Politika HALCOM SARAJEVO CA 3

Javni dio unutrašnjih pravila HALCOM SARAJEVO CA 3 za poslovne potvrde

CPName: EBB Sarajevo CA 3

CPOID: 1.3.6.1.4.1.5939.7.1.1

Dokument važi od: 23.10.2015

SADRŽAJ

1. UVOD 3
1.1 ZNAČENJE IZRAZA 4
2 ELEKTRONSKI PODACI, ELEKTRONSKE PORUKE I ELEKTRONSKI POTPIS 5
2.1 ELEKTRONSKI PODACI I PORUKE 5
2.2 PRIMANJE I SLANJE ELEKTRONSKIH PORUKA 5
2.3 VRIJEME I MJESTO SLANJA I PRIJEMA ELEKTRONSKE PORUKE 6
2.4 ELEKTRONSKI POTPIS 6
3.OPŠTE ODREDBE 6
3.1 NAMJENA I UPOTREBA POTVRDA 6
4.INFRASTRUKTURA HALCOM Sarajevo CA 3 7
4.1 OPŠTE KARAKTERISTIKE 7
4.1.1 Osnovni podaci o Halcom Sarajevo CA 3 7
4.1.2 Identitet 7
4.1.3 Lična potvrda podređenog ovjerioca 7
4.1.4 Šifrirani algoritmi, formati podataka i protokoli 7
4.1.5 Imenik 8
4.2 ZAŠTITNE MjERE I POUZDANOST 8
4.2.1 Zaštitne mjere i pouzdanost 8
4.3 ODGOVORNOST 8
4.3.1 Odgovornost 8
5. UPRAVLJANJE POTVRDAMA 8
5.1 OSNOVNA PRAVILA ZA UPRAVLJANJE POTVRDAMA 8
5.2 NARUDŽBENICA POTVRDE 9
5.3 IZDAVANJE POTVRDE 10
5.4 PERIOD PUNOVAŽNOSTI POTVRDE 10
5.5 OBNOVA POTVRDE 10
5.6 POSTUPAK OBNOVE POTVRDE 10
5.7 OPOZIV POTVRDE I OBJAVLJIVANJE U REGISTRU OPOZVANIH POTVRDA 10
(1) Opoziv potvrde vlasnik potvrde može zahtjevati bilo kada, ali ga mora zahtjevati u slučaju: 10
6. VLASNICI POTVRDE 11
6.1 ZAŠTITNE MJERE 11
6.2 PRAVA VLASNIKA POTVRDE 12
7. PRAVNA LICA 12
7.1 ZAŠTITNE MJERE 12
7.2 PRAVA PRAVNOG LICA 12
8. TREĆA LICA 13
8.1 ZAŠTITNE MJERE 13
8.2. PRAVA TREĆEG LICA 13
RJEČNIK TERMINA I SKRAĆENICA 14

1. UVOD

(1) Ova politika, koja predstavlja nedjeljivu cjelinu javnog rada unutrašnjih pravila ovjerioca Halcom Sarajevo CA 3 u odnosu na izdavanje poslovnih potvrda, uređuje cilj, djelovanje i metodologiju upravljanja poslovnim potvrdama, i sigurnosne zahtjeve, koje moraju ispunjavati ovjerilac Halcom Sarajevo CA 3, vlasnici i treća lica, koja se pozivaju na te potvrde, i odgovornost svih nabrojanih osoba.

(2) Halcom Sarajevo CA 3 je ovjerilac, koji izdaje i upravlja poslovnim potvrdama za ovjeru elektronskog potpisa. Halcom Sarajevo CA 3 djeluje u mreži ovjerilaca HALCOM-CA, koja je namijenjena izdavanju ličnih i opštih potvrda (u daljem tekstu potvrda) i obavljanju tehnoloških usluga u vezi sa elektronskim potpisima. Djelovanje u mreži uredjuju druga pravila i nije podređeno ovoj politici, niti je u bilo kakvoj vezi sa njom.

(3) Sve odredbe ove politike u odnosu na djelovanje Halcom Sarajevo CA 3 propisno su prenesene i podrobnije utvrđene u odredbama unutrašnje politike, koja predstavlja povjerljivi dio unutrašnjih pravila i koju čine dokumenti povjerljive prirode, koji definišu infrastrukturu, odredbe u vezi sa zaposlenim u Halcom Sarajevo CA 3 (nadležnosti, zadaci, ovlaštenja i zahtjevani uslovi pojedinih zaposlenih), fizička zaštita (pristup prostorijama, upravljanje mašinskom i programskom opremom), programska zaštita (zaštitni produžeci servera, zaštitne kopije…) i unutrašnji nadzor (kontrola fizičkih pristupa, ovlaštenja,…).

1.1 ZNAČENJE IZRAZA

Pojedini izrazi, upotrijebljeni u javnoj politici, imaju slijedeće značenje:

(1) **podaci u elektronskom obliku** su podaci, koji su oblikovani ili sačuvani na elektronski način;
(2) **elektronska poruka** je niz podataka, koji su poslani ili primljeni na elektronski način, što prije svega uključuje elektronsku razmjenu podataka i elektronsku poštu;
(3) **elektronski potpis** je niz podataka u elektronskom obliku, koji je sadržan, dodan ili logično povezan s drugim podacima, i namijenjen je provjeri istinitosti tih podataka i identifikaciji potpisnika uz pomoć kriptografije javnog i privatnog ključa;
(4) **bezbijedan elektronski potpis** je elektronski potpis, koji ispunjava slijedeće zahtjeve:
- da je povezan isključivo sa potpisnikom,
- da je iz njega moguće pouzdano utvrditi ko je potpisnik,
- da je ostvaren sredstvima za sigurno elektronsko potpisivanje, koja su isključivo pod nadzorom potpisnika,
- da je povezan sa podacima na koje se odnosi, tako da je vidljiva svaka kasnija izmjena tih podataka ili veze sa njima.

(5) **pošiljalac elektronske poruke** je lice, koje je samo poslalo elektronsku poruku, ili je poruka poslana u njegovo ime i u skladu sa njegovom voljom; posrednik elektronske poruke ne računa se kao pošiljalac te elektronske poruke;
(6) **adresant elektronske poruke** je lice, kome je pošiljalac namijenio elektronsku poruku;
(7) **primalac elektronske poruke** je lice, koje je primilo elektronsku poruku; posrednik elektronske poruke ne računa se kao primalac te elektronske poruke;
(8) **posrednik elektronske poruke** je lice, koje za drugo lice pošalje, primi, sačuva elektronsku poruku ili nudi druge usluge u vezi sa elektronskom porukom;
(9) **potpisnik** je lice, koje ostvari ili je u njeno ime i u skladu s njenom voljom ostvaren elektronski potpis;
(10) **informacijski sistem** je sistem za oblikovanje, slanje, primanje, čuvanje i druge obrade podataka u elektronskoj poruci;
(11) **podaci za elektronsko potpisivanje** su jednistveni podaci, kao što su šifre ili posebni šifrovani ključevi, koje potpisnik upotrebljava za oblikovanje elektronskog potpisa;
(12) **sredstvo za sigurno elektronsko potpisivanje** je instalirana programska ili mašinska oprema, koju potpisnik upotrebljava za oblikovanje elektronskog potpisa i ispunjava slijedeće zahtjeve:
- podaci za elektronsko potpisivanje moraju biti jedinstveni i njihova povjerljivost zagarantovana,
- podatke za elektronsko potpisivanje nije moguće u razumnom vremenu ili razumnim sredstvima konstatovati iz podataka za provjeru elektronskog potpisa, elektronski potpis je efikasno zaštićen od pronevjeravanja upotrebom trenutno dostupne tehnologije,
- potpisnik može pouzdano zaštiti svoje podatke za elektronsko potpisivanje od neovlaštenog pristupa,
- sredstvo za bezbijedno elektronsko potpisivanje ne smije promijeniti potpisane podatke ili spriječiti prikaz podataka potpisniku prije potpisa.

(13) **podaci za provjeru elektronskog potpisa** su jedinstveni podaci (javni ključevi za šifrovanje), koji se upotrebljavaju za provjeru elektronskog potpisa;
(14) **sredstvo za provjeru elektronskog potpisa** je instalirana programska ili mašinska oprema, koja se upotrebljava za provjeru elektronskog potpisa;
(15) **pravno lice** je pravno ili fizičko lice, registrovano za obavljanje djelatnosti;
(16) **potvrda** je potvrda u elektronskom obliku, koja povezuje podatke za provjeru elektronskog potpisa sa određenim licem (vlasnikom potvrde) i potvrđuje njegov identitet te ispunjava zahtjeve iz člana ovih opštih uslova i koju izdaje ovjerilac;
(17) **vlasnik potvrde** je ovlašteno odnosno zaposleno lice pravnog lica, kome se izda potvrda;
(18) **ovjerilac** je Halcom Sarajevo CA 3, koje izdaje potvrde i obavlja druge usluge u vezi sa elektronskim potpisima.

2 ELEKTRONSKI PODACI, ELEKTRONSKE PORUKE I ELEKTRONSKI POTPIS

2.1 ELEKTRONSKI PODACI I PORUKE

(1) Podacima u elektronskom obliku ne smije se odreći punovažnost ili dokazne vrijednosti samo zato što su u elektronskom obliku.

(2) Upotreba podataka za elektronsko potpisivanje bez znanja potpisnika ili vlasnika potvrde, koje se odnosi na te podatke ili sredstva, zabranjena je.

(3) Dokumentacija o poslovima izmedu ugovornih stranaka može se čuvati i u elektronskom obliku:
- ako su podaci, sadržani u elektronskom dokumentu ili zapisu dostupni i prikladni za kasniju upotrebu i
- ako su podaci čuvani u obliku u kojem su bili formirani, poslati ili primljeni, ili u nekom drugom obliku koji vjerodostojno predstavlja formirane, poslate ili primljene podatke i
- ako je iz sačuvane elektronske poruke moguće utvrditi odakle potiče, kome je poslata, i vrijeme i mjesto njegovog slanja ili prijema i
- ako upotrebljena tehnologija i postupci u dovoljnoj mjeri onemogućavaju promjenu ili brisanje podataka, koje ne bi bilo moguće jednostavno utvrditi, odnosno postoji pouzdano jamstvo o nepromjenljivosti poruke.

(4) Obaveza čuvanja dokumenata, zapisa ili podataka iz prethodnog stava, ne odnosi se na podatke čija jedina namjena je omogućavanje da elektronska poruka bude poslana ili primljena (komunikacioni podaci).

(5) Smatra se da su podaci u elektronskom obliku original ako odgovaraju uslovima iz prvog stava.

(6) Te odredbe ne važe za podatke za koje važeći propisi određuju drugačije uslove čuvanja.

(7) Smatra se, da elektronska poruka potiče od pošiljaoca:
- ako je pošalje pošiljalac sam ili
- ako je pošalje lice koju ovlasti pošiljalac, ili
- ako je pošalje informacioni sistem, koji je programirao sam pošiljalac, ili je sistem programiran po njegovom nalogu, da djeluje automatski ili
- ako je adresant za potvrdivanje porjekla poruke upotrijebio između primaoca i pošiljaoca u tu svrhu unaprijed dogovorenu tehnologiju i postupak.

(8) Odredba prethodnog stava ne važi za slučajeve:
- ako je pošiljalac obavijestio primaoca, da elektronska poruka nije njegova i ako je primalac imao vremena da odgovarajuće postupa ili
- ako je primalac znao ili bi morao znati, ako bi se ponašao kao brižni domaćin, ili
- ako bi upotrijebio dogovorenu tehnologiju i postupak, da elektronska poruka nije pošiljateljeva.

2.2 PRIMANJE I SLANJE ELEKTRONSKIH PORUKA

(1) Primalac ima pravo da ubroji svaku primljenu elektronsku poruku kao pojedinačnu poruku i da postupa u skladu s tim, osim u slučaju ako je elektronska poruka bila udvostručena i primalac je to znao ili bi morao znati, ako bi se ponašao kao brižan domačin ili ako bi upotrebio dogovorenu tehnologiju i postupak.

(2) Ako je pošiljalac u toku ili prije slanja elektronske poruke ili u samoj elektronskoj poruci

zahtjevao ili se sa primaocem dogovorio da se prijem poruke potvrdi, i naveo da elektronsku poruku uslovljava potvrdom o prijemu, računa se kao da elektronska poruka nije poslana, dok pošiljalac ne primi potvrdu u prijemu.

(3) Ako pošiljalac ne navede da elektronsku poruku uslovljava potvrdom o prijemu i potvrdu o prijemu ne primi u određenom ili dogovorenom roku, ili ako on nije bio određen ili dogovoren u razumnom roku, pošiljalac može obavijestiti primaoca da nije primio potvrdu o prijemu, i odrediti razuman rok u kojem mora primiti potvrdu o prijemu. Ako i u tom roku potvrdu o prijemu ne primi poslije prethodnog obavještenja primaoca, računa se da elektronska poruka nije poslana.

(4) Ako se pošiljalac sa primaocem nije dogovorio o obliku potvrde o prijemu elektronske poruke, računa se kao potvrda bilo kakva automatska ili druga potvrda primaoca, odnosno bilo kakvo ponašanje primaoca koje je dovoljno da pošiljalac sazna ili bi mogao saznati, da je elektronska poruka primljena.

(5) Ako pošiljalac od primaoca primi potvrdu o prijemu elektronske poruke, smatra se da je adresant primio tu elektronsku poruku, ali se ne smatra da je poslana elektronska poruka jednaka primljenoj.

2.3 VRIJEME I MJESTO SLANJA I PRIJEMA ELEKTRONSKE PORUKE

(1) Smatra se, da je elektronska poruka poslana kada ude u informacioni sistem izvan nadzora pošiljaoca.

(2) Kao vrijeme prijema elektronske poruke se smatra ono vrijeme kada elektronska poruka uđe u primaocev informacioni sistem.

(3) Kao mjesto odakle je elektronska poruka poslana smatra se mjesto gdje pošiljalac ima svoje sjedište odnosno stalno prebivalište u vrijeme slanja, a kao mjesto prijema elektronske poruke mjesto gdje primalac ima sjedište odnosno stalno prebivalište u vrijeme prijema.

(4) Ako pošiljalac, odnosno primalac, nema stalno prebivalište, kao mjesto odakle je elektronska poruka poslana odnosno gdje je primljena, prema prethodnom stavu, računa se njegovo prebivalište u vrijeme slanja, odnosno prijema elektronske poruke.

2.4 ELEKTRONSKI POTPIS

(1) Elektronskom potpisu se ne može uskratiti punovažnost niti dokazna vrijednost samo zbog elektronskog oblika, ili jer se temelji na potvrdi, ili potvrdi akreditovanog ovjerioca, ili jer nije oblikovan sredstvom za sigurno elektronsko potpisivanje.

(2) Kada su u pitanju podaci u elektronskom obliku, bezbjedan elektronski potpis, ovjeren potvrdom, jednako vrijedan je svojeručnom potpisu.

3.OPŠTE ODREDBE

3.1 NAMJENA I UPOTREBA POTVRDA

(1) Halcom Sarajevo CA 3 upravlja (izdaje i ovjerava, opoziva, produžuje, čuva i objavljuje) poslovnim potvrdama za ovjeru elektronskog potpisa (u daljem tekstu potvrde), koje su namjenjene ovlaštenim, odnosno zaposlenim osobama (u daljem tekstu vlasnici potvrda)

pravnim i fizičkim licima, registrovanim za obavljanje djelatnosti (u daljem tekstu pravna lica).

(2) Potvrde su namjenjene za upotrebu u specifičnim aplikacijama i za ciljeve, koje potvrdi i javno objavi Halcom Sarajevo CA 3, i to za:

- elektronsko bankarstvo,
- aplikacije G2B,
- "jedna za sve",
- potpisivanje elektronskih obrazaca.

(3) Da možemo govoriti o elektronskom potpisu potrebno je obezbijediti:

- šifrovanje podataka i poruka u elektronskom obliku,
- digitalno potpisivanje podataka i poruka u elektronskom obliku, i ovjeravanje identiteta potpisnika,
- sigurno brisanje podataka u elektronskom obliku.

4.INFRASTRUKTURA HALCOM Sarajevo CA 3

4.1 OPŠTE KARAKTERISTIKE

4.1.1 Osnovni podaci o Halcom Sarajevo CA 3

Adresa HALCOM Sarajevo CA 3:

HALCOM Sarajevo CA 3
Fra Anđela Zvizdovića 1
71000 Sarajevo
Bosna i Hercegovina
Tel.: (+387) 33 658 289
Fax: (+387) 33 612 671

4.1.2 Identitet

Halcom Sarajevo CA 3 predstavljaju slijedeći podaci:

C=SI, O=Halcom, CN=EBB Sarajevo CA 3
CPName Halcom Sarajevo CA 3
CPOID 1.3.6.1.4.1.5939.7.1.1

4.1.3 Lična potvrda podređenog ovjerioca

(1) HALCOM Sarajevo CA 3 je podređen HALCOM CA.

4.1.4 Šifrirani algoritmi, formati podataka i protokoli

(1) HALCOM Sarajevo CA 3 koristi:
- za potpisivanje potvrda algoritam RSA s parom ključeva dužine najmanje 2048 bita,
- za šifriranje podataka algoritmove Triple DES,
- sažeti algoritam SHA-256,
- format potvrda odgovara preporuci ITU-T za X.509 (1997) i ISO/IEC 9594-8:1997 te X.509 ver. 3 (v3),
- registri opozvanih potvrda odgovaraju preporuci ITU-T za X.509 (1997) i ISO/IEC 9594-

8:1997,
- protokol LDAP odgovara preporuci RFC 1777.

4.1.5 Imenik

(1) Sve potvrde ovjerioca temelje se na standardu X.509 i mogu biti javno objavljene u centralnom imeniku, o kome brine HALCOM CA i u kome je takođe i javni centralni registar opozvanih potvrda.

(2) Pristup imeniku je moguć po protokolu LDAP.

4.2 ZAŠTITNE MjERE I POUZDANOST

4.2.1 Zaštitne mjere i pouzdanost

(1) Oprema HALCOM Sarajevo CA 3 osigurana je i zaštićena protivpožarnim sistemom i sistemom za provjetravanje.

4.3 ODGOVORNOST

4.3.1 Odgovornost

(1) HALCOM Sarajevo CA 3 ne preuzima nikakvu odgovornost za podatke, koje vlasnik potvrde elektronski šifruje ili potpisuje, pa ni u slučaju kada je vlasnik ili treća osoba poštovala sve važeće propise, sve odredbe ove politike i druga pravila Halcom Sarajevo CA 3 odnosno poštovala sva njegova uputstva.

(2) HALCOM Sarajevo CA 3 garantuje usluge u vezi sa elektronskim potpisivanjem brižljivošću dobrog stručnjaka.

5. UPRAVLJANJE POTVRDAMA

5.1 OSNOVNA PRAVILA ZA UPRAVLJANJE POTVRDAMA

(1) Izdavanje i osnovne osobine potvrde:

- izdaje se na osnovu potpisanog obrasca od strane ovlaštenog lica, pravnog lica, osobe i budućeg vlasnika potvrde;
- HALCOM Sarajevo CA 3 je odgovoran samo za upravljanje izdatim potvrdama, kao i za čuvanje i objavljivanje potvrda u javno dostupnom imeniku po protokolu LDAP;
- HALCOM Sarajevo CA 3 ne odgovara za slučajeve do kojih bi došlo zbog pogrešne upotrebe potvrda, kao na primjer:
    - upotrebe potvrda u namjene, koje nisu predviđene ovom politikom,
    - nepravilne ili manjkave zaštite šifre ili posebnih ključeva, izdavanje poverljivih podataka ili ključeva trećim osobama,
    - bilo kakve zloupotrebe odnosno upada u informacijsko -komunikativni sistem vlasnika potvrde i time do podataka od strane treće osobe,
    - nedjelovanja ili lošeg djelovanja informacijsko-komunikativne infrastrukture vlasnika potvrde ili trećih osoba,
    - neprovjeravanja podataka i punovažnosti potvrda u registru opozvanih potvrda,

  - zbog upotrebe potvrda na nestandardni način ili na nelicencnoj programskoj opremi.
- HALCOM Sarajevo CA 3 nije odgovoran za sadržaj podataka, koji se šifruju ili potpisuju njegovim potvrdama ili za ponašanje vlasnika pri upotrebi istih;
- infrastruktura HALCOM Sarajevo CA 3 odgovara najvišim stepenima sigurnosti i zaštite potvrda i ključeva; punovažnost izdatih potvrda osigurana je samo, ako vlasnik poštuje i djeluje u skladu sa preporukama i standardima, koje predlaže HALCOM Sarajevo CA 3.

(2) Svaki vlasnik potvrde ima dva para ključeva za digitalno potpisivanje odnosno šifrovanje:

- privatni ključ za potpisivanje (u nastavku: ključ za potpisivanje),
- privatni ključ za dešifriranje (u nastavku: ključ za dešifriranje),
- javni ključ za verifikaciju potpisa (u nastavku: ključ za ovjeru potpisa) i
- javni ključ za šifriranje (u nastavku: ključ za šifriranje).

(3) Ključ za potpisivanje i dešifriranje ima samo vlasnik.

(4) Javno dostupni podaci iz potvrde su:
- varijanta,
- jednolični serijski broj,
- identitet HALCOM Sarajevo CA 3
- rok punovažnosti potvrde,
- identitet vlasnika potvrde i njegovog pravnog lica
- javni ključ za vlasnika,
- broj politike pod kojim je izdata potvrda(CPoid)
- drugi podaci, za koje tako odredi ta politika ili važeći propis.

(5) Svaki vlasnik potvrde može imati pod istim nabrojanim podacima samo jednu potvrdu.

(6) HALCOM Sarajevo CA 3 ne prenosi lične podatke o vlasnicima potvrda, osim ako se određeni podaci posebno ne zahtjevaju za izvođenje specifičnih podataka odnosno aplikacija, povezanih s potvrdama, ako je to odobrio vlasnik potvrde, ili na zahtjev nadležnog suda, sudije za prekršaje ili upravnog organa.

5.2 NARUDŽBENICA POTVRDE

(1) Potvrda se izdaje na osnovu pravilno ispunjene i potpisane narudžbenice potvrde (u nastavku narudžbenice) od strane pravnog lica i budućeg vlasnika. Narudžbenice su dostupne kod banke, koja djeluje kao prijavna služba.

(2) Zakoniti zastupnik pravnog lica potpisivanjem narudžbenice ovlasti budućeg vlasnika potvrde, da u ime i za račun pravnog lica elektronski potpiše zahtjev za obnovu potvrde, u skladu sa ovom politikom i važećim cjenovnikom HALCOM Sarajevo CA 3, ali samo pod uslovom da je elektronski potpis ovjeren validnom potvrdom koja je izdata ovlaštenom licu ovog pravnog lica.

(3) Prije izdavanja narudžbenice, banka pravno lice i budućeg vlasnika detaljno upoznaje sa politikom i obavještenjem o elektronskom potpisivanju i djelovanju ovjerioca Halcom Sarajevo CA 3.

(4) Prilikom prijema narudžbenice i zahtjeva, banka uz pomoć službeno potvrđene dokumentacije ili podataka iz službenih evidencija, provjerava identičnost pravnog lica i uz pomoć službenog dokumenta sa fotografijom identičnost ovlaštene osobe pravnog lica, koja je potpisala narudžbenicu.

5.3 IZDAVANJE POTVRDE

(1) Proizvodni postupak za potvrde i para ključeva na pametnim karticama sastavljen je od pet jasno odvojenih dijelova (ili funkcija), i njihovih propisno odvojenih podsistema:

- preidentifikacija kartica (generisanje i čuvanje ključeva na kartici, generisanje i čuvanje kodiranog PIN koda na kartici),
- priprema potvrde,
- identifikacija kartica (izdavanje i zapis potvrde, štampanje podataka vlasnika),
- ispisivanje PIN koda
- prenošenje potvrda na kartice i PIN koda, i obavještenja vlasnicima.

(2) Opisani postupak je zamišljen tako da ga ne može obaviti osoba sama pojedinačno.

(3) Vlasnik potvrde mora prilikom preuzimanja potvrde na pametnoj kartici odmah provjeriti podatke u potvrdi i o mogućim greškama ili problemima odmah obavijestiti banku.

5.4 PERIOD PUNOVAŽNOSTI POTVRDE

(1) Uobičajena punovažnost potvrde je tri (3) godine od izdavanja.

(2) HALCOM Sarajevo CA 3 može za pojedinačnu potvrdu odrediti i kraći rok punovažnosti.

5.5 OBNOVA POTVRDE

(1) Samo vlasnik potvrde može da traži obnovu sertifikata.

(2) Vlasnik potvrde može prije isteka validnosti potvrde, elektronskim putem da podnese zahtjev za izdavanje nove potvrde, koju potpiše još validnom potvrdom.

(3) Nakon isteka validnosti potvrde, vlasnik mora ponovo lično da dostavi zahtjev za reizdavanje potvrde.

5.6 POSTUPAK OBNOVE POTVRDE

Postupak obnove potvrde definisan je slijedećim koracima:

- HALCOM Sarajevo CA 3 vlasnika potvrde obavijesti o mogućnosti obnove potvrde,
- korisnik se identifikuje sa još validnom potvrdom (elektronski potpiše zahtjev za izdavanje potvrde, koja se proslijedi do HALCOM Sarajevo CA 3),
- obrada zahtjeva za izdavanje potvrde,
- korisnik otvara aplikaciju za obnovu potvrde,
- HALCOM Sarajevo CA 3 izda potvrdu (koju korisnik preuzima na postojeću pametnu karticu ili USB ključ) i obavesti korisnika putem aplikacije za obnovu.

5.7 OPOZIV POTVRDE I OBJAVLJIVANJE U REGISTRU OPOZVANIH POTVRDA

(1) Opoziv potvrde vlasnik potvrde može zahtjevati bilo kada, ali ga mora zahtjevati u slučaju:

- promjene prepoznatljivog imena (DN),
- kada nosilac potvrde izmjeni ključne podatke, povezane sa potvrdom (ime ili prezime, elektronsku adresu, posao i slično),
- kada se utvrdi ili posumnja da je došlo ili do otkrivanja ključa za potpisivanje ili do zloupotrebe potvrde,
- zamjene potvrde s drugom potvrdom, (npr. prilikom gubitka pametne kartice, gubitka šifre

za pristup podacima na kartici i slično).

(2) HALCOM Sarajevo CA 3 može opozvati potvrdu također i bez zahtjeva vlasnika u slučaju iz prvog pasusa, ili na osnovu zahtjeva nadležnog suda, sudije za prekršaje ili upravnog organa.

(3) Opoziv potvrde moguć je u radnom vremenu od 8.00 do 17.00 sati. Tačna uputstva za opoziv potvrde HALCOM Sarajevo CA 3 javno objavljuje.

(4) Opoziv potvrde važi izmedju vlasnika potvrde i HALCOM Sarajevo CA 3 od trenutka opoziva. U opozivu potvrde mora biti navedeno vrijeme opoziva.

(5) Opoziv uvjek važi od trenutka opoziva nadalje.

(6) Opoziv unazad nije dozvoljen.

(7) HALCOM Sarajevo CA 3 na osnovu pravilnog zahtjeva za opoziv potvrde, potvrdu će opozvati najkasnije za dvadeset četiri (24) sata. U tom periodu opozvana potvrda u imeniku će biti označena kao opozvana i dodata u registar opozvanih potvrda.

6. VLASNICI POTVRDE

6.1 ZAŠTITNE MJERE

(1) Vlasnik potvrde se obavezuje da će digitalno potpisivati samo dokumente, kod kojih zahtjev za punovažnost nije duži od roka punovažnosti potvrde, ili će ako je zahtjev za punovažnost dokumenta duži od roka punovažnosti dokumenta, vlasnik potvrde prije isteka važnosti potvrde zagarantovati da će takvi dokumenti ponovo biti odgovarajuće potpisani upotrebom novog punovažnog dokumenta.

(2) Vlasnik odnosno budući vlasnik potvrde dužan je da:
- pažljivo pročita ovu politiku prije potpisa narudžbenice potvrde, i da prati sva obavještenja HALCOM Sarajevo CA 3 i da se ponaša u skladu sa njima i ovom politikom,
- prati razvoj tehnologije odnosno obavještenja HALCOM Sarajevo CA 3 i na odgovarajući način osavremenjuje potrebnu mašinsku i programsku opremu za siguran rad sa potvrdama,
- upotrebaljava takvu programsku opremu, koja je u skladu sa obavještenjima HALCOM Sarajevo CA 3 (npr. sa dovoljno jakim kriptografskim modulima),
- ključ za potpisivanje i za sve druge povjerljive podatke štiti odgovarajućom šifrom ili na drugi način, tako da pristup njima ima samo vlasnik,
- svim izmjenama, koje su u vezi s potvrdom, odmah obavjesti HALCOM Sarajevo CA 3
- zahtjeva opoziv potvrde, ako je ključ za potpisivanje ugrožen na način, koji utiče na pozudanost upotrebe, ili ako postoji opasnost od zloupotrebe, ili ako su se izmijenili podaci koji su navedeni u potvrdi.

(3) Vlasnik potvrde mora da ispunjava sve zahtjeve ove politike i važećih propisa.

(4) Vlasnik potvrde se obavezuje da će upotrebljavati svoj par ključeva samo u periodu punovažnosti svoje potvrde.

(5) Vlasnik potvrde mora podatke i sredstva za elektronsko potpisivanje čuvati brižljivošću dobrog domaćina i upotrebljavati ih u skladu sa zahtjevima HALCOM Sarajevo CA 3, te spriječiti neovlašten pristup ovim podacima i sredstvima.

6.2 PRAVA VLASNIKA POTVRDE

(1) Vlasnik potvrde može bilo kada zahtjevati sve informacije u vezi sa punovažnošću potvrde, s obzirom na odredbe ove politike i obavještenja HALCOM Sarajevo CA 3

(2) Vlasnik može bilo kada zahtevati opoziv svoje potvrde.

(3) Vlasnik potvrde mora zahtjevati opoziv svoje potvrde, ako su podaci za elektronsko potpisivanje ili informacijski sistem vlasnika potvrde oštećeni ili ugroženi na način koji utiče na pouzdanost oblikovanja elektronskog potpisa, ili ako postoji opasnost zloupotrebe, ili ako su se izmijenili podaci koji su navedeni u potvrdi.

7. PRAVNA LICA

7.1 ZAŠTITNE MJERE

(1) Pravno lice se obavezuje da će vlasnici unutar nje ispunjavati sve odredbe ove politike i važećih propisa.

(2) Pravno lice je dužno da:

- obezbjedi da vlasnici pažljivo pročitaju ovu politiku prije potpisa narudžbenice potvrde, da prate sva obavještenja Halcom Sarajevo CA 3 i postupaju u skladu s njima i ovom politikom,
- osigura nesporno utvrđivanje identičnosti vlasnika potvrde unutar nje u skladu sa važećim propisima (službeni dokument sa fotografijom),
- prati razvoj tehnologije, odnosno obavještenja Halcom Sarajevo CA 3 i na odgovarajući način osavremenjuje potrebnu mašinsku i programsku opremu za siguran rad sa potvrdama, i upotrebljava takvu programsku opremu koja je u skladu sa obaviještenjima Halcom Sarajevo CA 3,
- svim izmjenama, koje su povezane sa potvrdom bilo kog vlasnika unutar nje, odmah obavijesti Halcom Sarajevo CA 3,
- zahtjeva opoziv potvrde, ako su se izmjenili podaci, koji su navedeni u potvrdi.

(3) Troškove potrebne mašinske ili programske opreme, koju predlaže Halcom Sarajevo CA 3 za sigurno čuvanje i korištenje potrebnih podataka za potvrdu na strani vlasnika potvrde, pokriva pravno lice.

7.2 PRAVA PRAVNOG LICA

(1) Pravno lice može bilo kada zahtjevati sve informacije u vezi sa punovažnošću potvrde, u vezi sa odredbama ove politike i obaviještenjima Halcom Sarajevo CA 3.

(2) Pravno lice ima jednaka prava kao vlasnik potvrde unutar nje uključujući i pravo da zahtjeva opoziv potvrde, osim prava na ključ za potpisivanje i drugih prava, za koja tako propisuju određeni propisi. Ako nosilac potvrde i pravno lice izvršavaju prava koja su međusobno suprotna, prevladavaju prava pravnog lica.

8. TREĆA LICA

8.1 ZAŠTITNE MJERE

(1) Pri prvoj upotrebi potvrde Halcom Sarajevo CA 3 po ovoj politici, treće lice, koje se poziva na potvrdu, mora pažljivo pročitati ovu politiku i od tada redovno pratiti sva ovbaviještenja Halcom Sarajevo CA 3.

(2) Treće lice mora uvijek u vremenu upotrebe potvrde detaljno provjeriti, da li potvrda nije u registru opozvanih potvrda.

(3) Ako potvrda sadrži podatke o trećem licu, ono je dužno da zahtjeva opoziv potvrde, ako sazna, da je posebni ključ ugrožen na način koji utiče na pouzdanost upotrebe, ili ako postoji opasnost od zloupotrebe, ili ako su se izmjenili podaci, koji su navedeni u potvrdi.

8.2. PRAVA TREĆEG LICA

(1) Treće lice može se do opoziva potvrde pozivati na takvu potvrdu.

(2) Treće lice može bilo kada zahtjevati sve informacije u vezi sa punovažnošću bilo koje izdate potvrde, s obzirom na odredbe ove politike, i obaviještenja Halcom Sarajevo CA 3.

RJEČNIK TERMINA I SKRAĆENICA

CA	Overilac potvrda. *Angl.: Certification Authority ali Certification Agency*
CCPS	Certificate and Card Production Service – usluga izrade potvrda i kartica i zajma: Izdavanje CA ključa za svakog podređenog ovjerioca Postavljanje CA parametara u CCPS za svakog podređenog ovjerioca Predoličavanje pametnih kartica, u skladu sa nizom standardizovanih proizvoda Izradu visoko kvalitetnih ključeva RSA sa najmanje 1024 bita Čuvanje integriteta predoličenih inteligentnih kartica sa transportnim PIN-om Nabavku predoličenih pametnih kartica za podređene overioce z LCM Oličavanje kartica konačnog entiteta sa povezivanjem podataka vlasnika i javnog ključa, dakle izdavanje potvrda x509 v3 i njihovo stavljanje u pametne kartice Nabavku kartica konačnog entiteta podređenim ovjeriocima, koji nemaju LCM
CPName	Naziv politike djelovanja ovjerioca (*Angl.:Certification Policy Name*), jednolično povezano sa međunarodnim brojem politike djelovanja CPOID (*Angl.:Certification Policy Object Identifier*)
CPOID	Međunarodni broj, koji jednolično određuje politiku djelovanja (*Angl.:Certification Policy Object IDentifier*).
CRL	Certificate Revocation List – spisak opozvanih digitalnih potvrda
DN	Jednolično razlikujući naziv (prim. definiciju Razlikujući naziv). *Angl.: Distinguished Name*
Imenik potvrda	Imenik potvrda po preporuci X.500, gdje su sačuvane potvrde po prepruci X.509 ver. 3, do kojih je moguć pristup po protokolu LDAP
LCM	Local Certificate Manager – sistem za upravljanje potvrdama kod podređenog ovjerioca
LDAP	Leightweight Directory Access Protocol je protokol, koji određuje pristup imeniku i specifikovan je po IETF (Internet Engineering Task Force) preporuci RFC 1777
Nedvosmislena identifikacija	Provjeravanje identiteta je lično provjeravanje identiteta osobe pomoću važećeg ličnog dokumenta ili elektronsko dokazivanje identiteta važećom potvrdom ovjerenom od strane Halcom Sarajevo CA 3 ili od strane Halcom Sarajevo CA 3 priznatih ovjerilaca.
Overilac potvrde	Fizička ili pravna osoba, koja izdaje potvrde ili izvršava druge usluge u vezi sa ovjerom ili elektronskim potpisima. *Angl.:Certification Authority (CA*).
Potvrda	Poslovna potvrda u elektronskom obliku, koja povezuje podatke za provjeravanje elektronskog potpisa sa određenom osobom te potvrđuje njen identitet. *Angl.: Certificate*
Prijavna služba	Služba ili osoba, koja prima molbe za potvrde i preuzima identifikovanje i provjeru identiteta budućih vlasnika u ime ovjerioca potvrda. *Angl.: Registration Authority (RA)*.
Razlikujući naziv	Jednoličan naziv (prim. definiciju DN) u potvrdi, koji nedvosmisleno i jednolično definiše korisnika u strukturi imenika. Primjer za osobu, zaposlenu v Halcom informatika d.o.o.: *cn*=ime prezime%serijski broj*, ou=Support , o=Halcom, c=SI*
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TLS	Transport Layer Security