OPŠTA PRAVILA PRUŽANJA USLUGA CERTIFIKOVANJA

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

SADRŽAJ

Na osnovu člana 42 stav 2 alineja 7 Statuta d.o.o. Servisni centar za elektronsko poslovanje 'e-mon', Odbor direktora, 15. septembra 2005.g. donosi

OPŠTA PRAVILA PRUŽANJA USLUGA CERTIFIKOVANJA

1. UVOD

Davalac usluga certifikovanja (certifikaciono tijelo) izdaje elektronske certifikate tako što formira elektronski potpis certifikata na osnovu svog privatnog ključa i asimetričnog kriptografskog algoritma. U tako formiranom elektronskom certifikatu, certifikaciono tijelo se identifikuje kao izdavač elektronskog certifikata, u skladu sa Zakonom o elektronskom potpisu.

1. Davalac usluga certifikovanja utvrđuje ova Opšta pravila pružanja usluga certifikovanja (u daljem tekstu: 'OP') koja korisnicima obezbjeđuju dovoljno informacija na osnovu kojih se mogu odlučiti o prihvatanju usluga i o obimu usluga.

Ovaj dokument se zasniva na sljedećim principima, i to:

1. OP definiše predmet rada certifikacionog tijela i definiše procese i način njihovog korišćenja pri formiranju i upravljanju elektronskim certifikatima. OP definiše zahtjeve poslovanja certifikacionog tijela i operativne procedure u cilju ispunjenja tih zahtjeva. Takodje, OP definišu način na koji certifikaciono tijelo ispunjava tehničke, organizacione i proceduralne zahtjeve poslovanja koji su identifikovani u Zakonu o elektronskom potpisu.
2. OP je javni dokument.

e-mon CA izdaje sljedeće vrste certifikata :

- Za pravna lica, registrovana za obavljanje djelatnosti – standardni SSCD certifikat,
- Za pravna lica, registrovana za obavljanje djelatnosti – standardni SSCD+ certifikat.
- Standardni certifikat za fizička lica,
- Standardni SSCD certifikat za fizička lica,
- Standardni SSCD+ certifikat za fizička lica.
- Standardni SSL certifikat za server,

- Standardni certifikat za agenta zaštite,
- Standardni certifikat za e-mail agenta zaštite.
- Standardni certifikat za publikaciju koda.

Ova OP su 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.
e-mon CA primjenjuje periodične evaluacije u cilju osiguravanja saglasnosti sa zahtjevima iz akreditacionih šema koje su navedene u Pravilniku o zaštiti sistema certifikovanja.

1.1 Pregled

Ova OP su namijenjena stvaranju uslova za pružanje certifikacionih usluga od strane e-mon CA, Podgorica. Ova OP se mogu 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 ovih OP imaju sljedeće oznake:

- **Standardni SSCD certifikat za pravno lice**
  OID Politike (1.3.6.1.4.1.19124.10.1.1.2.1.2.1)

- **Standardni SSCD+ certifikat za pravno lice**
  OID Politike (1.3.6.1.4.1.19124.10.1.1.2.1.2.2)

- **Standardni certifikat za fizičko lice**
  OID Politike (1.3.6.1.4.1.19124.10.1.1.2.2.1.1)
- **Standardni SSCD certifikat za fizičko lice**
  OID Politike (1.3.6.1.4.1.19124.10.1.1.2.2.2.1)
- **Standardni SSCD+ certifikat za fizičko lice**
  OID Politike (1.3.6.1.4.1.19124.10.1.1.2.2.2.2)

- **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)
- **Standardni certifikat za publikaciju koda**
  OID Politike (1.3.6.1.4.1.19124.10.1.1.2.4.1.1)

1.3 Okruženje i primjenljivost politike

Svrha ovih OP je da, prije svega, opiše odgovornosti i prava davaoca usluga certifikovanja (u daljem tekstu: „CA“), identifikatora korisnika/registracionih tijela (u daljem tekstu: „RA“ i „LRA“), i korisnika (korisnik – vlasnik certifikata). Procedure koje e-mon CA sprovodi u procesu izdavanja certifikata detaljno su opisane u Pravilniku o postupcima izdavanja certifikata.

1.3.1 e-mon CA

e-mon CA Podgorica je CA odgovoran za izdavanje ovih OP, a u cilju izdavanja određenih tipova elektronskih certifikata. e-mon CA je, takođe, i autoritet koji izdaje i druge pravilnike i politike koje se primjenjuju pri izdavanju e-mon CA elektronskih certifikata.

U cilju objavljivanja trećim stranama informacija koje se odnose na opozvane certifikate, vrši se odgovarajuća publikacija liste povučenih certifikata (CRL – Certificate Revocation List).

1.3.2 e-mon CA i Registraciona tijela/Identifikatori korisnika

e-mon CA pristupa svojim korisnicima putem mreže registracionih tijela (RA i LRA).

e-mon CA može ovlastiti druga pravna lica (RA) da vrše identifikaciju i autentikaciju budućih korisnika/vlasnika certifikata, ali ona ne izdaju i ne potpisuju certifikat (tj. RA vrši odgovarajuće poslove (identifikaciju korisnika) i u tom smislu je delegirano od CA).

RA može ovlastiti druga pravna lica (LRA) da vrše identifikaciju i autentikaciju budućih korisnika/vlasnika certifikata, ali ona ne izdaju i ne potpisuju certifikat (tj. LRA vrši odgovarajuće poslove (identifikaciju korisnika) i u tom smislu je delegirano od RA).

Ova registraciona tijela mogu biti:

- e-mon CA, 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 zahjteva 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 zahtjevima.

1.3.4 Korisnici

Korisnici e-mon CA usluga su pravna lica (kompanije) koje koriste certifikacione usluge. 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: 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 uvijek 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 primer 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.

Opšta pravila pružanja usluga certifikovanja (OP) – Imenovan skup pravila koji indicira primjenljivost certifikata na određeno okruženje i/ili na klasu aplikacija sa zajedničkim bezbjednosnim zahtjevima. Na primjer, određena OP 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 incijalnog objekta u putu, procesira u cilju provjere istog u posljednjem objektu na putu.

Davalac usluga certifikovanja/Certifikaciono tijelo (CA) – Pravno ili fizičko lice koje izdaje certificate ili pruža usluge u vezi sa elektronskim potpisom.

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

Identifikator korisnika/registraciono tijelo (RA) – Pravno lice koje je odgovorno za identifikaciju i autentikaciju budućih 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).

Lokalno registraciono tijelo (LRA) – Pravno lice koje je odgovorno za identifikaciju i autentikaciju budućih korisnika/vlasnika certifikata, ali koje ne izdaje i ne potpisuje certifikat (tj. LRA vrši odgovarajuće poslove (identifikaciju korisnika) i u tom smislu je delegirano od RA).

Treća strana/treca lica – 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.

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 programi koji se koriste za provjeru elektronskog potpisa.

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 izvešene funkcije/entiteti zadovoljavaju specifične formalne zahtjeve.

.

Zahtjev za certifikatom - Zahtjev poslat od strane korisnika koji zahtijeva certifikat (aplikant) ka CA u cilju izdavanja certifikata.

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

Autentifikacija – 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.

Istek certifikata – Kraj perioda validnosti certifikata.

Ekstenzije u certifikatu – Dodatna polja u certifikatu, pored osnovnih, koja daju bliže informacije o korisniku i CA, 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 opozvanih 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 uvjek 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/certifikovanje/davanje usluga certifikovanja – Proces izdavanja 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 primer 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.).

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

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

Smart kartica – Hardverski dio 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 pružanja usluga certifikovanja.

1.3.8 Kontaktni detalji

e-mon CA Podgorica ima sjediste 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 defiisane u ovim OP. e-mon CA koristi korisnički ugovor, ova OP (zajedno sa Pravilnikom o postupcima izdavanja certifikata) u cilju obezbjeđivanja uslova korišćenja e-mon CA certifikata od strane korisnika i trećih strana.

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

2.1.1 e-mon CA obaveze

Do nivoa specificiranog u odgovarajućim poglavljima ovih OP, e-mon CA garantuje:

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

- Regularno objavljivanje CRL liste u skladu sa ovim OP.
- Obavještavanje trećih strana o statusu povučenosti certifikata putem publikovanja CRL lista na e-mon CA repozitorijumu.
- Dostavljanja kopije ovih OP i ostalih primjenjlivih politika/pravilnika po zahtevu.

2.1.2 e-mon RA obaveze

e-mon RA se obavezuje na:

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

2.1.3 e-mon LRA obaveze

e-mon LRA se obavezuje na:

- Prijem zahtjeva za izdavanje e-mon CA certifikata u skladu sa ovim OP.
- Izvršavanje svih aktivnosti na verifikaciji i provjeri autentičnosti aplikanata u skladu sa opisom e-mon CA procedura i ovim OP.
- 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 ovim OP.
- Verifikaciju pouzdanosti i autentičnosti informacija dostavljenih od strane korisnika u vrijeme obnavljanja certifikata u skladu sa ovim OP.

2.1.4 Korisničke obaveze

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

- Posjedovanje 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.

- Obezbjeđivanje tačnih i preciznih informacija u njihovoj komunikaciji sa e-mon RA, LRA 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, razumijevanje i saglasnost sa svim stavovima i uslovima u ovim OP i drugim pridruženim politikama/pravilnicima koje su objavljene na e-mon CA repozitorijumu..
- Uzdržavanje od narušavanja integriteta i proizvođenja e-mon CA izdatog certifikata neispravnim.
- Korišćenje e-mon CA certifikata samo za legalne i autorizovane svrhe u skladu sa ovim OP.
- Obavještavanje e-mon CA, e-mon RA ili e-mon LRA 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 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.
- Uzdržavanje 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 obaveštavanje 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 OP 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 ovih OP i moraju postupati po odredbama ovih OP ili drugih pravilnika/politika izdatih od starne e-mon CA. Strane u komunikaciji demonstriraju prihvatanje uslova korišćenja navedenih u ovim OP dostavljanjem upita vezanih za status elektronskih certifikata ili bilo kojim drugim načinom koji pokazuje korišćenje ili oslanjanje na obezbijeđene 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 OP, drugi pravilnici, korisnički ugovor, itd.).
- Bilo koje druge usluge koje e-mon CA može reklamirati ili obezbijediti putem svog web sajta.

e-mon CA garantuje da strane koje pristupaju njegovom repozitorijumu, u cilju osiguranja, dobijaju pouzdane, ažurne i tačne informacije. e-mon CA, međutim, ne može prihvatiti bilo kakvu odgovornost koja je van ograničenja definisanih u ovim OP.

2.2 Odgovornost

e-mon CA ne prihvata bilo kakvu drugu odgovornost osim one koja je eksplicitno opisana u ovom dokumentu ili u propisima koji regulišu ovu oblast.

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

- Bilo kakav gubitak profita korisnika
- Bilo kakav gubitak podataka.
- Bilo koju indirektnu ili slučajnu štetu koja je prouzrokovana ili je vezana za korišćenje, isporuku, licencu, performanse ili neperformanse certifikata ili elektronskih potpisa.
- 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 korisnika.

2.3 Finansijska odgovornost

E-mon ce obeštetiti korisnika u slucaju nastanka štete, za troškove bilo koje vrste, ukoliko je ista nastala zbog propusta u radu e-mona, a u smislu kršenja odredbi ovih OP, drugih pravila ili politika izdatih od strane e-mona, kao i slučaju kršenja propisa koji regulišu ovu oblast.

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 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 namerom da se prevari e-mon CA, ili bilo koje lice koje prima i odnosi se prema dobijenom certifikatu.
- Neobezbjeđivanja odgovarajuće zaštite korisnikovog privatnog ključa. Korišćenja bezbjednog sistema kako je zahtijevano, ili neizvršenja odgovarajućih preventivnih mjera neophodnih da se spriječi 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 se primjenjuju na ovu oblast, uključujući one koji se odnose na zaštitu intelektualnih prava, viruse, pristup računarskim sistemima, itd.

2.4 Interpretacija i sprovođenje

Ovo poglavlje sadrži odredbe koje se odnose na interpretaciju i sprovođenje ovih OP, kao što su:

- Zakon koji se primjenjuje,
- Procedure za rješavanje sporova.

2.4.1 Uskladjenost sa zakonom

Ova OP su izdata u potpunosti u skladu sa odgovarajućom zakonskom regulativom Republike Crne Gore.

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 OP, strane u sporu prihvataju arbitražno tijelo koje će biti izabrano od strane Vlade Republike Crne Gore.

U slucaju da spor ne bude riješen u arbitražnom postupku, propisuje se mjesna nadležnost suda u Podgorici..

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 Objava i opoziv certifikata

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 i ova OP. 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 osjetljvosti, 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 tijela, root signing proceduru, itd.

e-mon CA publikuje statusne informacije o digitalnim certifikatima u određenim intervalima, u skladu sa ovim OP.

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 ovih i drugih pravila.

2.7 Provjera uskađenosti

e-mon CA prihvata periodični audit/provjeru saglasnosti svojih pravilnika, uključujući ova OP. 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 Republike Crne Gore.

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

2.8 Povjerljivost i tajnost poslovanja i podataka

e-mon CA se pridržava pravila zaštite privatnosti personalnih podataka i pravila povjerljivosti kako je opisano u ovom 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 Zastita intelektualne svojine/ autorskih prava

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 POTVRĐIVANJE IDENTITETA POTPISNIKA

e-mon CA održava dokumentovana praktična pravila i procedure u cilju autentikacije identiteta i/ili drugih atributa aplikanata/krajnjih korisnika e-mon CA certifikata što se izvršava prije 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 primjer X.500 distinguished imena.

Kada aplicira za e-mon CA certifikat, ime podnosioca zahtjeva mora biti u potpunosti sa odgovarajućim značenjem sem ako to nije eksplicintno 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 pravim 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 uvijek 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 Registracija potpisnika

U cilju realizacije procedure identifikacije i autentikacije za inicijalnu korisnikovu registraciju za svaki tip subjekta (CA, RA, LRA, 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).

- Zahtevi e-mon CA u smislu identifikacije i autentikacije organizacija koje su aplicirale za e-mon CA izdate certifikate, uključuju ali nijesu 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 nijesu ograničene na druge CA (treće strane), RA, LRA, 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, LRA, korisnik (u slučaju certifikata izdatih organizacijama ili informatičkim resursima kontrolisanim od strane organizacije), e-mon CA može primijeniti korake koji uključuju ali nijesu 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 prije 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.

3.1 Plansko obnavljanje certifikata

Po isteku certifikata ukoliko korisnik zahtijeva obnovu certifikata, na osnovu dotadašnjih podataka vrši se obnova istog (zanavljanje certifikata).

Prije isteka roka certifikata korisnik se obavijesti o skorom isticanju certifikata. On se potom obrati svojoj RA, LRA i na osnovu pismenog zahtjeva od strane tog RA, LRA vrši se obnavljanje certifikata.

3.2 Obnavljanje nakon opoziva

U slučaju gubitka, kompromitacije, oštećenja smart kartice na kojoj se nalazi certifikat, korisnik je dužan da opozove taj certifikat.

Korisnik može u ovom slučaju opozvati certifikat telefonskom putem ili kod RA, LRA. U slučaju opoziva telefonskim putem korisnik mora navesti lozinku za poništenje koju je unio u zahtjev za izdavanje certifikata. U slučaju opoziva certifikata kod RA, LRA mora imati neki identifikacioni dokument koji je potreban i prilikom podnošenja zahtjeva za izdavanje certifikata.

U tom slučaju, a na zahtjev korisnika, certifikat se opoziva i izdaje se novi certifikat.

3.3 Zahtjev za opoziv certifikata

U cilju sprovođenja procedura identifikacije i autentikacije za potrebe zahtjeva za opoziv certifikata za odgovarajuće tipove subjekata (CA, RA, LRA, korisnik i drugi participanti), e-mon CA zahtijeva korišćenje on-line autentikacionog mehanizma (autentikacija putem digitalnog certifikata, putem PIN broja, putem autorizacionog koda, putem lozinke za opoziv itd.) i zahtjevi se upućuju odgovarajućem e-mon RA. e-mon RA sprovodi takve zahtjeve do e-mon CA u cilju realizacije procedure povlačenja cerifikata.

4. OSNOVNI ZAHTJEVI

Svi učesnici u procesu certifikovanja, subordinate/intermediate (subject) RA, LRA, korisnici ili treća lica su u obavezi da informišu e-mon CA o svim promjenama u informacijama koje su objavljene u certifikatu za čitav period operativnog rada takvog certifikata.

4.1 Prijem zahtjeva za izdavanje certifikata

Podnosilac zahtjeva za izdavanje certifikata mora ispuniti odgovarajući obrazac koji se nalazi kao Prilog ovih OP.

Podnosilac zahtjeva za izdavanje certifikata garantuje da su podaci u obrascu tačni i precizni.

Što se tiče zahtjeva za izdavanje certifikata za pravna lica, e-mon CA zahtijeva da podnosilac zahtjeva bude opunomoćen za taj posao.

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

- Popunjavanje zahtjeva za certifikatom.
- 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.
- Potpisivanje korisničkog ugovora.

Za prijem zahtjeva za izdavanje certifikata nadležni su e-mon CA, RA ili LRA.

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

Nakon toga, e-mon CA, RA ili LRA ili prihvataju ili odbijaju zahtjev za izdavanje certifikata. Takvo prihvatanje ili odbijanje ne mora neophodno da bude obrazloženo podnosiocu zahtjeva ili bilo kojoj drugoj strani.

e-mon CA mora da izvrši aktivnosti i procesuira zahtjev za izdavanje certifikata u okviru vremenskog perioda od sedam (7) radnih dana, tj. u tom roku mora dostaviti odgovor podnosiocu zahtjeva.

4.2 Izdavanje certifikata

Nakon dostavljanja zahtjeva za izdavanje certifikata ili zahtjeva za obnavljanje certifikata e-mon RA vrši provjeru informacija iz dostavljene dokumentacije.

Nakon potvrđivanja dostavljenih informacija, e-mon RA prihvata ili odbija zahtjev za izdavanje/obnavljanje certifikata.

Nakon prihvatanja zahtjeva za izdavanje certifikata, e-mon RA šalje zahtjev za izdavanje certifikata do e-mon CA.

4.3 Dostavljanje/Prihvat certifikata

Izdati e-mon CA certifikat se smatra prihvaćenim od strane korisnika u sljedecim slučajevima:

- Potvrdom prijema poslata elektronskom poštom od strane korisnika,
- Preuzimanjem certifikata i para ključeva korišćenjem standardne on-line forme gdje je to moguće primijeniti,
- Korišćenjem certifikata prvi put,
- Istekom roka od petnaest (15) dana od dana izdavanja.

Bilo koja primjedba od strane korisnika na izdati certifikat mora biti dostavljena u pismenoj formi do e-mon CA, RA ili LRA (napr. u slučaju štamparskih grešaka i sl.). U tom slučaju RA ili LRA, tu činjenicu moraju potvrditi i poslati spisak pogreški u izdatom certifkatu koja uključuje sva polja u certifikatu koja sadrže pogrešne informacije.

4.4 Opoziv certifikata

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

- Gubitka, krađe, modifikacije, neautorizovanog objavljivanja ili neke druge kompromitacije privatnog ključa subjekta certifikata.
- Narušavanja materijalne obaveze koje su definisane ovim OP od strane korisnika.
- Kašnjenja ili spriječenosti u izvršavanju obaveza predvidjenih ovim OP od strane korisnika usljed prirodne katastrofe, računarskog ili komunikacionog otkaza, ili usljed drugog uzroka koji izlaze van kontrole CA.
- Promjene određenih informacija koje sadrži certifikat.

Korisnik mora u bilo koje vrijeme, ako se desi neki od gore pomenutih događaja, da kontaktira e-mon RA u cilju zahtjeva za opozivom. Pomenuti kontakt može biti on-line ili putem nekih nedigitalnih kanala. e-mon CA povlači certifikat promptno nakon verifikacije identiteta strane koja je zahtijevala povlačenje i potvrdom da je zahtjev podnijet u skladu sa procedurom zahtijevanom u ovim OP. Verifikacija identiteta može biti izvršena na osnovu informacionih elemenata koji su sadržani u identifikacionim podacima koje je korinsik 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 ažurira bar jednom dnevno.

Treće strane takodje moraju postupati u skladu sa ovim OP.

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

U cilju održavanja broja korisnika elektronskih certifikata, aproksimativno trideset (30) dana prije isticanja validnosti elektronskog certifikata, e-mon CA će činiti razumne napore da obavijesti korisnike putem elektronske pošte ili na neki drugi način, u vezi bliskog isticanja njihovog elektronskog certifikata.

4.5 Postupci provjere sigurnosnih mjera/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 vidjeti od samo strane autorizovanog osoblja, uključujući Sistem inžinjera CA Administratora.
- 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 periodično procenu nivoa zaštite sistema.

4.6 Arhiviranje certifikata i podataka

e-mon CA tako i na RA su dužni da čuvaju kompletnu dokumentaciju koja se odnosi na izdavanje, opoziv, ponovno izdavanje certifikata i druge radnje sa certifikatima.. Čuvanje dokumentacije se vrši po sljedećim pravilima

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

- Period čuvanja – e-mon CA čuva na bezbjedan način pomenute zapise o e-mon CA certifikatima za period koji je naznačen u e-mon CA u odgovarajućem pravilniku izdatom od strane e-mona, a u skladu sa pozitivnim propisima
- Zaštita arhive podrazumijeva:
    - Samo zapise koje administratori (zaposleni koje su zadužene za čuvanje 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, tj. da ne može doći do brisanja podataka iz arhive
    - Zaštita u odnosu na kvarenje medijuma na kojima se arhiva čuva, kao na primjer realizacija zahtijeva da se podaci periodično migriraju na svježe medijume.
- 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 izmjeni način čuvanja zapisa ako je to eventualno potrebno da bude u saglasnosti sa određenim akreditacionim šemama.

4.7 Zamjena certifikata

e-mon CA vrši izdavanje novog certifikata na osnovu pismenog zahtjeva od strane korisnika. E-mon CA može izdati novi certifikat, na osnovu zahtjeva korisnika, a u slučaju :

- Isteka važnosti dotadašnjeg certfikata
- Gubitka, krađe, modifikacije, neautorizovanog objavljivanja ili neke druge kompromitacije privatnog ključa certifikata.
- Opozivanja certifikata zbog narušavanja materijalne obaveze koje su definisane ovim OP od strane korisnika.
- Opozivanja certifikata zbog kašnjenja ili spriječenosti u izvršavanju obaveza predvidjenih ovim OP od strane korisnika usljed prirodne katastrofe, računarskog ili komunikacionog otkaza, ili usljed drugog uzroka koji izlaze van kontrole CA.
- Promjene određenih informacija koje sadrži certifikat.

4.8 Postupci otklanjanja posljedica šteta i nezgoda

U posebnim internim pravilima, e-mon CA dokumentuje procedure koje treba izvršiti pri rješavanju incidenata i izvještavanja 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 Prestanak 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 namjeri 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 ovim OP.
- 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 ista OP.

5. SADRŽAJ CERTIFIKATA I LISTE OPOZVANIH CERTIFIKATA (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 Opšta pravila	http://www.emonca.com/resources/cps.pdf	

5.1 Profil certifikata

e-mon CA izdaje sljedeće vrste certifikata za pravna lica:

- **Standardni SSCD certifikat za pravno lice**
- **Standardni SSCD+ certifikat za pravno lice**

Standardni SSCD certifikat za pravno lice

Ime profila	Standardni SSCD certifikat za pravno lice
Period validnosti certifikata	1 godina
Ekstenzija osnovnih ograničenja	End Entity
Čuvanje ključeva	SSCD
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 Email Protection
OID Politike	1.3.6.1.4.1.19124.10.1.1.2.1.2.1.
URL Opšta pravila	http://www.emonca.com/resources/cps.pdf

Standardni SSCD+ certifikat za pravno lice

Ime profila	Standardni SSCD+ certifikat za pravno lice
Period validnosti certifikata	1 year
Ekstenzija osnovnih ograničenja	End Entity
Čuvanje ključeva	SSCD
Generisanje ključeva od strane	e-mon CA
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 Email Protection
OID Politike	1.3.6.1.4.1.19124.10.1.1.2.1.2.2
URL Opšta pravila	http://www.emonca.com/resources/cps.pdf

e-mon CA izdaje sljedeće vrste certifikata za fizička lica:

- **Standardni certifikat za fizičko lice**
- **Standardni SSCD certifikat za fizičko lice**
- **Standardni SSCD+ certifikat za fizičko lice**

Standardni certifikat za fizičko lice

Ime profila	Standardni certifikat za fizičko lice
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 Email Protection
OID Politike	1.3.6.1.4.1.19124.10.1.1.2.2.1.1.
URL Opšta pravila	http://www.emonca.com/resources/cps.pdf

Standardni SSCD certifikat za fizičko lice

Ime profila	Standardni SSCD certifikat za fizičko lice
Period validnosti certifikata	1 godina
Ekstenzija osnovnih ograničenja	End Entity
Čuvanje ključeva	SSCD
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 Email Protection
OID Politike	1.3.6.1.4.1.19124.10.1.1.2.2.2.1.
URL Opšta pravila	http://www.emonca.com/resources/cps.pdf

Standardni SSCD+ certifikat za fizičko lice

Ime profila	Standardni SSCD+ certifikat za fizičko lice
Period validnosti certifikata	1 godina
Ekstenzija osnovnih ograničenja	End Entity
Čuvanje ključeva	SSCD
Generisanje ključeva od strane	e-mon CA
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 Email Protection
OID Politike	1.3.6.1.4.1.19124.10.1.1.2.2.2.2
URL Opšta pravila	http://www.emonca.com/resources/cps.pdf

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 Opšta pravila	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 Opšta pravila	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 Opšta pravila	http://www.emonca.com/resources/cps.pdf

- Standardni certifikat za publikaciju koda.

Standardni certifikat za publikaciju koda

Ime profila	Standardni certifikat za publikaciju koda
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
Ekstenzija naprednog korišćenja ključa	Code Signing
OID Politike	1.3.6.1.4.1.19124.10.1.1.2.4.1.1
URL Opšta pravila	http://www.emonca.com/resources/cps.pdf

5.2 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]

6. POSTUPCI SA DOKUMENTACIJOM (ADMINISTRIRANJE PRAVILA)

6.1 Postupak kod promjene sadržaja dokumentacije

Ova OP mogu se mijenjati odlukom nadležnog organa e-mon CA.

O svim promjenama na ovom dokumentu, e-mon CA će obavijestiti svoje korisnike obvjavljivanjem izmjena OP na svom web site-u, najkasnije narednog dana od dana nastanka promjene.

Promjene odredbi ovih OP stupaju na snagu u roku od 8 (osam) dana od dana objavljivanja na site-u, i nakon isteka tog roka smatra se da su korisnici upoznati sa istim.

6.2 Objavljivanje dokumentacije

6.2.1 Lista dokumentacije koja se ne objavljuje

e-mon neće objavljivati interna pravila kojima se obezbjedjuje ispravno sprovodjenje zaštitnih i sigurnosnih mjera u sistemu certifikovanja, i to iz razloga što taj dokument predstavlja poslovnu tajnu i dostupan je samo organu koji vrši nadzor nad radom davaoca usluga certifikovanja.

6.2.2. Procedura objavljivanja/distribuiranja dokumentacije

Ova OP, kao i ostale pravilnike, politike i druge dokumente koji se odnose na pružanje usluga certifikovanja, a koja ne predstavljaju poslovnu tajnu, e-mon CA objavljuje na svom web site-u, a na zahtjev korisnika, RA ili LRA, ista mogu biti dostavljena i u elektronskoj formi.

6.3 Postupak prihvatanja/odobravanja dokumentacije

E-mon CA je autoritet za administriranje (postupanje) sa ovim OP. e-mon CA je odgovoran za izdavanje, održavanje i interpretaciju ovih OP.

Bilo koja politika ili pravilnik izdat od strane e-mon CA mora obavezno da bude u saglasnosti za odredbama ovih OP..

7. ZAVRŠNE ODREDBE

7.1 Ova OP stupaju na snagu u roku od 8 dana od dana objavljivanja na web site-u davaoca usluga certifikovanja.
7.2. Na sva pitanja i odnose koji nijesu regulisani ovim OP primjenjuju se odredbe zakona i drugih propisa koji regulisu ovu oblast.

U Podgorici, 15. septembra 2005.g.

Odbor direktora

Miodrag Mirčetić s.r.