REPUBLIKA HRVATSKA
MINISTARSTVO GOSPODARSTVA

Klasa: 080-01/11-01/154
Urbroj:526-04-01-02-01/2-13-28

NACIONALNI PKI

KRATICE, REFERENCE I DEFINICIJE

Verzija 1.1

Datum 05. 11. 2013.

AUTORSKA PRAVA

PRIMJEDBE I PROMJENE

Mehanizam upravljanja primjedbama

Napisane i potpisane primjedbe na ovaj dokument moraju biti upućene u Povjerenstvu za donošene, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentacije i procedure.

Obavijest o finalnim promjenama

Povjerenstvu za donošene, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentacije i procedure će odrediti period za obavijest o finalnim promjenama.

PREGLED PROMJENA

Redni broj	Verzija	Točka	Opis promjene	Datum promjene
1	**1.0**		**Inicijalna verzija dokumenta**	**14. 10. 2013.**
2	**1.1**		**Usklađivanje sa zakonskom regulativom, ispravke u tekstu**	**05. 11. 2013.**

OBJAVA

Na temelju odluke o prihvaćanju i objave dokumenata NCARH-a donijete na sjcdnici Povjerenstva za donošenje. uvođenje i provedbu odluka koje se odnose na HR PKI dokumentacije i procedure održanoj dana 14. listopada 2013. godine. Ministarstvo gospodarstva objavljujc navedene dokumente.

U Zagrcbu, 05. studenog 2013.g

MINISTAR GOSPODARSTVA

Ivan Vrdoljak

Nacionalni PKI

Kratice, reference i definicije

Sadržaj

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

1. KRATICE

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

KRATICA	ZNAČENJE	
	Engleski	Hrvatski
ARL	Authority Revocation List	Lista opozvanih certifikacijskih tijela
CA	Certification Authority	Certifikacijsko tijelo
CP	Certification Policy	Opća pravila davanja usluga certificiranja
CPS	Certification Practice Statement	Pravilnik o postupcima certificiranja
CRL	Certificate Revocation List	Lista opozvanih certifikata
CSP	Certification Service Provider	Davatelj usluga certificiranja
DN	Distinguished Name	Razlikovno ime
DNS	Domain Name System	Sustav za prevođenje naziva računala u odgovarajuće IP adrese
DSA	Digital signature algorithm	Norma za digitalne potpise specificiran u FIPS 186-1
ISO	International Standards Organization	Međunarodna organizacija za stndarde
LDAP	Lightweight Directory Access Protocol	Protokol za pristup informacijskim direktorijima
LRA	Local Registration Authority	Lokalni registracijski ured
NCARH		Nacionalni CA za Republiku Hrvatsku
OID	Object Identifier	Identifikator objekta
PCA	Principal CA	Glavni CA
PIN	Personal Identification Number	Osobni tajni broj za aktivaciju smart kartice, USB tokena ili sličnog uređaja
PKCS	Public Key Cryptography System	Grupa normi za kriptografiju javnog

KRATICA	ZNAČENJE	
	Engleski	**Hrvatski**
		ključa
PKI	Public Key Infrastructure	Infrastruktura javnog ključa
PKIX-CMP	PKIX - Certificate Management Protocol	Protokol za upravljanje ključevima i certifikatima
PMA	Policy Management Authority	Tijelo za upravljanje pravilima certificiranja
RA	Registration Authority	Registracijski ured
SSCD	Secure Signature Creation Device	Sredstvo za izradu naprednog elektroničkog potpisa
SSL	Secure Sockets Layer	Kriptografski protokol za sigurnu razmjenu podataka putem Interneta
URL	Uniform Resource Locator	Internetska adresa određenog resursa
X.500		Serija ITU-T normi koje opisuju servis elektroničkog imenika.
X.501		ITU-T norma koja opisuje modele elektroničkih imenika
X.509		ITU-T norma koja opisuje certifikate povezane s javnim ključem 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. Zakon i podzakonski akti

[1] Zakon o elektroničkom potpisu (NN 10/02, 80/80)

[2] Pravilnik o evidenciji davatelja usluga certificiranja u Republici Hrvatskoj (NN 107/10)

[3] Pravilnik o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN 107/10, 89/13)

[4] Pravilnik o službenoj iskaznici inspektora za nadzor davatelja usluga certificiranja (NN 109/11)

[5] Popis normizacijskih dokumenata u području primjene Zakona o elektroničkom potpisu i Pravilnika o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata u poslovanju davatelja usluga certificiranja u Republici Hrvatskoj (NN 89/13)

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. Norme

[7] HRN ISO/IEC 15408-1:2013 Informacijska tehnologija -- Sigurnosne tehnike - Kriteriji za vrednovanje sigurnosti IT-a - 1. dio: Uvod i opći model

[8] HRN ISO/IEC 15408-2:2013 Informacijska tehnologija -- Sigurnosne tehnike - Kriteriji za vrednovanje sigurnosti IT-a - 2. dio: Funkcionalni zahtjevi za sigurnost

[9] HRN ISO/IEC 15408-3:2013 Informacijska tehnologija -- Sigurnosne tehnike - Kriteriji za vrednovanje sigurnosti IT-a -- 3. dio: Jamstveni zahtjevi za sigurnost

[10] FIPS PUB 140-1, minimum level 2 Federal Information Processing Standards Publication 140-1 - Security requirements for cryptographic modules, minimum level 2

[11] FIPS PUB 140-2, minimum level 2 Federal Information Processing Standards Publication 140-2 - Security requirements for cryptographic modules, minimum level 2

[12] CWA 14169 CEN Workshop Agreement CWA 14169 - Secure signature-creation devices "EAL 4+": 2004

[13] IETF RFC 3161 Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)

[14] HRN ISO/IEC 27001:2006 Informacijska tehnologija -- Sigurnosne tehnike - Sustavi upravljanja informacijskom sigurnošću – Zahtjevi (ISO/IEC 27001:2005)

[15] HRN ISO/IEC 27002:2006 Informacijska tehnologija -- Sigurnosne tehnike - Kodeks postupaka za upravljanje informacijskom sigurnošću (ISO/IEC 27002:2005) - istovjetna normi HRN ISO/IEC 17799:2006+Ispr.1:2007

[16] HRN ETSI/EN 319 401 V1.1.1:2013 Elektronički potpisi i infrastrukture (ESI) – Sveopći zahtjevi općih pravila za vjerodostojne davatelje usluga koje podržavaju elektroničke potpise (EN 319 401 V1.1.1:2013

[17] HRN ETSI/EN 319 411-2 V1.1.1:2013 Elektronički potpisi i infrastrukture (ESI) – Opća pravila i sigurnosni zahtjevi za vjerodostojne davatelje usluga certificiranja – 2. dio: Zahtjevi za opća pravila za certifikacijska tijela koja izdaju kvalificirane certifikate (EN 319 411-2 V1.1.1:2013)

[18] HRN ETSI/EN 319 411-3 V1.1.1:2013 Elektronički potpisi i infrastrukture (ESI) – Zahtjevi za opća pravila i sigurnost za vjerodostojne davatelje usluga koji izdaju certifikate – 3. dio: Opća pravila za certifikacijska tijela koja izdaju certifikate s javnim ključem (EN 319 411-3 V1.1.1:2013)

[19] HRS ETSI/TS 102 023 V 1.2.2:2009 Elektronički potpisi i infrastrukture (ESI) - Zahtjevi za osobe ovlaštene za otiskivanje vremena (ETSI TS 102 023 V1.2.2:2008)

[20] HRS ETSI/TS 101 861 V1.4.1:2012 Elektronički potpisi i infrastrukture (ESI) - Profil vremenskoga žiga (ETSI/TS 101 861 V1.4.1:2011)

[21] HRN ETSI/EN 319 412-5 V1.1.1:2013 Elektronički potpisi i infrastrukture (ESI) – Profili vjerodostojnih davatelja usluga koji izdaju certifikate – 5. dio: Proširenje za profil kvalificiranoga certifikata (EN 319 412-5 V1.1.1:2013)

[22] HRS ETSI/TS 102 176-1 V2.1.1:2012 Elektronički potpisi i infrastrukture (ESI) – Algoritmi i parametri za sigurne elektroničke potpise – 1. dio: Hash funkcije i asimetrični algoritmi (ETSI/TS 102 176-1 V2.1.1:2011)

[23] CWA 14167-1 CEN Workshop Agreement CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

[24] ITU-T Recommendation X.501 (2005) | ISO/IEC 9594-2:2005, Information technology - Open Systems Interconnection - The Directory: Models.

[25] NIST FIPS PUB 186-2: Digital Signature Standard (DSS)

[26] ANSI X9.31 - Digital signatures using reversible public key cryptography for the financial services industry (rDSA) **(1998)**

[27] CWA 14167-2 CEN Workshop Agreement CWA 14167-2:2004 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)

[28] CWA 14167-3 CEN Workshop Agreement CWA 14167-3:2004 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)

[29] CWA 14167-4 CEN Workshop Agreement CWA 14167-4:2004 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP

[30] IETF RFC 3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile

[31] IETF RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

2.4. NCARH dokumentacija

[32] NCARH Opća pravila davanja usluga certificiranja (CP)

Verzija 1.1

Opća pravila davanja usluga certificiranja - Certificate Policy (CP) *opisuje opća pravila za rad NCARH-a koje primjenjuje Ministarstvo gospodarstva sukladno Zakonu o elektroničkom potpisu.*

[33] NCARH Opća pravila sigurnosti

Verzija 1.1

Opća pravila sigurnosti opisuju temeljne sigurnosne postavke u HR PKI.

[34] Nacionalni PKI – Uspostava i organizacija

Verzija 1.1

Nacionalni PKI - Uspostava i organizacija – opisuje način uspostave i organizaciju Nacionalnog PKI u Hrvatskoj (HR PKI)

[35] Nacionalni PKI – Politike

Verzija 1.1

Nacionalni PKI – Politike – navodi opće javne uvjete za davatelje usluga certificiranja, korisnike i pouzdajuće strane u Nacionalnom PKI u Hrvatskoj (HR PKI)

3. DEFINICIJE

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

POJAM	ZNAČENJE
Akreditacija	Postupak u kojem akreditacijski tim provjerava je li davatelj usluga sposoban za obavljanje poslova izdavanja certifikata prikladnih za uporabu u HR PKI domeni.
Akreditacijski tim	Tim koji formira PMA HR PKI. Zadaća ovog tijela je provođenje postupka akreditacije (postupak provjere sposobnosti) davatelja usluga certificiranja.
Aktivacijski podaci	Tajni podaci potrebni za pristup ili aktivaciju kriptografskog modula. Aktivacijski podatak može biti PIN, zaporka ili elektronički ključ kojeg osoba zna ili posjeduje.
Asimetrični kriptografski sustav	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.
CA certifikat	Certifikat u kojem je kao subjekt certificiranja naveden (isti ili neki drugi) CA. CA certifikat sadrži naziv i javni ključ CA..
CA root certifikat	CA certifikat kojeg je izdao i potpisao taj isti CA, tj. subjekt certificiranja je isti CA koji sam sebi i izdaje certifikat. CA root certifikat sadrži javni ključ i naziv CA koji je izdao certifikat.
CA privatni potpisni ključ	Privatni ključ koji odgovara CA javnom ključu upisanom u CA certifikat i koji se koristi za potpisivanje certifikata.
CA privatni root ključ	Privatni ključ koji se upotrebljava za potpisivanje CA certifikata.
Certifikacijsko tijelo (CA)	Treća strana od povjerenja koja potvrđuje identitet subjekta certificiranja, izrađuje i potpisuje te za subjekt certificiranja izdaje traženi certifikat. CA izdaje i upravlja životnom ciklusom izdanih certifikata u skladu s objavljenim CP-om.
Certifikat	Potvrda u elektroničkom obliku koja: • imenuje i identificira subjekt certificiranja naveden u certifikatu, • sadrži subjektov javni ključ, • ima upisan vremenski period valjanosti certifikata, • ima značenje u skladu s važećim propisima i normama,

POJAM	ZNAČENJE
	• identificira CA koji izdaje certifikate, • elektronički je potpisan od strane CA.
Cross certifikat - povezujući certifikat	Certifikat koji se koristi za uspostavu odnosa povjerenja između dva ili više CA
Davatelj usluga certificiranja (CSP)	Pravna ili fizička osoba koja izdaje certifikate ili daje druge usluge povezane s elektroničkim potpisima.
Elektronički potpis	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.
Elektronički zapis	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.
Generiranje ključeva	Proces koji izrađuje niz simbola koji čine kriptografski ključ.
Glavni CA (Principal CA)	CA koji posjeduje samopotpisani certifikat i određen je za izdavanje povezujućih certifikata glavnim CA u drugim PKI domenama, te može biti subjekt povezujućih certifikata izdanih od strane glavnih CA u drugim PKI domenama ili od strane Mosnog CA.
Identifikator objekta (OID)	Identifikator koji predstavlja specifičan objekt. OID se sastoji od brojeva odijeljenih točkama i navedenih u hijerarhijskom poretku. Svaki broj identificira poseban čvor u stablu čvorova, počevši od korijena tog stabla.
Infrastruktura javnog ključa (PKI)	Arhitektura, organizacija, hardver, softver, osoblje, pravila, operativni postupci i procedure koje zajednički podržavaju implementaciju i rad kriptografskog sustava javnog ključa za upravljanje životnim ciklusom digitalnih certifikata.
Javni ključ (Public key)	Javno dostupan kriptografski ključ koji odgovara uparenom privatnom ključu. Javni ključ može služiti za provjeru elektroničkog potpisa (ako je javno objavljen kao dekripcijski ključ) ili za enkripciju podataka (ako je javno objavljen kao enkripcijski ključ).

POJAM	ZNAČENJE
Ključ	Generalni izraz korišten kroz cijelu dokumentaciju a obuhvaća sve definirane ključeve spomenute u ovoj tablici
Ključ za enkripciju	Privatni ključ iz para ključeva koji upotrebljava Subjekt za dekripciju poruke koja je enkriptirana javnim ključem iz para ključeva.
Korisnik	Fizička osoba-građanin ili poslovni subjekt kojima davatelj usluga certificiranja daje usluge, odnosno s kojim sklapa ugovor o korištenju usluga certificiranja.
Kriptografija javnog ključa	Tip kriptografije poznat i kao asimetrična kriptografija koja koristi par ključeva za sigurnu enkripciju i dekripciju poruka ili podataka.
Kriptografski modul	Softver ili uređaj određene razine sigurnosti koji: generira par ključeva štiti kriptografske informacije i/ili obavlja kriptografske funkcije
Kvalificirani certifikat	Elektronička potvrda kojom davatelj usluga izdavanja kvalificiranih certifikata potvrđuje napredni elektronički potpis. Kvalificirani certifikat izdaje davatelj usluga izdavanja kvalificiranog certifikata koji ispunjava uvjete propisane Zakonom o elektroničkom potpisu.
Kvalificirani ovjerovitelj	Pravna ili fizička osoba koja izdaje kvalifcirane certifikate ili daje druge usluge povezane s elektroničkim potpisima.
Lightweight Directory Access Protocol (LDAP)	Klijent-poslužitelj protokol korišten za pristup servisima X.500 imenika putem interneta
Lista opozvanih certifikata (CRL)	Potpisana lista koja ukazuje na skup certifikata koji se od strane izdavatelja certifikata više ne smatraju važećim.
Lista opozvanih ovjerovitelja (ARL)	Potpisana lista koja sadrži popis opozvanih CA certifikata, tj. CRL CA certifikata.
Napredni elektronički potpis	Elektronički potpis koji pouzdano jamči identitet potpisnika i koji: • je povezan isključivo s potpisnikom; • nedvojbeno identificira potpisnika; • nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika;

POJAM	ZNAČENJE
	• sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka.
Online provjera statusa certifikata	Provjera statusa valjanosti certifikata koja se obavlja online. Primjer online provjere statusa certifikata je i provjera opozvanosti certifikata pomoću online preuzete CRL. Ako se online provjera statusa certifikata obavlja preko CRL, provjerava se samo zadnje izdana CRL.
Opća pravila certificiranja-Certification Policy (CP)	Imenovani skup pravila koji ukazuje na primjenjivost certifikata za određenu skupinu i/ili klasu primjena sa zajedničkim zahtjevima na sigurnost.
Operativni period	Stvarno vrijeme valjanosti certifikata koje počinje vremenom početka važenja certifikata koje je označeno u certifikatu te završava najranijim od dva sljedeća događaja: • istekom roka valjanosti certifikata koje je označeno u certifikatu ili • trenutkom opoziva certifikata.
Operativno osoblje	Osobe koje su zaposlenici CA/RA i koje su kvalificirane za obavljanje takvih poslove.
Opoziv certifikata	Radnja koja certifikat nepovratno čini nevažećim od tog trenutka pa nadalje. Opoziv postaje važeći objavom CRL u kojoj je naznačen opoziv tog certifikata.
Out of-band	Komunikacija između dvije strane koja se odvija drugim kanalom u odnosu na uobičajeni i koja se sastoji od načina ili metoda, različitih od uobičajene metode komunikacije. Primjer out-of band komunikacije je metoda u kojoj jedna strana upotrebljava poštu za komuniciranje s drugom stranom da bi potvrdila uobičajenu komunikaciju koja se obavlja on-line.
Period valjanosti certifikata	Vremenski period tijekom kojeg vrijedi certifikat. Ovaj vremenski period počinje vremenom označenim u polju „vrijedi od“ i završava vremenom „vrijedi do“.
Povjerenstvo za donošene, uvođenje i provedbu odluka koje se odnose na HR PKI	Povjerenstvo (tijelo) Ministarstva gospodarstva koje je odgovorno za postavljanje, uvođenje i administriranje odluka koje se odnose na HR PKI politike, postupke i

POJAM	ZNAČENJE
dokumentacije i procedure **PMA (Policy Management Authority) za HR PKI**	dokumentaciju.
Podaci za izradu elektroničkog potpisa	Jedinstveni podaci, poput kodova ili privatnih kriptografskih ključeva, koje potpisnik koristi za izradu elektroničkog potpisa.
Podaci za verificiranje elektroničkog potpisa	Podaci poput kodova ili javnih kriptografskih ključeva, koji se koriste u svrhu verificiranja (ovjere) elektroničkog potpisa.
Potpisnik	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.
Pouzdajuća strana	Primatelj certifikata, koji djeluje temeljem razumnog pouzdanja u certifikat. Certifikat omogućuje pouzdajućoj strani provjeru cjelovitost i izvornosti elektronički potpisanog zapisa odnosno provjeru identiteta subjekta.
Pouzdan sustav	Informacijski sustav ili proizvod implementiran kao hardver ili softver koji daje pouzdane i autentične zapise zaštićene od izmjena i dodatno osigurava tehničku i kriptografsku sigurnost podržanih procesa, engl. Trustworthy System.
Povjerljiva uloga	Uloge o kojima ovisi sigurnost rada davatelja usluga izdavanja kvalificiranih certifikata. Povjerljive uloge (engl. Trusted Roles) i pripadne odgovornosti moraju biti jasno određene. Povjerljive uloge i odgovornosti opisane su u opisu posla djelatnika.
Pravilnik o postupcima certificiranja (CPS)	Dokument koji sadrži operativne postupke davatelja usluga certificiranja. Operativni postupci definirani Pravilnikom o postupcima certificiranja moraju biti sukladni odredbama definiranim u dokumentu Opća pravila davanja usluga certificiranja (CP).
Preporučena granica pouzdanja	CA-ov preporučeni najviši ukupni iznos za koji će pouzdajuća strana snositi rizik u transakciji ili komunikaciji u odnosu na izdani certifikat. Preporučena je granica pouzdanja različita za različite tipove certifikata. Preporučuje se da Pouzdajuća strana razmotri preporučenu granicu pouzdanja pri izboru pouzdanja na certifikat.

POJAM	ZNAČENJE
Prihvaćanje certifikata	Postupci i radnje podnositelja zahtjeva za izdavanje certifikata na osnovu kojih se može smatrati da je certifikat prihvaćen od strane potpisnika ili skrbnika. Npr., može se smatrati da je certifikat prihvaćen ukoliko je potpisnik ili skrbnik potpisao prihvaćanje izdanog certifikata ili ako CA unutar određenog vremena nije primio nikakvu reklamaciju od korisnika. Korisnik može poslati potpisanu poruku o prihvaćanju certifikata ili korisnik može poslati potpisanu poruku kojom odbija prihvatiti certifikat s time da u poruci naznači razlog za odbijanje certifikata i označi polja u certifikatu koja nisu točna ili potpuna.
Pripadajuća osoba	Fizička osoba zaposlena u poslovnom subjektu ili na drugi način povezana s poslovnim subjektom, a koja je od strane istog poslovnog subjekta autorizirana za dobivanje certifikata. Takav certifikat identificira osobu i poslovni subjekt te naznačuje da je ta osoba povezana s poslovnim subjektom.
Privatni ključ	Kriptografski ključ kojeg korisnik čuva u tajnosti, a koji odgovara uparenom javnom ključu. Koristi se za izradu elektroničkog potpisa ili za dekriptiranje podataka enkriptiranih odgovarajućim javnim ključem.
Razlikovno ime (DN)	Jedinstveno ime koje omogućava pronalaženje subjekta u imeniku.
Razumno povjerenje	Razumnim povjerenjem smatra se odluka pouzdajuće strane da se pouzda u certifikat ako je u vrijeme ostvarenja pouzdanja: • koristila certifikat u svrhe propisane CP-om, pod okolnostima u kojima je pouzdanje razumno i u dobroj namjeri te pod okolnostima koje su poznate ili bi trebale biti poznate pouzdajućoj strani prije ostvarenja pouzdanja; • provjerila da certifikat nije istekao u vrijeme ostvarenja pouzdanja, te da certifikat nije opozvan ili suspendiran, a što pouzdajuća strana treba utvrditi provodeći provjeru statusa certifikata temeljem zadnje izdane CRL liste kako je propisano u CP-u; • provjerila da su svi podaci o identitetu subjekta certifikata ispravno prikazani

POJAM	ZNAČENJE
	aplikacijom u koju se može pouzdati; • ako je u pitanju elektronički potpis, provjerila da je elektronički potpis izrađen privatnim ključem koji odgovara javnom ključu u certifikatu za vrijeme perioda valjanosti certifikata. Pouzdajuća strana snosi sve rizike pouzdanja u certifikat ako zna ili ima razloga smatrati da postoje činjenice koje mogu uzrokovati osobnu ili poslovnu štetu prouzročenu korištenjem certifikata.
Registracijski ured (RA)	Pravna ili fizička osoba ovlaštena od CA i zadužena za jednu ili više slijedećih radnji: identifikaciju i potvrdu identiteta tražitelja certifikata, prihvaćanje ili odbijanje zahtjeva za izdavanje certifikata, obradu zahtjeva za opoziv, suspenziju ili reaktivaciju certifikata, pokretanje opoziva, suspenzije ili reaktivacije certifikata, prihvaćanje ili odbijanje zahtjeva za obnovu certifikata.
Repozitorij	Sustav ili skup distribuiranih sustava koji pohranjuju certifikate i CRL, te služi kao sredstvo za distribuciju pohranjenih certifikata i CRL krajnjim korisnicima.
Sigurno sredstvo za izradu elektroničkog potpisa (SSCD)	Vidi pojam: „Sredstvo za izradu naprednog elektroničkog potpisa“.
Sredstvo za izradu elektroničkog potpisa	Odgovarajuća računalna oprema ili računalni program koji subjekt koristi pri izradi elektroničkog potpisa.
Sredstvo za izradu naprednoga elektroničkog potpisa	Sredstvo za izradu elektroničkog potpisa koje osigurava: • da se podaci za izradu naprednoga elektroničkog potpisa mogu pojaviti samo jednom te da je ostvarena -njihova sigurnost, • da se podaci za izradu naprednoga elektroničkog potpisa ne mogu ponoviti te da je potpis zaštićen od krivotvorenja pri korištenju postojeće raspoložive tehnologije, • da podatke za izradu naprednoga elektroničkog potpisa subjekt može pouzdano zaštititi protiv korištenja od strane drugih. 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

POJAM	ZNAČENJE
	elektroničkog potpisa.
Sredstvo za verificiranje potpisa	Odgovarajuća računalna oprema ili računalni program koji se koristi za primjenu podataka za verificiranje potpisa.
Subjekt ili subjekt certificiranja	Subjekt (certificiranja) je entitet za kojeg se izdaje certifikat, tj. može biti fizička osoba-građanin, pripadajuća osoba, poslovni subjekt i IT oprema (npr. poslužitelj, aplikacija i sl.). Podaci o subjektu sastavni su dio certifikata.
Subjekti	**Poslovni subjekt** 1. Pravne osobe, primjerice ▪ trgovačka društva, ▪ kreditne i financijske institucije, ▪ javne i privatne ustanove, ▪ udruge s pravnom osobnošću, ▪ neprofitne i nevladine organizacije s pravnom osobnošću, ▪ fondovi s pravnom osobnošću, ▪ jedinice lokalne i područne (regionalne) samouprave (općine, gradovi i županije) i dr. 2. Tijela javne vlasti, primjerice ▪ tijela državne vlasti, ▪ tijela državne uprave, ▪ državne agencije i dr. 3. Fizičke osobe s registriranom djelatnošću, primjerice ▪ obrtnici, ▪ odvjetnici, ▪ javni bilježnici, ▪ javni ovršitelji i dr. **Fizička osoba / građanin** Subjekt s građanskim (osobnim) identitetom
Tajni ključ (Secret key)	Ključ za enkripciju i dekripciju podataka u simetričnom kriptografskom sustavu. Sigurnost enkriptiranih podataka ovisi o čuvanju tajnosti ovog ključa.

POJAM	ZNAČENJE
Tražitelj certifikata	Poslovni subjekt i/ili fizička osoba koja podnosi zahtjev za izdavanje certifikata, podnositelj zahtjeva.
Ugovor o obavjanju usluga certificiranja	Ugovor između fizičke osobe, odnosno poslovnog subjekta zastupanog po ovlaštenoj osobi za zastupanje i davatelja usluge certificiranja koji detaljno opisuje prava i obveze svake strane u odnosu na certifikat koji se izdaje subjektu.