FINA PKI

IZMJENE I DOPUNE PRAVILNIKA O POSTUPCIMA CERTIFICIRANJA ZA NEKVALIFICIRANE CERTIFIKATE (dokument za javnu objavu) BR. 1/4.0

Datum stupanja na snagu: 31.12.2013.

Informacije o dokumentu Pravilnik o postupcima certificiranja za nekvalificirane certifikate

Ime dokumenta:	FINA PKI - Pravilnik o postupcima certificiranja za nekvalificirane certifikate (dokument za javnu objavu)
OID dokumenta:	1.3.124.1104.5.0.0.3.4.0
Tip dokumenta:	Pravilnik o postupcima certificiranja za nekvalificirane certifikate (CPS_{NQC})
Vlasnik dokumenta	FINA
Kontakt	pma@fina.hr

Povijest izmjena dokumenta Pravilnik o postupcima certificiranja za nekvalificirane certifikate

Verzija	Datum	Razlog izmjene
3.0	15.07.2002.	
3.1	15.9.2002.	Dopuna tipova certifikata i ispravci uočenih grešaka
3.2	31.03.2003.	Dopuna postupaka registracije i izdavanja certifikata, izmjena u razinama sigurnosti klasa certifikata
4.0	6.11.2013.	Usklađivanje s pravilnicima [4] i [5] i s preporukom IETF RFC 3647 [18]
Izmjene i dopune Pravilnika o postupcima certificiranja za nekvalificirane certifikate br. 1/4.0	31.12.2013.	Uvođenje profila FINA RDC poslovnog certifikata za IT opremu koji se koristi za elektronički potpis *Trusted* liste.

1. UVOD

(1) Izmjene i dopune Pravilnika o postupcima certificiranja za nekvalificirane certifikate br. 1/4.0 dopunjuju postojeću verziju Pravilnika o postupcima certificiranja za nekvalificirane certifikate (dokument za javnu objavu), Verzija 4.0, (OID dokumenta: 1.3.124.1104.5.0.0.3.4.0) profilom FINA RDC poslovnog certifikata za IT opremu koji se koristi samo za elektronički potpis *Trusted* liste Republike Hrvatske.

(2) Izmjene i dopune Pravilnika o postupcima certificiranja za nekvalificirane certifikate br. 1/4.0 ne utječu na druge tipove certifikata koji se izdaju prema Općim pravilima davanja usluga certificiranja, Verzija 4.0, (OID dokumenta: 1.3.124.1104.5.0.0.1.4.0).

2. IZMJENE I DOPUNE PRAVILNIKA O POSTUPCIMA CERTIFICIRANJA ZA NEKVALIFICIRANE CERTIFIKATE (DOKUMENT ZA JAVNU OBJAVU), VERZIJA 4.0

- U poglavlju „REFERENCE“ pod rednim brojem [13] dodaje se: „ETSI TS 119 612 V1.1.1:2013 Electronic Signatures and Infrastructures (ESI) - Trusted Lists“.

- U poglavlju „REFERENCE“ mijenjaju se reference iznad rednog broja [12] pa reference [13] – [47] postaju reference [14] – [48] u cijelom dokumentu Pravilnik o postupcima certificiranja za nekvalificirane certifikate (dokument za javnu objavu), Verzija 4.0.

- U točki „1.1.2. Tipovi certifikata“, u tablici „1.1. Tipovi certifikata“ u 10. retku pod oznakom „FINA RDC poslovni normalizirani certifikati za IT opremu“ dodaje se sljedeća alineja:

Certifikat za potpis *Trusted* liste (NCP+)	CP OID: 1.3.124.1104.5.11.8.4.2.

- U točki „1.3.3.1 Subjekti certificiranja“ 2. stavak zamjenjuje se sljedećim tekstom:

  „U slučaju kada je subjekt certificiranja IT oprema korisnik obvezatno određuje skrbnika certifikata. Skrbnik certifikata je fizička osoba zaposlena u poslovnom subjektu ili na drugi način povezana s poslovnim subjektom, a koja je od strane istog poslovnog subjekta autorizirana za preuzimanje, uporabu, čuvanje i brigu o privatnom ključu i pripadnom certifikatu izdanom za poslužitelj, aplikaciju, za potpis koda ili potpis *Trusted* liste.“

- U točki „1.4.1. Primjerena uporaba FINA RDC i FINA RDC-TDU autentifikacijskih NCP+ normaliziranih certifikata“ dodaje se točka „1.4.1.6 Primjerena uporaba FINA RDC certifikata za potpis *Trusted* liste“ koja glasi:

  „FINA RDC certifikati za potpis *Trusted* liste usklađeni su s općim pravilima za NCP+ norme HRN ETSI/EN 319 411-3 [11] i normizacijskim dokumentom ETSI TS 119 612 [13] te se izdaju ministarstvu nadležnom za gospodarstvo.

  Ovaj tip certifikata jamči elektronički identitet poslovnog subjekta koji je potpisao *Trusted* listu u svrhu provjere autentičnosti porijekla i osiguranje cjelovitosti *Trusted* liste.

  Ova točka odnosi se na jedan tip certifikata:

  - Certifikat za potpis *Trusted* liste (NCP+).

  Ovi certifikati izdaju se uz korištenje SSCD uređaja te imaju srednju razinu sigurnosti.

  Ekstenzija keyUsage označena je kritičnom te ima vrijednost postavljenu na *digitalSignature*. Ovaj tip certifikata ima i dodatnu ekstenziju extKeyUsage koja nije označena kritično, a koja ima vrijednost postavljenu na *id-tsl-kp-tslSigning*.

  Certifikat se smije koristiti samo za podršku elektroničkog potpisa *Trusted* liste.“

- U točki točki „1.4.1. Primjerena uporaba FINA RDC i FINA RDC-TDU autentifikacijskih NCP+ normaliziranih certifikata“ mijenja se numeracija točaka iznad rednog broja 1.4.1.5. pa tako dosadašnje točke 1.4.1.6. i 1.4.1.7. postaju točke 1.4.1.7 i 1.4.1.8.

- U točki „1.6.1 Definicije“ 57. redak tablice zamjenjuje se sljedećim retkom:

Skrbnik	Fizička osoba zaposlena u poslovnom subjektu ili na drugi način povezana s poslovnim subjektom, a koja je od strane istog poslovnog subjekta autorizirana za preuzimanje, uporabu, čuvanje i brigu o privatnom ključu i pripadnom certifikatu izdanom za poslužitelj, aplikaciju, za potpis koda i sl. Skrbnik pokreće zahtjeve za izdavanje, obnovu, opoziv, suspenziju ili reaktivaciju certifikata te je kontakt osoba za taj certifikat.

- U točki „1.6.1 Definicije“ kao 65. redak tablice dodaje se sljedeći redak:

***Trusted* lista**	Pouzdani popis davatelja usluga certificiranja koje nadziru/akreditiraju države članice. Popis koji pruža informacije o statusu i povijesti statusa vjerodostojnih usluga (uključujući usluge certificiranja) vjerodostojnih davatelja usluga s obzirom na usklađenost s odgovarajućim zahtjevima i relevantnim odredbama zakonske regulative.

- U točki „1.6.2. Kratice“ kao 24. redak tablice dodaje se sljedeći redak:

TL	Trusted List	Pouzdani popis davatelja usluga certificiranja koje nadziru/akreditiraju države članice.

- U točki „3.1.1. Tipovi imena“ kao 5. stavak dodaje se sljedeći tekst:

  „Polje „Subject“ u certifikatima koji se izdaju za potpis *Trusted* liste sadrži skraćeni naziv i identifikator ministarstva zaduženog za gospodarstvo te naziv uloge unutar nacionalnog operatera koja je ovlaštena za potpis.“

- U točki „3.1.4. Pravila tumačenja raznih oblika imena“ u tablici „3.2. Tumačenje oblika imena po X.501 normi“ 5. redak tablice zamjenjuju se sljedećim retkom:

Serial Number (SN)	- Identifikator pripadajuće osobe (potpisnika). - Ne koristi se za poslovne certifikate za IT opremu. - Za certifikate za potpis koda i certifikate za potpis *Trusted* liste vrijednost ovog polja je identifikator poslovnog subjekta.	Identifikator pripadajuće osobe (potpisnika)	Identifikator se sastoji od dvoslovčanog ISO koda države prebivališta pripadajuće osobe, jedanaesteroznamenkastog broja, te dva broja W i Z koji predstavljaju oznake koje imaju interno značenje za FINA PKI. Za potpisnike kojima je dodijeljen OIB jedanaesteroznamenkasti broj je OIB potpisnika. Za potpisnike kojima nije dodijeljen OIB i nemaju prebivalište u Hrvatskoj, jedanaesteroznamenkasti je broj jedinstveni broj kojeg dodjeljuje FINA CA.

- U točki „3.1.4. Pravila tumačenja raznih oblika imena“ u tablici „3.2. Tumačenje oblika imena po X.501 normi“ 6. redak tablice zamjenjuju se sljedećim retkom:

Common Name (CN)	Poslovni certifikati za pripadajuće osobe: - Ime i prezime pripadajuće osobe (potpisnika) Certifikati za poslužitelje: - FQDN poslužitelja; ili - IP adresa poslužitelja Certifikati za aplikacije: - naziv aplikacije Za certifikate za potpis koda: - skraćeni naziv poslovnog subjekta Za certifikate za potpis *Trusted* liste: - naziv uloge unutar ministarstva zaduženog za gospodarstvo koja je ovlaštena za potpis *Trusted* liste.	Ime i prezime pripadajuće osobe (potpisnika)	Za pripadajuće osobe: ime i prezime pripadajuće osobe (potpisnika) iz identifikacijske isprave. Za poslužitelje: FQDN ili IP adresa poslužitelja. Za potpis koda: skraćeni naziv poslovnog subjekta iz mjerodavnog registra.

- U točki „3.1.5. Jedinstvenost imena“ u 2. stavku kao 5. alineja dodaje se sljedeća alineja:
    - potpis *Trusted* liste osigurava se serijskim brojem (atribut SerialNumber) u razlikovnom imenu.
- U točki „4.3.1.1. Radnje FINA CA tijekom izdavanja NCP+ certifikata“ 2. stavak zamjenjuje se sljedećim tekstom:

  „Za tipove certifikata iz točke 6.1.1.3. stavak a) provode se postupci opisani niže u stavkama a) i b). Za tipove certifikata Certifikat za potpis Trusted liste (NCP+) i Administrativni N2 certifikat (NCP+) provodi se samo postupak naveden niže u stavci a).“

- U točki „4.3.1.1. Radnje FINA CA tijekom izdavanja NCP+ certifikata“ pod stavkom „a) Ključeve na SSCD uređaju generira FINA CA na svojoj lokaciji“ 6. alineja zamjenjuje se sljedećom alinejom:

    - FINA RA ovlaštena osoba potpisniku, odnosno skrbniku, dostavlja enkriptirani PIN SSCD uređaja putem e-mail poruke ili ga uručuje pri neposrednoj identifikaciji;

- U točki „4.3.1.1. Radnje FINA CA tijekom izdavanja NCP+ certifikata“ tekst u 6. stavku zamjenjuje se sljedećim tekstom:

  „Za tipove NCP+ certifikata iz točke 6.1.1.3. stavak b), d) i e) te iz točke 6.1.1.6. ovog CPS_{NQC} dokumenta, uz korištenje FININOG alternativnog web servisa za preuzimanje certifikata, koristi se sljedeći postupak:„

- U točki „4.7.3.1. Obrada zahtjeva za obnovom NCP+ certifikata“ tekst u 1. stavku zamjenjuje se sljedećim tekstom:

  „Za tipove certifikata iz točke 6.1.1.3. stavak a) provode se postupci opisani niže u stavkama a) i b). Za tipove certifikata Certifikat za potpis *Trusted* liste i Administrativni N2 certifikat (NCP+) provodi se samo postupak naveden niže u stavci a).“

- U točki „4.7.3.1. Obrada zahtjeva za obnovom NCP+ certifikata“ tekst u zadnjem stavku zamjenjuje se sljedećim tekstom:

  „Za tipove NCP+ certifikata iz točke 6.1.1.3. stavak b), d) i e) te iz točke 6.1.1.6. ovog CPS_{NQC} dokumenta, uz korištenje FININOG alternativnog web servisa za preuzimanje certifikata, koristi se postupak identičan postupku za inicijalno izdavanje certifikata ovog tipa iz točke 4.3.1.1. ovog CPS_{NQC} dokumenta.“

- U točki „4.8.1. Razlozi za izmjene unutar certifikata“ u 2. stavku kao 2. alineja dodaje se sljedeća alineja:
    - naziva uloge ovlaštene za potpis *Trusted* liste;

- U točki „4.9.1. Razlozi za opoziv“ u 1. stavku 5. alineja zamjenjuje se sljedećom alinejom:
    - ako korisnik iz bilo kojeg razloga nema više potrebu koristiti certifikat izdan za IT opremu, aplikacije, potpis koda, potpis *Trusted* liste ili vremenski žig;

- U točki „6.1.1.3. Generiranje para ključeva za NCP+ certifikate korisnika“ kao 3. stavak dodaje se sljedeći stavak:

  „c) Certifikat za potpis Trusted liste (NCP+)

Ovaj postupak se primjenjuje za Certifikat za potpis Trusted liste (NCP+). Generiranje parova ključeva za ovaj tip certifikata obavljaju ovlaštene osobe FINA CA, sukladno točki 5.2.2. ovog CPS_{NQC} dokumenta na SSCD uređaju u operativnom prostoru FINA PKI štićenog prostora iz točke 5.1.1. ovog CPS_{NQC} dokumenta, uz nadzor i upravljanje FINA CMS sustava."

- U točki „6.1.1.3. Generiranje para ključeva za NCP+ certifikate korisnika" mijenjaju se oznake stavaka c) i d) te postaju oznakama stavaka d) i e).

- U točki „6.1.2. Dostava privatnog ključa korisniku" kao 6. stavak dodaje se sljedeći tekst:

  „FINA CA generira privatni ključ za potpis *Trusted* liste unutar SSCD uređaja te se SSCD uređaj s privatnim ključem zaštićenim kanalom dostavlja u registracijski ured RA mreže i osobno se uručuje identificiranom skrbniku."

- U točki „6.1.5. Duljine ključeva" u 1. stavku kao 9. alineja dodaje se sljedeća alineja:

  - par ključeva za certifikate za potpis *Trusted* liste: 2048 bita, RSA;

- U točki „6.1.7. Namjene ključeva (po X.509 v3 polju uporabe ključa) kao 9. stavak dodaje se sljedeći tekst:

  „Ključevi za potpis *Trusted* liste namijenjeni su za elektronički potpis *Trusted* liste (X.509 v3 ekstenzija KeyUsage: *digitalSignature*; ekstenzija extKeyUsage: *id-tsl-kp-tslSigning*)."

- U točki „6.2.8. Metoda aktivacije privatnog ključa" 2. stavak zamjenjuje se sljedećim tekstom:

  „Privatni ključ certifikata izdanog za poslužitelj, aplikaciju, za potpis koda ili potpis *Trusted* liste aktivira samo pripadajući skrbnik korištenjem odgovarajućeg aktivacijskog podataka. Za vrijeme dok je privatni ključ aktivan skrbnik osigurava pravilnost njegove uporabe."

- U točki „6.4.1. Generiranje i instalacija aktivacijskih podataka" kao 6. stavak dodaje se sljedeći tekst:

  „Aktivacijske podatke za privatne ključeve za certifikate za potpis *Trusted* liste generira FINA CA."

- U točki „7.1.1.1.FINA RCD certifikati", pod stavkom „3. FINA RDC poslovni certifikati za IT opremu" kao 4. alineja dodaje se sljedeća alineja:

  - certifikati za potpis *Trusted* liste;

- U točki „7.1.1.1.FINA RCD certifikati“, pod stavkom „3. FINA RDC poslovni certifikati za IT opremu“ dodaje se sljedeći tekst:

  „Certifikati za potpis *Trusted* liste su definirani kao:

  - **Certifikat za potpis *Trusted* liste (NCP+)** – Normalizirani certifikat za potpis *Trusted* liste, srednje razine sigurnosti, uz korištenje SSCD uređaja. Ovaj tip certifikata ima definiran OID: **1.3.124.1104.5.11.8.4.2.** Generiranje ključeva ovog certifikata obavlja FINA CA u SSCD uređaju. Izdavanje ovog certifikata je u skladu s normom HRN ETSI/EN 319 411-3 (NCP+) [11]. Ove certifikate izdaje FINA RCD CA. Certifikat vrijedi najviše dvije godine.

  Osnovna polja i ekstenzije profila certifikata specifične za certifikat za *Trusted* Liste (NCP+) definirane su u tablici 7.19.“

- U točki „7.1.1.1.FINA RCD certifikati“, pod stavkom „3. FINA RDC poslovni certifikati za IT opremu“ dodaje se „Tablica 7.19. Specifična osnovna polja i ekstenzije profila certifikata za potpis *Trusted* liste (NCP+)“, kako slijedi:

Polje	Atribut	Vrijednost
Osnovna polja		
Subject	commonName	Croatian Trusted List Signer
	serialNumber	HR22413472900.W.11
	localityName	Zagreb
	organizationName	Ministarstvo gospodarstva
	countryName	HR
SubjectPublicKeyInfo	AlgorithmIdentifier	RSA 2048 bit
	subjectPublicKey	Javni ključ subjekta

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
CertificatePolicies	NE	policyIdentifier	Srednja razina sigurnosti OID: 1.3.124.1104.5.11.8.4.2
		policyQualifiers	CPS: http://rdc.fina.hr/cp/amdt1_cp4-0.pdf
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
Extended Key Usage	NE	id-tsl-kp-tslSigning	OID: 0.4.0.2331.3.0

Tablica 7.19. Specifična osnovna polja i ekstenzije profila certifikata za potpis Trusted liste (NCP+)

- U poglavlju „7. SADRŽAJ CERTIFIKATA, LISTA OPOZVANIH CERTIFIKATA I OCSP PROFILI“ mijenjaju se oznake za sve tablice u 7. Poglavlju iznad rednog broja 7.19. te tako oznake tablica 7.19 - 7.23 postaju oznakama tablica 7.20. - 7.24.