aplikacijama za izdavanje certifikata.

- Period čuvanja – e-mon CA čuva na bezbjedan način pomenute zapise o e-mon CA elektronskim certifikatima za period koji je naznačen u e-mon CA CPS dokumentu.
- Zaštita arhive – uslovi za zaštitu arhive uključuju:
 - Samo zapise koje administratori (zaposleni kojima su pridružene dužnosti čuvanja podataka) mogu da vide i arhiviraju.
 - Zaštita u odnosu na modifikaciju arhive, kao što je čuvanje podataka na medijumu na koga se može upisati samo jednom.
 - Zaštita u odnosu na brisanje arhive.
 - Zaštita u odnosu na kvarenje medijuma na kojima se arhiva čuva, kao na primer realizacija zahtjeva da se podaci periodično migriraju na svježije medijume.
- Procedure u cilju dobijanja i verifikacije arhivskih informacija – U cilju dobijanja i verifikacije arhivskih informacija e-mon CA i RA održavaju zapise pod jasnom hijerarhijskom kontrolom i sa jasnim opisom posla. e-mon CA čuva zapise u elektronskoj ili papirnoj formi. e-mon CA može zahtijevati od svojih RA, korisnika ili njihovih agenata da dostave odgovarajuća dokumenta u cilju podrške ovog zahtjeva. Ovi zapisi mogu biti čuvani u elektronskoj, papirnoj i u bilo kojoj drugoj formi za koju e-mon CA smatra da je odgovarajuća. e-mon CA može da izmijeni način čuvanja zapisa ako je to eventualno potrebno da bude u saglasnosti sa određenim akreditacionim šemama.

4.7 Izmjena ključeva

Ovo poglavlje nije primjenljivo.

4.8 Kompromitacija i oporavak u slučaju katastrofa

U posebnom internom dokumentu, e-mon CA dokumentuje procedure koje treba izvršiti pri rješavanju incidenata i izveštavanja u vezi sa kompromitacijom. e-mon CA dokumentuje procedure oporavka koje se koriste ukoliko su računarski resursi, softver, i/ili podaci neispravni ili se sumnja da su neispravni.

e-mon CA teži da ponovo uspostavi bezbjedno okruženje u koracima koji uključuju, ali nisu ograničeni samo na, povlačenje neispravnih, ili se sumnja da su neispravni, certifikata entiteta. Nakon toga, e-mon CA može ponovo izdati novi certifikat datom entitetu.

Plan kontinualnog poslovanja je implementiran u e-mon CA u cilju da osigura nastavak poslovanja nakon prirodne ili druge katastrofe.

4.9 Završetak rada CA ili RA

Prije nego što prekine svoje aktivnosti pružanja certifikacionih usluga, e-mon CA:

- Obezbjeđuje svojim korisnicima koji imaju validne certifikate informaciju o nameri da prestane pružanje certifikacione usluge, tj. da prestane da izvršava aktivnosti CA.
- Povlači sve certifikate koji su još uvek validni (tj. one koji nisu povučeni ili im je istekao rok važnosti) na kraju perioda obavještavanja bez zahtjeva za saglasnošću korisnika.
- Blagovremeno obavještava o povlačenju certifikata sve korisnike na koje se to odnosi.
- Čini razumne mjere u cilju zaštite zapisa koje čuva uskladu sa ovom CP.
- Ukoliko je to moguće, obezbjeđuje odgovarajuće mjere obezbjeđenja sukcesije u smislu ponovnog izdavanja certifikata od strane CA koje je sukcesor – nastavljač izdavanja certifikata – i koje poštuje isti CP dokument.

5. FIZIČKE, PROCEDURALNE I KADROVSKE BEZBJEDNOSNE KONTROLE

Ovo poglavlje opisuje netehničke bezbjednosne kontrole koje se koriste od strane e-mon CA u cilju realizacije funkcija generisanja ključeva, autentikacije subjekta, izdavanja certifikata, povlačenja certifikata, audita i arhiviranja.

5.1 Fizičke bezbjednosne kontrole

e-mon CA implementira fizičke kontrole u svojim prostorijama uključujući sljedeće:

- e-mon CA bezbjedne prostorije su locirane u prostoru koji odgovara za potrebe operacija visoke bezbjednosti. Postoje označene zone i zaključane kancelarije sa odgovarajućim sefovima.
- Fizički pristup je ograničen implementacijom odgovarajućih mehanizama kontrole pristupa iz jedne u drugu zonu bezbjednosti, kao i u zonu visoke bezbjednosti. U tom smislu, CA operacije su locirane u okviru bezbjedne računarske sobe koja je podržana fizičkim monitorisanjem i bezbjednosnim alarmima, kao i da je obezbijedena podrška da prelazak iz zone u zonu može biti izveden samo korišćenjem tokena i listi kontrole pristupa.
- Napajanje i ventilacija se izvršavaju sa redundansom visokog nivoa.
- Prostorije su zaštićene od poplava.
- Prevencija i zaštita, kao i mere u odnosu na zaštitu od požara su implementirane.
- Medijumi se čuvaju na bezbjedan način. Backup medijumi se takođe čuvaju na odvojenoj lokaciji koja je fizički obezbijedena i zaštićena od požara i poplava.
- Iznošenje smeća se takođe kontroliše.

5.2 Proceduralne kontrole

e-mon CA sprovodi kadrovsku i upravljačku praksu koja obezbjeđuje razumnu sigurnost u povjerljivost i kompetenciju zaposlenih, kao i zadovoljavajuće performance u vezi sa njihovim dužnostima u domenu tehnologija koje se odnose na elektronski potpis.

Svaki zaposleni e-mon CA potpisuje izjavu da će se pridržavati pravne regulative u vezi zaštite podataka, kao i da će zadovoljiti sve postavljene zahtjeve u vezi sa povjerljivošću.

Svi zaposleni u e-mon CA koji izvršavaju operacije upravljanja ključeva: administratori, oficiri bezbjednosti i sistem auditori, kao i bilo koje druge operacije koje materijalno utiču na takve operacije, se smatraju dužnostima na povjerljivim pozicijama.

e-mon CA sprovodi inicijalno istraživanje svih zaposlenih koji su kandidati za povjerljive uloge u cilju razumnog pokušaja određivanja njihove povjerljivosti i kompetencije.

Tamo gde se zahtijeva dualna kontrola, potrebno je da najmanje dva povjerljiva zaposlena e-mon CA iskažu njihova podijeljena znanja u cilju omogućavanja izvršenja tekućih operacija.

5.3 Kadrovske bezbjednosne kontrole

5.3.1 Kvalifikacija i iskustvo

e-mon CA izvršava provjere u cilju uspostave zahtijevane biografije, kvalifikacija, kao i iskustva neophodnog u cilju realizacije u okviru konteksta kompetencije specifičnog posla. Takve provjere biografije tipično uključuju:

- Kriminalne osude za ozbiljne zločine,
- Pogrešnu prezentaciju informacija od strane kandidata,
- Odgovarajuće reference.

5.3.2 Procedura provjere biografije

e-mon CA realizuje relevantne provjere eventualnih zaposlenih na bazi statusnih izvještaja koji su izdati od strane kompetentnih autoriteta, izjava trećih strana ili izjava samih potencijalnih zaposlenih.

5.3.3 Zahtjevi za obučenošću

e-mon CA obezbjeđuje obuku za svoje zaposlene u cilju realizacije funkcija poslovanja CA i RA.

5.3.4 Ponovna obuka

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

5.3.5 Rotacija poslova

Ovo poglavlje nije primjenljivo.

5.3.6 Kaznene mjere u odnosu na zaposlene

e-mon CA ima odgovarajuće mjere za kažnjavanje zaposlenih za neautorizovane aktivnosti, neautorizovano korišćenje autoriteta, kao i neautorizovano korišćenje sistema za svrhu sankcija za određene podvale u odgovornostima, koje mogu biti odgovarajuće u zavisnosti od različitih okolnosti.

5.3.7 Kontrole nezavisnih ugovarača

Nezavisni ugovarači su subjekti istih procedura zaštite privatnosti i uslova povjerljivosti kao i e-mon CA.

5.3.8 Dokumentacija za inicijalnu obuku i ponovnu obuku

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

6. TEHNIČKE BEZBJEDNOSNE KONTROLE

Ovo poglavlje definiše bezbjednosne mjere koje primjenjuje e-mon CA u cilju zaštite njegovih kriptografskih ključeva i aktivacionih podataka (kao na primjer PIN-ovi, lozinke, itd.).

6.1 Generisanje i instalacija asimetričnog para ključeva

6.1.1 Proces generisanja privatnog ključa e-mon CA

e-mon CA koristi bezbjedan proces generisanja svog root i ostalih privatnih ključeva u skladu sa dokumentovanom procedurom. e-mon CA distribuira dijeljene tajne za svoje privatne ključeve. e-mon CA je vlasnik privatnih ključeva i posjeduje autoritet da prenese odgovarajuće dijeljene tajne na autorizovane nosioce dijeljenih tajni.

Korišćenje privatnog ključa e-mon CA

Privatni ključ e-mon CA se koristi za elektronsko potpisivanje e-mon CA izdatih certifikata (prije svega za izdavanje subordinate/intermediate CA certifikata), liste povučenih certifikata, kao i akreditovanih root-potpisanih entiteta (CA trećih strana). Druge svrhe korišćenja su zabranjene.

Tip privatnog ključa e-mon CA

Za potrebe svog root privatnog ključa i odgovarajuće potpisivanje, e-mon CA koristi SHA-1/RSA kombinaciju hash i asimetričnog algoritma sa dužinom ključa od 4096 bita i periodom validnosti od 15 godina.

Za svoje subordinate/intermediate/operativne CA privatne ključeve i odgovarajući algoritam za elektronsko potpisivanje, e-mon CA koristi SHA-1/RSA kombinaciju algoritama sa dužinom ključa od 2048 bita, kao i periodom validnosti od 10 godina.

6.1.2 Generisanje ključa e-mon CA

e-mon CA bezbjedno generiše i štiti svoje sopstvene privatne ključeve, korišćenjem bezbjednih i pouzdanih sistema, i primjenjuje neophodne preventivne mjere u cilju sprječavanja kompromitacije ili neautorizovanog korišćenja. e-mon CA implementira i dokumentuje procedure generisanja ključeva, u skladu sa ovom CP. e-mon CA primjenjuje javne, internacionalne i Evropske standarde u vezi bezbjednih i pouzdanih sistema.

6.1.3 Uređaji za generisanje ključeva e-mon CA

Generisanje privatnog ključa e-mon CA se dešava u okviru bezbjednog kriptografskog uređaja koji zadovoljava odgovarajuće zahtjeve u skladu sa međunarodnim standardima, uključujući ISO 15782-1, FIPS 140-1 nivo 3, ANSI X9.66.

Kontrole generisanja ključeva e-mon CA

Generisanje privatnog ključa e-mon CA zahtijeva kontrolu od strane više od jednog, na odgovarajući način, autorizovanog zaposlenog koji imaju povjerljive pozicije i dužnosti. Autorizacija procedure generisanja ključeva se mora izvršiti od strane više od jednog člana upravne structure e-mon CA.

6.1.4 Čuvanje privatnog ključa e-mon CA

e-mon CA koristi bezbjedni kriptografski uređaj da čuva svoje privatne ključeve u skladu sa međunarodnim zahtjevima iskazanim u ISO 15782-1/FIPS 140-1/ANSI X9.66.

Kontrole čuvanja ključa e-mon CA

Procedura čuvanja privatnog ključa e-mon CA zahtijeva višestruke kontrole od strane na odgovarajući način autorizovanog osoblja sa povjerljivim rolama. Autorizacija procedure čuvanja ključeva i autorizacija odgovarajućeg osoblja mora biti izvršena od strane više od jednog člana upravne structure.

Backup ključeva e-mon CA

e-mon CA privatni ključ je backup-ovan, čuvan i može biti reaktiviran od strane višestrukih i na odgovarajući način autorizovanih zaposlenih koji imaju povjerljive role i pozicije. Pomenute procedure i zaposleni moraju biti autorizovani od strane više od jednog člana upravne structure.

Procedura dijeljenja tajni

Procedura dijeljenja tajni e-mon CA koristi višestruke autorizovane nosioce u cilju da zaštiti i poboljša povjerljivost privatnih ključeva i obezbijedi odgovarajuću proceduru oporavka ključa.

Prihvatanje dijeljenih tajni

Prije nego što nosilac dijeljene tajne prihvati dijeljenu tajnu on mora lično da se upozna sa kreiranjem, ponovnim kreiranjem i distribucijom tajne na njegovog sledećeg člana u lancu povjerljivosti.

Nosilac dijeljene tajne prima dijeljenu tajnu na fizičkom medijumu, kao što je određeni hardverski kriptografski modul koji je potvrđen za korišćenje od strane e-mon CA. e-mon CA čuva pisane zapise u vezi distribucije dijeljene tajne.

6.1.5 Distribucija privatnog ključa e-mon CA

e-mon CA dokumentuje njegovu sopstvenu distribuciju privatnog ključa i ima mogućnost da izmijeni način distribucije tokena u slučaju da staraoci tokena zahtijevaju da budu zamijenjeni u njihovim rolama kao staraoci tokena.

6.1.6 Uništavanje privatnog ključa e-mon CA

e-mon CA privatni ključevi se uništavaju na kraju njihovog životnog vijeka u cilju garancije da oni neće nikada biti ponovo aktivirani i korišćeni.

Privatni ključevi e-mon CA se uništavaju tako što se unište njihove primarne i backup kopije (CD ROM-ovi), brisanjem njihovih dijeljenih djelova/tajni i isključivanjem napajanja za sve hardverske module na kojima se čuvaju dati ključevi.

Proces uništavanja ključeva je dokumentovan i pridruženi zapisi su arhivirani.

6.2 Zaštita privatnog ključa

e-mon CA koristi odgovarajuće kriptografske uređaje u cilju relaizacije zadataka upravljanja ključevima CA. Pomenuti kriptografski uređaji su poznati pod imenom Hardverski bezbjednosni moduli (HSM - Hardware Security Modules).

Ovi uređaji zadovoljavaju zahtjeve iz FIPS PUB 140-1 nivo 3 ili viši, koji garantuju, između ostalog da je bilo koji pokušaj narušavanja integriteta uređaja ili kriptografske memorije istovremeno detektovan, i da privatni ključevi ne mogu da napuste uređaj nekriptovani.

Hardverski i softverski mehanizmi koji štite privatne ključeve CA su dokumentovani. Dokumenti prikazuju da su mehanizmi zaštite CA ključa u najmanju ruku ekvivalentne snage kao i sami CA ključevi koji se štite.

HSM uređaji ne smijeju da napuštaju e-mon CA prostorije izuzev rijetkih prilika unaprijed definisanih premještanja i preseljenja. e-mon CA čuvaju zapise u vezi svih tih premještanja ili preseljenja.

U slučaju da odgovarajući HSM zahtijeva održavanje ili popravku, koja se ne može izvršiti u okviru e-mon CA prostorija, oni se onda bezbjedno prenose do njihovog proizvođača uz poštovanje svih neophodnih bezbjednosnih mera, detaljno opisanih u CPS dokumentu.

Privatni ključ e-mon CA se koristi pod k od n kontrolom od strane više zaposlenih sa povjerljivim ulogama.

Privatni ključ e-mon CA se ne obnavlja.

Na kraju svake ceremonije generisanja ključeva, novi CA ključevi se upisuju u šifrovanoj formi na CD ROM (backup ključa za potrebe čuvanja). e-mon CA zapisuje

sve korake u proceduri backup-a ključa korišćenjem specifične forme za logovanje informacije.

Privatni ključevi e-mon CA se lokalno arhiviraju u okviru e-mon CA prostorija.

Nosioci dijeljenih tajni (staraoci) e-mon CA imaju zadatak da aktiviraju i deaktiviraju privatni ključ. Privatni ključ je tada aktivan u definisanom periodu vremena.

Privatni ključ e-mon CA će biti uništen na kraju svog životnog ciklusa.

6.3 Neki aspekti upravljanja parom ključeva

e-mon CA arhivira svoj sopstveni javni ključ. e-mon CA izdaje korisničke certifikate za periodom korišćenja kao što je naznačeno u certifikatima.

6.4 Aktivacioni podaci

e-mon CA bezbjedno čuva i arhivira aktivacione podatke pridružene njihovim sopstvenom privatnom ključu i operacijama.

6.5 Bezbjednosne kontrole računara

e-mon CA implementira bezbjednosne kontrole nad računarima koji se koriste.

6.6 Bezbjednosne kontrole životnog ciklusa

e-mon CA realizuje periodične razvojne i bezbjednosno upravljačke kontrole.

6.7 Mrežno bezbjednosne kontrole

e-mon CA održava i primjenjuje visok nivo sistema mrežne bezbjednosti, uključujući primjenu firewall uređaja i intrusion detection sistema.

6.8 Kontrole inženjeringa kriptografskih modula

e-mon CA realizuje periodične kontrole inženjeringa kriptografskih modula.

7. PROFILI CERTIFIKATA I CRL LISTE

Ovo poglavlje specificira formate certifikata i CRL lista.

Opšti profil e-mon CA certifikata:

Ime profila	xx certifikat za xx	
Period validnosti certifikata	x godina	
Ekstenzija osnovnih ograničenja	End Entity CA, Path length=x	
Čuvanje ključeva	SSCD Unspecified	
Generisanje ključeva od strane	Owner CSP	
Zajedničke ekstenzije	Authority Key Identifier Subject Key Identifier Authority Information Access CRL Distribution Point	
Primjenljiva dužina ključeva	1024, 2048	
Ekstenzija korišćenja ključa	Digital Signature Non-Repudiation Key Encipherment Data Encipherment Key Agreement	Certificate Signing CRL Signing Encipher Only Decipher Only
Ekstenzija naprednog korišćenja ključa	Client Authentication Server Authentication Email Protection Code Signing Timestamping	
OID Politike	1.3.6.1.4.1.19124.10.1.1.2.a.b.c a – Subject Category 1 - Organisations 2 - Individuals 3 - Resources 4 - Code Publishers b – Subject Key Assurance Level 1 - Standard 2 - Standard with SSCD 3 - Advanced 4 - Advanced with SSCD c – Private Key Generation Option 1 - Key generated by owner 2 - Key generated by certification service provider	
URL za politiku certifikacije	http://www.emonca.com/resources/cps.pdf	

7.1 Profil certifikata

e-mon CA izdaje sljedeće vrste certifikata za informatičke resurse pravnih i fizičkih lica:

- Standardni SSL certifikat za server,
- Standardni certifikat za agenta zaštite,
- Standardni certifikat za e-mail agenta zaštite.

Standardni SSL certifikat za server

Ime profila	Standardni SSL certifikat za server	
Period validnosti certifikata	1 godina	
Ekstenzija osnovnih ograničenja	End Entity	
Čuvanje ključeva	Nije specificirana lokacija	
Generisanje ključeva od strane	Owner	
Zajedničke ekstenzije	Authority Key Identifier Subject Key Identifier Authority Information Access CRL Distribution Point	
Primjenljiva dužina ključeva	1024, 2048	
Ekstenzija korišćenja ključa	Digital Signature Key Encipherment	
Ekstenzija naprednog korišćenja ključa	Server Authentication	
OID Politike	1.3.6.1.4.1.19124.10.1.1.2.3.1.1	
URL za politiku certifikacije	http://www.emonca.com/resources/cps.pdf	

Standardni certifikat za agenta zaštite

Ime profila	Standardni certifikat za agenta zaštite	
Period validnosti certifikata	1 godina	
Ekstenzija osnovnih ograničenja	End Entity	
Čuvanje ključeva	Nije specificirana lokacija	
Generisanje ključeva od strane	Owner	
Zajedničke ekstenzije	Authority Key Identifier Subject Key Identifier Authority Information Access CRL Distribution Point	
Primjenljiva dužina ključeva	1024, 2048	
Ekstenzija korišćenja ključa	Digital Signature Non-Repudiation Key Encipherment	
Ekstenzija naprednog korišćenja ključa	Client Authentication Server Authentication	
OID Politike	1.3.6.1.4.1.19124.10.1.1.2.3.1.1	
URL za politiku certifikacije	http://www.emonca.com/resources/cps.pdf	

Standardni certifikat za e-mail agenta zaštite

Ime profila	Standardni certifikat za e-mail agenta zaštite	
Period validnosti certifikata	1 godina	
Ekstenzija osnovnih ograničenja	End Entity	
Čuvanje ključeva	Nije specificirana lokacija	
Generisanje ključeva od strane	Owner	
Zajedničke ekstenzije	Authority Key Identifier Subject Key Identifier Authority Information Access CRL Distribution Point	
Primjenljiva dužina ključeva	1024, 2048	
Ekstenzija korišćenja ključa	Digital Signature Non-Repudiation Key Encipherment	
Ekstenzija naprednog korišćenja ključa	Email Protection	
OID Politike	1.3.6.1.4.1.19124.10.1.1.2.3.1.1	
URL za politiku certifikacije	http://www.emonca.com/resources/cps.pdf	

7.2 Profil CRL liste

U skladu sa IETF PKIX RFC 2459, e-mon CA podržava izdavanje CRL lista koje su u saglasnosti sa sljedećim uslovima korišćenja:

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

Profil e-mon CA CRL (Certificate Revocation List) liste je prikazan u sljedećoj tabeli:

Version	[Version 1]	
Issuer Name	CountryName=[Root Certificate Country Name], OrganizationName=[Root Certificate Organization], commonName=[Root Certificate Common Name]	
This Update	[Date of Issuance]	
Next Update	[Date of Issuance + 3 hours]	
Revoked certificates	CRL Entries	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

8. ADMINISTRIRANJE POLITIKE

e-mon CA autoritet za upravljanje politikom upravlja ovom CP. e-mon CA je odgovoran za registraciju, održavanje i interpretaciju ove CP.

U cilju root signing procedura i kao operator povjerljive mreže, e-mon CA potvrđuje mogućnost da neko drugo CA može da postane član pomenute mreže povjerenja. Takvo potvrđivanje se uspostavlja na bazi audit procedure koja se izvršava nad osnovnim dokumentima, CP i CPS, koji su dostavljeni od takvog partnera. e-mon CA može biti konsultovan u odnosu na CP i CPS dokumentaciju takvog CA treće strane.

U cilju potvrđivanja CP i CPS dokumenata od CA treće strane i uspostave određenog nivoa ili relevantnosti u skladu sa e-mon CA CP i CPS dokumentima, e-mon CA izvršava sljedeće korake:

- Uspostava ugovornog odnosa.
- Definisanje poslovnog okruženja i projektnog konteksta.
- Realizuje za potrebe treće strane jedan audit izveštaj o jednom broju suštinskih tačaka koje uključuju ali nisu ograničene na sledeće:
 - Kontaktne informacije CA
 - Tip certifikata, validacione procedure i korišćenje
 - Ograničenja u pouzdanosti i odgovornosti
 - Obaveze strana koje su uključene u procedure životnog veka certifikata
 - Proveru statusa certifikata
 - Registracione procedure
 - Model CA i RA
 - Primjenljivi ugovori
 - Politika privatnosti
 - Zakon koji se primenjuje, rešavanje žalbi i sporova.
- Akredituje CA treće strane.

Bilo koja politika koja je potvrđena od strane e-mon CA mora obavezno da bude u saglasnosti za odredbama ovog e-mon CA CP dokumenta.