FINA

OPĆA PRAVILA DAVANJA USLUGA IZDAVANJA NAPREDNIH VREMENSKIH ŽIGOVA

Verzija 1.0

Datum objave: 7.12.2015.

Datum stupanja na snagu: 7.12.2015.

OID Dokumenta: 1.3.124.1104.2.2.1.1.0

Informacije o dokumentu

Ime dokumenta:	Fina - Opća pravila davanja usluga izdavanja naprednih vremenskih žigova
OID dokumenta:	1.3.124.1104.2.2.1.1.0
Tip dokumenta:	Opća pravila davanja usluga izdavanja vremenskog žiga (*Time-stamp policy*, TP)
Oznaka distribucije	Javno
Vlasnik dokumenta	Financijska agencija, Fina
Kontakt	pma@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
1.0	07.12.2015.	Inicijalna verzija

SADRŽAJ:

AUTORSKA PRAVA

REFERENTNE DOKUMENTIRANE INFORMACIJE

Temeljni zakon

[1] Zakon o elektroničkom potpisu (NN 10/2002)

[2] Zakon o izmjenama i dopunama zakona o elektroničkom potpisu (NN 80/2008)

[3] Zakon o izmjeni zakona o elektroničkom potpisu (NN 30/2014)

Podzakonski akti

[4] Pravilnik o evidenciji davatelja usluga certificiranja u Republici Hrvatskoj (NN 107/2010)

[5] 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 107/2010)

[6] Pravilnik o izmjenama i dopunama Pravilnika o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN 89/2013)

[7] Popis normizacijskih dokumenata u području primjene Zakona o elektroničkom potpisu i Pravilnika o izradi elektroničkog potpisa, uporabi sredstva 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 89/2013)

Ostala zakonska regulativa

[8] Zakon o zaštiti osobnih podataka (NN106/2012)

[9] Uredba o djelokrugu, sadržaju i nositelju poslova certificiranja elektroničkih potpisa za tijela državne uprave (NN 146/2004)

Direktive Europskog parlamenta

[10] Direktiva 1999/93/EZ Europskog parlamenta i Vijeća od 13. prosinca 1999. o okviru Zajednice za elektroničke potpise

Normizacijski dokumenti

[11] 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)

[12] 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)

[13] ETSI TS 119 312 V1.1.1:2014 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

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

[15] 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)

[16] CEN Workshop Agreement 14167-1:2003 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

[17] IETF RFC 3161 (2001) Internet X.509: Public Key Infrastructure: Time Stamp Protocol (TSP)

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

[19] ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements

[20] ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls

[21] NIST FIPS PUB 140-2:2002 - Security Requirements for Cryptographic Modules

Finini dokumenti

[22] Fina - Opća pravila davanja usluga certificiranja Fina Root CA

[23] Fina - Opća pravila davanja usluga certificiranja

[24] Fina - Pravilnik o postupcima certificiranja za nekvalificirane certifikate, (CPS_{NQC})

1. UVODNE OZNAKE I TEMELJNI PODACI

Fina PKI je inicijalno osmišljen i uspostavljen u Financijskoj agenciji (Fina) kao treća strana od povjerenja (*Trusted Third Party*) s ciljem davanja usluga certificiranja za građane, pravne osobe i tijela javne vlasti. Fina kao davatelj usluga certificiranja omogućuje stvaranje odnosa povjerenja potrebnog za korištenje i razvitak elektroničkog poslovanja (e-poslovanje) i elektroničke javne uprave (e-uprava). Promoviranjem ovih usluga certificiranja i njihova korištenja Fina želi poticati i olakšati razvitak e-poslovanja i e-uprave.

Fina, kao hrvatska tvrtka u državnom vlasništvu, s polustoljetnom tradicijom na području financijskih usluga, partner je državi te surađuje s Hrvatskom narodnom bankom i uspješno posluje s bankama, brojnim poslovnim sustavima i drugim poslovnim subjektima u Republici Hrvatskoj. Informatički sustav Fine prokušan je najzahtjevnijim poslovima od nacionalne važnosti, a visoka profesionalna razina stručnih timova omogućuje pripremu i provedbu različitih projekata.

Tradicija, obavljanje pouzdanih usluga i orijentiranost prema pružanju elektroničkih usluga za poslovne subjekte i tijela javne vlasti glavni su razlozi zbog kojih je Fina prepoznata kao treća strana od povjerenja u e-poslovanju i e-upravi.

Fina je kao davatelj usluga izdavanja kvalificiranih certifikata i vremenskih žigova upisana pod evidencijskim brojem HR-QC-2008-07-16-1 u evidenciju davatelja usluga certificiranja u Republici Hrvatskoj koju vodi ministarstvo nadležno za gospodarstvo.

Finin servis izdavanja naprednih vremenskih žigova pod nazivom Fina QTSA 2015 dio je postojeće Fina PKI produkcijske okoline i može se koristiti za bilo koju primjenu koja zahtjeva pouzdano utvrđivanje postojanja određenog elektroničkog zapisa prije nekog vremenskog trenutka. Napredni vremenski žig kojeg izdaje Fina QTSA 2015 koristi se i za očuvanje dugotrajnosti elektroničkih potpisa.

Fina QTSA 2015 izdaje napredne vremenske žigove koji se mogu koristiti zajedno s kvalificiranim certifikatima, a izdaju se na sustavu koji je po razini sigurnosti izjednačen sa sustavom za izdavanje kvalificiranih certifikata.

Certifikat za Fina QTSA 2015 izdaje Finino certifikacijsko tijelo (CA) Fina RDC 2015, a napredni vremenski žigovi potpisuju se RSA privatnim ključem Fina QTSA 2015 servisa, duljine 2048 bitova uz korištenje kriptografskih algoritama SHA-256 i RSA.

2. DEFINICIJE I KRATICE

2.1. Definicije

POJAM	DEFINICIJA
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.
Autentifikacija	Proces provjere korisničkog identiteta, tj. provjera da li je korisnik upravo taj za kojeg se predstavlja. Autentifikacija korisnika provodi se u cilju dobivanja pristupa određenim podacima, odnosno računalnim resursima.
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; • identificira CA koji je izdao certifikat; • elektronički je potpisana od strane CA.
Davatelj usluga certificiranja (CSP)	Pravna ili fizička osoba koja izdaje certifikate ili daje druge usluge povezane s elektroničkim potpisima. Druge usluge povezane s elektroničkim potpisom mogu biti npr. usluga izdavanja vremenskog žiga, usluga izrade elektroničkog potpisa, usluga verifikacije elektroničkog potpisa, usluga dugotrajnog čuvanja elektronički potpisanih zapisa i sl.
Davatelj usluga izdavanja vremenskog žiga	Pravna ili fizička osoba koja izdaje vremenski žig.
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 utvrđivanje 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.
Enkripcija	Proces u kriptografiji kojim se podaci mijenjaju tako da se informacije učine nerazumljivim za subjekte koje ne posjeduju odgovarajući dekripcijski ključ. Uporabom dekripcijskog ključa u postupku dekripcije ove se informacije ponovno mogu učiniti razumljivim.
FINA PKI	Infrastruktura javnog ključa (PKI) uspostavljena u FINI koja je namijenjena za pružanje usluga certificiranja fizičkim osobama – građanima, poslovnim subjektima i tijelima državne uprave, a koja je uspostavljena kao treća strana od povjerenja (engl. Trusted Third Party).
Fina RA mreža	Mreža registracijskih ureda u FINI, a sastoji se od središnjeg Fina RA i Fina LRA ureda.

POJAM	DEFINICIJA
Fizička osoba - građanin	Fizička osoba koja uslugu izdavanja vremenskog žiga koristi u vlastito ime i za vlastiti račun i isključuje fizičku osobu s registriranom djelatnošću, fizičku osobu u obavljanju slobodnog zanimanja te fizičku osobu koja nastupa u ime i za račun druge fizičke ili pravne osobe (pripadajuća osoba).
Generiranje ključeva	Proces koji izrađuje niz simbola koji čine kriptografski ključ.
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.
Izjava o davanju usluga izdavanja vremenskog žiga	Skup izjava o općim pravilima i postupcima davatelja usluga izdavanja vremenskog žiga koje zahtijevaju posebno naglašavanje ili objavu korisnicima i pouzdajućim stranama.
Javni imenik	Informatički sustav u nadležnosti CA koji služi za *online* objavu dokumenata i informacija vezanih uz certifikate, uključujući i informacije o valjanosti ili opozvanosti 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).
Jedinica za izradu vremenskog žiga (TSU)	Hardver i softver združen u jednu cjelinu koja u danom trenutku ima samo jedan aktivan potpisni ključ za izradu vremenskog žiga.
Koordinirano svjetsko vrijeme (UTC)	Vremenska ljestvica koja se temelji na sekundi kako je definirana ITU-R preporukom TF.460-5. Za većinu primjena u praksi UTC je ekvivalentan srednjem sunčevom vremenu na nultom meridijanu (0°). Točnije, UTC je kompromis između vrlo stabilnog atomskog vremena (*Temps Atomique International* - TAI) i sunčevog vremena koje se izvodi iz nepravilne rotacije Zemlje (u odnosu na dogovoreno Greenwich srednje zvjezdano vrijeme (GMST)).
Korisnik	Fizička osoba-građanin ili poslovni subjekt kojima davatelj usluga izdavanja vremenskog žiga daje uslugu, odnosno s kojim sklapa ugovoru o pružanju usluge izdavanja vremenskog žiga.
Kriptografski modul	Softver ili uređaj određene razine sigurnosti koji: • generira par ključeva; i/ili • 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.
***Lightweight Directory Acess Protocol* (LDAP)**	Aplikacijski protokol koji radi iznad TCP/IP sloja, a služi za pristup i održavanje distribuiranih usluga povezivanja, pretraživanja i izmjena informacija putem mrežnog internetskog protokola.
Lista opozvanih certifikata (CRL)	Potpisana lista koja ukazuje na skup certifikata koji se od strane izdavatelja certifikata više ne smatraju važećim.

POJAM	DEFINICIJA
Napredan vremenski žig	Elektronički potpisana potvrda izdavatelja naprednog vremenskog žiga koja potvrđuje sadržaj podataka na koji se odnosi u navedenom vremenu i koja ispunjava uvjete za napredan elektronički potpis.
***Online* provjera statusa certifikata (OCSP)**	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 davanja usluge certificiranja - *Certificate Policy* (CP)	Imenovani skup pravila koji ukazuje na primjenjivost certifikata za određenu skupinu i/ili klasu primjena sa zajedničkim zahtjevima na sigurnost.
Opća pravila davanja usluge izdavanja vremenskog žiga - *Time-Stamp Policy* (TP)	Imenovani skup pravila koji ukazuje na primjenjivost vremenskog žiga za određenu skupinu i/ili klasu primjena sa zajedničkim zahtjevima na sigurnost.
Opoziv certifikata	Radnja koja certifikat nepovratno čini nevažećim od tog trenutka pa na nadalje. Opoziv postaje važećim objavom CRL u kojoj je naznačen i opoziv tog certifikata.
Par ključeva	Dva matematički povezana kriptografska ključa (privatni ključ i njegov odgovarajući javni ključ), koji imaju sljedeća svojstva: • jedan ključ iz para ključeva može biti korišten za enkripciju podataka, a koji se mogu dekriptirati samo korištenjem drugog ključa iz istog para ključeva, i • u slučaju poznavanja samo jednog ključa nije moguće (u razumnom vremenu i uz poznatu tehnologiju) otkriti drugi ključ.
Period valjanosti certifikata	Vremenski period tijekom kojeg vrijedi certifikat. Ovaj vremenski period počinje vremenom označenim u polju „vrijedi od“ i završava vremenom „vrijedi do“.
***Policy Management Authority* (PMA)**	Tijelo koje je ovlašteno i odgovorno za izradu, uvođenje i administriranje pravila davanja usluga certificiranja, pripadnu dokumentaciju i procedure te za kontrolu provođenja istih.
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 i dr. • javni ovršitelji i dr.

POJAM	DEFINICIJA
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 vremenskog žiga koji se pouzdaje u taj vremenski žig.
Povjerljive uloge	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), odnosno Općim pravilima davanja usluga izdavanja vremenskog žiga.
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 korištenje usluge izdavanja vremenskog žiga.
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.
Profil certifikata	Detaljan popis i opis gradivnih elemenata certifikata i njihovih vrijednosti.
Profil vremenskog žiga	Detaljan popis i opis gradivnih elemenata vremenskog žiga i njihovih vrijednosti.
Razumno pouzdanje	Razumnim pouzdanjem 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 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 TSA i zadužena za registraciju korisnika.
Sredstvo elektroničke identifikacije	Materijalna i/ili nematerijalna jedinica koja sadrži osobne identifikacijske podatke i koja se koristi za autentikaciju na *online* uslugu.
Suspenzija certifikata	Postupak kojim certifikat privremeno postaje nevažećim.

POJAM	DEFINICIJA
Tijelo za upravljanje pravilima certificiranja (PMA)	Tijelo koje je ovlašteno i odgovorno za izradu, uvođenje i administriranje pravila davanja usluga certificiranja, pripadnu dokumentaciju i procedure te za kontrolu provođenja istih.
Tijelo (tijela) državne uprave (TDU)	Tijelo državne uprave je tijelo državne vlasti nadležno za obavljanje poslova državne uprave u upravnom području za koje je nadležno. Tijela državne uprave su ministarstva, državni uredi Vlade Republike Hrvatske, državne upravne organizacije i uredi državne uprave u županijama ili druga tijela državne uprave utvrđena mjerodavnim važećim zakonom.
QTSA sustav	Sustav IT komponenti koje osiguravaju izvedbu servisa naprednog vremenskog žiga.
Ugovor o pružanju usluge izdavanja vremenskog žiga	Ugovor između korisnika i davatelja usluga izdavanja vremenskog žiga koji detaljno opisuje prava i obveze svake strane u odnosu na vremenski žig koji se izdaje korisniku.
Verificiranje potpisa	Proces kojeg provodi primatelj neposredno nakon izrade elektroničkog potpisa ili kasnije, kako bi utvrdio valjanost elektroničkog potpisa i njegovu usklađenost s važećim pravilima uporabe potpisa.
Vjerodostojan 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*.

2.2. Kratice

KRATICA	PUNI NAZIV	ZNAČENJE
CA	*Certification Authority*	Certifikacijsko tijelo
CP	*Certificate Policy*	Opća pravila davanja usluga certificiranja
CPS_{NQC}	*Certificate Practice Statement for Non-Qualified Certificates*	Pravilnik o postupcima certificiranja za nekvalificirane certifikate
CRL	*Certificate Revocation List*	Lista opozvanih certifikata
CSP	*Certification Service Provider*	Davatelj usluga certificiranja
HSM	*Hardware Security Module*	Hardverski kriptografski modul
LRA	*Local Registration Authority*	Lokalni registracijski ured
OCSP	*Online Certificate Status Protocol*	*Online* provjera statusa certifikata
OID	*Object Identifier*	Identifikator objekta
PKI	*Public Key Infrastructure*	Infrastruktura javnog ključa
PMA	*Policy Management Authority*	Tijelo za upravljanje pravilima certificiranja
QTSA	*Qualified Time-Stamping Authority*	Davatelj usluga izdavanja naprednog vremenskog žiga
RA	*Registration Authority*	Registracijski ured
SSL	*Secure Sockets Layer*	Kriptografski protokol za sigurnu razmjenu podataka putem Interneta
TP	*Time-Stamp Policy*	Opća pravila davanja usluge izdavanja vremenskog žiga

KRATICA	PUNI NAZIV	ZNAČENJE
TSU	*Time-Stamping Unit*	Jedinica za izradu vremenskog žiga
URL	*Uniform Resource Locator*	Internetska adresa određenog resursa
UTC	*Coordinated Universal Time*	Koordinirano svjetsko vrijeme

3. OPĆI KONCEPT

3.1. Usluga izdavanja vremenskih žigova

Finina usluga izdavanja naprednih vremenskih žigova je usluga koja temeljem zahtjeva korisniku usluge izdaje napredan vremenski žig (u daljem tekstu: vremenski žig).

Usluga izdavanja vremenskog žiga sastoji se od dva dijela:

- izdavanje vremenskog žiga;
- upravljanje izdavanjem vremenskog žiga.

Izdavanje vremenskih žigova obuhvaća aktivnosti vezane uz izradu vremenskog žiga, a upravljanje izdavanjem vremenskih žigova obuhvaća nadzor i upravljanje nad radom usluge na način propisan ovim Općim pravilima davanja usluga izdavanja naprednih vremenskih žigova.

Fina kao davatelj usluga izdavanja naprednih vremenskih žigova (u daljem tekstu: Fina QTSA) vremenske žigove izdaje sukladno Zakonu o elektroničkom potpisu [1], Zakonu o izmjenama i dopunama zakona o elektroničkom potpisu [2], Zakonu o izmjeni zakona o elektroničkom potpisu [3], podzakonskim aktima [4], [5], [6] i [7] te europskoj Direktivi o elektroničkim potpisima [10].

Fina QTSA 2015 servis može za svoje usluge koristiti više TSU jedinica. Svaka TSU jedinica u tom slučaju posjeduje vlastiti privatni potpisni ključ kojeg koristi za elektroničko potpisivanje vremenskog žiga.

Fina QTSA ima obvezu izdavati vremenske žigove koje je naknadno moguće pravilno identificirati sukladno točki 4.2. ovog TP dokumenta.

3.2. Sudionici Fina QTSA 2015 servisa

3.2.1. Davatelj usluga izdavanja vremenskih žigova

Fina preko servisa Fina QTSA 2015 pruža uslugu izdavanja naprednih vremenskih žigova kroz Finin servis vremenske ovjere (u daljnjem tekstu: usluga izdavanja vremenskih žigova), a na vjerodostojnoj informacijsko komunikacijskoj infrastrukturi za izdavanje vremenskih žigova.

3.2.2. Tijelo za upravljanje pravilima certificiranja

Tijelo za upravljanje pravilima certificiranja u Fini je Fina PMA. Fina PMA je tijelo ovlašteno i odgovorno za izradu, uvođenje i administriranje pravila davanja usluga certificiranja, pripadnu dokumentaciju i postupke te za kontrolu provođenja istih.

3.2.3. Korisnici

Korisnici servisa Fina QTSA 2015 su fizičke osobe-građani ili poslovni subjekti koji s Finom ugovaraju korištenje usluga certificiranja.

Korisnici usluge izdavanja vremenskog žiga mogu biti:

- poslovni subjekti;
- fizičke osobe unutar poslovnih subjekata (pripadajuće osobe);

- fizičke osobe – građani.

3.2.4. Registracijski uredi

Poslovi registracije korisnika za Fina QTSA 2015 obavljaju se u registracijskim uredima Fine. Za potrebe registracije korisnika za Fina QTSA 2015, Fina može s drugim poslovnim subjektom ugovoriti obavljanje usluge registracije.

Fina ima organiziranu mrežu registracijskih ureda (u daljnjem tekstu: RA mreža) koja obavlja poslove registracije korisnika za Fina QTSA 2015.

Fina RA mrežu čini mreža lokalnih registracijskih ureda (u daljnjem tekstu: Fina LRA) u poslovnoj mreži Fine te Središnji Fina RA. Registraciju korisnika u Fina RA mreži provodi Fina LRA, a iznimno i Središnji Fina RA. U Fina LRA registraciju provode zaposlenici Fine zaduženi za poslove LRA (u daljnjem tekstu LRA službenici). Poslovima registracije u Fina RA mreži koordinira Središnji Fina RA koji je središnja komunikacijska točka Fina RA mreže.

Fina QTSA može odrediti i drugi odgovarajući način registracije korisnika.

3.2.5. Pouzdajuće strane

Pouzdajuće strane su fizičke osobe ili poslovni subjekti koji su primatelji vremenskih žigova i djeluju temeljem razumnog pouzdanja u vremenske žigove koje izdaje Fina QTSA 2015.

3.2.6. Ostali sudionici

Ostali sudionici Fina QTSA 2015 su pravne osobe koje ne pružaju i ne koriste usluge certificiranja, ali sudjeluju u dijelovima procesa vezanim uz davanje usluga certificiranja. U ovu grupu sudionika spadaju proizvođači i distributeri hardvera i softvera korištenih u Fina QTSA 2015 servisu, odnosno u Fina PKI, neovisni ocjenitelji i dr.

3.3. Opća pravila i Pravilnik o postupcima izdavanja vremenskog žiga

Ovaj dokument Fina - Opća pravila davanja usluga izdavanja naprednih vremenskih žigova (engl.: *Time-Stamp Policy,* u daljem tekstu: TP) odgovara dokumentu „Opća pravila davanja usluga ugradnje naprednog vremenskog žiga“ definiranom u Pravilniku o evidenciji davatelja usluga certificiranja [4] te sadrži temeljna pravila i skup načela za davanje usluga izdavanja naprednih vremenskih žigova koja su usklađene sa zakonskom regulativom o elektroničkom potpisu u Republici Hrvatskoj. Detaljni opis pravila i postupaka iz opsega ovog TP dokumenta nalazi se u dokumentu Fina - Pravilnik o postupcima certificiranja za nekvalificirane certifikate [24] (u daljem tekstu: CPS_{NQC}).

4. OPĆA PRAVILA DAVANJA USLUGE IZDAVANJA VREMENSKOG ŽIGA

4.1. Pregled

Ovaj TP dokument ne postavlja nikakva dodatna ograničenja u odnosu na uporabu vremenskog žiga, osim uvjeta postavljenih u ugovoru o pružanju usluge izdavanja vremenskog žiga.

Primijenjena tehnologija vremenskog žiga zasniva se na kriptografiji javnog ključa, X.509 certifikatima i pouzdanim servisima točnog vremena.

Sadržaj ovog TP dokumenta usklađen je s normizacijskim dokumentima:

- HRS ETSI/TS 102 023 [14],
- HRS ETSI/TS 101 861 [11],
- HRS ETSI/TS 102 176-1 [12],
- ETSI TS 119 312 [13].

Svrha ovog TP dokumenta je definiranje i uređivanje pravila i načela prema kojima trebaju postupati Fina QTSA, korisnici usluge izdavanja vremenskog žiga (u daljnjem tekstu: korisnici) i pouzdajuće strane.

4.2. Naziv dokumenta i identifikacijski podaci

OID za Finu dodijeljen je od strane *British Standards Institution* (BSI) *International Code Designator* (ICD). Na temelju tog OID-a Fina je za potrebe davanja usluge izdavanja vremenskih žigova dodijelila OID: 1.3.124.1104.2.

U nastavku je naveden naziv ovog dokumenta i pripadajući identifikacijski podaci.

- Naziv: Fina - Opća pravila davanja usluge izdavanja naprednog vremenskih žigova
- Verzija: 1.0
- Datum objave: 07.12.2015.
- Datum stupanja na snagu: 07.12.2015.
- OID: 1.3.124.1104.2.2.1.1.0

Navedeni OID predstavlja identifikator ovog TP dokumenta (TP OID) i nalazi se u svakom izdanom vremenskom žigu.

4.2.1. Postupci kod promjene sadržaja dokumentacije

Promjene sadržaja dokumenta obavljaju se na temelju internih prijedloga i zahtjeva za usklađivanjem sa zakonskom regulativom i mjerodavnim normama. Nova verzija dokumenta ima oznaku datuma objave, datuma stupanja na snagu i novi broj verzije.

Napisane i potpisane primjedbe na ovaj dokument mogu su uputiti na poštansku ili e-mail adresu iz točke 4.2.4. ovog TP dokumenta. Odluke o prihvaćanju primjedbi su diskreciono pravo Fine.

4.2.2. Objavljivanje dokumentacije

Ovaj dokument javno je objavljen na internetskim stranicama http://www.fina.hr/finadigicert.

4.2.3. Postupci prihvaćanja/odobravanja dokumentacije

Promjene u Fina QTSA dokumentaciji prihvaća i odobrava Fina PMA.

4.2.4. Kontakt podaci

Kontakt podaci za administraciju i sadržaj ovog TP dokumenta:

Poštanska adresa:

Fina
Sektor financijskih i elektroničkih usluga
Ured za upravljanje politikom e-poslovanja
Koturaška cesta 43
10000 Zagreb
Hrvatska

telefon: +385-1-6128-171

telefax: +385-1-6304-081

E-mail: pma@fina.hr

4.3. Korisnici i područje primjene usluga

Usluga izdavanja vremenskog žiga koristi se za osiguranje postojanosti nekog elektroničkog zapisa u vremenu te za dokazivanje postojanja elektroničkog zapisa prije određenog vremenskog trenutka. Vremenski žig kojeg izdaje davatelj usluga vremenskog žiga pouzdano povezuje sažetak (engl. *hash*) određenog elektroničkog zapisa s točnim vremenom izdavanja vremenskog žiga. Izdavatelj vremenskog žiga potpisuje vremenski žig svojim elektroničkim potpisom i time zaštićuje cjelovitost vremenskog žiga i identificira sebe kao izdavatelja vremenskog žiga.

Vremenski žig koristi se i u području elektroničkog potpisa za pouzdanu verifikaciju elektroničkog potpisa i nakon opoziva ili isteka valjanosti potpisnog certifikata. Svaki certifikat za vrijeme njegovog perioda važenja može u bilo kojem trenutku biti opozvan te se ni jedan elektronički potpis izrađen na osnovu već opozvanog certifikata ne smije smatrati valjanim. Pouzdana provjera valjanosti elektroničkog potpisa nakon isteka potpisnog certifikata omogućuje se korištenjem vremenskog žiga ugrađenog u elektronički potpisani zapis jer vremenski žig omogućuje pouzdan dokaz da je određeni podatak postojao prije vremena navedenog u vremenskom žigu.

Napredni vremenski žig koristi se u području naprednog elektroničkog potpisa temeljenog na kvalificiranom certifikatu za pouzdanu verifikaciju elektroničkog potpisa i nakon opoziva ili isteka valjanosti potpisnog kvalificiranog certifikata.

Finina usluga izdavanja vremenskih žigova može se koristiti za bilo koju primjenu koja zahtjeva pouzdano utvrđivanje postojanja određenog elektroničkog zapisa prije nekog vremenskog trenutka. Vremenski žig izdan u skladu s ovim TP dokumentom može se koristiti i za očuvanje dugotrajnosti elektroničkih potpisa.

Usluga izdavanja vremenskog žiga podrazumijeva izdavanje vremenskih žigova koji se ugrađuju u elektroničke potpise i time osiguravaju vremensku postojanost elektroničkog zapisa i nakon isteka, odnosno opoziva potpisnog certifikata te time omogućuju dugotrajnu valjanost elektroničkog potpisa. Vremenski žig može se koristiti i za drugu primjenu koja zahtjeva pouzdano utvrđivanje postojanja elektroničkog zapisa prije nekog određenog vremena. Usluga izdavanja vremenskog žiga može se koristiti za elektroničke transakcije, obrasce, arhivirane podatke, itd.

Nije dozvoljena uporaba vremenskog žiga za one podatke, odnosno elektroničke zapise čiji je sadržaj protivan Ustavu Republike Hrvatske, prisilnim propisima ili moralu društva.

4.4. Usklađenost Općih pravila davanja usluga izdavanja vremenskog žiga

4.4.1. Usklađenost sa zakonom

Za tumačenje odredaba ovog TP dokumenta mjerodavne su odredbe Zakona o elektroničkom potpisu [1], [2] i [3], podzakonskih akata [4], [5] i [6] donesenih temeljem tog zakona te normizacijskih dokumenata i preporuka na koje isti upućuju [7].

Ovaj TP dokument i davanje usluga izdavanja naprednih vremenskih žigova obuhvaćene ovim TP dokumentom usklađeni su s propisima navedenim u ovoj točki.

4.4.2. Provjera usklađenosti

Inspekcijski nadzor nad radom Fina QTSA reguliran je Zakonom o elektroničkom potpisu [1], [2] i [3], a provodi ga ministarstvo nadležno za gospodarstvo.

Nadzor nad radom davatelja usluga izdavanja vremenskog žiga u području prikupljanja, uporabe i zaštite osobnih podataka korisnika mogu provoditi i državna te druga tijela određena zakonom i drugim propisima koji uređuju zaštitu osobnih podataka.

Unutarnju kontrolu provođenja propisanih postupaka vezanih uz rad Fina QTSA i provedbu unutarnjeg procesa odobravanja rada Fina QTSA sukladno pravilima definiranim u ovom TP dokumentu provodi Fina PMA.

Provjera usklađenosti izdavanja vremenskog žiga provodi se sukladno normizacijskom dokumentu HRS ETSI/TS 102 023 [14] i zakonskoj regulativi iz točke 4.4.1. ovog TP dokumenta.

4.4.3. Učestalost ili okolnosti provjere usklađenosti

Provjera usklađenosti rada Fina QTSA 2015 provodi se redovito, najmanje jedanput godišnje.

Provjeru usklađenosti potrebno je provesti i prije početka rada novog TSU te nakon značajnijih promjena u radu Fina QTSA 2105, odnosno nakon katastrofe ili sumnje u kompromitiranje sustava.

4.4.4. Identitet/kvalifikacije ocjenitelja

Interni ocjenitelji moraju:

- raspolagati znanjima i razumijevanjem odredbi HRS ETSI/TS 102 023 [14] te odredbi iz normizacijskog dokumenta CWA 14167-1 [16];
- raspolagati aktualnim znanjima i vještinama iz PKI područja, tehnologije vremenske ovjere te područja informacijske sigurnosti;
- poznavati zakonsku regulativu iz područja davanja usluga certificiranja.

4.4.5. Odnos ocjenitelja s tijelom koje se ocjenjuje

Interni ocjenitelji moraju biti dovoljno organizacijski odvojeni od Fina QTSA kako bi obavljali neovisnu/neutralnu provjeru.

4.4.6. Predmeti provjera

Pri provjeri usklađenosti ocjenitelji provjeravaju postupa li Fina QTSA 2015 prema ovom TP dokumentu, internom CPS_{NQC} [24] dokumentu te ostaloj mjerodavnoj dokumentaciji.

4.4.7. Mjere u slučaju neusklađenosti

U slučaju neusklađenosti u radu Fina QTSA 2015, ocjenitelj izrađuje izvještaj i dostavlja ga u Fina PMA na osnovu kojeg Fina PMA izrađuje plan akcija, mjera i postupaka koje će poduzeti kako bi se otklonile neusklađenosti navedene u izvješću ocjenitelja. Ako Fina QTSA 2015 ne provede akcije za otklanjanje neusklađenosti, Fina PMA može donijeti odluke o akcijama koje će biti primjerene težini neusklađenosti.

Fina QTSA mora voditi interni dnevnik vremenskih razdoblja u kojima Fina QTSA 2015 servis nije radio u skladu s ovim TP dokumentom, s navedenim razlozima neusklađenosti.

4.4.8. Priopćavanje rezultata

Fina PMA kao nadležno tijelo, dužno je izvještaj o provjeri usklađenosti i plan akcija, mjera i postupaka koje će se poduzeti, ukoliko su otkrivene neusklađenosti, dostaviti svim odgovornim osobama unutar Fina PKI, odnosno Fina QTSA koje su odgovorne za rad pojedinih dijelova sustava u kojima je izvedena provjera usklađenosti.

U cilju dokazivanja usklađenosti, korisnicima i pouzdajućim stranama na zahtjev je dostupan izvještaj o provjeri usklađenosti koju je obavio interni ili vanjski neovisni ocjenitelj.

Rezultate vanjske provjere usklađenosti Fina može javno objaviti. Rezultati se objavljuju na internetskim stranicama http://www.fina.hr/finadigicert.

5. OBVEZE I ODGOVORNOSTI

5.1. Obveze sudionika Fina QTSA 2015 servisa

5.1.1. Obveze Fina QTSA

Fina kao davatelj usluga izdavanja naprednih vremenskih žigova (Fina QTSA) obvezuje se na točnost podataka o vremenu ugrađenog u vremenski žig. Podatak o UTC vremenu kojeg se ugrađuje u svaki pojedini vremenski žig ima odstupanje manje od +/- 1 s.

Fina također ima obvezu:

- provoditi davanje usluga izdavanja vremenskog žiga u skladu sa Zakonom o elektroničkom potpisu [1], [2] i [3], podzakonskim propisima [4], [5], [6] i [7] donesenim temeljem Zakona [1], [2] i [3], međunarodnim normama i preporukama, ovim TP dokumentom te drugim aktima Fine vezanim uz obavljanje usluga izdavanja vremenskog žiga;
- provoditi izdavanje vremenskog žiga na vjerodostojnom sustavu, a potpisivanje vremenskog žiga na opremi koja udovoljava zahtjevima iz točke 6.2.6. ovog TP dokumenta;
- provoditi zahtijevane sigurnosne mjere za zaštitu prostora i opreme sustava za izdavanje vremenskog žiga;
- osigurati nesmetan rad i maksimalnu raspoloživost usluga izdavanja vremenskih žigova sukladno najboljoj poslovnoj praksi;
- objaviti akte koji mogu biti javno dostupni na internetskim stranicama http://www.fina.hr/finadigicert;
- obavljati usluge izdavanja vremenskog žiga s pažnjom dobrog stručnjaka;
- primjenjivati u svom poslovanju organizacijske i tehničke mjere zaštite podataka prikupljenih od korisnika pri ugovaranju korištenja ove usluge i te podatke čuvati kao poslovnu tajnu te ih koristiti isključivo za potrebe usluga certificiranja iz opsega ovog TP dokumenta i dodatnih usluga certificiranja iz skupa Fina PKI usluga (npr. izdavanje certifikata);
- primjenjivati odredbe Zakona o zaštiti osobnih podataka [8] i drugih propisa kojima je uređena zaštita osobnih podataka te tajnost podataka u Republici Hrvatskoj;
- ne povređivati intelektualno vlasništvo, licenčna i druga prava;
- rješavati zastoje i greške u radu sustava za izdavanje vremenskih žigova u najkraćem mogućem roku;
- planirati održavanje i daljnji razvoj sustava za izdavanje vremenskog žiga sukladno važećim normama i razvoju tehnologije.

5.1.2. Obveze korisnika

Korisnik je obvezan prilikom predaje zahtjeva za korištenje usluga izdavanja vremenskog žiga, na temelju kojeg ugovara korištenje usluge, u zahtjevu navesti točne i istinite osobne podatke te odmah obavijestiti Finu, kao davatelja usluge, o svakoj promjeni tih podataka.

Korisnik kojem se izdaje vremenski žig treba verificirati elektronički potpis Fina QTSA 2015 na zaprimljenom vremenskom žigu i provjeriti valjanost Fina QTSA 2015 certifikata. Opozvanost Fina QTSA 2015 certifikata provjerava se putem CRL koju izdaje Fina RDC 2015 i koja se objavljuje na web poslužitelju kao i na LDAP imeničkom poslužitelju. Adrese na kojima se objavljuje CRL lista za provjeru opozvanost Fina QTSA 2015 certifikata navedene su u CRL *Distribution Points* ekstenziji Fina QTSA 2015 certifikata sukladno profilu certifikata za vremenski žig opisanom u točki 6.2.19. ovog TP dokumenta.

Informacija o *online* provjeri statusa opozvanosti izdanih certifikata u realnom vremenu dostupna je i korištenjem Fininog OCSP servisa.

Internetska adresa Fininog OCSP servisa je http://ocsp.fina.hr, a upisana je u ekstenziji *Authority Information Access* Fina QTSA 2015 certifikata, kao i svakog certifikata kojeg izdaju Finini CA-ovi.

Korisnik se obvezuje da neće zahtijevati izdavanje vremenskog žiga za one podatke, odnosno elektroničke zapise čiji je sadržaj protivan Ustavu Republike Hrvatske, prisilnim propisima ili moralu društva. U protivnom odgovara Fini za svu štetu.

Korisnik je obvezan s pažnjom dobrog domaćina, odnosno gospodarstvenika čuvati privatni ključ i pripadajuće aktivacijske podatke koji se odnose na certifikat kojim pristupa usluzi izdavanja vremenskog žiga, sukladno relevantnim propisima. Korisnik se obvezuje da nitko drugi neovlašten neće imati pristup privatnom ključu i aktivacijskim podacima koje se odnose na certifikat kojim pristupa ovoj usluzi.

Korisnik je obvezan s pažnjom dobrog domaćina, odnosno gospodarstvenika pravodobno na internetskim stranicama http://www.fina.hr/finadigicert pratiti i upoznati se s objavljenim izmjenama i/ili dopunama ovog TP dokumenta.

Korisnik je obvezan za korištenje usluge izdavanja vremenskog žiga plaćati Fini naknadu sukladno cjeniku Fina QTSA usluga iz točke 6.5.1. ovog TP dokumenta.

5.1.3. Obveze pouzdajućih strana

Prije pouzdanja u vremenski žig pouzdajuća strana mora:

- obaviti verifikaciju potpisa vremenskog žiga;
- provjeriti na važećoj listi opozvanih certifikata (CRL), ili korištenjem *online* Fininog OCSP servisa opozvanost Fina QTSA 2015 certifikata čijim je pripadnim privatnim TSU ključem potpisan vremenski žig.

U slučaju verificiranja vremenskog žiga nakon isteka vremena važenja Fina QTSA 2015 certifikata, pouzdajuća strana treba provjeriti da li se kriptografski *hash* algoritam te potpisni kriptografski algoritam i duljina potpisnog TSU ključa kojima je potpisan vremenski žig još uvijek smatraju sigurnim.

Pouzdajuća strana obvezna je pridržavati se odredbi ovog TP dokumenta.

5.2. Odgovornosti sudionika Fina QTSA 2015 servisa

5.2.1. Odgovornosti Fina QTSA

Fina kao davatelj usluga izdavanja vremenskog žiga ima punu odgovornost za davanje usluga izdavanja vremenskog žiga i za ispunjenje svih zahtjeva propisanih ovim TP dokumentom.

Fina ima odgovornost da svi zahtjevi koji se odnose na davanje usluga izdavanja vremenskog žiga, što uključuje postupke koje se odnose na izdavanje vremenskog žiga, nadzor sustava i sigurnosne kontrole, budu u skladu s odredbama ovog TP dokumenta.

Ovaj TP dokument je integralni dio ugovora o pružanju usluge izdavanja vremenskog žiga kojeg sklapaju korisnik i Fina kao davatelj usluga izdavanja vremenskog žiga.

5.2.1.1. Odricanje od odgovornosti Fina QTSA

Osim onog što je za Finu, kao davatelja usluge, izričito navedeno u točkama 5.1.1. i 5.2.1. ovog TP dokumenta i točki 9.6.1. i 9.6.2. Općih pravila davanja usluga certificiranja [23], Fina ne odgovora ni za koje drugo jamstvo ili odgovornost, posebno ne u slučaju ako bi do odgovornosti Fine prema danim jamstvima došlo zbog povrede jamstava i odgovornosti drugih sudionika navedenih u točkama 5.1.2. i 5.1.3., odnosno 5.2.2. i 5.2.3. ovog TP dokumenta.

Fina nije odgovorna za štete uključujući indirektne i specijalne, štete za slučaj nezgode, za slučaj nepogode s posljedicama ili za bilo koji gubitak dobiti, gubitak podataka ili druge indirektne štete koje su proizašle iz veze s uslugama vremenskog žiga:

- za štete pretrpljene u vremenu od opoziva potpisnog korisničkog certifikata do izdavanja sljedeće CRL, ukoliko se isti koristi uz vremenski žig;
- za štete zbog korištenja usluge vremenskog žiga u ime korisnika, kada korištenje usluge nije autorizirano od strane korisnika;
- za štete prouzročene lažnom ili nemarnom uporabom potpisnog korisničkog certifikata uz kojeg se koristi vremenski žig ili nemarne provjere CRL-a;
- za štete nastale kao rezultat neispravnosti i pogrešaka u softveru i hardveru korisnika i pouzdajuće strane.

5.2.2. Odgovornosti korisnika

Korisnik je odgovoran za sadržaj podataka, odnosno elektroničkog zapisa za koji traži izdavanje vremenskog žiga.

Korisnik je odgovoran da korisnička aplikacija koju koristi za ugradnju vremenskog žiga osigurava potpunu interoperabilnost s Fina QTSA 2015 sustavom.

Korisnik odgovara za štetu koju prouzroči otkrivanjem svojeg privatnog ključa i/ili pripadajućih aktivacijskih podataka koji se odnose na certifikat kojim pristupa usluzi izdavanja vremenskog žiga.

Korisnik odgovara za potpunost i točnost, odnosno istinitost svih podataka koje je naveo u zahtjevu za korištenje usluga izdavanja vremenskog žiga na temelju kojeg je ugovorio korištenje usluge.

Korisnik odgovara za nepravilnosti koje su nastale zbog neispunjavanja obveza utvrđenih u točki 5.1.2. ovog TP dokumenta.

Korisniku koji ne postupa u skladu s preuzetim obvezama može se privremeno ili trajno uskratiti usluga izdavanja vremenskog žiga te može izgubiti sva prava proizašla iz ugovora o pružanju usluga izdavanja vremenskog žiga.

5.2.3. Odgovornosti pouzdajućih strana

Pouzdajuća strana koja se, ne poštujući odredbe iz ovog TP dokumenta te protivno utvrđenim obvezama iz točke 5.1.3., pouzdaje u nevažeći vremenski žig, snosi sama sve rizike pouzdanja u takav vremenski žig.

Pouzdajuća strana snosi sve rizike pouzdanja u vremenski žig ako zna ili ima razloga smatrati da postoje činjenice koje mogu uzrokovati osobnu ili poslovnu štetu prouzročenu korištenjem vremenskog žiga.

6. ZAHTJEVI ZA Fina QTSA POSTUPKE

6.1. Pravilnik o postupcima i Izjava o davanju usluga

6.1.1. Pravilnik o postupcima izdavanja vremenskog žiga

Postupci vezani uz izdavanje vremenskog žiga opisani su u CPS_{NQC} [24] dokumentu.

Fina obavještava sve korisnike i pouzdajuće strane o uvjetima korištenja usluga izdavanja vremenskog žiga kroz Uvjete o pružanju usluge izdavanja vremenskog žiga.

Sadržaj i odobravanje CPS_{NQC} [24] dokumenta provodi Fina PMA kao nadzorno tijelo.

U slučaju promjena ovog TP dokumenta i CPS_{NQC} [24] dokumenta, Fina PMA će objaviti na internetskim stranicama http://www.fina.hr/finadigicert da je odobrila nove verzije dokumenata i datum od kada isti počinju važiti.

6.1.2. Izjava o davanju usluga izdavanja vremenskog žiga

Izjava o davanju usluga izdavanja naprednog vremenskog žiga objavljena je na internetskim stranicamahttp://www.fina.hr/finadigicert.

Ova izjava sadrži:

- kontakt podatke za Fina QTSA;
- informaciju o aktualnoj verziji TP dokumenta u primjeni;
- informaciju o barem jednom *hash* algoritmu koji se može upotrijebiti za reprezentaciju podataka za koje se traži vremenski žig;
- očekivano vremensko trajanje potpisa kojim je potpisan vremenski žig;
- točnost vremena u vremenskom žigu (UTC);
- ograničenja u korištenju usluge izdavanja vremenskog žiga;
- obveze Fina QTSA, korisnika i pouzdajućih strana;
- informacije o načinu provjere vremenskog žiga koji osigurava razumno povjerenje pouzdajuće strane;
- vremensko razdoblje u kojem se čuvaju zapisi dnevnika Fina QTSA 2015 sustava;
- primijenjena regulativa i izjava o zadovoljenju zakonskih zahtjeva;
- ograničenja odgovornosti;
- procedure u slučaju spora.

6.2. Upravljanje životnim ciklusom ključeva Fina QTSA 2015

6.2.1. Generiranje Fina QTSA 2015 para ključeva

TSU par ključeva za Fina QTSA 2015 sustav mora biti generiran na takav način da se ni u jednom trenutku ne može pojaviti nezaštićen.

TSU par ključeva za Fina QTSA 2015 sustav generira se, uz minimalno dualnu kontrolu ovlaštenih osoba Fina QTSA, u HSM modulu koji zadovoljava zahtjeve iz točke 6.2.6. ovog TP dokumenta. HSM kojim se štiti privatni ključ Fina QTSA 2015 smješten je u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora, koji je ujedno i Fina QTSA štićeni prostor (u daljem tekstu zajedničkim nazivom: Fina PKI štićeni prostor), a opisan je u točki 6.4.3.1. ovog TP dokumenta. Upravljanje privatnim ključem Fina QTSA 2015 provodi se fizičkim pristupom HSM-u uz minimalno dualnu kontrolu te autorizacijom dvije ovlaštene osobe s povjerljivim ulogama u Fina QTSA.

Privatni TSU ključ za Fina QTSA 2015 čuva se u HSM modulu koji zadovoljava zahtjeve navedene u točki 6.2.6. ovog TP dokumenta.

U postupku generiranja para TSU ključeva za Fina QTSA 2015 sudjeluju sljedeće ovlaštene osobe s povjerljivim ulogama u Fina QTSA:

- Službenik za sigurnost, 1 osoba;
- Administrator sustava, 3 osobe;
- Službenik za nadzor sustava, 1 osoba.

O provedenom generiranju TSU ključeva vodi se zapisnik s priloženim dnevnicima sustava.

6.2.2. Dostava javnog TSU ključa pouzdajućim stranama

Javni TSU ključ Fina QTSA 2015 servisa služi za provjeru potpisa vremenskog žiga, a nalazi se u certifikatu Fina QTSA 2015 servisa koji je objavljen na LDAP imeničkom poslužitelju rdc-ldap2.fina.hr te na internetskim stranicamahttp://www.fina.hr/finadigicert. Certifikat za Fina QTSA 2015 servis izdaje Finino certifikacijsko tijelo (CA): Fina RDC 2015, a sukladno Općim pravilima davanja usluga certificiranja [23] i CPS_{NQC} [24] dokumentu.

6.2.3. Duljine ključeva

Duljina TSU ključeva Fina QTSA 2015 servisa i algoritmi za potpisivanje vremenskog žiga su:

- RSA kriptografski algoritam s dužinom ključa od 2048 bita;
- *sha256WithRSA* algoritam.

6.2.4. Generiranje i provjera kvalitete parametara javnog ključa

Ključevi koje upotrebljava Fina QTSA 2015 generiraju se sukladno normizacijskom dokumentu ETSI TS 119 312 [13].

6.2.5. Namjene ključeva (po X.509 v3 polju uporabe ključa)

Privatni TSU ključ za Fina QTSA 2015 koristi se samo za elektronički potpis vremenskih žigova.

6.2.6. Norme i upravljačke funkcije kriptografskog modula

HSM modul kojim TSU obavlja potpisivanje vremenskog žiga zadovoljava zahtjeve prema FIPS 140-2 [21], razina 3.

6.2.7. Upravljanje privatnim TSU ključem od strane više osoba (n od m)

Upravljanje privatnim ključem od strane više osoba sigurnosni je mjera koja zahtijeva autorizaciju više ovlaštenih osoba za pristup privatnom TSU ključu za potpis vremenskog žiga. Taj mehanizam sprječava jednu osobu da sama pristupi privatnom potpisnom TSU ključu Fina QTSA 2015 servisa.

Upravljanje privatnim TSU ključem Fina QTSA 2015 provodi se fizičkim pristupom HSM-u uz minimalno dualnu kontrolu te autorizacijom dvije ovlaštene osobe s povjerljivim ulogama u Fina QTSA.

6.2.8. Sigurno skladištenje privatnog ključa (*key escrow*)

Sigurno skladištenje privatnih TSU ključeva za Fina QTSA 2015 ne primjenjuje se.

6.2.9. Sigurnosno kopiranje privatnog ključa

Sigurnosne kopije privatnog TSU ključa Fina QTSA 2015 čuvaju se u enkriptiranom obliku na magnetskim trakama u kontroliranom broju kopija privatnog ključa u sigurnom prostoru najviše razine sigurnosti unutar Fina PKI štićenih prostora na odvojenim lokacijama.

Sigurnosne kopije privatnog TSU ključa Fina QTSA 2015 zaštićene su mjerama koje pružaju jednaku ili višu razinu sigurnosti u odnosu na privatni ključ u uporabi.

Ne postoje druge kopije privatnog TSU ključa Fina QTSA 2015, osim navedenih.

Sigurnosno kopiranje privatnog TSU ključa izvodi se pod minimalno dualnom kontrolom i samo od strane ovlaštenog osoblja Fina QTSA iz točke 6.2.1. ovog TP dokumenta. Privatni TSU ključ kopira se i dohvaća iz kriptografskog modula isključivo u enkriptiranom obliku.

6.2.10. Arhiviranje privatnog ključa

Privatni TSU ključevi Fina QTSA 2015 ne arhiviraju se.

6.2.11. Prijenos privatnog ključa u ili iz kriptografskog modula

Ako privatni TSU ključ Fina QTSA 2015 treba prenijeti iz ili u HSM, za vrijeme dok je izvan HSM-a privatni TSU ključ je zaštićen na način koji osigurava jednaku razinu sigurnosti kao i kad se nalazi u HSM-u. Postupak prijenosa privatnog TSU ključa provode samo ovlaštene osobe s povjerljivim ulogama u Fina QTSA, uz minimalno dualnu kontrolu.

Za prijenos privatnog TSU ključa Fina QTSA 2015 sustava iz jednog HSM-a u drugi mora se osigurati da se privatni TSU ključ prenosi samo u HSM jednake ili više razine sigurnosti u odnosu na HSM iz kojega se privatni ključ prenosi.

Privatni TSU ključ Fina QTSA 2015 sustava mora biti enkriptiran tijekom prijenosa i ne smije se ni u jednom trenutku pojaviti nezaštićen dok je izvan kriptografskog modula.

6.2.12. Spremanje privatnog ključa u kriptografskom modulu

Privatni TSU ključevi Fina QTSA 2015 zaštićeni su HSM modulima koji zadovoljavaju zahtjeve iz točke 6.2.6. ovog TP dokumenta i mogu se koristiti jedino ako su propisno aktivirani.

6.2.13. Generiranje i instalacija aktivacijskih podataka

Aktivacijski podaci povezani s privatnim TSU ključem za Fina QTSA 2015 generiraju se i instaliraju prilikom postupka generiranja pripadajućeg privatnog ključa.

6.2.14. Zaštita aktivacijskih podataka

Aktivacijski podaci povezani s privatnim TSU ključem za Fina QTSA 2015 podijeljeni su na hardverska sredstva za aktivaciju, sukladno točki 6.2.7. ovog TP dokumenta, a koja se zaštićena pripadajućim PIN-ovima te se na siguran način čuvaju u Fina PKI štićenom prostoru.

6.2.15. Metoda aktivacije privatnog TSU ključa

Aktivacija privatnih TSU ključeva za Fina QTSA 2015 provodi se pod dualnom kontrolom ovlaštenih osoba s povjerljivom ulogom Administrator sustava u Fina QTSA. Svaka od ovih ovlaštenih osoba za aktivaciju HSM-a upotrebljava hardversko sredstvo za aktivaciju i pripadajući tajni PIN. Privatni TSU ključ mora se čuvati u zaštićenom obliku kad je deaktiviran.

6.2.16. Metoda deaktivacije privatnog TSU ključa

Deaktivacija privatnog TSU ključa Fina QTSA 2015 provodi se pod dualnom kontrolom ovlaštenih osoba s povjerljivom ulogom Administrator sustava u Fina QTSA.

Privatni TSU ključevi Fina QTSA 2015 sustava deaktiviraju se:

- zaustavljanjem Fina QTSA 2015 serverskog procesa,
- odjavom s HSM-a,
- isključenjem HSM-a,
- isključenjem servera povezanim s HSM-om.

6.2.17. Metoda uništavanja privatnog TSU ključa

Postupak uništavanja privatnog TSU ključa Fina QTSA 2015 provodi se na siguran način, nakon isteka perioda njegove valjanosti, a izvodi se od strane ovlaštenih osoba s povjerljivim ulogama u Fina PKI, pod minimalno dualnom kontrolom sukladno postupcima opisanim u Fininoj internoj dokumentaciji.

Postupak uništavanja privatnih TSU ključeva osigurava da se nakon uništavanja privatni ključevi ni na koji način ne mogu oporaviti ili ponovno koristiti.

Postupak se dokumentira i arhivira.

6.2.18. Arhiviranje javnog ključa

Javni TSU ključ Fina QTSA 2015 servisa sastavni je dio pripadajućeg Fina QTSA 2015 certifikata koji se arhivira sukladno točkama 6.4.15., 6.4.16. i 6.4.17. ovog TP dokumenta.

6.2.19. Profil certifikata vremenskog žiga

Vremenski žig kojeg izdaje Fina QTSA 2015 servis potpisan je privatnim TSU ključem, čiji pripadajući certifikat ima profil opisan u ovoj točki TP-a.

Osnovni podaci o certifikatu kojim Fina QTSA 2015 servis potpisuje vremenske žigove dani su u Tablici 1.

Polje	Atribut	Vrijednost
Osnovna polja		
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	Serijski broj certifikata s entropijom od 64 bita (duljina serijskog broja:16 ili 17 bajtova)
signatureAlgorithm	AlgorithmIdentifier	sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11
signatureValue		Vrijednost potpisa izdavatelja certifikata

Polje	Atribut	Vrijednost
Osnovna polja		
Issuer	commonName (CN)	Fina RDC 2015
	organizationName (O)	Financijska agencija
	countryName (C)	HR
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + do 10 godina
Subject	commonName (CN)	CN = Fina QTSA1 2015
	organizationName (O)	O=Financijska agencija
	countryName (C)	HR
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption OID: 1.2.840.113549.1.1.1
	subjectPublicKey	Javni ključ subjekta: 2048 bita

Polje	Kritično	Atribut	Vrijednost
Ekstenzije			
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	DA	timeStamping	OID: 1.3.6.1.5.5.7.3.8
certificatePolicies	NE	policyIdentifier	OID: 1.3.124.1104.5.12.52.4.3
		cPSuri	http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-0-hr.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CP5-0-en.pdf
		policyQualifierID	CPS
CRLDistributionPoints	NE	DistributionPoint	[1]URI: http://rdc.fina.hr/RDC2015/FinaRDCCA2015.crl URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2015, O=Financijska agencija, C=HR?certificateRevocationList;binary [2]DirName:/C=HR/O=Financijska agencija/CN=Fina RDC 2015/CN=CRLx
AuthorityKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash vrijednost (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
SubjectKeyIdentifier	NE	keyIdentifier	160-bit SHA-1 hash vrijednost (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	http://ocsp.fina.hr
		id-ad-caIssuers	http://rdc.fina.hr/RDC2015/FinaRDCCA2015.cer

Tablica 1. Osnovna polja i ekstenzije profila certifikata za vremenski žig

Certifikat za Fina QTSA 2015 servis izdaje Finino certifikacijsko tijelo (CA): Fina RDC 2015.

6.2.20. OID certifikata za vremenski žig

CP OID certifikata za vremenski žig: 1.3.124.1104.5.12.52.4.3

6.2.21. Period valjanosti Fina QTSA 2015 certifikata i korištenja para ključeva

Certifikat za vremenski žig izdan sukladno ovom TP-dokumentu ima period valjanosti od 10 godina.

Vremenski period valjanosti privatnog TSU ključa jednak je vremenskom periodu valjanosti pripadajućeg certifikata. Certifikati i pripadajući ključevi ne smiju se upotrebljavati nakon isteka roka valjanosti certifikata ili nakon opoziva certifikata.

6.2.22. Generiranje novog TSU ključa

Generiranje novog TSU ključa i njegova uspostava za Fina QTSA 2015 provodi se pravovremeno prije isteka perioda valjanosti Fina QTSA 2015 certifikata. Generiranje se provodi na način opisan u točki 6.2.1. ovog TP dokumenta.

6.2.23. Kraj životnog vijeka TSU ključeva

Privatni TSU ključ Fina QTSA 2015 ne smije se koristiti po isteku perioda važenja Fina QTSA 2015 certifikata. Fina QTSA ne smije biti u mogućnosti izdavati vremenske žigove nakon isteka važenja Fina QTSA 2015 certifikata.

Fina QTSA provodi operativne postupke prema kojima se osigurava pravovremeno generiranje novih TSU ključeva, prije isteka valjanosti postojećih TSU ključeva. Po isteku valjanosti, privatni TSU ključevi i njihove kopije sigurno se uništavaju sukladno točki 6.2.17. ovog TP dokumenta, tako da ne postoji niti jedna njihova kopija te iste nije moguće ponovo koristiti.

6.2.23.1. Opoziv i suspenzija certifikata

Suspenzija certifikata za Fina QTSA 2015 servis nije dozvoljena.

6.2.23.1.1 Profil CRL

Profil CRL sukladan je preporuci IETF RFC 5280 [18]

6.2.23.1.2 Razlozi za opoziv

Fina QTSA 2015 certifikat može se opozvati iz sljedećih razloga:

- ako dođe do kompromitiranja privatnog ključa,
- ako neka od informacija sadržanih u certifikatu postane netočna,
- u slučaju trajne nedosupnosti ili gubitka privatnog ključa,
- u slučaju da korišteni kriptografski algoritmi i parametri prestanu pružati zahtijevanu sigurnost i zaštitu,
- ako Fina QTSA 2015 prestaje s radom, a Fina nije u mogućnosti osigurati nastavak obavljanja usluga certificiranja kod drugog davatelja usluga,
- ako certifikat nije izdan sukladno zahtjevu ili odredbama iz ovog TP dokumenta.

6.2.24. Upravljanje životnim ciklusom kriptografskih modula

Fina QTSA mora osigurati da kriptografski moduli nisu mijenjani tijekom transporta ili tijekom skladištenja.

Instalaciju i aktivaciju kriptografskih modula u Fina PKI štićenom prostoru provodi ovlašteno osoblje Fina QTSA koje ima ovlasti za izvršavanje operacija upravljanja kriptografskim modulom.

Fina QTSA kontinuirano provjerava i osigurava da kriptografski moduli rade ispravno.

Na kraju radnog vijeka kriptografskog modula, privatni ključevi u modulu se uništavaju.

Postupak za rukovanje kriptografskim modulima opisan je u internim Fina QTSA dokumentima.

6.2.25. Ocjena kriptografskog modula

Ocjena HSM-ova za Fina QTSA 2015 provodi se sukladno zahtjevima opisanim u točki 6.2.6. ovog TP dokumenta.

6.3. Izdavanje vremenskog žiga

Svaki vremenski žig kojeg izdaje Fina QTSA 2015 sadrži TP OID - jedinstveni identifikator ovog TP dokumenta. Vremenski žig kojeg izdaje Fina QTSA 2015 sadrži datum i vrijeme koje je u skladu sa stvarnim UTC vremenom. Podatak o točnom vremenu dobiva se od Fininih satelitskih prijemnika. Podešavanje glavnog sata Fininih satelitskih prijemnika aktivira se automatski nakon otkrivanja razlike između UTC vremena primljenog putem satelita i glavnog sata, ukoliko je razlika veća od +/-250 ns.

Fina posjeduje satelitske prijemnike signala točnog vremena s kojima se Fina QTSA 2015 automatski sinkronizira.

U slučaju nedostupnosti satelitskog signala iz bilo kojeg razloga, Fina QTSA 2015 automatski prelazi na rad s internim izvorom točnog vremena koji osigurava zadanu točnost u odnosu na stvarno UTC vrijeme u trajanju od najviše 24 sata od početka nedostupnosti satelitskog signala.

Fina QTSA 2015 pruža uslugu izdavanja vremenskog žiga samo registriranim korisnicima.

6.3.1. Sklapanje ugovora

Ugovor o pružanju usluga izdavanja vremenskog žiga je ugovor koji sukladno Uvjetima o pružanju usluge izdavanja vremenskog žiga, općim propisima obveznog prava, TP-a i propisima koji uređuju pružanje usluge vremenskog žiga, sklapaju korisnici iz točke 3.2.3. ovog TP dokumenta i Fina kao davatelj usluge.

6.3.2. Identifikacija i autentifikacija

Registrirani korisnici pristupaju usluzi izdavanja vremenskog žiga uz obveznu autentifikaciju autentifikacijskim certifikatom (SSL/TLS uz klijentsku autentifikaciju certifikatom – *two-way* SSL) kojeg je izdalo Finino certifikacijsko tijelo (CA): Fina RDC 2015 ili Fina RDC-TDU 2015.

Fina QTSA može odobriti i drugi odgovarajući način autentifikacije korisnika.

6.3.3. Prihvaćanje ili odbijanje zahtjeva za izdavanje vremenskog žiga

Korisnik koji od Fina QTSA 2015 zahtjeva izdavanje vremenskog žiga mora ostvariti autentificiranu konekciju s komunikacijskim poslužiteljem Fina QTSA 2015 sustava. U slučaju neuspjele konekcije transakcija će biti prekinuta, a korisnik će na odgovarajući način biti obaviješten o neuspjeloj konekciji.

Klijentska aplikacija na strani korisnika koja se koristi za ugradnju vremenskog žiga, treba podržavati protokol za vremenski žig sukladan s IETF RFC 3161 [17].

Fina QTSA 2015 servis prihvaća profil zahtjeva za izdavanje vremenskog žiga usklađen s IETF RFC 3161 [17] te vremenski žig izdaje prema profilu koji je usklađen s IETF RFC 3161 [17].

6.3.4. Vrijeme obrade zahtjeva za izdavanje vremenskog žiga

Fina QTSA ne definira fiksan vremenski rok za obradu zahtjeva za izdavanje vremenskog žiga budući da to vrijeme ovisi o više aktivnosti, od kojih su neke vezane samo uz elektronički prijenos zahtjeva od strane korisnika do prijama na strani Fina QTSA 2015 sustava.

Informativno okvirno vrijeme potrebno za generiranje zahtjeva za izdavanje vremenskog žiga na strani korisnika je reda veličine sekunde.

Okvirno vrijeme potrebno TSU za generiranje vremenskog žiga na Fina QTSA 2015 sustavu je reda veličine ms.

U slučaju većeg broja zahtjeva za izdavanje vremenskog žiga u približno isto vrijeme tada vrijeme obrade zahtjeva može varirati.

6.3.5. Vremenski žig

Fina QTSA 2015 osigurava da se vremenski žigovi izdaju na siguran način i sa točnom oznakom vremena. Za svaki vremenski žig mora se osigurati:

- da sadrži OID TP dokumenta po kojem je izdan (TP OID);
- da ima jedinstveni identifikator;
- da se vrijeme korišteno u TSU može povezati sa stvarnim vremenom dostavljenim od pouzdanog izvora;
- da sadrži točan podatak o vremenu iz TSU u vrijeme izdavanja vremenskog žiga;
- da sadrži *hash* reprezentaciju elektroničkog zapisa za koji se izdaje vremenski žig;
- da je potpisan privatnim TSU ključem koji ima isključivu namjenu potpisivanja vremenskog žiga;
- identifikator države u kojoj je Fina QTSA ima sjedište;
- identifikator za Fina QTSA 2015;
- identifikator TSU koja je izdala vremenski žig.

Vremenski žig mora biti izdan sukladno preporukom ITF RFC 3161 [17] i normizacijskom dokumentom HRS ETSI/TS 102 023 [14] i profilom usklađenim s normizacijskim dokumentom HRS ETSI/TS 101 861 [11].

6.3.6. Profil vremenskog žiga

Osnovni podaci o profilu naprednih vremenskih žigova koje će izdavati Fina QTSA 2015 servis dani su u Tablici 2.

Polje	Vrijednost za nanapredni vremenski žig kojeg izdaje Fina QTSA 2015 servis
Version	V1, vrijednost="1"
Policy OID	1.3.124.1104.2.2.1.1.0
messageImprint	**Podržani hash algoritmi:** • **hashAlgorithm: sha-1 (OID: 1.3.14.3.2.26) i** • **hashAlgorithm: sha-256 (OID: 2.16.840.1.101.3.4.2.1)**
serialNumber	Cijeli broj
genTime	UTC vrijeme, razlučivost od 1 sekunde

Polje	Vrijednost za nanapredni vremenski žig kojeg izdaje Fina QTSA 2015 servis
Nonce	Cijeli broj
signatureAlgorithm	**sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)**

Tablica 2. Osnovni podaci o naprednom vremenskog žigu kojeg izdaje Fina QTSA 2015 servis

6.3.7. Sinkronizacija sata s UTC

Fina QTSA mora osigurati da je vrijeme Fina QTSA 2015 sustava sinkronizirano s UTC vremenom, unutar preciznosti propisane u točki 5.1. ovog TP dokumenta, a posebno:

- periodičnom kalibracijom sata;
- zaštitom od neautorizirane izmjene vremena TSU;
- detekcijom ispada iz sinkroniziranosti s UTC vremenom;
- uračunavanjem „*leap second*“ događaja.

6.4. Fina QTSA upravljanje i djelovanje

Mjere fizičke zaštite, postupci koje Fina QTSA primjenjuje u zaštiti Fina QTSA 2015 sustava, kao i postupci provjere sustava, upravljanja i radnih postupaka u Fina QTSA interne su prirode te se njihovi detalji ne objavljuju javno. Detaljnije mjere i postupci opisani su u Fininim internim dokumentima koji su na raspolaganju ovlaštenim tijelima koja provode nadzor nad davateljem usluga izdavanja vremenskog žiga.

Fina snosi punu odgovornost za davanje usluga izdavanja vremenskog žiga putem Fina QTSA 2015 servisa i odgovorna je za siguran i ispravan rad jedne ili više TSU jedinica koje izrađuju vremenski žig.

6.4.1. Klasifikacija informacijske imovine i procjena rizika

Fina QTSA 2015 ima provedenu procjenu rizika iz koje su određene sigurnosne kontrole i operativne procedure vezane uz sustav izdavanja vremenskog žiga i propadajuću opremu te moguće ugroze istih.

6.4.2. Osoblje Fina QTSA

Identifikacija ovlaštenih zaposlenika i određivanje prava pristupa za obavljanje pojedinih zadataka u skladu s organizacijom Fina QTSA provodi se kroz sigurnosne postupke i procedure provjere te se ostvaruje pomoću sigurnosnih mehanizama na sustavu.

Prije početka rada na poslovima Fina QTSA, Fina provodi odgovarajuće provjere kandidata da bi procijenila njihovu sposobnost i pouzdanost u skladu s potrebama poslova Fina QTSA.

U slučaju izvođenja neovlaštene ili zlonamjerne radnje koju je izvela ovlaštena osoba u Fina QTSA primjenjuju se odredbe važeće zakonske regulative i internih pravilnika Fine.

Detaljniji opis odabira, provjere, identifikacije i potvrđivanja identiteta ovlaštenih zaposlenika te način njihova uključenja na pristupne liste pojedinih Fina QTSA resursa nalazi se u točkama 5.2. i 5.3. CPS_{NQC} [24] dokumenta.

Broj ovlaštenih osoba s povjerljivim ulogama u Fina QTSA za obavljanje pojedine zadaće na Fina QTSA 2015 sustavu naveden je u točki 5.2.2. CPS_{NQC} dokumenta.

6.4.2.1. Povjerljive uloge

Upravljanje informacijskim sustavom, sustavom upravljanja certifikatima, poslovima zaštite i kontrole te poslovi pravne zaštite i nadzora djelovanja Fina QTSA 2015 sustava obavljaju se u unutar odvojenih organizacijskih dijelova Fine.

Fina osigurava da sve ovlaštene osobe koje obavljaju poslove vezane uz Fina QTSA 2015 sustav imaju dodijeljene odgovarajuće povjerljive uloge.

Povjerljive uloge dodjeljuju se ovlaštenim zaposlenicima iz nadležnih organizacijskih dijelova Fine i čine temelj povjerenja u Fina QTSA. Svaka povjerljiva uloga je dokumentirana s jasno definiranim opisom poslova i odgovornostima.

Povjerljive uloge uključuju uloge Službenika za sigurnost, Administratora sustava, Operatera sustava i Službenika za nadzor sustava.

Djelatnici kojima su povjerene povjerljive uloge ne smiju biti izloženi sukobu interesa.

Povjerljive uloge, ovlaštenja i odgovornosti Fina QTSA osoblja navedene su u točki 5.2.1. CPS_{NQC} [24] dokumenta i u opisu poslova onih djelatnika kojima su dodijeljene povjerljive uloge.

6.4.2.2. Broj osoba potrebnih za obavljanje zadataka

Poslove u Fina QTSA obavljaju isključivo ovlaštene osobe. Fina ima stalno zaposlen dovoljan broj stručnih osoba sa znanjem, iskustvom i kvalifikacijama koji je potreban u Fina QTSA za davanja usluga iz opsega ovog TP dokumenta.

Rad u Fina PKI štićenom prostoru provodi se isključivo uz istovremenu prisutnost najmanje dvije ovlaštene osobe s ulogama u Fina QTSA koje imaju pravo pristupa određenom dijelu sustava.

6.4.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu

Identifikacija ovlaštenih osoba i određivanje prava pristupa za obavljanje određenih poslova provodi se u skladu s organizacijom Fina QTSA, kroz sigurnosne procedure i postupke provjere te se ostvaruje pomoću sigurnosnih mehanizama u sustavu.

6.4.2.4. Uloge koje zahtijevaju odvajanje dužnosti

Za poslove povezane uz Fina QTSA provodi se sljedeće odvajanje dužnosti:

- Službenik za sigurnost ne smije obavljati poslove Službenika za nadzor sustava;
- Administrator sustava ne smije obavljati poslove Službenika za sigurnost ili poslove Službenika za nadzor sustava.

6.4.2.5. Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

Fina osigurava da sve ovlaštene osobe koje obavljaju poslove vezane uz Fina QTSA 2015 sustav imaju odgovarajuća stručna znanja u radu na području tehnologije vremenske ovjere, elektroničkog potpisivanja, mehanizama kalibracije i sinkronizacije Fina QTSA satova s UTC vremenom, da kod obnašanja povjerljivih uloga primjenjuju sigurnosne postupke te da imaju iskustvo u provedbi mjera sigurnosti u informatičkim sustavima.

Zaposlenici Fine koji rade na poslovima u Fina QTSA ne smiju biti u radnom, odnosno poslovnom odnosu s drugim davateljima usluga certificiranja.

6.4.2.6. Procedure provjere primjerenosti osoblja

Prije početka rada na poslovima u Fina QTSA, Fina provodi odgovarajuće provjere kandidata da bi procijenila njihovu sposobnost i pouzdanost u skladu s potrebama poslova u Fina QTSA.

6.4.2.7. Zahtjevi za školovanjem

Ovlaštenim osobama s povjerljivim ulogama u Fina QTSA osigurava se školovanje i usavršavanje sukladno ulogama koje su im dodijeljene.

6.4.2.8. Učestalost i uvjeti za obnovu znanja

Usavršavanje specijalističkih znanja i vještina ovlaštenih osoba s povjerljivim ulogama u Fina QTSA obavlja se pri dodjeli uloge i prema potrebi.

6.4.2.9. Učestalost i slijed izmjene zaposlenika

Promjena poslova zaposlenika obavlja se kada se za to javi potreba, ovisno o zahtjevima organizacijskih jedinica Fine ili na temelju zahtjeva zaposlenika.

6.4.2.10. Kazne za neovlaštene radnje

U slučaju izvođenja neovlaštene radnje ili zlonamjerne radnje koju je izvela ovlaštena osoba u Fina QTSA primjenjuju se odredbe važeće zakonske regulative i internih pravilnika Fine.

6.4.2.11. Zahtjevi na vanjske suradnike

Vanjskim suradnicima ne dodjeljuju se uloge na sustavima u Fina QTSA.

Vanjskim suradnicima pristup u Fina PKI štićeni prostor dopušten je jedino uz dualnu pratnju ovlaštenih osoba s ulogama u Fina QTSA.

Zahtjevi na vanjske suradnike određuju se ugovorom sklopljenim između Fine i vanjskog suradnika.

Fizički pristup vanjskim suradnicima Fina QTSA 2015 sustavu te fizički pristup repozitoriju i arhivi propisan je Fininim internim procedurama odobravanja i kontrole pristupa opremi za izdavanje digitalnih certifikata i vremenskih žigova.

6.4.2.12. Dokumentacija koja je dostupna osoblju

Ovlaštenim osobama u Fina QTSA dostupna je dokumentacija potrebna za obavljanje njihovih radnih zadataka sukladno dodijeljenim ulogama i pripadnim ovlaštenjima.

6.4.3. Kontrole fizičke sigurnosti

Fina kao davatelj usluga certificiranja primjenjuje mjere fizičke zaštite Fina QTSA 2015 sustava s ciljem smanjenja rizika na najmanju prihvatljivu mjeru i u skladu s poslovnom politikom Fine, važećom zakonskom regulativom i međunarodnim preporukama.

6.4.3.1. Lokacija objekta i njegova konstrukcija

Primarni produkcijski sustav certificiranja Fine u sklopu kojeg se nalazi i Fina QTSA 2015 sustav smješten je na primarnoj produkcijskoj lokaciji, u zgradi Fine, u posebnom štićenom prostoru izdvojenom za tu namjenu uz primjenu više razina fizičke i tehničke zaštite.

Sekundarni sustav certificiranja Fine u sklopu kojeg se nalazi i sekundarni Fina QTSA 2015 sustav namijenjen je za preuzimanje funkcija primarnog produkcijskog sustava certificiranja u slučaju prestanka rada primarnog produkcijskog sustava do njegovog oporavka te ponovnog uspostavljanja njegovih servisa. Sekundarni sustav certificiranja smješten je na udaljenoj pričuvnoj lokaciji Fine i u odnosu na primarni sustav udovoljava jednakim ili višim sigurnosnim zahtjevima.

6.4.3.2. Fizički pristup

Fizički pristup Fina QTSA 2015 sustavu te fizički pristup repozitoriju i arhivi dopušten je isključivo ovlaštenim zaposlenicima Fine u skladu s njihovim ulogama i ovlastima.

O svakom fizičkom pristupu Fina PKI štićenom prostoru vodi se evidencija.

6.4.3.3. Sustavi za napajanje i klimatizaciju

Fina PKI štićeni prostor u kojem se nalazi Fina QTSA 2015 sustav te pripadajući uređaji opskrbljeni su neprekidnim napajanjem električnom energijom i klimatizacijom koja je dimenzionirana na način da osigura odgovarajuće radne uvjete i u slučaju prekida vanjskog napajanja.

6.4.3.4. Opasnost od poplave

Oprema Fina QTSA 2015 sustava smještena je na lokacijama koje su osigurane od poplave.

6.4.3.5. Protupožarna zaštita

Oprema Fina QTSA 2015 sustava zaštićena je sustavom protupožarne zaštite sukladno propisanoj i važećoj zakonskoj regulativi te Fininim internim dokumentima.

6.4.3.6. Pohrana medija

Sigurnosne kopije Fina QTSA 2015 sustava, sigurnosne kopije podataka i arhive, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na siguran način kako bi se zaštitile od oštećenja, otuđenja ili neovlaštenog pristupa.

6.4.3.7. Zbrinjavanje otpada

Dokumenti i podaci u papirnatom i elektroničkom obliku koji se nalaze u Fina PKI štićenom prostoru, a za koje ne postoji potreba arhiviranja, na siguran način se odstranjuju i uništavaju.

Zbrinjavanje otpada iz Fina PKI štićenog prostora odvija se pod nadzorom ovlaštenih osoba s ulogama u Fina PKI, odnosno Fina QTSA.

Iz sustava arhive na siguran način se odstranjuju i uništavaju dokumenti i podaci u papirnatom i elektroničkom obliku za koje je istekla potreba za daljnjim arhiviranjem.

6.4.3.8. Sigurnosne kopije na drugoj lokaciji

Sigurnosne kopije Fina QTSA 2015 sustava, arhivske ili sigurnosne kopije podataka, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na odvojenoj lokaciji iz točke 6.4.3.1. ovog TP dokumenta, izdvojeno od primarnog produkcijskog sustava certificiranja. Ove su sigurnosne kopije u odnosu na njihove originale zaštićene jednakom ili višom razinom mjera fizičke zaštite.

6.4.4. Posebni tehnički zahtjevi na računalnu sigurnost

Fina osigurava da su svi zahtjevi na računalnu sigurnost Fina QTSA sustava usklađeni s normama HRS ETSI/TS 102 023 [14] i HRN ETSI/EN 319 411-2 [15] te sa zahtjevima iz dokumenta CEN Workshop Agreement 14167-1 [16].

Računalni resursi štite se mjerama sigurnosti prema ISO/IEC 27001 [19] i ISO/IEC 27002 [20] normi.

6.4.5. Kontrola sigurnosti računalnog sustava

Fina QTSA osigurava sigurno i ispravno davanje usluge izdavanja vremenskog žiga. Integritet komponenti i podataka u Fina QTSA sustavu adekvatno je zaštićen od napada virusa, neprijateljskog koda i djelovanja neautoriziranih programskih sustava. Mediji za pohranu podataka Fina QTSA 2015 zaštićeni su od oštećenja, krađe, neautoriziranog pristupa ili uništavanja. Ovi postupci su pod kontrolom osoblja kojima su dodijeljene pripadne uloge. Svaki djelatnik koji obnaša zadaće upravljanja odgovoran je za planiranje i implementaciju sigurnosne politike i pripadnih postupaka.

Fina QTSA 2015 sustav zadovoljava niže navedene uvjete zaštite:

- kontrola pristupa servisima i korisničkim ulogama djelatnika;
- razdvojenost dužnosti korisničkih uloga djelatnika;
- autentifikacija za korištenje korisničkih uloga djelatnika;
- arhiviranje podataka o zabilježenim događajima;
- revizija događaja koji se odnose na sigurnost;
- povjerljivost podataka za autentifikaciju Fina QTSA korisničkih uloga i osoba koje ih provode;
- postupci za vraćanje ključeva i obnovu funkcionalnosti Fina QTSA 2015 sustava;
- čvrste granice područja za procese koji su osjetljivi na sigurnost.

6.4.6. Kontrola pristupa prostoru, opremi i sredstvima

Fina QTSA je ima uspostavljenu odgovarajuću fizičku sigurnost radi ograničavanja pristupa informatičkoj opremi (hardveru i softveru) koja se upotrebljava za davanje usluge izdavanja vremenskog žiga. Pristup ovoj informatičkoj opremi ograničen je na ovlaštene osobe s ulogama u Fina QTSA. Pristup se kontrolira sustavom za kontrolu pristupa. Stalnu kontrolu pristupa provodi zaduženo osoblje ili se ona provodi elektronički.

Fina QTSA osigurava punu fizičku kontrolu pristupa kritičnim servisima Fina QTSA 2015 u cilju onemogućavanja neautoriziranog fizičkog pristupa.

Za izvođenje i upravljanje servisu za izdavanje vremenskog žiga:

- ograničen je fizički pristup resursima Fina QTSA svim neautoriziranim osobama, a omogućen je samo uz odobrenje i pratnju ovlaštenih osoba;
- ugrađene su kontrole koje onemogućavaju kompromitiranje Fina QTSA 2015 sustava zbog krađe ili neautorizirane izmjene podataka, odnosno dijelova informatičkog sustava Fina QTSA 2015.

Upravljanje Fina QTSA 2015 sustavom izvodi se iz fizički štićenog okruženja radi visoke razine zaštite od neautoriziranog pristupa sustavu upravljanja i podacima. Fizička zaštita izvedena je na

način da je određeno fizičko sigurnosno okružje oko upravljačkih resursa Fina QTSA. Fizičke i sigurnosne kontrole štite resurse Fina QTSA.

6.4.7. Kontrola sigurnosti mrežnog sustava

Sve lokalne mrežne komponente smještene su na fizički zaštićenim mjestima.

Mrežni promet je filtriran i nadziran. Fina QTSA oprema zaštićena je od svih poznatih oblika napada koji dolaze putem računalne mreže. Svi mrežni portovi i servisi koji se ne upotrebljavaju su isključeni. Na Fina QTSA opremi instaliran je i upogonjen samo mrežni softver koji je potreban za obavljanje davanja usluge certificiranja.

6.4.8. Kontrola sigurnosti radnog vijeka sustava

Fina QTSA 2015 sustav koristi autentične i vjerodostojne sustave i proizvode. Oprema (hardver i softver) Fina QTSA 2015 sustava prije instaliranja treba biti zaštićeno pakirana i isporučena povjerljivom metodom. Oprema Fina QTSA 2015 sustava ne smije sadržavati nikakve druge aplikacije koje nisu dio Fina QTSA 2015 konfiguracije. Nadogradnja opreme treba biti nabavljena na isti način kao i primarna oprema te treba biti instalirana na definirani način od povjerljive i stručne osobe.

Fina QTSA 2015 softver koji se nabavlja treba biti isporučen je u originalnom pakiranju i mora postojati metoda verifikacije kojom se utvrđuje da je softver koji je na sustavu:

- izvorni softver proizvođača softvera;
- da nije bio modificiran prije instalacije;
- da softver ima točnu verziju koja se namjerava upotrebljavati.

6.4.9. Postupci provjere sigurnosnih mjera

Fina QTSA u svojim dnevnicima sustava bilježi sve važne događaje povezane s radom Fina QTSA 2015 sustava. Informacije o događajima koji se bilježe automatski se prikupljaju.

Svi važni događaji u Fina QTSA 2015 sustavu koji se odnose na izdavanje vremenskih žigova zapisuju se kao revizijski zapisi u dnevnicima sustava. Revizijski zapisi sadrže:

- svi događaji vezani uz izdavanje i obnovu Fina QTSA 2015 certifikata;
- svi događaji vezani uz upravljanje životnim ciklusom privatnog TSU ključa Fina QTSA 2015;
- sve greške povezane s izvorom točnog vremena, uključujući i odstupanje izvan dopuštenih granica u odnosu na izvor točnog vremena.

Detaljniji opis postupanja s dnevnicima sustava Fina QTSA 2015 navedeni su u točki 5.4. CPS_{NQC} dokumenta [24] i internim dokumentima Fine.

Kopije dnevnika sustava izrađuju se na dnevnoj osnovi.

Informacije o događajima čuvaju se na Fina QTSA 2015 opremi dok ne budu prenesene u prikladnu arhivu. Gdjegod je to moguće, premještanje dnevnika sustava iz Fina QTSA 2015 opreme u arhivu izvodi se automatski, a u ostalim slučajevima premještanje obavlja ovlaštena osoba. Dnevnici sustava zadržavaju se kao arhivski zapisi u skladu s točkom 6.4.14. ovog TP dokumenta.

Zabilježeni događaji mogu se analizirati u cilju procjene mogućnosti povrede Fina QTSA 2015 sustava.

Fina QTSA nije obavezan slati obavijest osobi, poslovnom subjektu, uređaju ili aplikaciji koja je prouzročila događaj zabilježen na Fina QTSA 2015 opremi.

6.4.10. Postupci otklanjanja posljedica šteta i nezgoda

Fina QTSA na odgovarajući način reagira na incident, koordinirano, pravovremeno i u najkraćem mogućem vremenu na način definiran u točki 5.7. CPS_{NQC} [24] dokumenta. Sve dostupne informacije o incidentima bilježe se u dnevnicima sustava. Ovi događaji u najkraćem mogućem roku dojavljuju se odgovornim osobama, u prvom redu osobama odgovornim za rad Fina QTSA 2015.

U slučaju događaja koji bi ugrozili sigurnost i pouzdanje u uslugu izdavanja vremenskog žiga, Fina QTSA je obvezan na odgovarajući način o tome izvijestiti korisnike i pouzdajuće strane.

U slučaju detekcije gubitka ili kompromitiranja privatnog TSU ključa Fina QTSA 2015 servisa Fina QTSA će zaustaviti izdavanje vremenskog žiga, dok se u potpunosti ne provedu postupci obnove pouzdanja u sustav.

U slučaju kompromitiranja sustava kroz duži vremenski period, Fina QTSA će objaviti dodatne informacije kojima je moguće identificirati one vremenske žigove koji su bili kompromitirani.

6.4.11. Odstupanje izvora točnog vremena

U slučaju detekcije gubitka kalibracije, odnosno ispada iz sinkronizacije glavnog sata Fina QTSA 2015 izvan propisanog odstupanja Fina QTSA će zaustaviti izdavanje vremenskog žiga, dok se u potpunosti ne provedu postupci obnove pouzdanja u sustav.

6.4.12. Plan kontinuiteta poslovanja

Fina ima Plan kontinuiteta poslovanja Fina PKI koji uključuje i servis izdavanja vremenskih žigova čija je svrha uspostava sustava nadležnosti i odgovornosti te određivanje postupaka koji se izvršavaju u slučaju katastrofe. Cilj plana je osiguravanje kontinuiteta poslovanja u slučaju incidenta koji ozbiljnije ugrožava poslovni proces. Plan kontinuiteta poslovanja Fina PKI sadrži i plan oporavka od katastrofe.

6.4.13. Prestanak rada Fina QTSA

U slučaju prestanka obavljanja usluge izdavanja vremenskog žiga (ukidanje usluge), iz bilo kojeg razloga, Fina će učiniti sve što je u njenoj moći kako bi se minimalizirao utjecaj prestanka rada servisa na poslovni proces korisnika ili pouzdajuće strane.

U slučaju prestanka obavljanja usluge izdavanja vremenskog žiga Fina će na prikladan način obavijestiti sve korisnike, pouzdajuće strane i ministarstvo nadležno za gospodarstvo o mogućem planiranom prestanku davanja usluge najmanje tri mjeseca prije planiranog prestanka davanja usluga certificiranja.

U slučaju prestanka obavljanja usluga izdavanja vremenskog žiga Fina će osigurati kod drugog davatelja usluga izdavanja vremenskog žiga nastavak obavljanja usluga za korisnike s kojima je sklopljen ugovor o pružanju usluge izdavanja vremenskog žiga, ukoliko postoji davatelj takve

usluge iste kvalitete usluge kao Fina QTSA, te će mu dostaviti svu dokumentaciju u svezi s obavljanjem usluga izdavanja vremenskog žiga za Fina QTSA koji prestaje s radom.

Fina će osigurati ili prenijeti drugom pouzdanom poslovnom subjektu obvezu održavanja dostupnosti Fina QTSA certifikata s javnim ključem pouzdajućim stranama u razumnom vremenskom periodu.

Fina će osigurati nastavak održavanja svoje baze podataka, koja je nužna za utvrđivanje ispravnosti vremenskog žiga u svrhu pružanja dokaza u sudskim, upravnim i drugim postupcima, u skladu s važećim odredbama zakonske regulative, ili će s drugim poslovnim subjektom ugovoriti održavanja iste.

Ukoliko Fina ne osigura održavanje navedenih podataka tada će Fina svu dokumentaciju vezanu uz obavljanje usluga izdavanja vremenskog žiga dostaviti ministarstvu nadležnom za gospodarstvo.

Fina će osigurati sve potrebne korake, kojima će biti opozvani i objavljen opoziv svih certifikata Fina QTSA 2015.

6.4.14. Arhiviranje podataka

Fina QTSA arhivira sljedeće podatke, odnosno zapise koji, ovisno o tipu, mogu biti u elektroničkom i/ili papirnatom obliku:

- dnevnici sustava;
- podaci o fizičkim osobama i poslovnim subjektima iz postupaka registracije i ugovaranja korištenja usluge izdavanja vremenskog žiga;
- izdani vremenski žigovi;
- tehnički podaci nastali bilježenjem rada Fina QTSA 2015 *sustava*;
- zapisi koji se odnose na događaje povezane s životnim ciklusom TSU ključeva i pripadnih certifikata;
- zapisnici;
- drugi dokumenti Fina QTSA sukladno važećim propisima.

Svaki zapis koji se arhivira treba sadržavati podatak o vremenu koje se odnosi na taj zapis.

Detaljan opis arhiviranih podataka i dokumentacije nalazi se u točki 5.5. CPS_{NQC} [24] dokumenta.

U svrhu čuvanja zapisa izrađuju se i sigurnosne kopije koje se čuvaju na drugoj lokaciji, izdvojenoj od Fina QTSA 2015 sustava u upotrebi

Arhivirani podaci i dokumentacija zaštićuju se mehanizmima i postupcima propisane razine sigurnosti koje osiguravaju povjerljivost i cjelovitost arhive. Arhiva se štiti od neovlaštene izrade, modificiranja i brisanja podataka. Kopije zapisa, u odnosu na zapise na primarnoj produkcijskoj lokaciji Fina QTSA 2015 sustava, zaštićuju se jednakom ili višom razinom zaštite.

Arhivirani zapisi koji se odnose na izdavanje vremenskog žiga biti će dostupni i po isteku važenja privatnog TSU ključa.

6.4.15. Vremenski period arhiviranja

Svi arhivirani podaci i dokumentacija čuvaju se najmanje 10 godina.

6.4.16. Zaštita arhive

Arhivirani podaci i dokumentacija zaštićuju se mehanizmima i postupcima razine sigurnosti koja osigurava povjerljivost i cjelovitost arhive. Arhiva se štiti od neovlaštenog pregleda, modificiranja, oštećenja i brisanja.

Pregled arhiviranih podataka i dokumentacije u Fina QTSA obavlja Službenik za nadzor sustava.

Pristup arhiviranim podacima i dokumentaciji o registraciji korisnika u papirnatom obliku dopušten je Službeniku za nadzor sustava i osobama ovlaštenim osobama koji obavljaju poslove arhiviranja.

Arhivirani zapisi su na zahtjev raspoloživi samo ovlaštenim tijelima, posebice u svrhu pružanja dokaza o izdanom certifikatu i vremenskom žigu za potrebe sudskih postupaka.

6.4.17. Postupci izrade sigurnosnih kopija arhive

Sigurnosna kopija elektroničkog dijela arhive Fina QTSA 2015 sustava izrađuje se u Fina PKI štićenom prostoru na primarnoj produkcijskoj lokaciji te se na siguran način čuva u Fina PKI štićenom prostoru na udaljenoj pričuvnoj lokaciji iz točke 6.4.3.1. ovog TP dokumenta.

6.4.18. Zahtjevi na zaštitu zapisa vremenskim žigom

Nema odredbi.

6.4.19. Sustav prikupljanja arhiva (unutarnji ili vanjski)

Zapisi za arhiviranje prikupljaju se na način koji ovisi o vrsti zapisa i mjestu na kojem su prikupljeni.

Zapisi za arhiviranje vezani uz rad Fina QTSA 2015 sustava prikupljaju se i arhiviraju interno.

6.4.20. Postupci pristupa i verifikacije podataka iz arhiva

Pristup zapisima iz arhive imaju samo osobe ovlaštene za pristup tim podacima, a sukladno internim Fininim dokumentima. Verifikacija podataka iz arhive obavlja se provjerom njihove cjelovitosti.

6.5. OSTALE POSLOVNE I PRAVNE ODREDBE

6.5.1. Naknada za usluge

Fina QTSA, sukladno uvjetima iz sklopljenog ugovora o pružanju usluge izdavanja vremenskog žiga mora obavijestiti korisnike ili pouzdajuće strane o svim uslugama koje će se naplaćivati. Ukoliko posebnim ugovorom nije drugačije određeno, usluge se naplaćuju sukladno cjeniku Fina QTSA usluga.

Cjenik Fina QTSA usluga i njegove izmjene objavljuju se na internetskoj stranici http://www.fina.hr/finadigicert.

Fina zadržava pravo izmjene cjenika.

6.5.2. Financijska odgovornost

Fina kao davatelj usluga certificiranja raspolaže financijskim sredstvima koja osiguravaju nesmetano pružanje usluga certificiranja neovisno o broju korisnika usluga i za cijelo vrijeme obavljanja usluga certificiranja.

6.5.3. Ograničenje odgovornosti

Finina ukupna financijska odgovornost za vremenske žigove izdane prema ovom TP dokumentu i za transakcije obavljene na temelju pouzdavanja u tako izdane vremenske žigove iznosi najviše 100.000,00 kuna.

6.5.4. Povjerljivost poslovnih podataka

6.5.4.1. Opseg povjerljivih poslovnih podataka

Povjerljivi poslovni podaci su svi podaci, u bilo kojem obliku, koje na bilo koji način između sebe razmjene sudionici u svezi s uspostavom i pružanjem usluga certificiranja, a koje sudionici označe povjerljivim, ili određenom vrstom ili stupnjem tajnosti, ili koji su po prirodi povjerljivi jer bi njihovo neovlašteno otkrivanje moglo prouzročiti štetu sudioniku.

Tajne informacije su i datoteke s podacima, podaci u bilo kojem obliku, sistemska i aplikacijska dokumentacija, dokumentacija sustava, operativne procedure, planovi, interni akti, poslovni procesi, interni materijali za izobrazbu, zapisi internih revizija te osobni podaci i slično. Također, tajne informacije su programski kôd, aplikacijski i sistemski softver te ostali softver u Fina QTSA 2015 sustavu.

Sve informacije koje se odnose na način kojim Fina QTSA upravlja TSU ključevima i Fina QTSA 2015 sustavom za izdavanje vremenskih žigova smatraju se tajnim informacijama.

Povjerljivi su i svi podaci koji se odnose na način i na sredstva kojim Fina CA-ovi upravljaju certifikatima.

Pristup tajnim informacijama ograničava se na ovlaštene osobe, kojima su te informacije potrebne radi obavljanja dodijeljenih im dužnosti.

6.5.4.2. Podaci koji se ne smatraju povjerljivim poslovnim podacima

Poslovni podaci u bilo kojem obliku koje na bilo koji način između sebe razmjene sudionici u svezi s uspostavom i davanjem usluga certificiranja, a koje sudionici ne označe povjerljivim, ili određenom vrstom ili stupnjem tajnosti, ili koji po svojoj prirodi nisu povjerljivi, jer se njihovim neovlaštenim otkrivanjem ne bi mogla prouzročiti šteta sudioniku, su podaci koji se ne smatraju povjerljivim poslovnim podacima.

Poslovni podaci koji se ugrađuju u sadržaj certifikata, koji se prikazuju u javnim evidencijama i/ili registrima, koji se za potrebe davanja usluge certificiranja moraju propisano voditi, ne smatraju se povjerljivim poslovnim podacima.

6.5.4.3. Odgovornost za zaštitu povjerljivih poslovnih podataka

Svaki sudionik obvezan je štititi povjerljive poslovne podatke iz točke 6.5.4.1. ovog TP dokumenta, koje je saznao na bilo koji način, sukladno propisima koji uređuju zaštitu podataka prema vrsti podatka, odnosno vrsti i stupnju tajnosti podataka. U protivnom odgovara za nastalu štetu.

6.5.5. Povjerljivost osobnih podataka

6.5.5.1. Opseg povjerljivih poslovnih podataka

U postupku registracije korisnika i nakon toga, Fina je ovlaštena prikupljati osobne podatke koji su potrebni za valjano utvrđivanje identiteta korisnika te druge podatke potrebne za valjano davanje usluga certificiranja. Osobni podaci koje prikupi Fina i koji nisu sadržaj certifikata, koji se ne prikazuju u javnim evidencijama i/ili registrima koji se za potrebe davanja usluge certificiranja moraju propisano voditi, su povjerljivi osobni podaci koje Fina propisano štiti.

6.5.5.2. Osobni podaci koji nisu povjerljivi

Osobni podaci koje u postupku registracije korisnika i nakon toga prikupi Fina i koji su sadržaj certifikata, koji se prikazuju u javnim evidencijama i/ili registrima, koji se za potrebe davanja usluge certificiranja moraju propisano voditi, su osobni podaci koji zbog dostupnosti svima zainteresiranima nisu povjerljivi.

6.5.5.3. Odgovornost za zaštitu osobnih podataka

Fina je odgovorna su za zaštitu osobnih podatka, sukladno odredbama Zakona o zaštiti osobnih podataka [8] i drugih propisa, posebno onih kojima je uređena zaštita osobnih podataka u Republici Hrvatskoj.

6.5.5.4. Zaštita osobnih podataka

Fina primjenjuje odredbe Zakona o zaštiti osobnih podataka [8] i drugih propisa kojima je uređena zaštita osobnih podataka te tajnost podataka u Republici Hrvatskoj.

6.5.5.5. Plan zaštite osobnih podataka

Fina planira i provodi propisane tehničke, kadrovske i organizacijske mjere za zaštitu osobnih podataka od slučajne ili namjerne zlouporabe, uništenja, gubitka, neovlaštenih promjena ili dostupa.

6.5.5.6. Ovlaštenje za korištenje osobnih podataka

Fina je ovlaštena, osim za potrebe ispunjenja zakonskih obveza, odnosno ugovornih obveza po ugovoru o certificiranju, koristiti osobne podatke samo temeljem pisane privole korisnika koja se može dati u zahtjevu za izdavanje certifikata ili kasnije.

6.5.6. Dostupnost podataka mjerodavnim tijelima

Fina neće činiti dostupnima podatke iz točaka 6.5.4.1. i 6.5.5.1. ovog TP dokumenta osim u slučajevima propisanim zakonom ili kada to pisano zahtjeva mjerodavni sud, upravno ili neko drugo mjerodavno državno tijelo.

6.5.7. Ostale okolnosti objave podataka

Nema odredbi.

6.5.8. Zaštita intelektualnog vlasništva

Ovaj TP dokument je Finino vlasništvo, administriran je od strane Fina PMA te je podložan zaštiti autorskih prava prema zakonima u Republici Hrvatskoj. Nije dopušteno njegovo neovlašteno mijenjanje ili korištenje njegovih dijelova bez prethodne dozvole vlasnika.

Privatni TSU ključevi koji se koriste za potpisivanje vremenskih žigova smatraju se vlasništvom Fine.

Softver trećih strana koji se koristi u Fina QTSA 2015 sustavu koristi se u skladu s odredbama prava korištenja.

6.5.9. Postupak rješavanja sporova

U slučaju spora ili neslaganja među sudionicima povodom radnji i/ili postupaka glede pružanja usluge certificiranja uređene ovim TP dokumentom, isti će se nastojati razriješiti sporazumno. Ako sporazumno razrješenje spora nije moguće, isti će se razriješiti pred mjerodavnim sudom u Zagrebu uz primjenu hrvatskog prava.

Korisnik, odnosno pravna ili fizička osoba može Fini uputiti prigovor ako smatra da u njegovu slučaju postoji odstupanje sadržaja usluge u odnosu na ugovoreno. Fina će povodom prigovora odgovoriti podnositelju prigovora. Prigovor se upućuje pisano u papirnatom ili elektroničkom obliku na sljedeće kontakt podatke:

Kontaktni podaci za dostavu dopisa prema Fini	
Poštanska adresa:	Fina Centar elektroničkog poslovanja, (za Fina RDC) Ulica grada Vukovara 70 10000 Zagreb Hrvatska
E-mail:	info.rdc@fina.hr
Telefax:	+385-1-6304-081