



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

Klasa: 330-01/04-01/30

Urbroj: 526-01/04-03

NACIONALNI PKI

POLITIKE
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** je 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 će odrediti 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.siječnja 2004.godine, Ministarstvo gospodarstva, rada i poduzetništva objavljuje navedene dokumente.

U Zagrebu 15. ožujka 2004.g.


MINISTAR
Branko Vukelić

Sadržaj

1. IZJAVA O PKI POLITICI (POLICY DISCLOSURE STATEMENT - PDS)	1
1.1. Usklađenost politika NCARH i kvalificiranog ovjervitelja	1
1.2. Ograničenje pouzdanja u certifikate	1
1.3. Obveze subjekta	2
1.4. Obveze pouzdajuće strane	2
1.5. Odgovornosti	2
1.5.1. Odgovornosti Ministarstva i NCARH	2
1.5.2. Odgovornosti kvalificiranih ovjervitelja	2
1.6. Ograničenje odgovornosti	3
1.6.1. Ograničenje odgovornosti Ministarstva i NCARH	3
1.6.2. Ograničenje odgovornosti kvalificiranih ovjervitelja	3
1.7. Rješavanje sporova	3
2. POLITIKA O TAJNOSTI INFORMACIJA (PRIVACY POLICY)	5
2.1. Informacije koje nisu tajne	5
2.2. Klasifikacija tajnih informacija	5
2.2.1. Sadržaj zahtjeva za izdavanje certifikata.....	5
2.2.2. Privatni ključ	5
2.2.3. CA i RA informacije	6
2.3. Dopušteno prikupljanje tajnih informacija	6
2.4. Ispravljanje tajnih informacija	6
2.5. Davanje informacija trećoj strani	6
2.6. Rješavanje sporova	6
3. POLITIKA O SIGURNOSTI (SECURITY POLICY)	7
3.1. Zahtjevi i obvezujući principi	7
3.1.1. Cjelovitost – integritet	7
3.1.2. Raspoloživost	7
3.2. Smisao i cilj	7
3.2.1. Implementacija	8
3.3. Opća pravila sigurnosti	8
3.3.1. Procedure.....	8
3.3.2. Usklađenost	8
4. CERTIFIKATI	9
4.1. Certifikati koje izdaje NCARH	9
4.2. Certifikati koje izdaju kvalificirani ovjervitelji	9
4.2.1. Profili.....	9
4.2.2. Sadržaj certifikata.....	9
4.2.3. Namjena	9
4.2.4. Razine sigurnosti	10
4.2.5. Dopuštene aplikacije	11
4.2.6. Zabranjene aplikacije	11
4.3. Certifikati za krajnje korisnike	11
4.3.1. Osobni certifikati.....	11
4.3.2. Poslovni certifikati	12
4.3.3. Certifikat za poslužitelje.....	12

Nacionalni PKI

Politike

Sadržaj

4.3.4. Certifikati za uređaje	12
4.3.5. Certifikati za servise/aplikacije	12
4.4. Administrativni CA certifikati.....	12
4.5. Testni i demo certifikati.....	12
4.6. Ostali tipovi	12

1. IZJAVA O PKI POLITICI (Policy Disclosure Statement - PDS)

Ministarstvo gospodarstva, rada i poduzetništva (dalje u tekstu Ministarstvo) će izvršavati svoje obaveze sukladno zakonima, pravilnicima, PKI standardima i EU preporukama.

Ministarstvo, ovom objavom PKI politika, daje opće javne uvjete koji se odnose na njegove postupke i koje želi javno izložiti ovjerviteljima, subjektima i pouzdajućim stranama.

1.1. Usklađenost politika NCARH i kvalificiranog ovjervitelja

NCARH će se cross certificirati sa CA kvalificiranog ovjervitelja, koji provodi politiku izdavanja certifikata sukladno sljedećim traženjima:

1. odredbama Zakona o elektroničkom potpisu [1].
2. odredbama Pravilnika o evidenciji davatelja usluga certificiranja elektroničkih potpisa i Pravilnika o registru davatelja usluga certificiranja elektroničkih potpisa koji izdaju kvalificirane certifikate pravilnici [2, 3].
3. udruživost s politikama NCARH za izdavanje kvalificiranih certifikata.
4. tehničku izvedbu kvalificiranih certifikata prema propisanom profilu za kvalificirani certifikat.
5. kvalificirani će ovjervitelj svakom tipu kvalificiranog certifikata kojeg izdaje u HR PKI, dodijeliti vlastiti jedinstveni identifikator (OID). Identifikator u certifikatu je oznaka politike iz njegovog CP-a prema kojoj se certifikat objavljuje.
6. kvalificirani ovjervitelj se nadalje treba pridržavati:
 - Pravilnika 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 i
 - Pravilnika o tehničkim pravilima i uvjetima povezivanja sustava certificiranja elektroničkih potpisa.

1.2. Ograničenje pouzdanja u certifikate

1. Kvalificirani će ovjervitelj pohranjivat informacije o svim izdanim certifikatima za period od 10 godina.
2. NCARH će pohranjivat sve informacije o izdanim certifikatima za period od 10 godina.
3. Kvalificirani će ovjervitelj izdavati kvalificirane certifikate, koji su udruživi sa NCARH, s periodom važenja do 60 mjeseci (5 godina),
4. Povezujući certifikati (*cross-certificates*) koje NCARH izdaje kvalificiranom ovjervitelju izdavati će se s periodom važenja do 60 mjeseci (5 godina).
5. NCARH povezujući certifikat se može koristiti za verifikaciju upisa kvalificiranog ovjervitelja u Registar kvalificiranih ovjervitelja, koje održava OA NCARH.

Nacionalni PKI

Politike

6. Kvalificirani certifikati ovjervitelja nisu važeći u sustavu HR PKI ako ne postoji odgovarajuća dozvola koja je izdana ovjervitelju (povezujući certifikat), kojom se odobrava upotreba njegovog tipa certifikata u HR PKI.

1.3. Obveze subjekta

Kvalificirani ovjervitelj treba obavijestiti subjekta o njegovim obvezama te nastojat osigurati provedbu tih obveza. Obveze koje treba provoditi subjekt propisane su u politikama za izdavanje certifikata.

1.4. Obveze pouzdajuće strane

Pouzdanja strana može se ograničeno pouzdati u certifikat subjekta koji pripada HR PKI ako:

1. Provjeri ispravnost certifikata subjekta (valjanost, suspenzija, opoziv) prema postupcima koje propisuje kvalificirani ovjervitelj.
2. Provjeri postojanje, valjanost i ispravnost povezujućeg certifikata (cross-certifikata) koji NCARH izdaje kvalificiranom ovjervitelju.
3. Provjeri valjanost i ispravnost root NCARH certifikata. Pouzdajuća strana treba na siguran način preuzeti izvorni root NCARH certifikat, da bi mogla verificirati sve certifikate na putu povjerenja.

Informacije o valjanosti povezujućeg certifikata i root certifikata NCARH Pouzdajuća strana može potražiti na servisu za provjeru valjanosti certifikata koji održava NCARH. Ovaj servis objavljuje informaciju o stanju certifikata periodično svakih 30 dana. Lista nevažećih povezujućih certifikata (*cross-certificates*) objavljuje se u obliku ARL liste (*Authority Revocation List*) i može se preuzeti iz javnog repozitorija NCARH.

1.5. Odgovornosti

1.5.1. Odgovornosti Ministarstva i NCARH

1. Ministarstvo i NCARH odgovorni su za ispravnu objavu, održavanje životnog ciklusa i servis za provjeru valjanosti povezujućih NCARH certifikata.
2. Ministarstvo i NCARH su isto tako odgovorni za sve vlastite certifikate i zaštitu vlastitih tajnih ključeva:
 - *NCARH root CA certifikat i njemu pripadajući tajni ključ i*
 - *Pripadajuće certifikate i ključeve koji služe za upravljanje sa NCARH.*

1.5.2. Odgovornosti kvalificiranih ovjervitelja

Za poslove inicijalnog izdavanja i upravljanja životnim ciklusom certifikata izdanih subjektima, punu odgovornost preuzimaju kvalificirani ovjervitelji.

1.6. Ograničenje odgovornosti

1.6.1. Ograničenje odgovornosti Ministarstva i NCARH

Ministarstvo i NCARH ne odgovaraju za:

1. operativne propuste kvalificiranih ovjervitelja kod inicijalnog izdavanja certifikata Subjektima
2. operativne propuste kvalificiranih ovjervitelja kod upravljanja životnim ciklusom certifikata izdanih subjektima
3. operativne propuste Pouzdajućih strana kod validacije certifikata subjekata
4. obveze subjekata, čiji su certifikati povezani u HR PKI

1.6.2. Ograničenje odgovornosti kvalificiranih ovjervitelja

Kvalificirani ovjervitelji i njegov(i) CA(-ovi) nisu odgovorni za:

1. obveze subjekata kojima su izdali certifikate
2. operativne propuste Pouzdajućih strana kod validacije certifikata

1.7. Rješavanje sporova

Svi će mogući sporovi između strana koje se povezuju u HR PKI bit rješavani sukladno zakonima Republike Hrvatske i od strane nadležnog suda u Republici Hrvatskoj.

2. POLITIKA O TAJNOSTI INFORMACIJA (Privacy Policy)

2.1. Informacije koje nisu tajne

Certifikati i informacije o statusima certifikata, informacije o osobama i organizacijama koje se nalaze u certifikatima ili u javnim imenicima ne smatraju se tajnim informacijama. Informacija koja se nalazi na pojedinačnom certifikatu i informacija o statusu certifikata neće se smatrati tajnom kada se ta informacija koristi u skladu s namjerama provođenja PKI servisa.

2.2. Klasifikacija tajnih informacija

2.2.1. Sadržaj zahtjeva za izdavanje certifikata

Davatelj usluga certificiranja procesira zahtjeve za izdavanje certifikata. Informacije koje su potrebne za podnošenje zahtjeva za izdavanje certifikata upotrebljavaju se za popunjavanje polja po X.509 standardu profila certifikata.

I&A informacije koje se prikupljaju tijekom registracijskog procesa (primjerice, JMBG, prebivalište-adresa stanovanja, e-mail adresa i podaci o poslovanju tvrtke) smatraju se tajnim i povjerljivim.

Davatelj će usluga prikupiti dovoljno informacija radi valjanog utvrđivanja subjekta identiteta (osobe ili tvrtke) i poduzet će razumne mjere za zaštitu takvih informacija.

Količina informacija o identitetu subjekta ovisi o razini sigurnosti certifikata.

Informacije o dokazu subjekta identiteta smatraju se povjerljivim informacijama i kao takve zahtijevaju strogu zaštitu od neautoriziranog otkrivanja.

Sve informacije o subjektovom identitetu, koje se nalaze na fizičkom medijima koje čuva davatelj usluga, čuvaju se u sigurnim kontejnerima, koji su pod kontrolom logičkog i fizičkog pristupa.

2.2.2. Privatni ključ

Privatni su ključevi povjerljive informacije, te se stoga privatni ključevi moraju držati u najstrožoj tajnosti. Nema okolnosti pod kojima bi se privatni ključ pojavio nešifriran izvan kriptomodula.

Privatni ključevi koji su generirani tijekom procesa registracije dostavljaju se sigurnim kanalom subjektu ili se generiraju na subjektovom računalu.

Davatelj usluga nema pristup privatnim ključevima subjekata.

Nacionalni PKI

Politike

2.2.3. CA i RA informacije

Sve informacije koje nisu javne, spremljene lokalno na CA i/ili RA opremi (ne nalaze se u Repozitoriju) smatraju se povjerljivima. Pristup tim informacijama ograničava se na službene osobe, kojima su te informacije potrebne radi obavljanja njihovih službenih dužnosti.

Sve informacije koje se odnose na način kojim CA upravlja certifikatima smatraju se povjerljivim.

2.3. Dopušteno prikupljanje tajnih informacija

CA i RA će prikupljati samo one informacije o osobama i o organizacijama (Subjektima), koje su neophodne za pravilno izdavanje certifikata. Radi pravilnog vođenja administracije, CA i RA mogu zahtijevati informacije koji neće biti u certifikatu (JMBG, ID brojevi, adrese, brojevi telefona), ali takve informacije neće biti korištene pri izdavanju i radu sa certifikatom. Prikupljanje osobnih informacija može biti uvjetovano i drugim zakonima koji se odnose na prikupljanje, održavanje i zaštitu takvih informacija.

2.4. Ispravljanje tajnih informacija

Subjektima mora biti omogućen pristup da isprave ili izmjene svoje osobne ili podatke o organizaciji. CA ili RA mora pružiti te informacije na zahtjev i nakon poduzimanja prikladnih postupaka za autentificiranje identiteta strane koja zahtijeva pristup tim informacijama.

2.5. Davanje informacija trećoj strani

Davatelji usluga certificiranja neće trećoj strani otkrivati informacije koje se smatraju tajnom, osim kada se zahtijeva otkrivanje po nalogu suda.

2.6. Rješavanje sporova

Svi će mogući sporovi o otkrivanju tajnih informacija u HR PKI bit rješavani sukladno zakonima Republike Hrvatske i od strane nadležnog suda u Republici Hrvatskoj.

3. POLITIKA O SIGURNOSTI (SECURITY POLICY)

Politika o sigurnosti je strateški dokument i odražava poslovne potrebe PMA za zaštitom PKI sustava. Politika sigurnosti sadrži:

- zahtjeve PMA u provedbi zaštite i obvezujućih principa poslovanja u HR PKI,
- smisao i cilj sigurnosti u HR PKI.

3.1. Zahtjevi i obvezujući principi

3.1.1. Cjelovitost – integritet

Zahtjevi za izdavanje certifikata i informacije u certifikatu u okviru CA sustava i X.500 imenika ne mogu se mijenjati, brisati ili dodavati ni na koji način od strane operativnog osoblja OA NCARH ili davatelja usluga certificiranja. Ovo je nametnuto uporabom stroge logičke i fizičke kontrole pristupa operativnog osoblja CA sustavu kombinirano s kontinuiranim nadgledanjem pristupa CA mreži.

Samo autorizirano CA i RA operativno osoblje ima dozvolu za dodavanje novih zahtjeva u CA sustav. Takvi registracijski zahtjevi ne mogu biti mijenjani, brisani ili dodavani ni na koji način. Nadgledanje na razini aplikacije i podatkovne osnove u CA sustavu uvedeno je da bi se kontrolirao i evidentirao pristup tim informacijama.

3.1.2. Raspoloživost

U skladu sa HR PKI politikom davanja usluga, X.500 imenik mora biti dostupan klijentima 24 sata na dan i 7 dana u tjednu.

Nemogućnost da klijenti pristupe toj podatkovnoj osnovici znači da se zahtjevi za validaciju certifikata ne mogu procesirati sve do ponovnog uspostavljanja servisa. To znači da korisnik neće moći koristiti svoju PKI aplikaciju ili se pouzdati na certifikat. Za NCARH i Davatelja usluga certificiranja je imperativ održavanje mogućnosti da klijenti mogu neprekidno pristupati PKI servisima.

CRL mora biti dostupna u svako vrijeme da bi se osiguralo da klijenti imaju mogućnost provjeriti da certifikat s kojim oni rade nije bio opozvan ili suspendiran. Nemogućnost da klijent provede tu provjeru može rezultirati odobrenje transakcije koja inače ne bi bila odobrena.

3.2. Smisao i cilj

Smisao i cilj sigurnosti u HR PKI sustavu je ovaj:

- preventivno spriječiti svaku neautoriziranu akciju,
- otkriti, bilježiti i istražiti svaku neautoriziranu akciju koja se pojavi,
- poduzeti potrebne mjere za prekid neautorizirane akcije koja je u tijeku.

Nacionalni PKI

Politike

3.2.1. Implementacija

Pristup se implementaciji sigurnosti temelji na spoznaji da se sigurnost planira i izvodi iz sljedećih ključnih područja:

- arhitektura i planiranje,
- tehnologija,
- upravljanje i kontrola.

3.2.1.1. Arhitektura i planiranje

Ovo se odnosi na postignutu razinu sigurnosti pri izvedbi PKI infrastrukture, barijere koje ograničavaju fizički pristup resursima (mjesto gdje se nalazi tehnologija, informacije na fizičkim medijima itd.), i logičke kontrole pristupa osjetljivim aplikacijama i servisima.

3.2.1.2. Tehnologija

Tehnološki se element sigurnosti odnosi na opremu koja podržava politike i procedure upravljanja sigurnošću.

3.2.1.3. Upravljanje i kontrola

Upravljanje i kontrola se odnosi na sigurnost infrastrukture i na kontrolu osoblja uključenih u održavanje sigurne okoline, njihove zadaće i odgovornost.

3.3. Opća pravila sigurnosti

Ovaj je dokument skup sigurnosnih propisa, postupaka i procedura koji opisuju kako se sredstvima/resursima (uređaji, aplikacije, infrastruktura, servisi, informacije i osoblje) upravlja, kako se one štite i distribuiraju.

Krajnji je cilj Općih pravila sigurnosti, kreiranje okvira koji će osigurati, kada bude pravilno implementiran, da HR PKI postigne najvišu moguću razinu sigurnosti.

Opća se pravila sigurnosti odnose na cijeli sustav na kojem se temelji HR PKI i uvodi procedure po kojima se uspješno i sigurno obavljaju operativni PKI poslovi.

3.3.1. Procedure

Procedure se vežu uz Opća pravila sigurnosti ili se referenciraju direktno na stavke Politike o sigurnosti. U procedurama se opisuju tehnološki i operativni postupci i zadaci koji se moraju obaviti da bi se proveli objavljeni i prihvaćeni principi zaštite i pravila koja iz njih slijede.

3.3.2. Usklađenost

Kroz Opća će pravila sigurnosti NCARH i Davatelj usluga certificiranja ispuniti zakonske i objavljene poslovne obveze koje se odnose na zaštitu interesa krajnjih korisnika PKI servisa, a koji uključuju zaštitu i tajnost podataka propisanu zakonom, pravilnicima, standardima i PKI pravilnicima Davatelja usluga certificiranja.

Navodi iz Općih pravila sigurnosti trebaju biti u skladu s poznatim međunarodnim PKI standardima.

4. CERTIFIKATI

4.1. Certifikati koje izdaje NCARH

NCARH izdaje sljedeće tipove certifikata:

1. Upravljačke certifikate (root CA certifikat i administrativne certifikate), koji služe za izvođenje CA operacija i za autentifikaciju osoblja koje upravlja infrastrukturom NCARH.
2. Certifikate kvalificiranim ovjerviteljima kao elektronički oblik dozvole (sukladno Pravilniku [3], članak 14.) s kojom je moguće elektronički potvrditi identitet i autentičnost kvalificiranog ovjervitelja, kojem je izdana dozvola.
3. Povezujuće certifikate (cross-certificates), koji se izdaju kvalificiranim ovjerviteljima i služe kao elektronička potvrda o kompatibilnosti politika kvalificiranog ovjervitelja i politika povezivanja u HR PKI.

4.2. Certifikati koje izdaju kvalificirani ovjervitelji

4.2.1. Profili

4.2.1.1. Normalizirani profil

Normalizirani se profil koristi za elektronički potpis članak 3. Zakona [1]. Ostale temeljne karakteristike:

- Oznaka prema EU: NC i NC+ (+ = SSCD – Smart kartica).
- Profil i ekstenzije prema X.509 v.3.
- Uporaba ključa = elektronički potpis i enkripcija ključa (key usage = *Digital Signature & Key Encipherment*).

4.2.1.2. Kvalificirani profil

Kvalificirani se profil koristi za napredni elektronički potpis članak 5. Zakona [1]. Ostale temeljne karakteristike:

- Oznaka prema EU: QC i QC+ (+ = SSCD - Smart kartica).
- Profil i ekstenzije prema X.509 v.3.
- Uporaba ključa = neporecivost (key usage = nonRepudiation)

4.2.2. Sadržaj certifikata

Sadržaj certifikata je opisan u točki 7. CP-a.

4.2.3. Namjena

Certifikati se izdaju za dvije svrhe:

- enkripciju (Confidentiality Key) ili
- potpis

Nacionalni PKI

Politike

- elektronički potpis, ili
- napredni elektronički potpis

Certifikati za elektronički potpis su namijenjeni provjeri elektroničkog potpisa u aplikacijama u kojima se:

- zahtijeva autentifikacija identiteta strana u komunikaciji,
- traži uspostava čvrste veze između poruke ili datoteke i njihovog tvorca pomoću potpisa (neporecivost potpisanog sadržaja), i/ili
- zahtijeva potvrda izvornog sadržaja i cjelovitosti poruke ili datoteke.

4.2.4. Razine sigurnosti

CA izdaje kvalificirane certifikate tri razine sigurnosti:

- standardni,
- srednji i
- visoki.

Razina sigurnosti	Područje primjene
Standardna	Ova razina omogućuje standardnu razinu sigurnosti prikladnu u okolinama u kojima postoje rizici i posljedice prouzrokovane kompromitiranjem podataka, ali nemaju veću važnost. To može biti pristup tajnim podacima gdje vjerojatnost zlonamjernog pristupa nije velika. U ovoj sigurnosnoj razini se podrazumijeva da je mala vjerojatnost da korisnici budu zlonamjerni.
Srednja	Ova je razina prikladna za okoline u kojima su rizici i posljedice kompromitiranja podataka umjereni. Može se koristiti u transakcijama koje imaju znatnu novčanu vrijednost ili rizik od krivotvorenja, ili one koje imaju pristup tajnim informacijama u kojima je znatna vjerojatnost zlonamjernog pristupa.
Visoka	Ova je razina prikladna za upotrebu u transakcijama u kojima je ugroženost podataka visoka, ili su posljedice propusta u sustavu zaštite visoke. To su transakcije vrlo visoke vrijednosti ili postoji visoki rizik od krivotvorenja.

Subjekti i pouzdajuće strane su odgovorne za određivanje koja je razina sigurnosti prikladna za namjenu određene transakcije. Faktori koje subjekti i pouzdajuće strana trebaju razmatrati pri donošenju takve odluke, uključuju sljedeće:

- pravne zahtjeve za identifikaciju druge strane, zaštitu tajnosti ili privatnosti informacije, ili pravnu prihvatljivost elektroničkog potpisa koji se može primijeniti.
- sve činjenice koje se nalaze u certifikatu ili o kojima je pouzdajuća strana izvještena, uključujući ovaj CP.

- ekonomsku vrijednost transakcije ili komunikacije, ako je to primjenjivo,
- potencijalne gubitke ili štetu koja može biti uzrokovana pogrešnom identifikacijom ili gubitak povjerenja ili tajnosti informacija u aplikaciji, transakciji ili komunikaciji,
- primjenjivost hrvatskih zakona,
- preporučena granica pouzdanja koja se primjenjuje na tipove certifikata,
- prijašnji način poslovanja sa subjektom,
- običaj (navika) trgovanja (razmjene), posebno trgovanja koje se obavlja pouzdanim sustavima ili drugim metodama temeljenim na računalskim sustavima, i
- bilo koji pokazatelj prikladnosti ili neprikladnosti, ili druge činjenice o kojima pouzdajuća strana zna, a koje se odnose na subjekta i/ili aplikaciju, komunikaciju ili transakciju.

4.2.5. Dopuštene aplikacije

Certifikat je primjenjiv, ali ne i ograničen na aplikacije elektroničkog poslovanja koje:

- omogućavaju pristup temeljen na autentifikaciji i sigurnoj komunikaciji s online izvorima informacija, uključujući one koje distribuiraju informacije uz plaćanje ili po ugovoru i one koje imaju na raspolaganju osobne ili ograničene informacije subjekta, kao što su financijske ustanove, državne agencije, zdravstvene institucije, osiguravajuća društva i drugi,
- omogućavaju podršku za potpisivanje obrazaca i druge aplikacijske procese u državnim i ostalim organizacijama,
- traže potpisivanje, enkripciju, dekrpciju i/ili provjeru elektroničkih poruka i elektroničkog potpisa na ugovorima, kreditnim pismima, raznim novčanim transakcijama, bankovnim izvodima i drugoj elektroničkoj dokumentaciji u elektroničkom poslovanju.

4.2.6. Zabranjene aplikacije

Certifikat se ne smije koristiti u onim aplikacijama za koje zakonom ili drugim propisima nije dopušteno korištenje elektroničkog potpisa članak 6. Zakona [1].

4.3. Certifikati za krajnje korisnike

4.3.1. Osobni certifikati

Izdaju se fizičkim osobama - građanima. Postoje sljedeći stupnjevi osobnih certifikata:

- standardni,
- srednji i
- visoki.

Nacionalni PKI

Politike

4.3.2. Poslovni certifikati

Izdaju se ovlaštenim osobama zaposlenim kod poslovnog subjekta. Postoje sljedeći stupnjevi poslovnih certifikata:

- standardni,
- srednji i
- visoki.

4.3.3. Certifikat za poslužitelje

Izdaju se poslužiteljima.

4.3.4. Certifikati za uređaje

Izdaju se elektroničkim uređajima.

4.3.5. Certifikati za servise/aplikacije

Izdaju se servisima/aplikacijama.

4.4. Administrativni CA certifikati

Koriste se samo pri radu sa PKI. Sljedeće osoblje koristi certifikate:

- CA glavni korisnici i administratori,
- RA/LRA osoblje, i
- drugo osoblje ako je potrebno.

4.5. Testni i demo certifikati

Izdaju se samo u svrhe testiranja i demonstracije certifikata koji se izdaju u HR PKI.

4.6. Ostali tipovi

Ako je dopušteno CP-om i nakon odobrenja PMA.