REPUBLIKA HRVATSKA
MINISTARSTVO GOSPODARSTVA

Klasa: 080-01/11-01/154
Urbroj: 526-04-01-02-01/2-13-30

NACIONALNI PKI

POLITIKE
Verzija 1.2
Datum 05. 11. 2013.

AUTORSKA PRAVA

PRIMJEDBE I PROMJENE

Mehanizam upravljanja primjedbama

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

Obavijest o finalnim promjenama

PMA HR PKI će odrediti period za obavijest o promjenama dokumenta.

PREGLED PROMJENA

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

OBJAVA

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

U Zagrebu 05. studenog 2013.g.

MINISTAR GOSPODARSTVA

Ivan Vrdoljak

Sadržaj

Sadržaj

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

Na temelju ovlasti te Zakonu [1] Ministarstvo gospodarstva (dalje u tekstu Ministarstvo) je nadležno za implementaciju PKI u Republici Hrvatskoj.

Ministarstvo, ovom objavom PKI politika, daje na uvid opće javne uvjete CSP-ovima, korisnicima i pouzdajućim stranama.

1.1. Usklađenost politika NCARH i davatelja usluga izdavanja certifikata prikladnih za uporabu u HR PKI

NCARH će se uzajamno certificirati sa CA CSP- om koji provodi politiku izdavanja certifikata sukladno:

1. odredbama Zakona [1];
2. odredbama Pravilnika o evidenciji davatelja usluga certificiranja u Republici Hrvatskoj [2];
3. odredbama Pravilnika o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata [3];
4. s jednako vrijednim politikama NCARH za izdavanje certifikata;
5. profilu za kvalificirane certifikate u skladu s točkom 4,2.1.2. i za normalizirane certifikate u skladu s točkom 4.2.1.1. ovog dokumenta;
6. obavezi da CSP svakom tipu certifikata dodjeljuje jedinstveni identifikator (OID).

1.2. Ograničenje pouzdanja u certifikate

1. CSP će pohranjivati i čuvati informacije o svim izdanim certifikatima najmanje 10 godina;
2. NCARH će pohranjivati i čuvati sve informacije o izdanim certifikatima najmanje 10 godina;
3. CSP će izdavati certifikate, koji su udruživi sa NCARH, s periodom važenja do 60 mjeseci (5 godina);
4. povezujući certifikati koje NCARH izdaje CSP-u izdavati će se s periodom važenja do 60 mjeseci (5 godina).

1.3. Obveze subjekta

CSP 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

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

1. provjeri ispravnost certifikata subjekta (valjanost, suspenzija, opoziv) prema postupcima koje propisuje CSP;
2. provjeri postojanje, valjanost i ispravnost povezujućeg certifikata koji NCARH izdaje CSP-u ;
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 pronaći na servisu za provjeru valjanosti certifikata koji održava NCARH. Ovaj servis objavljuje informaciju o statusu certifikata periodično svakih 30 dana. Lista nevažećih povezujućih certifikata objavljuje se u obliku ARL liste 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 informacija o certificiranju, održavanje životnog ciklusa certifikata i servis za provjeru valjanosti povezujućih NCARH certifikata.
2. Ministarstvo i NCARH su isto tako odgovorni za sve vlastite certifikate i zaštitu vlastitih privatnih ključeva:
    - *NCARH root CA certifikat i njemu pripadajući privatni ključ; i*
    - *pripadajuće certifikate i ključeve koji služe za upravljanje NCARH-om.*

1.5.2. Odgovornosti CSP-a

Za poslove inicijalnog izdavanja i upravljanja životnim ciklusom certifikata izdanih subjektima, potpunu odgovornost preuzimaju CSP-ovi.

1.6. Ograničenje odgovornosti

1.6.1. Ograničenje odgovornosti Ministarstva i NCARH

Ministarstvo i NCARH ne odgovaraju za:

1. operativne propuste CSP-a kod inicijalnog izdavanja certifikata Subjektima;
2. operativne propuste CSP-a 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 CSP-a

CSP 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 domenu biti rješavani sukladno zakonima Republike Hrvatske i od strane nadležnog suda u Republici Hrvatskoj.

2. POLITIKA TAJNOSTI INFORMACIJA

2.1. Informacije koje nisu tajne

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

2.2. Klasifikacija tajnih informacija

2.2.1. Sadržaj zahtjeva za izdavanje certifikata

CSP obrađuje 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.

Informacije koje se prikupljaju tijekom registracijskog procesa (primjerice, OIB, mjesto prebivališta, adresa stanovanja, e-mail adresa i podaci o poslovanju tvrtke) smatraju se tajnim i povjerljivim.

CSP će prikupiti dovoljno informacija radi valjanog utvrđivanja subjektova identiteta (fizičke osobe ili poslovnog subjekta) i poduzeti će razumne mjere za zaštitu takvih informacija.

Količina i vrsta informacija o identitetu subjekta ovisi o razini sigurnosti certifikata.

Informacije o dokazu subjektova 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 CSP, 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. Privatni ključ mora uvijek biti enkriptiran dok je izvan kriptografskog modula. Privatni ključevi koji su generirani tijekom procesa registracije dostavljaju se subjektu sigurnim kanalom ili se generiraju na subjektovom računalu.

CSP nema pristup privatnim ključevima subjekata.

2.2.3. CA i RA informacije

Sve informacije koje nisu javne, spremljene su lokalno na CA i/ili RA opremi, tj.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 fizičkim osobama i o poslovnim subjektima, koje su neophodne za pravilno izdavanje certifikata. Radi pravilnog vođenja administracije, CA i RA mogu zahtijevati informacije koji neće biti u certifikatu (OIB, adrese, telefonski brojevi), ali takve informacije će 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 biti rješavani sukladno zakonima Republike Hrvatske i od strane nadležnog suda u Republici Hrvatskoj.

3. POLITIKA SIGURNOSTI

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

- zahtjeve PMA HR PKI 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 osigurano mehanizmima kontrole i zaštite pristupa operativnog osoblja CA sustavu, kombinirano s kontinuiranim nadgledanjem pristupa CA mreži.

Samo ovlašteno CA i RA operativno osoblje ima dozvolu za dodavanje novih zahtjeva za izdavanje certifikata u CA sustav. Takvi registracijski zahtjevi ne mogu biti mijenjani, brisani ili dodavani ni na koji način. Nadgledanje na razini aplikacije i podatkovne osnovice 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 izdavanja certifikata, X.500 imenik mora biti dostupan pouzdajućim stranama 24 sata na dan, 7 dana u tjednu.

Nemogućnost da pouzdajuće strane 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 CSP je imperativ održavanje mogućnosti da korisnici i pouzdajuće strane mogu neprekidno pristupati HR PKI servisima.

CRL mora biti dostupna u svako vrijeme da bi se osiguralo da pouzdajuće strane imaju mogućnost provjeriti da certifikat s kojim rade nije bio opozvan ili suspendiran. Nemogućnost da pouzdajuća strana provede tu provjeru može rezultirati odobrenjem transakcije koja ne smije bila odobrena.

3.2. Smisao i cilj

Smisao i cilj sigurnosti u HR PKI sustavu je:

- 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.

3.2.1. Implementacija

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

- arhitektura i planiranje;
- primjena tehnologija;
- upravljanje i kontrola.

3.2.1.1. Arhitektura i planiranje

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

3.2.1.2. Primjena 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

Opća pravila sigurnosti je dokument sa skupom sigurnosnih propisa, postupaka i procedura koje opisuju kako se sredstvima/resursima (uređaji, aplikacije, infrastruktura, servisi, informacije i osoblje) upravlja te kako se one štite i distribuiraju.

Krajnji cilj Općih pravila sigurnosti je stvaranje okvira kojim se osigurava postizanje najviše moguće razumne razine sigurnosti u HR PKI domeni.

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 pravila sigurnosti NCARH i CSP–ovi ispunjavaju 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, normama i pravilnicima CSP-ova.

Odredbe iz Općih pravila sigurnosti trebaju biti u skladu s priznatim međunarodnim normama iz područja PKI.

4. CERTIFIKATI

4.1. Certifikati koje izdaje NCARH

NCARH izdaje sljedeće tipove certifikata:

1. upravljačke certifikate (administrativne certifikate), koji služe za izvođenje CA operacija i za autentifikaciju osoblja koje upravlja infrastrukturom NCARH;
2. povezujuće certifikate koji se izdaju CSP-ovima i služe kao elektronička potvrda o kompatibilnosti politika CSP-ova i politika povezivanja u HR PKI domenu.

4.2. Certifikati koje izdaju CSP-ovi

4.2.1. Profili certifikata

4.2.1.1. Profil normaliziranog certifikata

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

- oznaka prema EU: NCP i NCP+ (NCP+ je oznaka za politiku izdavanja normaliziranog certifikata koji se izdaje na SSCD uređaju);
- profil i ekstenzije prema normizacijskom dokumentu HRN ETSI/EN 319 411-3[18];
- ekstenzija uporabe ključa ima vrijednost elektronički potpis i enkripcija ključa (key usage = *Digital Signature & Key Encipherment*).

4.2.1.2. Profil kvalificiranog certifikata

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

- oznaka prema EU: QCP i QCP+ (QCP+ je oznaka za politiku izdavanja kvalificiranog certifikata koji se izdaje na SSCD uređaju);
- profil i ekstenzije prema normizacijskim dokumentima HRN ETSI/EN 319 411-2 [17], HRN ETSI/EN 319 412-5 [21];
- ekstenzija uporabe ključa ima vrijednost 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;

- Potpis;
  - 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
- zahtjeva potvrda izvornog sadržaja i cjelovitosti poruke ili datoteke.

4.2.4. Razine sigurnosti

CA izdaje certifikate tri razine sigurnosti:

- standardna,
- srednja i
- visoka.

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 informacije koje se nalaze u certifikatu ili o kojima je pouzdajuća strana izvještena, uključujući 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;
- način trgovinske razmjene, posebno trgovanja koje se obavlja pouzdanim sustavima ili drugim metodama temeljenim na računalnim 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. Dopušteno područje uporabe

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

- omogućava pristup temeljen na autentifikaciji i sigurnoj komunikaciji s online izvorima informacija, uključujući one sustave koji distribuiraju informacije uz plaćanje ili po ugovoru te one sustave koji imaju na raspolaganju osobne ili ograničene informacije subjekta, kao što su financijske ustanove, državne agencije, zdravstvene institucije, osiguravajuća društva i drugi,,
- omogućava podršku za potpisivanje obrazaca i druge aplikacijske procese u državnim i ostalim organizacijama;
- traži potpisivanje, enkripciju, dekripciju 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. Zabranjena područja uporabe

Certifikat se ne smije koristiti u onim primjenama za koje zakonom ili drugim propisima nije dopušteno korištenje elektroničkog potpisa.

4.3. Certifikati za krajnje korisnike

4.3.1. Osobni certifikati

Izdaju se fizičkim osobama - građanima. Postoje sljedeće razine sigurnosti osobnih certifikata:

- standardna;
- srednja i
- visoka.

4.3.2. Poslovni certifikati

Izdaju se ovlaštenim osobama zaposlenim kod poslovnog subjekta. Postoje sljedeće razine sigurnosti poslovnih certifikata:

- standardna;
- srednja i
- visoka.

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 HR PKI sustavom. Sljedeće osoblje koristi certifikate:

- ovlašteni CA glavni korisnici i administratori;
- ovlašteno RA/LRA osoblje i
- drugo ovlašteno 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 HR PKI.