



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

Klasa: 330-01/04-01/30

Urbroj: 526-01/04-01

# **NACIONALNI PKI**

**KRATICE, REFERENCE I DEFINICIJE**

**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.

## **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 će odrediti period za obavijest o finalnim promjenama.

## **PREGLED PROMJENA**

<b>Redni broj</b>	<b>Verzija</b>	<b>Točka</b>	<b>Opis promjene</b>	<b>Datum promjene</b>



## **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.siječnja 2004.godine, Ministarstvo gospodarstva, rada i poduzetništva objavljuje navedene dokumente.

U Zagrebu 15. ožujka 2004.g.

  
**MINISTAR**  
**Branko Vukelić**



# Nacionalni PKI

## Kratice, reference i definicije

### Sadržaj

1. KRATICE .....	1
2. REFERENCE .....	3
3. DEFINICIJE.....	5



# Nacionalni PKI

## Kratice, reference i definicije

---

Cjelokupna se HR PKI dokumentacija referencira na zakone, pravilnike, direktive, standarde i NCARH dokumentaciju, nadalje uvodi se standard za tumačenja pojedinih pojmova i kratice koje se koriste u HR PKI dokumentaciji.

### 1. KRATICE

Za cjelokupnu se HR PKI / NCARH dokumentaciju uvodi jedinstvena definicija kratice kako slijedi:

KRATICA	ZNAČENJE	
	Engleski	Hrvatski
ARL	Authority Revocation List	Lista opozvanih ovjervitelja
CA	Certification Authority	Ovjervitelj
CP	Certification Policy	Opća pravila certificiranja
CPS	Certification Practice Statement	Izjava o postupcima izdavanja certifikata
CRL	Certificate Revocation List	Lista opozvanih certifikata
CSP	Certification Service Provider	Davatelj usluga certificiranja
DLL	Dynamically linked library	
DN	Distinguished Name	Jedinstveno ime
DNS	Domain Name System	
DSA	Digital signature algorithm	Algoritam elektroničkog potpisivanja
ECDSA	Eliptic Curve Digital signature algorithm	Algoritam elektroničkog potpisivanja koji koristi eliptičke krivulje (za asimetrično kriptiranje)
HW	Hardware	Sklopovlje
I&A	Identification and Authentication	Identifikacija i autentifikacija
ISO	International Standards Organization	Međunarodna organizacija za standarde
LDAP	Lightweight Directory Access Protocol	
LRA	Local Registration Authority	Lokalni registracijski ured
NCARH		Nacionalni CA za Republiku Hrvatsku
OID	Object Identifier	Identifikator objekta

# Nacionalni PKI

## Kratice, reference i definicije

---

KRATICA	ZNAČENJE	
	Engleski	Hrvatski
PCA	Principal Certification Authority	Glavni CA
PIN	Personal Identification Number	Osobni identifikacijski broj
PKCS	Public Key Cryptography System	Kriptografski sustav javnog ključa
PKI	Public Key Infrastructure	Infrastruktura javnog ključa
PKIX-CMP	PKIX - Certificate Management Protocol	
PMA	Policy Management Authority	Povjerenstvo za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i procedure Vidjeti značenje u tablici definicija
RA	Registration Authority	Registracijski ured
RCA	Root Certification Authority	Osnovni ( <i>glavni ili početni</i> ) ojerovitelj
SS	Shared Secret	Zajednička tajna
SSCD	Secure Signature Creation Device	Sigurno sredstvo za izradu elektroničkog potpisa
SSL	Secure Sockets Layer	
SW	Software	Programska podrška
URL	Uniform Resource Locator	
X.500		ITU-T standard koji opisuje protokol imenika organiziran u okviru države, regije, organizacije itd.
X.501		ITU-T standard za upotrebu DN u X.500 imeniku
X.509		ITU-T standard za certifikate X.509 verzija 3. odnosi se na certifikate koji mogu imati ekstenzije

## 2. REFERENCE

U cjelokupnu će se HR PKI / NCARH dokumentaciju reference ugrađivat po brojevima kako slijedi:

### 2.1. Zakoni i pravilnici

- [1] **Zakon o elektroničkom potpisu (NN 10/02)**
- [2] **Pravilnik o evidenciji davatelja usluga certificiranja elektroničkih potpisa (NN 54/02)**
- [3] **Pravilnik o registru davatelja usluga certificiranja elektroničkih potpisa koji izdaju kvalificirane certifikate (NN 54/02)**
- [4] **Pravilnik o mjerama i postupcima uporabe i zaštite elektroničkog potpisa i naprednog elektroničkog potpisa, sredstava za izradu elektroničkog potpisa, naprednog elektroničkog potpisa i sustava certificiranja i obveznog osiguranja davatelja usluga izdavanja kvalificiranih certifikata (NN 54/02)**
- [5] **Pravilnik o tehničkim pravilima i uvjetima povezivanja sustava certificiranja elektroničkih potpisa (NN 89/02)**

### 2.2. Direktiva Europskog parlamenta

- [6] **Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.**

### 2.3. Standardi

- [7] **ETSI TS 101 456 v.1.2.1 (2002-04):**
  - *Policy requirements for certification authorities issuing qualified certificates.*
- [8] **ETSI TS 101 862:**
  - *Qualified certificate profile.*
- [9] **IETF RFC 2527:**
  - *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*
- [10] **IETF RFC 2459:**
  - *Internet X.509 Public Key Infrastructure Certificate and CRL Profile.*
- [11] **IETF RFC 3049:**
  - *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*
- [12] **BS 7799-2:1999**
  - *Information security management – Specification for information security management systems*
- [13] **CWA 14172-2**
  - *EESSI Conformity Assessment Guidance – Part 2. Certification Authority services and processes*

# Nacionalni PKI

## Kratice, reference i definicije

---

- [14] EN 45012:1998
  - *General requirements for bodies operating assessment and certification/registration of quality systems*
- [15] ISO 17799
  - *Information security management – Code of practice for information security management*
- [16] ISO 19011:2002
  - *Guidelines for quality and environmental management systems auditing*

### 2.4. NCARH dokumentacija

- [17] NCARH Opća pravila certificiranja (CP)

*Verzija 1.0*

*Opća pravila certificiranja - Certificate Policy (CP) opisuje postupke koje primjenjuje Ministarstvo gospodarstva, rada i poduzetništva, da bi se ispunili zahtjevi iz Zakona o elektroničkom potpisu.*

- [18] NCARH Opća pravila o sigurnosti

*Verzija 1.0*

*Opća pravila o sigurnosti opisuju temeljne sigurnosne postavke u HR PKI.*

### 2.5. Poslovnici

- [19] Poslovnik o radu Povjerenstva za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i procedure

### 3. DEFINICIJE

Pojedini izrazi koji se koriste u HR PKI / NCARH dokumentaciji imaju sljedeća značenja kako slijedi:

POJAM	ZNAČENJE
<b>Akreditacija</b>	Postupak u kojem akreditacijski tim provjerava je li CA sposoban za obavljanje poslova izdavanja kvalificiranih certifikata.
<b>Akreditacijski tim</b>	Tim koji formira PMA HRPKI. Zadaća ovog tijela je provođenje postupka akreditacije (postupak provjere sposobnosti) davatelja usluga certificiranja.
<b>Aktivacijski podaci</b>	Tajni podaci potrebni za pristup ili aktivaciju kriptomodula (primjerice PIN, lozinka ili ključ koji posjeduje osoba, a služi za otključavanje privatnog ključa prije kreiranja elektroničkog potpisa ili dekripcije)
<b>Asimetrični kriptografski sustav</b>	Asimetrični kriptografski sustav jest sustav koji u načelu omogućuje enkripciju i dekripciju podataka s različitim ključevima koji su međusobno asocirani. Poznavanjem samo jednog od ključeva nije moguće jednostavno izlučiti drugi ključ.
<b>CA certifikat</b>	Početni certifikat u certifikacijskom lancu PKI hijerarhije. CA certifikat je izrađen kao dio uspostave i aktivacije CA. CA certifikat sadrži javni ključ koji odgovara CA privatnom potpisnom ključu koji se koristi za kreiranje ili upravljanje certifikatima. CA certifikati i njihovi korespondirajući javni ključevi mogu biti ugrađeni u SW ili poslani elektroničkim putem ili preko dostavljača Pouzdajućim stranama u svrhu uspostave certifikacijskog lanca.
<b>CA privatni potpisni ključ</b>	Privatni ključ koji odgovara CA javnom ključu upisanom u CA certifikat i koji se koristi za potpisivanje certifikata.
<b>CA privatni root ključ</b>	Privatni ključ koji se upotrebljava za potpisivanje CA certifikata.
<b>Certifikat</b>	Zapis u elektroničkom obliku koji: <ul style="list-style-type: none"><li>▪ identificira CA organizaciju koja izdaje certifikate</li><li>▪ je elektronički potpisan od strane CA</li><li>▪ imenuje ili identificira Subjekta</li><li>▪ identificira period valjanosti certifikata</li><li>▪ ima značenje u skladu s primjenjivim zakonima i</li></ul>

# Nacionalni PKI

## Kratice, reference i definicije

---

POJAM	ZNAČENJE
	standardima Certifikat ne uključuje samo njegov aktualni sadržaj nego i sve dokumente na koje se poziva ili koji su u njega ugrađeni.
<b>Cross certifikat - povezujući certifikat</b>	Certifikat koji se koristi za uspostavu odnosa povjerenja između dva ili više CA
<b>Davatelj usluga certificiranja (CSP)</b>	Pravna ili fizička osoba koja izdaje certifikate i osigurava druge servise koji su povezani s infrastrukturom koja omogućuje elektronički potpis.
<b>Dokazivanje identiteta od treće strane</b>	Dokazivanje identiteta od treće strane je proces kojim CA potvrđuje informacije o subjektu koje je dobio kroz registraciju, provjerom preko drugih organizacija koje daju informacijske servise.
<b>Dozvola za obavljanje usluga certificiranja s izdavanjem kvalificiranih certifikata</b>	Dokument koji izdaje Ministarstvo gospodarstva, rada i poduzetništva onim podnositeljima zahtjeva koji ispunjavaju uvjete predviđene Zakonom o elektroničkom potpisu i pripadajućim pravilnicima.
<b>Elektronički uređaj</b>	Računalni HW ili drugo elektroničko ili automatsko sredstvo, konfigurirano i osposobljeno od osobe, koje radi kao njen agent, i koje inicira ili odgovara na elektroničke poruke, u cjelosti ili djelomično, bez kontrole ili intervencije te osobe.
<b>Elektronički potpis</b>	Skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta.
<b>Elektronički zapis</b>	Cjelovit skup podataka koji su elektronički generirani, poslani, primljeni ili sačuvani na elektroničkom, magnetnom, optičkom ili drugom mediju. Sadržaj elektroničkog zapisa uključuje sve oblike pisanog i drugog teksta, podatke, slike i crteže, karte, zvuk, glazbu, govor, računalne baze podataka.
<b>Generiranje ključeva</b>	Proces kreiranja para ključeva
<b>Identifikacija i Autentifikacija (I&amp;A)</b>	I&A je utvrđivanje i potvrda identiteta korisnika certifikata (fizičke osobe (građanina) i poslovnog subjekta) odgovarajućim upitima i provjerama
<b>Identifikator objekta (OID)</b>	Jedinstveni alfanumerički/numerički identifikator registriran pod ISO standardom za određivanje specifičnog

# Nacionalni PKI

## Kratice, reference i definicije

---

POJAM	ZNAČENJE
	objekta ili klase objekata.
<b>Ime subjekta</b>	Polje certifikata koje sadrži jedinstveni identifikator imena Subjekta
<b>Infrastruktura javnog ključa (PKI)</b>	Arhitektura, organizacija, tehnike, operativni zahvati i procedure koje zajednički podržavaju implementaciju i rad sustava kriptografije javnog ključa temeljenog na certifikatima.
<b>Izdavanje certifikata</b>	Radnje obavljene od strane CA (ovjervitelja) u kreiranju certifikata, navođenjem sebe kao ovjervitelja kao i obavještanje tražitelja o sadržaju certifikata, njegovoj spremnosti i dostupnosti za prihvaćanje
<b>Izjava o postupcima izdavanja certifikata (CPS)</b>	Dokument koji sadrži operativne postupke prema IETF RFC 2527 koje CA koristi pri kreiranju, izdavanju, upravljanju i opozivu certifikata, sukladno politikama definiranim u CP-u
<b>Javni ključ (Public key)</b>	Javni ključ u PKI je ključ koji je javno dostupan i služi za provjeru elektroničkog potpisa.
<b>Jedinstveno ime subjekta (DN)</b>	<p>Jedinstveno ime omogućava pronalaženje subjekta u imeniku.</p> <p><b>Poslovni certifikati</b></p> <p>Jedinstveno ime u poslovnom certifikatu formira se iz sljedećih atributa:</p> <ul style="list-style-type: none"> <li>▪ naziv organizacije i organizacijskog dijela</li> <li>▪ matični (ID) broj</li> <li>▪ prezime i ime ovlaštene osobe</li> <li>▪ serijski broj</li> </ul> <p><b>Osobni certifikati</b></p> <p>Jedinstveno ime u osobnom certifikatu formira se iz sljedećih atributa:</p> <ul style="list-style-type: none"> <li>▪ prezime i ime</li> <li>▪ serijski broj</li> </ul>
<b>Klijent</b>	Klijent kojemu CA pruža PKI usluge (fizičke osobe/građani i poslovni subjekti)
<b>Ključ</b>	Generalni izraz korišten kroz cijelu dokumentaciju a obuhvaća sve definirane ključeve spomenute u ovoj tablici

# Nacionalni PKI

## Kratice, reference i definicije

---

POJAM	ZNAČENJE
<b>Ključ za enkripciju</b>	Privatni ključ iz para ključeva koji upotrebljava Subjekt za dekripciju poruke koja je enkriptirana javnim ključem iz para ključeva.
<b>Krajnji korisnik</b>	Subjekt ili Pouzdajuća strana
<b>Kriptografija javnog ključa</b>	Tip kriptografije poznat i kao asimetrična kriptografija koja koristi par ključeva za sigurnu enkripciju i dekripciju poruka
<b>Kriptomodul</b>	Siguran softver ili uređaj koji: <ul style="list-style-type: none"><li>▪ generira par ključeva</li><li>▪ sprema kriptografske informacije i/ili</li><li>▪ obavlja kriptografske funkcije</li></ul>
<b>Kvalificirani certifikat</b>	Certifikat koji udovoljava zahtjevima iz članka 11. Zakona [1] i koji izdaje kvalificirani ovjerovitelj a koji ispunjava uvjete iz članka 17. Zakona [1].
<b>Kvalificirani ovjerovitelj</b>	Pravna ili fizička osoba koja izdaje kvalificirane certifikate ili daje druge usluge povezane s elektroničkim potpisima.
<b>Lightweight Directory Access Protocol (LDAP)</b>	Klijent-poslužitelj protokol korišten za pristup servisima x.500 imenika putem interneta
<b>Lista opozvanih certifikata (CRL)</b>	Podatkovna osnovica ili druga vrsta liste koja sadrži popis certifikata opozvanih prije isteka njihovog perioda valjanosti
<b>Lista opozvanih ovjerovitelja (ARL)</b>	Popis (lista) opozvanih CA certifikata. ARL je CRL CA certifikata
<b>Napredni elektronički potpis</b>	Elektronički potpis koji pouzdano jamči identitet potpisnika i koji udovoljava zahtjevima sadržanim u članku 4. Zakona [1], odnosno elektronički potpis koji: <ul style="list-style-type: none"><li>▪ je povezan isključivo sa Subjektom</li><li>▪ nedvojbeno identificira Subjekta</li><li>▪ nastaje korištenjem sredstava kojima Subjekt može samostalno upravljati i koja su isključivo pod nadzorom Subjekta</li><li>▪ sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka</li></ul>
<b>Online provjera statusa</b>	Provjera valjanosti statusa certifikata online u realnom vremenu. Online provjera statusa koja uključuje CRL, sastoji se u provjeri zadnje izdane CRL (ne uključuje uvid u spremljene CRL)

# Nacionalni PKI

## Kratice, reference i definicije

POJAM	ZNAČENJE
<b>Opća pravila certificiranja-Certification Policy (CP)</b>	Dokument koji sadrži skup pravila prema IETF RFC 2527 koji dokazuju primjenjivost certifikata na određenu zajednicu i klase aplikacija, te precizira identifikacijski i autentifikacijski proces potreban prije izdavanja certifikata, sadržaj certifikata i ostale dozvoljene načine korištenja certifikata
<b>Operativni period</b>	Stvarno vrijeme valjanosti certifikata, koje počinje s prvim danom perioda valjanosti certifikata i završava najranije: <ul style="list-style-type: none"><li>▪ istekom perioda valjanosti koji je označen u certifikatu, ili</li><li>▪ opozivom certifikata</li></ul>
<b>Operativno osoblje</b>	Osobe koje su zaposlenici CA/RA i one su kvalificirane za takve poslove.
<b>Opoziv</b>	Radnja koja certifikat čini nevažećim od tog trenutka pa nadalje. Opoziv postaje važeći objavom ili uvrštenjem u podatkovnu osnovicu opozvanih certifikata (uključenjem u CRL).
<b>Out of-band</b>	Komunikacija drugim kanalom između dvije strane koja se sastoji od načina ili metode, različite od tekuće metode komunikacija, primjerice metoda u kojoj jedna strana upotrebljava poštu za komuniciranje s drugom stranom da bi potvrdila tekuću komunikaciju koja se dogodila kroz online aplikaciju.
<b>Ovjerovitelj (CA)</b>	Pravna ili fizička osoba autorizirana od PMA da izdaje i potpisuje certifikate u skladu sa CP-om.
<b>Ovlaštena osoba u poslovnom certifikatu</b>	Osoba koja je član organizacije, i koja je autorizirana od organizacije za dobivanje certifikata, koji identificira organizaciju i činjenicu da je osoba povezana s organizacijom.
<b>Par ključeva</b>	Dva matematički povezana ključa (privatni ključ i njegov odgovarajući javni ključ), koja imaju svojstva da: <ul style="list-style-type: none"><li>▪ jedan ključ može biti iskorišten za enkripciju komunikacije koja može biti dekriptirana samo korištenjem drugog ključa, i</li><li>▪ je u slučaju poznavanja samo jednog ključa nemoguće otkriti drugi ključ</li></ul>
<b>Period valjanosti</b>	Period valjanosti certifikata koji počinje: <ul style="list-style-type: none"><li>▪ "Vrijedi od" i završava danom</li><li>▪ "Vrijedi do", ili</li></ul>

# Nacionalni PKI

## Kratice, reference i definicije

POJAM	ZNAČENJE
	<ul style="list-style-type: none"><li>▪ "Datum aktiviranja" i završava danom</li><li>▪ "Datum isteka"</li></ul>
<b>Povjerenstvo za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i procedure (PMA - Policy Management Authority)</b>	Povjerenstvo (tijelo) Ministarstva gospodarstva, rada i poduzetništva koje je odgovorno za postavljanje, uvođenje i administriranje odluka koje se odnose na HR PKI politike, procedure i dokumentaciju.
<b>Podaci za izradu elektroničkog potpisa</b>	Jedinstveni podaci, poput kodova ili privatnih kriptografskih ključeva, koje potpisnik koristi za izradu elektroničkog potpisa.
<b>Podaci za verificiranje elektroničkog potpisa</b>	Podaci poput kodova ili javnih kriptografskih ključeva, koji se koriste u svrhu verificiranja (ovjere) elektroničkog potpisa.
<b>Politika za izdavanje kvalificiranih certifikata</b>	Politika za izdavanje kvalificiranih certifikata koja zadovoljava sve odredbe Zakona [1] i direktive EU [10]
<b>Potpisnik</b>	Osoba koja posjeduje sredstvo za izradu elektroničkog potpisa kojim se potpisuje, a koja djeluje u svoje ime ili u ime fizičke ili pravne osobe koju predstavlja.
<b>Pouzdanja strana</b>	Primatelj certifikata, koji djeluje temeljem pouzdanja u certifikat. Certifikat mu omogućuje provjeru cjelovitost i izvornosti elektronički potpisanog zapisa ( <i>Relaying party</i> prema IETF RFC 2527)
<b>Pouzdan sustav</b>	Računalni HW i SW koji: <ul style="list-style-type: none"><li>▪ je razumno siguran od upada i zlouporabe</li><li>▪ omogućuje razumnu razinu raspoloživosti, i</li><li>▪ razumno je prikladan za izvođenje funkcija koje su mu namijenjene</li></ul>
<b>Povjerljiva korisnička uloga</b>	Korisnička uloga koja obavlja poslove koji mogu prouzročiti sigurnosne probleme ako se nepropisno obavljaju, bilo slučajno ili zlonamjerno. Poslovi povjerljivih korisničkih uloga su temelj povjerenja u cjelokupan PKI.
<b>Preporučena granica pouzdanja</b>	CA-ov preporučeni najviši ukupni iznos za koji će pouzdanja strana snositi rizik u transakciji ili komunikaciji u odnosu na izdani certifikat. Preporučena je granica pouzdanja različita za različite tipove certifikata. Preporučuje se da Pouzdanja strana razmotri preporučenu granicu pouzdanja pri izboru pouzdanja na certifikat.

# Nacionalni PKI

## Kratice, reference i definicije

POJAM	ZNAČENJE
<b>Prihvaćanje</b>	Postupak Subjekta koji pokreće prava i obveze Subjekta koja se odnose na certifikat a u skladu sa "Ugovorom o izdavanju certifikata" . Pokazivanje prihvaćanja može uključiti bez ograničenja: <ul style="list-style-type: none"><li>▪ upotrebu certifikata (poslije izdavanja)</li><li>▪ propust da se obavijesti CA o problemima sa certifikatom u razumnom vremenu nakon primanja certifikata, ili</li><li>▪ druge postupke prihvaćanja</li></ul>
<b>Priručnik o sigurnosti i operativnom radu u registracijskom uredu (RA)</b>	Priručnik i/ili druge publikacije koje mogu biti u elektroničkoj formi, koji opisuju sigurnosne i opće operativne standarde i pravila rada u registracijskom uredu
<b>Privatni ključ</b>	Ključ iz para ključeva koji u tajnosti drži Subjekt, koristi se za kreiranje elektroničkog potpisa ili za dekrptiranje poruka i podataka enkriptiranih odgovarajućim javnim ključem
<b>Razumno povjerenje</b>	Za potrebe PKI, odluka Pouzdajuće strane da se pouzda u certifikat, smatrat će se razumnim povjerenjem ako je strana: <ul style="list-style-type: none"><li>▪ provjerila da je elektronički potpis koji je u pitanju, kreiran privatnim ključem koji odgovara javnom ključu u certifikatu za vrijeme perioda valjanosti certifikata i da komunikacija potpisana elektroničkim potpisom nije bila izmijenjena</li><li>▪ provjerila da je certifikat koji je u pitanju, bio valjan u vrijeme njezinog pouzdanja, provodeći provjeru statusa certifikata kako je propisano od strane CA</li><li>▪ koristila certifikat za svrhe propisane CP-om ili CPS-om, pod okolnostima u kojima je povjerenje razumno i u dobroj namjeri, pod okolnostima koje su poznate ili bi trebale biti poznate Pouzdajućoj strani prije davanja povjerenja.</li><li>▪ pouzdajuća strana podnosi sve rizike povjerenja u certifikat ako zna ili ima razloga smatrati da postoje činjenice koje mogu uzrokovati osobnu ili poslovnu štetu uzrokovanu korištenjem certifikata</li></ul>
<b>Registracijski ured (RA)</b>	Pravna ili fizička osoba koju je po CPS-u ili ugovorom ovlastio CA za prihvata i obradu zahtjeva za izdavanje certifikata, te provjeru identiteta potencijalnih Subjekata, i za kontrolu informacija sadržanih u zahtjevu za izdavanje certifikata u skladu sa uputama iz CP-a, CPS-a i

# Nacionalni PKI

## Kratice, reference i definicije

---

POJAM	ZNAČENJE
	pripadajućih ugovora
<b>Repozitorij</b>	Informatički (online) sustav koji održava CA, te služi za spremanje i dohvat certifikata i drugih informacija koje se odnose na certifikat, uključujući informacije vezane uz valjanost certifikata ili opozive.
<b>Sadržaj certifikata</b>	Protokol koji se navodi u poglavlju 7. CP-a koji definira dopušteni oblik i sadržaj polja certifikata, koji identificiraju CA, subjekt, period valjanosti certifikata te druge informacije koje identificiraju subjekt.
<b>Shared secret (SS)</b>	Aktivacijski podaci koji služe kao pomoć stranama pri autentificiranju identiteta i uspostavljanju prikladnog kanala komunikacija. U svrhu utvrđivanja identiteta između RA i subjekta, SS se može sastojati od PIN-a ili online bankovne lozinke koju su razmijenili samo RA i subjekt, ali ne i CA. U svrhu utvrđivanja identiteta između subjekta i CA, to je potrebno za izdavanje certifikata, SS se sastoji od drugog aktivacijskog podatka koji se razmjenjuje između RA, Subjekta i CA.
<b>Sigurno sredstvo za izradu elektroničkog potpisa (SSCD / kriptomodul)</b>	<p>Sredstvo koje mora osigurati slijedeće:</p> <ul style="list-style-type: none"><li>▪ da se podaci za izradu naprednoga elektroničkog potpisa mogu pojaviti samo jednom te da je ostvarena njihova sigurnost,</li><li>▪ da se podaci za izradu naprednoga elektroničkog potpisa ne mogu ponoviti te da je potpis zaštićen od krivotvorenja pri korištenju postojeće raspoložive tehnologije,</li><li>▪ da podatke za izradu naprednoga elektroničkog potpisa Subjekt može pouzdano zaštititi protiv korištenja od strane drugih.</li></ul> <p>Sredstvo za izradu naprednoga elektroničkog potpisa ne smije pri izradi naprednoga elektroničkog potpisa promijeniti podatke koji se potpisuju ili onemogućiti subjektu uvid u te podatke prije procesa izrade naprednoga elektroničkog potpisa.</p>
<b>Sredstvo za izradu elektroničkog potpisa</b>	Odgovarajuća računalna oprema ili računalni program koji Subjekt koristi pri izradi elektroničkog potpisa.
<b>Sredstvo za izradu naprednoga elektroničkog potpisa</b>	Sredstvo za izradu potpisa koje udovoljava zahtjevima iz članka 9. Zakona o elektroničkom potpisu [1].

# Nacionalni PKI

## Kratice, reference i definicije

---

POJAM	ZNAČENJE
Sredstvo za verificiranje potpisa	Odgovarajuća računalna oprema ili računalni program koji se koristi za primjenu podataka za verificiranje potpisa.
Strogi PIN ili lozinka	Alfanumerički kod od najmanje osam znakova koji se upotrebljava za pristup zaključanom sustavu
Subjekt	Osoba ili organizacija koja: <ul style="list-style-type: none"><li>▪ je imenovana ili identificirana u certifikatu, ili je odgovorna za imenovani elektronički uređaj, kao subjekt certifikata, i</li><li>▪ posjeduje privatni ključ koji korespondira javnom ključu navedenom u certifikatu</li></ul> Subjekt je osoba ili organizacija čije ime se pojavljuje u certifikatu i koji tvrdi da upotrebljava certifikat i korespondirajuće ključeve u skladu s CP-om.
Subjekti	<b>Poslovni subjekt</b> Subjekt s pravnim identitetom (registrirana djelatnost prema zakonima RH), primjerice: <ul style="list-style-type: none"><li>▪ poduzeća (trgovačka društva)</li><li>▪ fondovi</li><li>▪ banke i financijske institucije</li><li>▪ komore</li><li>▪ tijelo državne uprave</li><li>▪ tijelo lokalne uprave i samouprave</li><li>▪ vladina tijela</li><li>▪ vladine agencije</li><li>▪ nevladine organizacije</li><li>▪ sveučilište</li><li>▪ vjerske zajednice</li><li>▪ udruge</li><li>▪ političke stranke</li><li>▪ humanitarne organizacije</li><li>▪ posebne interesne grupe</li><li>▪ neprofitne organizacije</li><li>▪ javni bilježnici</li><li>▪ odvjetnici</li><li>▪ stomatolozi i liječnici (privatne ordinacije)</li><li>▪ obrtnici</li><li>▪ itd...</li></ul> <b>Fizička osoba / građanin</b> Subjekt s građanskim (osobnim) identitetom

# Nacionalni PKI

## Kratice, reference i definicije

POJAM	ZNAČENJE
<b>Sudionici</b>	Davatelji usluga certificiranja, korisnici autorizirani za sudjelovanje u PKI, te subjekti koji su definirani u CP-u.
<b>Tajni ključ (Secret key)</b>	Tajni ključ u sustavu javnog ključa, a koji je dostupan samo potpisniku. Tajni ključ omogućuje izradu vlastitog elektroničkog potpisa.
<b>Tehnika razdvajanja znanja</b>	Sigurnosna procedura prema kojoj niti jedna osoba sama ne posjeduje opremu, znanje ili vještine da pristupi osjetljivim ili povjerljivim informacijama u svezi sa PKI-om
<b>Tražitelj certifikata</b>	Poslovni subjekt ili osoba koja je predala informacije potrebne za podnošenje zahtjeva u svrhu izdavanja ili obnovu certifikata
<b>Ugovor o izdavanju certifikata</b>	Ugovor između Subjekta i CA i/ili RA koji detaljno opisuje procedure, prava i obveze svake strane u odnosu na certifikat koji se izdaje Subjektu
<b>Zone sa ograničenim pristupom</b>	<p><b>Prijemna zona</b></p> <p>Ulaz u radni prostor, u kojem se obavlja inicijalni kontakt između javnosti i CA ili RA, gdje se obavljaju servisi, izmjenjuju informacije, i kontrolira pristup zonama koje su ograničene za pristup. Postoji kontrola aktivnosti u prijemnoj zoni od osoblja koje je tamo zaposleno, od drugog osoblja ili od čuvarske službe. Pristup klijentima limitiran na određeno vrijeme u danu (radno vrijeme).</p> <p><b>Operativna zona</b></p> <p>Prostor u koji je pristup dopušten jedino osobama zaposlenim u njemu te osobama u propisanoj pratnji. Operativna zona mora biti barem periodički kontrolirana i preporučuje se pristup samo iz sigurnosnog pretprostora.</p> <p><b>Sigurnosna zona</b></p> <p>Područje u koje je pristup ograničen i dopušten samo autoriziranom osoblju i autoriziranim i pravilno praćenim posjetiteljima. Sigurnosne zone bi trebale biti dostupne preko operativne zone i kroz posebno ulazno mjesto. Sigurnosna zona ne treba biti posebno odijeljena od operativne zone. Sigurnosna zona trebala bi biti nadgledana 24 sata na dan i 7 dana u tjednu. Nadgledanje provodi osoblje i/ili elektronički uređaji.</p> <p><b>Zona visoke sigurnosti</b></p> <p>Područje u koje je pristup kontroliran na ulaznoj točki i</p>

# Nacionalni PKI

## Kratice, reference i definicije

---

POJAM	ZNAČENJE
	ograničen na autorizirano i prikladno provjereno osoblje i pravilno praćene posjetitelje. Pristup ovom području moguć je samo iz sigurnosne zone. Ovo je područje posebno odvojeno od sigurnosne i operativne zone. Zona visoke sigurnosti se nadgleda 24 sata na dan i 7 dana u tjednu. Nadgledanje provodi osoblje i/ili elektronički uređaji.