PRAVILNIK O ZAŠTITI SISTEMA 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

PRAVILNIK O ZAŠTITI SISTEMA CERTIFIKOVANJA

1. KONTROLA SIGURNOSTI OPREME, POSTUPKA I OSOBLJA

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.

1.1 Kontrola prostora, opreme i sredstava

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 obezbjeđena 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 mjere 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 obezbijeđena i zaštićena od požara i poplava.
- Iznošenje smeća se takođe kontroliše.

1.2 Kontrola postupka i radnih procesa

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.

1.3 Kontrola osoblja

1.3.1 Stručnost

e-mon CA izvršava provjere u cilju uspostave zahtjevane 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 prezentacija informacija od strane kandidata,
- Odgovarajuće reference.

1.3.2 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.

1.3.3 Zahtjevi za obučenošću

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

1.3.4 Ponovna obuka

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

1.3.5 Kaznene mere 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.

1.3.6 Kontrole nezavisnih ugovarača

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

1.3.7 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.

2. KONTROLA TEHNIČKE SIGURNOSTI RADA SISTEMA CERTIFIKOVANJA

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

2.1 Izrada sopstvenog certifikata

2.1.1 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 poseduje 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 peridom 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.

2.1.2 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 sprečavanja kompromitacije ili neautorizovanog korišćenja. e-mon CA implementira i dokumentuje procedure generisanja ključeva, u skladu sa ovom CP. e-mon CA primjenjuje javen, internacionalne i Evropske standarde u vezi bezbjednih i pouzdanih sistema.

2.1.3 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.

2.1.4 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 zahteva 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 strukture.

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 strukture.

Procedura dijeljenja tajni

Procedura dijeljenja tajni e-mon CA koristi višestruke autorizovane nosioce u cilju da zaštiti i poboljša poverljivost 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 kreiranje 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.

2.1.5 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.

2.1.6 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 dijelova/tajni i isključivanjem napajanja za sve hardverske module na kojima se čuvaju dati ključevi.

Proces uništavanja ključeva je dokumentovan i pridruženi zapisi su arhivirani.

2.2 Zaštita podataka za izradu sopstvenog elektronskog potpisa

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 smiju da napuštaju e-mon CA prostorije izuzev rijetkih prilika unaprijed definisanih premiještanja i preseljenja. e-mon CA čuvaju zapise u vezi svih tih premiještanja 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.

2.3 Neki aspekti upravljanja podacima za izradu elektronskog potpisa

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

2.4 Podaci za pristup potpisu davaoca usluga (Aktivacioni podaci)

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

2.5 Kontrola sigurnosti računarskog sistema

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

2.6 Kontrola sigurnosti radnog vijeka sistema

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

2.7 Kontrola sigurnosti mrežnog sistema

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

2.8 Kontrola sigurnosti kriptografskih modula

e-mon CA realizuje periodične kontrole inženjeringa kriptografskih modula.

3. ZAVRŠNE ODREDBE

3.1 Ova OP stupaju na snagu u roku od 8 dana od dana objavljivanja na web site-u davaoca usluga certifikovanja.

3.2 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.