REPUBLIKA HRVATSKA
MINISTARSTVO GOSPODARSTVA

Klasa: 080-01/11-01/154
Urbroj: 526-04-01-02-01/2-13-29

NACIONALNI PKI

USPOSTAVA I ORGANIZACIJA

Verzija 1.2

Datum: 05. 11. 2013.

Nacionalni PKI
Uspostava i organizacija

AUTORSKA PRAVA

PRIMJEDBE I PROMJENE

Mehanizam upravljanja primjedbama

Napisane i potpisane primjedbe na ovaj dokument moraju biti upućene Povjerenstvu za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i postupke (dalje u tekstu: PMA HR PKI).

Obavijest o finalnim promjenama

Povjerenstvo za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i postupke određuje vremenski period za obavijest o promjenama dokumenta.

PREGLED PROMJENA

Redni broj	Verzija	Točka	Opis promjene	Datum promjene
1	**1.1**		**Usklađivanje s zaključcima HR PKI povjerenstva**	**14. 10. 2013.**
2	**1.2**		**Usklađivanje sa zakonskom regulativom u RH**	**05. 11. 2013.**

Nacionalni PKI

Uspostava i organizacija

OBJAVA

Na temelju odluke o prihvaćanju i objavi dokumenata NCARH-a donijete na sjednici Povjerenstva za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju održanoj dana 14. listopada.2013.godine, Ministarstvo gospodarstva objavljuje navedene dokumente.

U Zagrebu 05. studenog 2013.g.

MINISTAR GOSPODARSTVA

Nacionalni PKI

Uspostava i organizacija

SADRŽAJ

1. UVOD

Na temelju Pravilnika [2] Ministarstvo gospodarstva (dalje u tekstu Ministarstvo) je nadležno za implementaciju Infrastrukture javnog ključa - Public Key Infrastrukture (PKI) u Republici Hrvatskoj.

Zakon [1] koji je usklađen s Direktivom EU [5] definira pravni okvir za uporabu elektroničkog potpisa u RH.

1.1. Infrastruktura javnog ključa - Public Key Infrastructure (PKI)

Elektroničke transakcije i elektroničko poslovanje postaju uobičajeni način za sve vrste poslovanja preko javnih, privatnih i poslovnih mreža.

Iznimno je važan element u elektroničkom poslovanju mogućnost utvrđivanja izvornosti i cjelovitosti elektroničke informacije, na sličan način kao što se utvrđuje izvornost vlastoručno potpisanih dokumenata. Provjeru izvornosti i cjelovitosti informacije u elektroničkom obliku moguće je ostvariti uporabom elektroničkog potpisa. Realizacija elektroničkog potpisa moguća je korištenjem infrastrukture javnog ključa (PKI) koja je zasnovana na primjeni asimetričnog kriptografskog sustava.

Korištenjem PKI omogućava se zaštita izvornosti, cjelovitosti i tajnosti informacija te se omogućuje pouzdana autentifikacija u prijavi na elektroničke usluge. PKI upravlja generiranjem i distribucijom javnog i privatnog ključa, životnim ciklusom certifikata te objavljivanjem certifikata u imenicima.

Infrastrukturu javnog ključa (PKI) čine:

- Tijelo za upravljanje pravilima certificiranja (PMA);
- Certifikacijsko tijelo (CA);
- Registracijsko tijelo (RA);
- Repozitorij;
- Arhiva;
- Korisnici;
- Pouzdajuće strane.

1.2. Tripartitno povjerenje

Tripartitno povjerenje odnosi se na situaciju u kojoj dvije strane unaprijed vjeruju jedna drugoj, iako prethodno nisu uspostavile poslovnu ili osobnu vezu. Povjerenje između ovih dviju strana je moguće ostvariti jer svaka od njih ima uspostavljen odnos sa zajedničkom trećom stranom koja je jamac za uspostavu povjerenja između prve dvije strane.

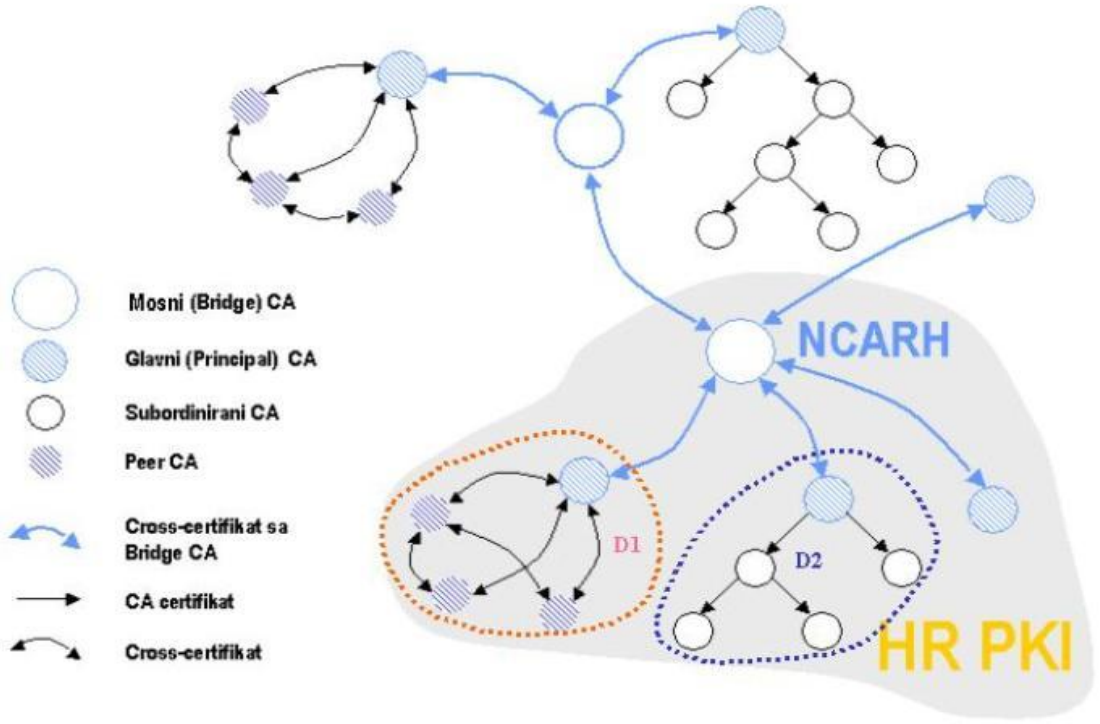
1.3. PKI u Republici Hrvatskoj

Nacionalni PKI u Republici Hrvatskoj se temelji na konceptu mosnog CA (eng. bridge CA). Mosni CA omogućuje certifikacijske veze između glavnih CA-ova (eng. principal CA, PCA) pojedinih PKI domena. Koncept mosnog CA omogućuje spajanje PKI domena u cilju omogućavanja povjerenja u elektroničkom poslovanju za:

- građane,
- državu, tijela državne uprave, tijela lokalne uprave i samouprave,
- investicijski, financijski i bankovni sektor,
- sektor gospodarstva i trgovine,
- itd.

1.3.1. Arhitektura PKI sustava

Na sljedećoj slici je prikazana arhitektura PKI u RH, njegova interoperabilnost i mogućnost povezivanja s drugim PKI domenama izvan RH.



1.3.2. Mosni (Bridge) CA

U svakoj PKI domeni postoji glavni CA (PCA) kao poznata početna točka povjerenja za svoju PKI domenu. PCA pojedine PKI domene se certificira povezujućim certifikatom

(eng. cross certificate) s mosnim CA-om. Povjerenje između PKI domena se postiže usklađenjem (mapiranjem) općih pravila certificiranja (CP-a) između PCA-ova i mosnog CA.

Mosni CA je certifikacijsko tijelo koje u tako stvorenoj povezanoj PKI domeni služi za upravljanje povezujućim certifikatima ostvarujući unilateralno ili bilateralno certificiranje s PCA-ovima unutar pojedine PKI domene.

Mosni CA ne izdaje certifikate krajnjim korisnicima.

1.3.3. PKI domena i arhitektura povjerenja

PKI domena je domena povjerenja kojom upravlja jedan PMA. Unutar iste PKI domene mogu poslovati jedan ili više CA-ova. Svaka PKI domena ima jedan glavni CA (PCA) i vlastiti repozitorij. Povjerenje je usklađeno arhitekturom pojedine PKI domene koja može biti hijerarhijska, povezujuća, miješana ili arhitektura mosnog CA.

1.3.3.1. PKI domena s arhitekturom povezujućeg povjerenja

Glavni CA

Domena s arhitekturom povezujućeg povjerenja ima jedan glavni CA (PCA) koji se međusobno certificira povezujućim certifikatima s mosnim CA-om.

Istorazinski CA

Istorazinski CA (eng. peer CA) je CA iz PKI domene s arhitekturom povezujućeg povjerenja koji ima samopotpisani certifikat. Ovaj certifikat se distribuira njegovim korisnicima koji ga koriste za početak certifikacijske staze. Istorazinski CA-ovi certificiraju se povezujućim certifikatom s drugim CA-ovima unutar svoje PKI domene.

1.3.3.2. PKI domena s arhitekturom hijerarhijskog povjerenja

Root CA

U domeni s arhitekturom hijerarhijskog povjerenja, root CA je početna točka povjerenja. Subjekti i pouzdajuće strane imaju samopotpisani root CA certifikat i započinju stazu povjerenja od te točke. Za hijerarhijske domene povjerenja root CA je glavni (principal) CA.

Subordinirani CA

Subordinirani CA je CA u PKI domeni s arhitekturom hijerarhijskog povjerenja kojim se ne započinje staza povjerenja.

Staza povjerenja započinje od root CA. Subordinirani CA dobiva certifikat od svog nadređenog CA. Subordinirani CA može imati subordinirane CA-ove kojima on izdaje certifikat.

1.4. Nacionalni CA za Republiku Hrvatsku

Nacionalni CA za Republiku Hrvatsku (dalje u tekstu: NCARH), djeluje kao provoditelj povjerenja u HR PKI domeni i uspostavlja vezu između pojedinih PKI domena unutar i izvan Republike Hrvatske.

NCAHR povezuje PKI domene povjerenja parom povezujućih certifikata s PCA-ovima pojedinih PKI domena. NCARH je mosni CA koji djeluje kao most povjerenja i time osigurava:

- povezivanje PKI domena povjerenja unutar Republike Hrvatske te uspostavlja **HR PKI** domenu**,**
- povezivanje HR PKI domene povjerenja s domenama povjerenja izvan Republike Hrvatske.

2. ULOGE/ODGOVORNOSTI U HR PKI

2.1. Ministarstvo gospodarstva

Ministarstvo gospodarstva, (dalje u tekstu: Ministarstvo) nadležno je za provedbu Zakona o elektroničkom potpisu i pripadajućih Pravilnika.

Ministarstvo vodi Evidenciju davatelja usluga certificiranja u Republici Hrvatskoj, te provodi inspekcijski nadzor nad radom davatelja usluga certificiranja

Ministarstvo upisuje davatelje usluga certificiranja u Evidenciju davatelja usluga certificiranja u Republici Hrvatskoj (dalje u tekstu: Evidencija), odmah nakon što davatelj usluge certificiranja podnese prijavu kojom obavještava Ministarstvo o početku obavljanja usluga.

Ministarstvo ima status davatelja usluga certificiranja te je identifikacija Ministarstva kao davatelja usluga ugrađena u sadržaj Evidencije.

2.2. PMA HR PKI

2.2.1.1. Uloga

Ulogu **PMA HR PKI** obavlja Povjerenstvo za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i postupke (dalje u tekstu: PMA HR PKI).

PMA HR PKI donosi, upravlja i objavljuje politike u HR PKI domeni i upravlja radom NCARH i pripadnog repozitorija.

2.2.1.2. Odgovornosti

Ministarstvo provodi inspekcijski nadzor nad NCARH-om i svim glavnim CA-ovima davatelja usluga certificiranja koji interoperiraju s NCARH-om.

PMA HR PKI je odgovoran za sljedeće:

1. identifikaciju međunarodnih i europskih normi iz područja PKI i njihovu implementaciju u HR PKI,
2. uspostavu, odobravanje, održavanje i objavu CP-a za NCARH,
3. odobravanje operativnih postupaka u HR PKI,
4. uspostavu i odobravanje prikladnih mehanizama kontrola i izvještajnih procedura za HR PKI,
5. prihvaćanje zahtjeva od strane davatelj usluga certificiranja koji žele interoperirati s NCARH-om te izdavanje povezujućih certifikata za glavni CA davatelja usluga certificiranja,
6. opoziv certifikata glavnog CA davatelja usluga certificiranja,
7. poticanje na suradnju s prekograničnim PKI domenama,
8. donošenje smjernica za rad i daljnji razvoj NCARH-a.

PMA HR PKI organizira kvartalne sastanke s CA i RA predstavnicima sa sljedećim točkama dnevnog reda:

1. izmjene u CP, CPS i drugim pravilnicima za NCARH,
2. pregled procedura i postupaka koje se odnose na PKI,
3. predlaganje poboljšanja, proširivanja i izmjene NCARH konfiguracije (hardver, softver, lokacije smještaja sustava, itd.),
4. incidenti i nerutinski događaji,
5. povezivanja s drugim PKI domenama,
6. promjene u popisu obvezujućih normi ili u korištenju tehnologije,
7. specijalni izvještaji i studije.

PMA HR PKI može naručiti neovisnu reviziju usklađenosti NCARH, njegovih CP, CPS, planova, procedura i operacija (PMA HR PKI može sugerirati područja revizije, ali ne može ograničiti svrhu revizije). Rezultate revizije pregledava PMA HR PKI i izdati naloge za promjene ako je to potrebno,

2.3. Akreditacija za povezivanje u HR PKI domenu

CSP koji se udružuje u HR PKI mora zadovoljiti akreditacijske kriterije za dobrovoljnu akreditaciju davatelja usluga certificiranja koje objavljuje Hrvatska akreditacijska agencija uz dodatno zadovoljenje usklađenosti politika certificiranja CSP-a s politikama certificiranja NCARH-a.

Za provjeru usklađenosti odgovoran je PMA HR PKI. Provjeru može provesti PMA HR PKI ili može ovlastiti mjerodavno tijelo ili stručni tim.

3. USLUGE CERTIFICIRANJA I DAVATELJI USLUGA

3.1. Nacionalni CA za Republiku Hrvatsku

Na temelju odluke PMA HR PKI, Nacionalni CA za Republiku Hrvatsku (NCARH) izdaje povezujuće certifikate svim davateljima usluga izdavanja certifikata prikladnih za uporabu u HR PKI, a koji ispunjavaju uvjete udruživanja u HR PKI domenu.

3.1.1. Usluge NCARH

Ministarstvo može sklopiti ugovor o obavljanju operativnih usluga za NCARH s fizičkom ili pravnom osobom koja ispunjava uvjete propisane Zakonom [1] i Pravilnicima [2 i 3].

Identifikaciju davatelja usluga certificiranja radi njegovog udruživanja u HR PKI domenu provodi Operativno tijelo Nacionalnog CA za Republiku Hrvatsku (Operation Authority Nacionalnog CA za Republiku Hrvatsku, dalje u tekstu OA NCARH).

Usluge OA NCARH su:

1. Izdavanje povezujućeg certifikata za glavni CA CSP-a u cilju udruživanja u HR PKI domenu,
2. Implementacija funkcija certificiranja povezujućim certifikatima u HR PKI domeni za međusobni rad više davatelja CSP-ova i više tipova certifikata,
3. Provjera korisničkog certifikata u svezi s njegovom pripadnošću HR PKI domeni, što omogućuje pouzdajućoj strani donošenje odluke o prihvaćanju certifikata izdanog od strane CSP-a koji je udružen u HR PKI domenu.
4. Vođenje Evidencije davatelja usluga certificiranja u Republici Hrvatskoj u elektroničkom obliku. Evidencija se javno objavljuje i sadrži informacije o davateljima usluga certificiranja.

3.2. Certifikacijsko tijelo (CA)

Certifikacijsko tijelo (dalje u tekstu: CA) je **POVJERLJIVA TREĆA STRANA** čija je glavna odgovornost pravilno i sigurno potvrđivanje identiteta korisnika.

Izdavanjem certifikata CA potvrđuje da javni ključ koji je ugrađen u certifikat odgovara određenom privatnom ključu. Certifikat uspostavlja elektronički identitet osobe, poslovnog subjekta, aplikacije/servisa, uređaja ili poslužitelja na Internetu.

Da bi se čvrsto vezale informacije o privatnom ključu korisnika i druge informacije, npr. ime i prezime korisnika u certifikatu, CA elektronički potpisuje certifikat svojim privatnim potpisnim ključem.

CA-ovo elektroničko potpisivanje certifikata daje tri važna elementa sigurnosti i povjerenja u izdani certifikat:

1. valjan elektronički potpis na certifikatu je garancija integriteta certifikata,

2. budući da je CA jedina strana koja može pristupiti svom privatnom potpisnom ključu, svatko tko verificira CA-ov potpis u certifikatu se može pouzdati da je samo taj CA mogao izraditi i potpisati korisnikov certifikat.
3. Budući da samo CA ima pristup do svog privatnog potpisnog ključa, CA ne može poricati da je potpisao certifikat (neporecivost).

CA je povjerljiva treća strana u HR PKI domeni i zbog toga CA-ovi moraju biti neovisni, neutralni, pouzdani i prihvatljivi za sve strane koje sudjeluju u komunikaciji.

3.2.1. Usluge CA

CA krajnjim korisnicima pruža sljedeće usluge certificiranja:

1. registracija korisnika;
2. izrada certifikata;
3. isporuka i objava certifikata;
4. upravljanje opozivom certifikata;
5. davanje statusa opozvanosti certifikata.

3.2.1.1. Registracija

Registracija je usluga verifikacije identiteta subjekta i bilježenje informacija korištenih za obavljanje te verifikacije, a prema potrebi i bilježenje nekih specifičnih dodatnih atributa subjekta. Dobiveni rezultat prosljeđuje se usluzi izrade certifikata. Ova usluga može dodatno uključiti provjeru da li subjekt posjeduje privatni ključ koji je povezan s njegovim javnim ključem. Ova se provjera provodi kada korisnik sam generira svoj par ključeva.

3.2.1.2. Izrada certifikata

Izrada certifikata je usluga formiranja i potpisivanja certifikata. U certifikat se upisuju podaci o identitetu subjekta, njegov javni ključ i drugi atributi koji su prethodno bili utvrđeni u procesu registracije.

3.2.1.3. Isporuka i objava certifikata

Isporuka i objava certifikata je usluga isporuke certifikata sukladno ugovoru sa subjektom te usluga objave certifikata kojom se omogućuje dostupnost certifikata pouzdajućim stranama. Ova usluga dodatno može subjektima i pouzdajućim stranama distribuirati informacije o CA, informacije o njegovim politikama i postupcima te opcionalno, objaviti sadržaj posebnih ugovora koje CA sklapa sa subjektima.

3.2.1.4. Upravljanje opozivom certifikata

Ova usluga obrađuje sve zahtjeve i poruke povezane s opozivom certifikata, s ciljem poduzimanja akcija koje će trajno onemogućiti upotrebu nekog certifikata. Rezultati ove usluge se dalje prosljeđuju usluzi davanja statusa opozvanosti certifikata.

3.2.1.5. Davanje statusa opozvanosti certifikata

Ova usluga daje informaciju o statusu opozvanosti certifikata pouzdajućim stranama. Prije ostvarenja pouzdavanja u certifikat, pouzdajuća strana mora provesti provjeru statusa certifikata u cilju utvrđivanja njegove opozvanosti.

Provjera valjanosti i statusa certifikata obavlja se korištenjem CRL liste.

Opoziv certifikata postaje važećim objavom CRL u kojoj je naznačen opoziv tog certifikata.

4. OBAVLJANJE USLUGA CERTIFICIRANJA

4.1. Uvjeti koje mora zadovoljiti davatelj usluga izdavanja certifikata

Uvjeti koje mora zadovoljit davatelj usluga izdavanja certifikata:

Članak 17. Zakona [1]

Davatelj usluga izdavanja kvalificiranih certifikata mora ispunjavati sljedeće uvjete:

1. dokazanu sposobnost i pouzdanost za sigurnu provedbu usluge certificiranja,
2. osigurane uvjete djelovanja sigurnog i ažurnog registra potpisnika te provedbu sigurnog i trenutačnog prekida, odnosno opoziva usluge certificiranja na zahtjev potpisnika,
3. osigurano točno utvrđivanje datuma i vremena (sata i minute) izdavanja ili opoziva certifikata,
4. osiguranu provjeru, na odgovarajući način i u skladu s propisima, identiteta i, ako je potrebno, bilo koja dodatna obilježja osobe za koju se izdaje certifikat,
5. zaposleno osoblje specijalističkog znanja i iskustva potrebnog za pružanje usluga certificiranja, posebice sa sposobnostima na upravljačkoj razini, stručnosti u primjeni tehnologija elektroničkog potpisa i odgovarajućih sigurnosnih procedura, te osiguranu primjenu odgovarajućih upravnih postupaka,
6. pouzdane sustave i proizvode koji su zaštićeni od preinaka i osiguravaju tehničku i kriptografsku sigurnost procesa,
7. pouzdane mjere protiv krivotvorenja, te u slučajevima u kojima generira podatke elektroničkog potpisa, zaštićen i povjerljiv proces generiranja takovih podataka,
8. osiguranu zadovoljavajuću razinu financijskih resursa kako bi mogli djelovati u skladu sa zahtjevima utvrđenima ovim Zakonom,
9. osiguranu pohranu svih relevantnih informacija koje se odnose na kvalificirani certifikat tijekom odgovarajućega vremenskog razdoblja, posebice u svrhu pružanja dokaza o certifikatu za potrebe sudskih postupaka,
10. sigurnosni sustav koji onemogućuje kopiranje podataka za izradu potpisa za osobe za koje se pruža usluga certificiranja,
11. prije sklapanja ugovornog odnosa s osobom koja traži uslugu certificiranja za svoj elektronički potpis, obavijestiti tu osobu u pisanom obliku o preciznim uvjetima koji se odnose na uporabu certifikata, uključujući ograničenja uporabe

certifikata, o postojanju dragovoljnih programa ovlašćivanja i postupaka u slučaju prigovora i žalbi te kod rješavanja međusobnih sporova. Na zahtjev trećih osoba koje vrše uvid u odnosni certifikat odgovarajući dijelovi ovih podataka moraju se staviti na uvid,

12. pouzdani sustav pohranjivanja certifikata u obliku koji omogućuje provjeru kako bi:
    a. unos i promjene radile samo ovlaštene osobe,
    b. izvornost podataka bila podobna za provjeru,
    c. certifikat bio javno dostupan na uvid u slučajevima kad je potpisnik odobrio,
    d. bilo koja tehnička promjena koja bi mogla narušiti sigurnosne zahtjeve bila vidljiva davatelju usluge certificiranja.

Uvjeti koje mora zadovoljit davatelj usluga izdavanja normaliziranih certifikata su jednaki uvjetima koje mora zadovoljiti davatelj usluga izdavanja kvalificiranih certifikata. Svi uvjeti koji se odnose na kvalificirane certifikate, moraju se adekvatno primijeniti na izdavanje normaliziranih certifikata.

4.2. Postupak prijave u Evidenciju

Prema Zakonu [1] davatelji usluga certificiranja ne trebaju dozvolu za početak obavljanja usluga.

Sukladno čl. 15. Zakona [1] davatelj usluga certificiranja mora prijaviti Ministarstvu početak obavljanja usluga certificiranja.

Sukladno čl. 16. Zakona [1] Ministarstvo je nadležno za vođenje evidencije o davateljima usluga certificiranja. Evidencija davatelja usluga certificiranja je javna i vodi se u elektroničkom obliku.

Davatelji usluga izdavanja certificiranja koji obavljaju usluge izdavanja kvalificiranih certifikata moraju u svojim internim pravilima uzeti u obzir sigurnosne zahtjeve određene Zakonom [1].

Davatelj usluga izdavanja certifikata obavlja usluge na temelju ispunjenja uvjeta iz Zakona o elektroničkom potpisu i pravilnika donijetih na temelju tog zakona.

4.2.1. Prijava za upis u Evidenciju

Sukladno čl. 4. i čl. 6. Pravilnika [2] prijava za upis u Evidenciju se podnosi najmanje osam dana prije početka obavljanja usluga certificiranja, na obrascu koji se nalazi u Prilogu 1. Pravilnika o evidenciji davatelja usluga certificiranja u Republici Hrvatskoj.

Uz prijavu o početku obavljanja usluga certificiranja ili u slučajevima promjena u obavljanju usluge, davatelj usluga certificiranja mora priložiti svoje interne akte o načinu i postupcima pružanja usluga certificiranja te o tehničkoj infrastrukturi.

4.2.1.1. Dokumentiranje identiteta davatelja usluga

Članak 6. Pravilnika [2] definira koje podatke i dokumentaciju mora davatelj usluga predati u prijavi o početku obavljanja usluga certificiranja u Republici Hrvatskoj.

Članak 6. Pravilnika [2]

(1) Davatelj usluga certificiranja u prijavi o početku obavljanja usluga certificiranja u Republici Hrvatskoj mora navesti sljedeće:

1. opće podatke o davatelju usluga certificiranja (naziv tvrtke, prezime i ime obrtnika, matični broj/osobni identifikacijski broj davatelja usluga, djelatnost);
2. opće podatke o odgovornoj osobi, ovlaštenim predstavnicima ili zastupnicima, vlasniku – suvlasnicima (stručna sprema odgovorne osobe, specijalnost u struci, iskustvo u struci);
3. dokaze o ispunjenosti uvjeta propisanih Zakonom o elektroničkom potpisu (dalje u tekstu: Zakon) i podzakonskim aktima.

(2) Podaci iz stavka 1. točke 1. i 2. ovoga članka upisuju se u obrazac prijave za upis u Evidenciju (Prilog 1. Pravilnika [2]).

(3) Davatelj usluga izdavanja kvalificiranih certifikata pored podataka iz stavka 1., točaka 1. – 3., dostavlja i dokaz o kakvoći poslovanja ili garanciju strukovne organizacije ili udruge s ovlastima izdavanja garancija.

4.2.1.2. Dokumentacija koja se dostavlja uz prijavu za upis u evidenciju

Članak 7. Pravilnika [2] definira dokumentaciju koju davatelj usluga certificiranja mora dostaviti Ministarstvu uz obrazac prijave za upis u Evidenciju.

Uz obrazac prijave za upis u Evidenciju, koji se nalazi u Prilogu 1. Pravilnika [2], CSP mora u svrhu dokazivanja ispunjavanja uvjeta iz članka 6. stavka 1. točke 3. ovoga Pravilnika, kao i u slučaju promjena u obavljanju tih usluga, Ministarstvu dostaviti sljedeće:

1. interni Pravilnik o postupcima certificiranja (o načinima i postupcima pružanja usluga certificiranja te tehničkoj infrastrukturi) i Opća pravila davanja usluga certificiranja;
2. ispravu o unutarnjoj organizaciji; (npr. statut, akt o osnivanju, obrtnica i dr.);
3. opis tehničke i programske osnovice i sustava fizičke zaštite uređaja, opreme i podataka;
4. opis sigurnosnih rješenja zaštite od neovlaštenog pristupa sustavu i podacima te zaštite integriteta podataka i tajnosti informacija;

5. popis osoblja koje izvršava stručno-tehničke poslove davanja usluga certificiranja, vođenja baza podataka i upravljanja informacijskim sustavom s naznačenim podacima o stručnoj osposobljenosti i radnom statusu;
6. izjava odgovorne osobe pod moralnom i materijalnom odgovornošću da su podaci iz točaka 1.-5. ovog članka istiniti.

Članak 8. Pravilnika [2]

Davatelj usluga certificiranja koji obavlja usluge izdavanja kvalificiranih certifikata mora, uz isprave iz članka 7. Pravilnika [2], dostaviti i sljedeće:

1. ispravu o politici poslovanja (podatke o trgovačkom društvu ili obrtniku kojima se pobliže opisuje dosadašnja djelatnost, reference, tržišna snaga i kvaliteta djelovanja) i vlasničkim odnosima (npr. izvod iz knjige udjela, obrtnica i dr.);
2. Posebna unutarnja pravila o postupcima izdavanja kvalificiranih certifikata i zaštite sustava certificiranja i dopunska unutarnja pravila kojima se osigurava ispravno provođenje zaštitnih i sigurnosnih mjera u sustavu certificiranja;
3. Opća pravila davanja usluga ugradnje naprednog vremenskog žiga;
4. opis sustava fizičke i tehničke zaštite uređaja, opreme i podataka sukladno odredbama Zakona kroz interni Pravilnik o provođenju zaštite sustava certificiranja;
5. opis sigurnosnih rješenja zaštite od neovlaštenog pristupa informacijama;
6. popis i preslike potvrda o stručnoj spremi osoblja koje izvršava stručno – tehničke i organizacijske te upravljačke poslove u sustavu usluga certificiranja i vođenja registra potpisnika;
7. presliku police obveznog osiguranja od odgovornosti za štete u iznosu propisanom pravilnikom kojim se uređuje izrada elektroničkog potpisa, uporaba sredstava za izradu elektroničkog potpisa, opći i posebni uvjeti poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata;
8. ispravu koja dokazuje kvalitetu i stručnosti podnositelja zahtjeva (ISO certifikat, strukovna licenca u području informacijske i komunikacijske tehnologije ili akreditacijska isprava);
9. izjava odgovorne osobe pod moralnom i materijalnom odgovornošću da su podaci iz točaka 1.-8. ovog članka istiniti.

4.3. Postupak upisa u Evidenciju

Sukladno čl. 16. Zakona [1] Ministarstvo upisuje davatelje usluga certificiranja u Evidenciju davatelja usluga certificiranja u Republici Hrvatskoj (dalje u tekstu:

evidencija), odmah nakon što davatelj usluge certificiranja podnese prijavu kojom obavještava Ministarstvo o početku obavljanja usluga.

Sukladno čl. 11. Pravilnika [2] Uredna prijava je prijava koja sadrži sve podatke i sve isprave propisane člancima 6., 7. i 8. Pravilnika [2]. Ministarstvo će odmah po primitku uredne prijave upisati davatelja usluga certificiranja u Evidenciju.

4.4. Tajnost podataka

Ministarstvo, PMA HR PKI i HAA obvezuju se čuvati u strogoj tajnosti sve informacije, pismene ili usmene, koje su primili od davatelja usluga certificiranja i njegovih CA-ova, osim ako Zakon [1] zahtijeva otkrivanje takvih podataka. Informacije koje se nalaze u Evidenciji su javno dostupne.

5. POVEZIVANJE S NCARH

Ovdje su opisane glavne procedure koje mora slijediti Ministarstvo, PMA HR PKI i HAA pri procjeni sposobnosti CA-a davatelja usluga certificiranja koji je podnio zahtjev za povezivanje s NCARH-om.

5.1.1. Ocjena

Sljedeći se termini odnose na ocjenu ispunjavanja zahtjeva pri postupcima dobrovoljne akreditacije:

Zadovoljava	- u potpunosti je ispunjen navedeni zahtjev;
Manjkavost	- djelomično/nepotpuno ispunjen navedeni zahtjev;
Neusklađenost	- nije ipunjen navedeni zahtjev.

5.1.2. Povjerenje

Dobrovoljna akreditacija daje trećim stranama - krajnjim korisnicima CA certifikata, povjerenje da je implementirani CA sustav davatelja usluga izdavanja certifikata siguran i ispunjava uvjete iz Zakona [1] i pravilnika [2 i 3].

5.2. Uvjeti koje treba ispuniti CA

Dobrovoljna akreditacija davatelja usluga certificiranja provodi se prema Upitniku za ocjenjivanje davatelja usluga certificiranja HAA, a na temelju zahtjeva iz Zakona [1], Pravilnika [2 i 3] i Popisa normizacijskih dokumenata [5].

5.3. Postupci dobrovoljne akreditacije CA-a

Postupak dobrovoljne akreditacije davatelja usluga provodi se sukladno Pravilima za dobrovoljnu akreditaciju davatelja usluga certificiranja u području elektroničkog potpisa kojeg izrađuje HAA.

Nakon uspješno provedenog postupka dobrovoljne akreditacije, a na prijedlog vodećeg ocjenitelja, ravnateljica HAA izdaje Potvrdu o dobrovoljnoj akreditaciji davatelja usluga certificiranja u području elektroničkog potpisa. U sklopu Potvrde specificiraju se poslovi izdavanja certifikata i druge usluge povezane s elektroničkim potpisima, te koje zakonske i podzakonske dokumente te norme i tehničke specifikacije je davatelj usluga zadovoljio za poslove navedene u Potvrdi.

5.3.1. Pregled dokumentacije

Svrha i cilj pregleda dokumentacije je da se utvrdi dokumentiranost funkcija sustava upravljanja aktivnostima CA, te da se utvrdi pridržava li se CA u dokumentima CP i CPS zahtjeva odgovarajućih međunarodnih normi.

Osim pregleda dokumentacije vezane uz aktivnosti CA ova faza provjere usklađenosti može uključivati i verifikaciju pravne osobnosti, provjeru pokrića od odgovornosti te analizu internih revizija.

U slučaju da ocjeniteljska skupina HAA utvrdi neusklađenosti i manjkavosti u dokumentaciji može se odrediti razumni rok u kojem CA treba otkloniti utvrđene nedostatke u dokumentaciji.

Izvještaj o pregledu i usklađenosti dokumentacije dostavlja se CA.

5.3.2. Revizija implementacije CA sustava

Akreditacijski tim provodi reviziju implementacije CA sustava u svrhu utvrđivanja pridržava li se CA svojih pravila i postupaka te da li su primijenjeni postupci u skladu sa zahtjevima odgovarajućih međunarodnih normi. Zapažanja se bilježe u revizijskom izvještaju. Izvještaj za svaki kriterij treba sadržavati opis načina na koji CA ispunjava kriterij. Akreditacijski tim daje CA-u revizijski izvještaj.

Akreditacijski tim procjenjuje realne mogućnosti provedbe korektivnih akcija u razumnom roku koje treba poduzeti CA i koje se odnose na otklanjanje utvrđenih manjkavosti u implementaciji CA sustava.

5.4. Odluka o izdavanju povezujućeg certifikata

PMA HR PKI donosi konačnu odluku o izdavanju povezujućeg certifikata na temelju rezultata provjere usklađenosti iz točke 2.2.

CA poduzima korektivne akcije u roku od 60 dana, ako je ustanovljena jedna ili više neusklađenosti. Četiri ili više manjkavosti u odnosu na isti zahtjev kvalificiraju se kao neusklađenost.

Zahtjev će bit odbijen ako nakon korektivnih akcija postoje još neusklađenosti.

Povezujući certifikat će se izdati ako nema neusklađenosti. U slučaju manjkavosti PMA HR PKI daje CA-u mogućnost poduzimanja korektivnih akcija koje će biti provjerene pri sljedećem periodičkom ili izvanrednom pregledu CA poslovanja.

Certifikat je valjan za period od pet godina za pravnu osobu upisanu u sudski registar u RH, odnosno tri godine za pravnu osobu sa sjedištem u inozemstvu za koju se potvrda izdaje pravnoj osobi u Republici Hrvatskoj koja ju zastupa, odnosno predstavlja, isključivši pritom slučajeve suspenzije, opoziva, povlačenja ili prekida rada.

5.5. Pritužbe

Pritužbe na rad i odluke PMA HR PKI mogu se uputiti Ministarstvu.

6. INSPEKCIJSKI NADZOR NAD RADOM DAVATELJA USLUGA CERTIFICIRANJA

Inspekcijski nadzor nad radom davatelja usluga certificiranja provodi Ministarstvo u skladu sa Zakonom [1], Pravilnicima [2 i 3], te Državni inspektorat prema odredbama posebnog zakona.

6.1. Ovlasti Ministarstva

Prema Zakonu [1] Ministarstvo provodi inspekcijski nadzor nad radom davatelja usluga certificiranja.

Članak 36. Zakona [1]

Inspekcijski nadzor nad radom davatelja usluga certificiranja provodi Ministarstvo i Državni inspektorat prema odredbama posebnog zakona.

Nadzor nad radom davatelja usluga certificiranja u području prikupljanja, uporabe i zaštite osobnih podataka potpisnika mogu provoditi i državna te druga tijela određena zakonom i drugim propisima koji uređuju zaštitu osobnih podataka.

Članak 37. Zakona [1]

U okviru inspekcijskog nadzora Ministarstvo je ovlašteno za nadzor nad evidentiranim davateljima usluga certificiranja, te:

- utvrđuje jesu li ispunjeni uvjeti propisani Zakonom [1] i provedbenim propisima donesenim na temelju Zakona [1],
- nadzire pravilnost primjene propisanih postupaka i organizacijsko-tehničkih mjera te primjenu internih pravila koja su u svezi s uvjetima propisanima Zakonom [1] i provedbenim propisima donesenim na temelju Zakona [1].

Ako davatelj usluga certificiranja ne ispunjava uvjete propisane Zakonom [1] i Pravilnicima [2 i 3], ovlašteno tijelo će donijeti rješenje kojim se privremeno zabranjuje davanje usluga certificiranja.

Članak 38. Zakona [1]
Davatelj usluga certificiranja je dužan radi provedbe inspekcijskog nadzora omogućiti ovlaštenom tijelu za provedbu inspekcijskog nadzora neograničen uvid u podatke o poslovanju, uvid u poslovnu dokumentaciju, pristup registru potpisnika i pridruženoj računalnoj opremi i uređajima.

6.2. Svrha inspekcije

Svrha je inspekcije provjeriti postupa li davatelj usluga certificiranja prema Zakonu [1], Pravilnicima [2, 3,], CP-u, CPS-u i prema ostalim dokumentima koje je prezentirao Ministarstvu uz prijavu o početku obavljanja usluga certificiranja.

6.3. Područja koja pokriva inspekcija

6.3.1. Provjera usklađenosti

Provjera usklađenosti će provjeriti sljedeće:

- opisuje li važeća verzija CPS-a dovoljno detaljno tehničke i proceduralne CA postupke i postupke osoblja;
- provodi li CA procedure prema CPS-u;
- provodi li RA procedure prema CPS-u i prema ostaloj CA dokumentaciji.

6.3.2. CA/RA postupci

Posebno se provjerava kako CA i RA provode niže naznačene postupke, a koji moraju biti naznačeni u CPS-u i u odgovarajućim elementima CP-a:

6.3.2.1. Identifikacija i autentifikacija subjekta

- inicijalna registracija;
- autentifikacija za rutinsku obnovu ključeva i certifikata;
- autentifikacija za obnovu ključeva i certifikata nakon opoziva;
- autentifikacija zahtjeva za opoziv.

6.3.2.2. Operativni zahtjevi

- obrada zahtjeva za izdavanje certifikata;
- izdavanje certifikata;
- prihvaćanje certifikata;
- suspenzija i opoziv certifikata;
- arhiviranje zapisa;
- izmjena ključeva.

6.3.2.3. Sadržaj certifikata i CRL

- sadržaj certifikata;
- sadržaj CRL.

6.3.2.4. Postupci s dokumentacijom

- postupci pri promjeni sadržaja dokumentacije;
- objavljivanje dokumentacije;
- postupci prihvaćanja CPS-a.

6.3.2.5. Osoblje

- korisničke uloge;
- kontrola osoblja.

6.3.2.6. Fizička i proceduralna sigurnost sustava

- revizijske procedure sustava sigurnosti;

- kontrole fizičke sigurnosti;
- proceduralne kontrole;
- oporavak sustava nakon incidenta;
- prestanak rada CA.

6.3.2.7. Tehnička sigurnost sustava

- generiranje para ključeva i instaliranje;
- zaštita privatnog ključa;
- ostali aspekti upravljanja parom ključeva;
- aktivacijski podaci;
- kontrole računalne sigurnosti;
- tehničke kontrole životnog ciklusa;
- kontrole sigurnosti računalne mreže;
- kontrole izvedbe kriptografskih modula.

6.4. Rezultati inspekcije

6.4.1. Objava

Ministarstvo nadležno za gospodarstvo će objaviti rezultate inspekcije i zahtijevane korektivne akcije. Te će informacije biti dostupne certifikacijskim tijelima, subjektima i pouzdajućim stranama.

6.4.2. Korektivne akcije

U slučaju da su otkrivene nepravilnosti u radu, CA mora prema PMA HR PKI poslati i prezentirati/obrazložiti plan korektivnih akcija koje će poduzeti da bi se otklonile nepravilnosti koje su navedene u izvještaju inspekcije.

6.5. Sankcije

Ministarstvo nakon izvršenih inspekcija u kojima su utvrđene nepravilnosti podnosi prekršajne prijave protiv potpisnika, fizičke osobe ili odgovorne osobe, pravne osobe koja zastupa potpisnika ili davatelja usluga certificiranja za učinjene prekršaje propisane odredbama članaka 39., 40. i 41. Zakona [1].
Ako davatelj usluga certificiranja ne ispunjava uvjete propisane Zakonom i provedbenim propisima donesenim na temelju ovoga Zakona, ovlašteno tijelo će donijeti rješenje kojim se privremeno zabranjuje davanje usluga certificiranja.

U slučaju opoziva CA certifikata davatelja usluga certificiranja, Ministarstvo briše ime CA iz evidencije davatelja usluga certificiranja u Republici Hrvatskoj. U slučajevima privremenog ili trajnog prekida davanja usluga certificiranja davatelja usluga certificiranja, PMA HR PKI će donijeti odluku o prekidu interoperiranja s tim davatelj usluga.

6.5.1. Smanjenje razine sigurnosti izdanih certifikata

PMA HR PKI ima pravo smanjiti razinu sigurnosti svih certifikata koje izdaje CA davatelja usluga izdavanja certifikata ako davatelj usluga ne poduzme korektivne akcije u periodu od 30 dana nakon što je formalno obaviješten od PMA HR PKI o potrebi da poduzme korektivne akcije.

6.5.2. Opoziv CA certifikata

PMA HR PKI ima pravo opozvati CA certifikat ako davatelj usluga izdavanja certifikata ne poduzme korektivne akcije u periodu od 30 dana nakon što je formalno obaviješten o potrebi da poduzme korektivne akcije

7. NAKNADE ZA USLUGE

7.1. Usluge bez naknade

Naknade se ne mogu naplaćivati za pristup i pregled CP-a i CPS-a te ostalih dokumenata koji su klasificirani kao **Javna dokumentacija u HR PKI.**

7.1.1. Povrat naplaćene naknade

Sve naknade koje su naplaćene krajnjim korisnicima certifikata, a nisu objavljene u cjeniku, definirane i obuhvaćene CP-om, CPS-om i ugovorima sa subjektima, pouzdajućim stranama i RA moraju se vratiti krajnjim korisnicima certifikata.

7.2. Cjenici usluga

CSP naplaćuje naknade za usluge prema objavljenom cjeniku ili prema posebnom ugovoru sa korisnicima.

CSP je dužan cjenik usluga javno objaviti.