



**REPUBLIKA HRVATSKA**  
**MINISTARSTVO GOSPODARSTVA, RADA I PODUZETNIŠTVA**  
*10000 ZAGREB - Ulica grada Vukovara 78*

Klasa: 330-01/04-01/30

Urbroj: 526-01/04-02

# **NACIONALNI PKI**

## **USPOSTAVA I ORGANIZACIJA**

**Verzija 1.0**

**Datum 22.01.2004.**



## AUTORSKA PRAVA

Ovaj je dokument u vlasništvu Ministarstva gospodarstva, rada i poduzetništva i FINE i podložan je zaštiti autorskih prava prema zakonima Republike Hrvatske.

## KRATICE, REFERENCE I DEFINICIJE

Cjelokupna se dokumentacija referencira na zakone, pravilnike, direktive, standarde i NCARH dokumentaciju, nadalje definirani su standardi za tumačenja pojedinih kratica i pojmova koje se koriste u HR PKI i NCARH dokumentaciji.

Dokument **Kratice, reference i definicije** u privitku.

## 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 procedure.

### Obavijest o finalnim promjenama

Povjerenstvo za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i procedure odredit će period za obavijest o finalnim promjenama.

## PREGLED PROMJENA

Redni broj	Verzija	Točka	Opis promjene	Datum promjene



## **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 22.01.2004.godine, Ministarstvo gospodarstva, rada i poduzetništva objavljuje navedene dokumente.

U Zagrebu 15. ožujka 2004.g.

**MINISTAR**  
**Branko Vukelić**



# Nacionalni PKI

## Uspostava i organizacija sustava

### Sadržaj

<b>1. UVOD</b> .....	<b>1</b>
<b>1.1. Infrastruktura javnog ključa - Public Key Infrastructure (PKI)</b> .....	<b>1</b>
<b>1.2. Tripartitno povjerenje</b> .....	<b>1</b>
<b>1.3. PKI u Republici Hrvatskoj</b> .....	<b>2</b>
1.3.1. Arhitektura PKI sustava .....	2
1.3.2. Mosni (Bridge) CA.....	2
1.3.3. Domena i arhitektura povjerenja .....	3
<b>1.4. Nacionalni CA za Republiku Hrvatsku</b> .....	<b>3</b>
<b>2. ULOGE/ODGOVORNOSTI U HR PKI</b> .....	<b>5</b>
<b>2.1. Ministarstvo gospodarstva, rada i poduzetništva</b> .....	<b>5</b>
2.1.1. PMA HR PKI .....	5
2.1.2. HR PKI Akreditacijski tim .....	6
<b>2.2. Ministarstvo znanosti, obrazovanja i športa</b> .....	<b>6</b>
<b>3. DAVATELJI I USLUGE CERTIFICIRANJA</b> .....	<b>7</b>
<b>3.1. Nacionalni CA za Republiku Hrvatsku</b> .....	<b>7</b>
3.1.1. Usluge NCARH.....	7
<b>3.2. Ovjerovitelj (CA)</b> .....	<b>7</b>
3.2.1. Usluge CA .....	8
<b>4. OBAVLJANJE USLUGA CERTIFICIRANJA</b> .....	<b>11</b>
<b>4.1. Dobivanje dozvole za rad</b> .....	<b>11</b>
<b>4.2. Postupak dobivanja dozvole</b> .....	<b>12</b>
4.2.1. Zahtjevnica .....	12
4.2.2. Dokumentiranje poslovne sposobnosti .....	13
<b>4.3. Izdavanje dozvole i upis u registar</b> .....	<b>14</b>
<b>4.4. Tajnost podataka</b> .....	<b>14</b>
<b>5. CROSS CERTIFICIRANJE</b> .....	<b>15</b>
<b>5.1. Definicije</b> .....	<b>15</b>
5.1.1. Ocjena.....	15
5.1.2. Povjerenje.....	15
5.1.3. Uvjeti koje treba ispuniti CA.....	15
<b>5.2. Postupci akreditacije CA-a</b> .....	<b>15</b>
5.2.1. Preliminarna procjena (nije obvezna).....	15
5.2.2. Pregled dokumentacije .....	16
5.2.3. Revizija implementacije CA sustava .....	16
<b>5.3. Odluka o izdavanju cross certifikata</b> .....	<b>16</b>
<b>5.4. Pritužbe</b> .....	<b>16</b>
<b>6. INSPEKCIJSKI NADZOR NAD RADOM DAVATELJA USLUGA CERTIFICIRANJA</b> .....	<b>17</b>
<b>6.1. Ovlasti Ministarstva</b> .....	<b>17</b>
<b>6.2. Svrha inspekcije</b> .....	<b>17</b>
<b>6.3. Područja koja pokriva inspekcija</b> .....	<b>18</b>
6.3.1. Provjera usklađenosti .....	18
6.3.2. CA/RA postupci .....	18

# Nacionalni PKI

## Uspostava i organizacija

## Sadržaj

<b>6.4. Rezultati inspekcije.....</b>	<b>19</b>
6.4.1. Objava .....	19
6.4.2. Korektivne akcije .....	19
<b>6.5. Sankcije.....</b>	<b>19</b>
6.5.1. Smanjenje razine sigurnosti izdanih certifikata.....	20
6.5.2. Opoziv CA certifikata .....	20
<b>7. NAKNADE ZA USLUGE.....</b>	<b>21</b>
<b>7.1. Usluge bez naknade .....</b>	<b>21</b>
7.1.1. Povrat naplaćene naknade .....	21
<b>7.2. Cjenici usluga .....</b>	<b>21</b>
7.2.1. Naknade za temeljne usluge .....	21
7.2.2. Naknade za ostale usluge .....	21

## 1. UVOD

Na temelju ovlasti te Zakonu [1] Ministarstvo gospodarstva, rada i poduzetništva (u daljnjem tekstu Ministarstvo) se odlučilo za implementaciju Infrastrukture javnog ključa - Public Key Infrastrukture (PKI) u Republici Hrvatskoj.

Zakon [1] koji se referencira na smjernice EU [6] 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 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. Infrastruktura koja omogućuje uporabu elektroničkog potpisa naziva se infrastruktura javnog ključa (PKI) i ostvaruje se primjenom asimetričnog kriptografskog sustava.

PKI omogućava tajnost, kontrolu pristupa, integritet, autentifikaciju, neporecivost servisa. PKI upravlja generiranjem i distribucijom javnog i privatnog ključa i objavljuje certifikate u imenicima.

PKI se definira kao:

- Povjerenstvo za upravljanje politikama (Policy Management Authority - PMA),
- Ovjerovitelj (Certification Authority - CA),
- Repozitorij certifikata,
- Sustav opoziva certifikata,
- Sustav backupiranja i obnove ključeva,
- Podrška za neporecivost,
- Automatska obnova ključeva,
- Upravljanje s povješću ključeva,
- Cross certificiranje,
- Vremenski žig,
- SW na strani klijenta.

### 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. To se događa zato jer svaka od njih ima uspostavljen odnos sa zajedničkom trećom stranom, ta je treća strana jamac za uspostavu povjerenja između prve dvije.

# Nacionalni PKI

## Uspostava i organizacija

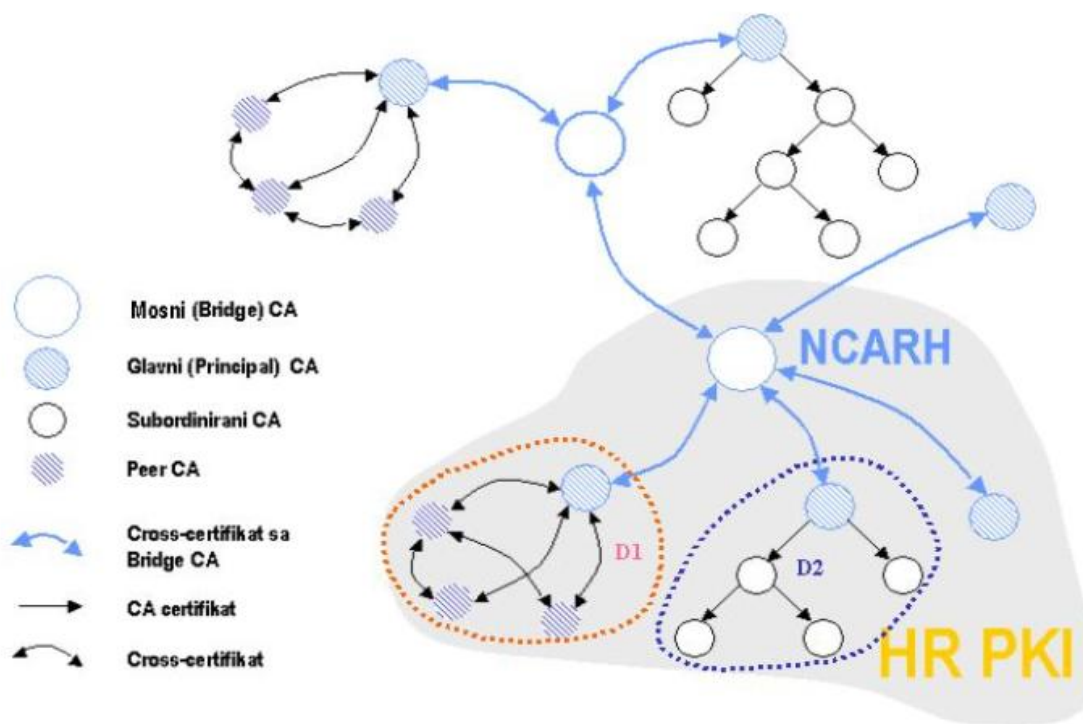
### 1.3. PKI u Republici Hrvatskoj

Nacionalni PKI u RH se temelji na konceptu Bridge CA. Bridge CA omogućuje certifikacijske veze između glavnih (principal) CA-ova (PCA) različitih PKI domena. Ovaj koncept omogućuje spajanje PKI domena za elektroničko poslovanje subjektima kao što su:

- građani,
- država, 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 je slici prezentirana arhitektura PKI u RH, interoperabilnost i povezivanje s drugim PKI domenama izvan RH.



#### 1.3.2. Mosni (Bridge) CA

Prema definiciji Bridge CA, u svakoj domeni PKI postoji glavni (principal) ovjerovitelj (PCA) kao poznata početna točka povjerenja za svoju domenu koji se cross certificira s drugim PCA-om. Povjerenje se postiže usklađenjem (mapiranjem) politika (CP-a) različitih PCA-ova

### 1.3.3. Domena i arhitektura povjerenja

Domena povjerenja je domena kojom upravlja jedan PMA, unutar iste domene može posloovati jedan ili više CA-ova. Svaka domena ima jedan glavni (principal) CA (PCA) i vlastiti repozitorij. Povjerenje može biti hijerarhijsko ili povezujuće.

#### 1.3.3.1. Domena s arhitekturom povezujućeg povjerenja

##### Glavni (Principal) CA

Domena s arhitekturom povezujućeg povjerenja ima jedan glavni CA koji se cross-certificira s Bridge CA.

##### Peer CA

Peer CA je CA iz domene arhitekture s povezujućem povjerenjem ima samopotpisani certifikat koji je distribuiran njegovim korisnicima i koji oni koriste za početak certifikacijske staze. Peer CA-ovi cross-certificiraju s drugim CA-ovima unutar svoje domene povjerenja.

#### 1.3.3.2. 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 domeni s arhitekturom hijerarhijskog povjerenja koji ne započinje stazu povjerenja, povjerenje starta 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 Hrvatsku (dalje u tekstu NCARH), djeluje kao provoditelj povjerenja u domeni HR PKI i uspostavlja vezu između PKI domena unutar i izvan Republike Hrvatske.

NCAHR povezuje domene povjerenja parom cross-certifikata sa PCA-ovima. NCARH je "most povjerenja" (Bridge of trust) i osigurava:

- povezivanje domena povjerenja unutar RH pod imenom **HR PKI**,
- povezivanje domene povjerenja HR PKI s domenama povjerenja izvan Republike Hrvatske,
- izdavanje ARL za CA unutar HRPKI



## 2. ULOGE/ODGOVORNOSTI U HR PKI

### 2.1. Ministarstvo gospodarstva, rada i poduzetništva

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

Ministarstvo izdaje dozvolu za obavljanje usluga certificiranja s izdavanjem kvalificiranih certifikata onim podnositeljima zahtjeva koji ispunjavaju uvjete predviđene Zakonom [1] i pravilnicima [2,3,4 i 5]. Rješenje o ispunjavanju uvjeta donosi se na temelju uvida u dokumentaciju priloženu uz zahtjev za izdavanje dozvole, izravnim razgovorom s ovlaštenim predstavnicima podnositelja zahtjeva te, po potrebi, izravnim uvidom u ispunjenost uvjeta na lokaciji podnositelja zahtjeva.

Ministarstvo ima status ovjervitelja te se identifikacija ministarstva kao ovjervitelja ugrađuje u sadržaj dozvole koju izdaje i u elektroničkom obliku.

Ministarstvo vodi Evidenciju davatelja usluga certificiranja elektroničkih potpisa i Registar davatelja usluga certificiranja elektroničkih potpisa koji izdaju kvalificirane certifikate, te provodi inspeksijski nadzor nad radom davatelja usluga certificiranja.

#### 2.1.1. PMA HR PKI

##### 2.1.1.1. Uloga

**PMA HR PKI** postavlja/upravlja i objavljuje politike u domeni HR PKI i upravlja radom NCARH i repozitorijom.

##### 2.1.1.2. Odgovornosti

PMA je odgovoran za certificiranje i akreditaciju unutar cjelokupne HR PKI i ima odgovornost za nadzor svih PKI operacija. PMA je također odgovoran za sljedeće:

1. uspostavu i odobravanje operativnih standarda i procedura u HR PKI,
2. uspostavu i odobravanje prikladnih mehanizama kontrola i izvještajnih procedura za HR PKI,
3. odobravanje i opoziv certifikata za CA,
4. donošenje odluka u slučaju sporova između CA i RA,
5. uspostavu, odobravanje, održavanje i objavljivanje CP-a za NCARH.,

PMA organizira kvartalne sastanke sa CA i RA predstavnicima sa sljedećim karakterističnim točkama dnevnog reda:

- izmjene u pravilnicima (CP, CPS, Opća pravila sigurnosti),
- pregled procedura koje se odnose na PKI i postupci za pohranjivanje zapisa,
- predlaganje poboljšanja, proširivanja i izmjene NCARH CA konfiguracije (HW, SW, lokacije, itd.),
- incidenti i nerutinski događaji,

# Nacionalni PKI

## Uspostava i organizacija

---

- povezivanja s drugim PKI domenama,
- promjene u standardima ili tehnologiji,
- specijalni izvještaji i studije.

PMA će godišnje:

- naručiti neovisnu reviziju usklađenosti NCARH, njegovih CP, CPS, planova, procedura i operacija (PMA može sugerirati područja revizije, ali ne može ograničiti svrhu revizije),
- pregledati rezultate revizije i izdati naloge za promjene ako je to potrebno,
- pregledati CP i CPS za NCARH i dopustiti ispravke ako je potrebno.

### 2.1.2. HR PKI Akreditacijski tim

Tim koji može formirati PMA HR PKI, a na prijedlog Ministarstva. Zadaća je ovog tima da zajedno s Ministarstvom provodi postupak akreditacije (postupak provjere tehnološke i informatičke sposobnosti) davatelja usluga certificiranja.

## 2.2. Ministarstvo znanosti, obrazovanja i športa

Ministarstvo znanosti, obrazovanja i športa određuje prema Pravilniku [5] tehnička pravila i uvjete povezivanja sustava certificiranja elektroničkih potpisa.

### 3. DAVATELJI I USLUGE CERTIFICIRANJA

#### 3.1. Nacionalni CA za Republiku Hrvatsku

Nacionalni CA za Republiku Hrvatsku (dalje u tekstu NCARH) na temelju odluke PMA HR PKI, izdaje povezujući cross certifikat svim kvalificiranim ovjerviteljima koji ispunjavaju uvjete udruživanja u HR PKI sustav.

##### 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 podzakonskim aktima – pravilnicima [2, 3, 4 i 5]. Identifikacija davatelja usluga je Operation Authority Nacionalnog CA za Republiku Hrvatsku (dalje u tekstu OA NCARH).

Servisi OA NCARH su:

1. Izdavanje elektroničkog oblika dozvole, s kojom je moguće elektronički potvrditi autentičnost kvalificiranog ovjervitelja kojem se izdaje dozvola za rad (Pravilnik [2], članak 14.).
2. Vođenje elektroničkog oblika registra u kojem se javno objavljuju informacije o kvalificiranim ovjerviteljima.
3. Implementacija funkcija cross-certificiranja u HR PKI za međusobni rad više kvalificiranih ovjervitelja i više tipova kvalificiranih certifikata.
4. Provjeru korisničkog certifikata u svezi s njegovom pripadnošću HR PKI-u, što omogućuje pouzdajućoj strani aplikacije u kojima prihvaća kvalificirane certifikate od više kvalificiranih ovjervitelja koji su povezani u HR PKI.

Elektronički oblik dozvole ima profil standardnog X.509 certifikata s dodatnim proširenjima (ekstenzijama), prema kojima je moguće provjeravati udruživost korisničkih certifikata koje izdaju različiti kvalificirani ovjervitelji u HR PKI.

#### 3.2. Ovjervitelj (CA)

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

CA potvrđuje izdavanjem certifikata da određeni javni ključ odgovara određenom privatnom ključu. Certifikat uspostavlja digitalni 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 korisnika) u certifikatu, CA elektronički potpisuje certifikat svojim privatnim potpisnim ključem. CA-ov elektronički potpis daje tri važna elementa sigurnosti i povjerenja u certifikat.

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

# Nacionalni PKI

## Uspostava i organizacija

---

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

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

### 3.2.1. Usluge CA

CA će krajnim korisnicima pružati slijedeće certifikacijske servise:

1. Registracija zahtjeva
2. Generiranje certifikata
3. Distribucija certifikata
4. Prihvaćanje certifikata
5. Upravljanje certifikatom

#### 3.2.1.1. Registracija

Registracija je usluga verifikacije i bilježenja identiteta subjekta i prema potrebi bilježenje nekih specifičnih dodatnih atributa subjekta. Dobiven rezultat prosljeđuje se servisu za generiranje certifikata. Ovaj servis može dodatno uključiti provjeru da li subjekt posjeduje tajni ključ koji se asocira s njegovim javnim ključem. Ova se provjera provodi kada korisnik sam generira svoje ključeve.

#### 3.2.1.2. Generiranje certifikata

Generiranje 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. Distribucija certifikata

Distribucija certifikata je usluga isporuke certifikata sukladno ugovoru sa subjektom. Dodatno ovaj servis može subjektima i pouzdajućim stranama distribuirati informacije o CA, informacije o njegovim politikama i postupcima i opcionalno objaviti sadržaj posebnih ugovora koje CA sklupa sa subjektima.

#### 3.2.1.4. Prihvaćanje certifikata

Prihvaćanje certifikata je usluga bilježenja prihvaćanja certifikata od subjekta. Činom prihvaćanja certifikata od subjekta, certifikat postaje pravomoćan. Certifikati koji nisu prihvaćeni od subjekata ne evidentiraju se u imeniku.

### 3.2.1.5. Upravljanje certifikatom

Ovaj servis obrađuje sve zahtjeve i poruke povezane s prestankom valjanosti certifikata, s ciljem poduzimanja akcija koje će privremeno ili trajno onemogućiti upotrebu nekog certifikata. Rezultati ovog servisa se dalje proslijeđuju servisu koji izvješćuje o stanju valjanosti certifikata.



## **4. OBAVLJANJE USLUGA CERTIFICIRANJA**

### **4.1. Dobivanje dozvole za rad**

Prema Zakonu [1] kvalificirani ovjеровitelj mora ispuniti sljedeće uvjete:

#### **Članak 12.**

Davatelj usluga certificiranja može obavljati usluge certificiranja ako ima:

1. osiguranu organizaciju rada koja jamči kvalitetu izvođenja usluge certificiranja,
2. financijska i materijalna sredstva koja su dovoljna za trajnije izvođenje usluge certificiranja i pokrivanje mogućih šteta, naknade na ime osiguranja i slično,
3. osoblje koje je kvalificirano za izvršavanje odgovarajućih stručno-tehničkih poslova davatelja usluga certificiranja, vođenja registra potpisnika i zaštite osobnih podataka,
4. tehničku i programsku osnovicu koja podržava međunarodne standarde za provedbu usluge certificiranja,
5. sustav fizičke zaštite uređaja, opreme i podataka,
6. sigurnosna rješenja zaštite od neovlaštenog pristupa i oštećenja informacija.

#### **Članak 17.**

Davatelj usluga izdavanja kvalificiranih certifikata mora ispunjavati uz uvjete sadržane u članku 12. ovoga Zakona i sljedeće uvjete:

1. dokazanu sposobnost sigurne provedbe usluga 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 administrativnih i upravljačkih postupaka koji odgovaraju priznatim standardima,
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 takvih podataka,
8. dovoljne financijske resurse za rad u suglasju sa zahtjevima postavljenim za djelovanje financijskih institucija, posebno rizicima iz odgovornosti za štete (prikladnim osiguranjem za štete),

# Nacionalni PKI

## Uspostava i organizacija

---

9. sustav pohrane relevantnih informacija koje se odnose na kvalificirane certifikate za određeno vrijeme, posebno za pružanje evidencije certifikata za potrebe određenih postupaka,
10. sigurnosni sustav koji onemogućuje pohranjivanje i kopiranje podataka za izradu potpisa za osobe u ime kojih se pruža usluga certificiranja,
11. sustav informiranja osoba koje traže uslugu certificiranja o točnim uvjetima korištenja usluga, uključujući bilo koja ograničenja pri korištenju kao i postupaka za rješavanje pritužbi i žalbi. Takve informacije, koje mogu biti dostavljene elektronički, moraju biti napisane i pripremljene u razumljivom obliku na hrvatskom jeziku i latiničnom pismu. Relevantni dijelovi tih informacija moraju također biti raspoloživi na zahtjev trećih osoba koje koriste certifikat,
12. pouzdani sustav pohranjivanja certifikata u obliku koji omogućuje provjeru da bi:
  - a. unos i promjene radile samo ovlaštene osobe,
  - b. informacije mogle biti provjerene za autentifikaciju,
  - c. certifikat bio javno raspoloživ za pretraživanje samo u onim slučajevima za koje je registrirani potpisnik dobio ovlaštenja,
  - d. bilo koja tehnička promjena koja bi mogla narušiti sigurnosne zahtjeve bila poznata davatelju usluge certificiranja.

### 4.2. Postupak dobivanja dozvole

Prema Zakonu [1] dobivanje je dozvole upravni postupak i vodi ga Ministarstvo.

#### Članak 18.

Davatelj usluga izdavanja kvalificiranih certifikata obavlja usluge na temelju dozvole koju izdaje Ministarstvo, na zahtjev davatelja usluge.

Dozvola za izdavanje kvalificiranih certifikata (u daljnjem tekstu: dozvola) ima važnost rješenja izdanog u upravnom postupku.

Dozvola se izdaje u roku od 15 dana od dana podnošenja urednog zahtjeva.

U upravnom postupku za izdavanje dozvole u pitanjima koja nisu uređena ovim Zakonom primjenjuju se odredbe **Zakona o općem upravnom postupku**.

#### 4.2.1. Zahtjevnica

Članak 3. Pravilnika [3] definira način podnošenja Zahtjeva za izdavanje dozvole za obavljanje usluga certificiranja s izdavanjem kvalificiranih certifikata

#### Članak 3.

Davatelj usluga certificiranja u svrhu obavljanja usluga izdavanja kvalificiranih certifikata (kvalificirani ovjervitelj) podnosi Ministarstvu gospodarstva (u daljnjem tekstu: Ministarstvo) zahtjev u pisanom obliku na obrascu Zahtjeva za izdavanje dozvole za obavljanje usluga certificiranja s izdavanjem kvalificiranih certifikata (u daljnjem tekstu: Zahtjevnica) iz Priloga 1.

ovoga Pravilnika i koji je njegov sastavni dio, te elektroničkim putem kroz strukturirani obrazac koji se nalazi u za to predviđenom računalnom sustavu/informacijskoj bazi Registra davatelja usluga certificiranja koji izdaju kvalificirane certifikate, i koji su istovjetni obrascu na papiru.

#### 4.2.1.1. Dokumentiranje identiteta davatelja usluga

Članak 4. Pravilnika [3] definira koje podatke i dokumentaciju mora davatelj usluga predati uz podatke sadržane u Zahtjevnici

##### Članak 4.

Podnositelj zahtjeva za dobivanje dozvole treba uz podatke sadržane u Zahtjevnici priložiti sljedeće:

1. podatke o trgovačkom društvu ili obrtniku kojima se pobliže opisuje dosadašnja djelatnost, reference, tržišna snaga i kvaliteta djelovanja (Quality of Service),
2. dopunske podatke o odgovornoj osobi vezano za stručnu spremu, specijalnost u struci, iskustvo u struci, reference,
3. dopunske podatke o vlasniku-suvlasnicima vezano za stručnu spremu, specijalnost u struci, iskustvo u struci, reference,
4. dokaz o kakvoći poslovanja (ISO specifikacija) ili garanciju (strukovne organizacije/udruge s ovlastima izdavanja garancija),
5. dokaze o ispunjavanju općih uvjeta sadržanih u članku 12. i uvjeta sadržanih u članku 17. Zakona o elektroničkom potpisu, te uvjeta sadržanih u Pravilniku o mjerama i postupcima uporabe i zaštite elektroničkog potpisa, sredstava za izradu elektroničkog potpisa i sustava certificiranja.

#### 4.2.2. Dokumentiranje poslovne sposobnosti

Članak 5. Pravilnika [3] definira što mora podnositelj priložiti u svrhu dokazivanja uvjeta iz Pravilnika [3] Članka 4. stavka 1. točke 5.

##### Članak 5.

U svrhu dokazivanja uvjeta iz članka 4. stavka 1. točke 5. ovoga Pravilnika, podnositelj zahtjeva mora priložiti sljedeće:

1. Izvod iz trgovačkog registra odnosno izvod iz obrtnog registra,
2. Račun dobiti i gubitka i bilancu stanja za pravne osobe, odnosno prijavu poreza na dohodak za fizičke osobe-obrtnike za prethodne tri godine i proteklo razdoblje u godini u kojoj se predaje zahtjev,
3. Podatke o bonitetu (Obrazac BON-1) za pravne osobe i podatke o solventnosti (Obrazac BON-2) za pravne osobe i fizičke osobe-obrtnike,
4. Dokument o organizaciji, politici poslovanja i vlasničkim odnosima,
5. Opća pravila pružanja usluga certificiranja i Pravilnik o postupcima certificiranja (sukladno članku 11. Pravilnika o mjerama i postupcima uporabe i zaštite elektroničkog potpisa, sredstava za izradu elektroničkog potpisa i sustava certificiranja),

# Nacionalni PKI

## Uspostava i organizacija

---

6. Opis sustava fizičke i tehničke zaštite uređaja, opreme i podataka sukladno članku 12. i 17. Zakona o elektroničkom potpisu kroz Pravilnik o provođenju zaštite sustava certificiranja sukladno članku 41. Pravilnika o mjerama i postupcima uporabe i zaštite elektroničkog potpisa, sredstava za izradu elektroničkog potpisa i sustava certificiranja,
7. Opis sigurnosnih rješenja zaštite od neovlaštenog pristupa informacijama,
8. Popis i potvrde o stručnoj spremi osoblja koje izvršava stručno-tehničke i organizacijske te upravljačke poslove u sustavu usluga certificiranja i vođenja registra potpisnika,
9. Presliku police obveznog osiguranja od odgovornosti za štete u iznosu propisanom Pravilnikom o mjerama i postupcima uporabe i zaštite elektroničkog potpisa, sredstava za izradu elektroničkog potpisa i sustava certificiranja,
10. Dokument o kvaliteti i stručnosti podnositelja zahtjeva (ISO serija 9000, strukovne licence u području informacijske i telekomunikacijske tehnologije).

### 4.3. Izdavanje dozvole i upis u registar

Članak 6. i 7. Pravilnika [3] definiraju izdavanje dozvole i upis u registar

#### Članak 6.

Ministarstvo izdaje dozvolu za obavljanje usluga certificiranja s izdavanjem kvalificiranih certifikata onim podnositeljima zahtjeva koji ispunjavaju uvjete predviđene Zakonom, ovim Pravilnikom, Pravilnikom o mjerama i postupcima uporabe i zaštite elektroničkog potpisa, sredstava za izradu elektroničkog potpisa i sustava certificiranja te Pravilnikom o tehničkim uvjetima i normama povezivanja sustava certificiranja.

Rješenje o ispunjavanju uvjeta iz stavka 1. ovog članka donosi se na temelju uvida u dokumentaciju priloženu uz zahtjev za izdavanje dozvole, izravnim razgovorom s ovlaštenim predstavnikom (predstavicima) podnositelja zahtjeva te, po potrebi, izravnim uvidom u ispunjenost uvjeta na lokaciji podnositelja zahtjeva.

#### Članak 7.

Podaci o kvalificiranom ovjervitelju kojemu se izdaje dozvola odnosno odobrava izmjena podataka po već odobrenoj dozvoli trenutno se upisuju u Knjigu kvalificiranih ovjervitelja te u Imenik kvalificiranih ovjervitelja.

### 4.4. Tajnost podataka

Ministarstvo (PMA i akreditacijski tim) obvezuje se čuvati u strogoj tajnosti sve informacije, pismene ili usmene koje je primilo od ovjervitelja i njegovih CA-ova, osim ako zakon zahtijeva otkrivanje takvih podataka. Informacije koje se nalaze u dozvoli za rad bit će javno dostupne.

## 5. CROSS CERTIFICIRANJE

Ovdje su opisane glavne procedure koje mora slijediti akreditacijski tim i Ministarstvo pri procjeni sposobnosti CA-a CSP-a koji je podnio zahtjev za cross certificiranje sa NCARH-om.

### 5.1. Definicije

#### 5.1.1. Ocjena

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

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

#### 5.1.2. Povjerenje

Akreditacija daje trećim stranama - krajnjim korisnicima CA certifikata, povjerenje da je implementirani CA sustav ovjerovitelja koji izdaje kvalificirane certifikate siguran i ispunjava uvjete iz Zakona [1] i pravilnika [2, 3, 4 i 5].

#### 5.1.3. Uvjeti koje treba ispuniti CA

Prema Članku 12. Pravilnika [4] uvjeti koje treba ispuniti CA detaljno su opisani i u tekućoj verziji ETSI [7].

CA mora pokazati da sustav koji upravlja izdavanjem kvalificiranih certifikata ispunjava zahtjeve njegovog CP-a, odnosno da:

- a. ispunjava obveze koje su definirane u ETSI [7] - točka 6.1.
  - *Obveze CA*
- b. ima implementirane kontrole prema kojima se ispunjavaju zahtjevi navedeni u ETSI [7] - točka 7.
  - *CPS,*
  - *PKI upravljanje životnim ciklusom certifikata i ključevima,*
  - *upravljanje sigurnošću i operativnim radom CA,*
  - *organizacijski uvjeti.*

### 5.2. Postupci akreditacije CA-a

#### 5.2.1. Preliminarna procjena (nije obvezna)

Akreditacijski tim može provesti preliminarnu reviziju da bi dobilo globalnu sliku o ispunjavanju uvjeta navedenih u 5.2.3. Zapažanja će bit navedena u posebnom izvještaju koji će biti raspoloživ i CA-u. CA odlučuje hoće ili nastaviti akreditacijski proces.

# Nacionalni PKI

## Uspostava i organizacija

---

### 5.2.2. Pregled dokumentacije

Akreditacijski tim mora imati na raspolaganju kopije relevantnih dokumenata (CP i CPS). Jedan ili više članova tima pregledava dokumentaciju te zapažanja navode u izvještaju o pregledu dokumentacije koji se dostavlja CA-u.

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

### 5.2.3. Revizija implementacije CA sustava

Akreditacijski tim provodi reviziju implementacije CA sustava. Zapažanja se bilježe u revizijskom izvještaju. Izvještaj treba sadržavati za svaki kriterij opis načina na koji CA ispunjava kriterij. Akreditacijski tim daje CA-u revizijski izvještaj, očitovanje CA-a treba biti u pismenom obliku u roku od četiri tjedna.

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.

## 5.3. Odluka o izdavanju cross certifikata

PMA HR PKI donosi konačnu odluku o izdavanju cross certifikata na temelju prijedloga akreditacijskog tima.

Akreditacijski tim predlaže odluku na temelju izvještaja o pregledu dokumentacije, revizijskog izvještaja o implementaciji CA sustava i komentara na CA-ov izvještaj ili CA-ovih komentara na izvještaj.

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 biti odbijen ako nakon korektivnih akcija postoje još neusklađenosti.

Certifikat će se izdati ako nema neusklađenosti. U slučaju manjkavosti akreditacijski tim 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 dozvola izdaje pravnoj osobi u Republici Hrvatskoj koja ju zastupa, odnosno predstavlja, isključivši pritom slučajeve suspenzije, opoziva, povlačenja ili prekida rada.

## 5.4. Pritužbe

Pritužbe na rad i odluke PMA-a mogu se proslijediti Ministarstvu.

## **6. INSPEKCIJSKI NADZOR NAD RADOM DAVATELJA USLUGA CERTIFICIRANJA**

Inspekcijski nadzor nad radom davatelja usluga certificiranja provodi se u skladu sa Zakonom [1], Pravilnicima [2, 3, 4 i 5] i prema preporukama ISO 19011 "Guidelines for quality and environmental management systems auditing".

### **6.1. Ovlasti Ministarstva**

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

#### **Članak 36.**

Inspekcijski nadzor nad radom davatelja usluga certificiranja provodi Ministarstvo.

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.**

U okviru inspekcijskog nadzora Ministarstvo nadzire rad registriranih, odnosno evidentiranih davatelja usluga certificiranja, te:

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

Ako registrirani, odnosno evidentirani davatelj usluga certificiranja ne ispunjava uvjete propisane ovim Zakonom i provedbenim propisima donesenim na temelju ovoga Zakona, državni službenik Ministarstva ovlašten za provedbu inspekcijskog nadzora donosi rješenje u upravnom postupku kojim se privremeno zabranjuje davanje usluga certificiranja.

#### **Članak 38.**

Davatelj je usluga certificiranja dužan radi provedbe inspekcijskog nadzora omogućiti državnim službenicima Ministarstva ovlaštenim 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, 4 i 5], CP-u, CPS-u i prema ostalim dokumentima koje je prezentirao Ministarstvu kao dokumentaciju za dobivanje dozvole za obavljanje usluga certificiranja.

# Nacionalni PKI

## Uspostava i organizacija

---

### 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 dolje naznačene postupke, a koji moraju biti naznačeni u CPS-u i u korespondirajućim elementima CP-a:

##### 6.3.2.1. Identifikacija i autentifikacija subjekta

- Inicijalna registracija,
- Autentifikacija za rutinsku obnovu certifikata i ključa,
- Autentifikacija za obnovu certifikata i ključa nakon opoziva,
- Autentifikacija zahtjeva za opoziv.

##### 6.3.2.2. Operativni zahtjevi

- Obrada zahtjeva za certifikat,
- 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, i
- 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 mreže, i
- Kontrole izvedbe kriptografskih modula.

## 6.4. Rezultati inspekcije

### 6.4.1. Objava

PMA HR PKI će objaviti rezultate inspekcije, zahtijevane korektivne akcije i te će informacije bit dostupne ovjeroviteljima, subjektima i pouzdajućim stranama.

### 6.4.2. Korektivne akcije

U slučaju da su otkrivene nepravilnosti u radu, CA mora 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 članka 39., 40. i 41. Zakona [1].

Ako se tijekom inspekcije utvrdi da registrirani davatelj usluga certificiranja ne ispunjava uvjete propisane Zakonom i provedbenim propisima, državni službenik Ministarstva ovlašten za provedbu inspeksijskog nadzora donosi rješenje u upravnom postupku kojim se privremeno ili trajno zabranjuje davanje usluga certificiranja.

U slučaju opoziva CA certifikata i/ili ukidanja dozvole za rad kvalificiranom ovjerovitelju, Ministarstvo briše ime CA iz registra kvalificiranih ovjerovitelja.

# Nacionalni PKI

## Uspostava i organizacija

---

### 6.5.1. Smanjenje razine sigurnosti izdanih certifikata

PMA HR PKI ima pravo smanjiti razinu sigurnosti svih certifikata koje izdaje CA kvalificiranog ovjervitelja subjektima ako kvalificirani ovjervitelj 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 kvalificirani ovjervitelj 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 i 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

Kvalificirani ovjervitelj naplaćuje naknade za usluge prema publiciranom cjeniku ili prema posebnom ugovoru te mora obavijestiti Ministarstvo i krajnje korisnike (subjekte i pouzdajuće strane) o svim uslugama koje će se naplaćivat.

#### 7.2.1. Naknade za temeljne usluge

Naknade za ove usluge nalaze se u sljedećoj tablici:

Vrsta usluge	CSP - opis usluge	Iznos naknade
Inicijalno izdavanje		
Obnova		
Suspenzija		
Opoziv		
Pristup arhivi		
Ostalo		

#### 7.2.2. Naknade za ostale usluge

CA i RA mogu odrediti i naplaćivati razumne naknade za ostale PKI usluge. Naknade za ove usluge nalaze se u sljedećoj tablici:

Vrsta usluge	CSP - opis usluge	Iznos naknade
Isporuka i implementacija SW za LRA službenika		
Obuka i priručnik za LRA službenika		

# Nacionalni PKI

## Uspostava i organizacija

---

Vrsta usluge	CSP - opis usluge	Iznos naknade
Isporuka HW za PKI klijenta (kriptomodul i čitač)		
Isporuka SW za PKI klijenta		
Pomoć krajnjim korisnicima pri implementaciji i operativnom korištenju PKI HW, SW i certifikata		
Obuka o sigurnosti		
Ostalo		