FINA PKI

OPĆA PRAVILA DAVANJA USLUGA IZDAVANJA VREMENSKOG ŽIGA

Verzija 1.2

Datum objave: 31.10.2013.

Datum stupanja na snagu: 7.11.2013.

OID Dokumenta: 1.3.124.1104.2.1.1.1.2

Informacije o dokumentu

Ime dokumenta:	FINA PKI – Opća pravila davanja usluga izdavanja vremenskog žiga
OID dokumenta:	1.3.124.1104.2.1.1.1.2
Tip dokumenta:	Opća pravila davanja usluga izdavanja vremenskog žiga (*Time-stamp policy*, TP)
Oznaka distribucije	Javno
Vlasnik dokumenta	FINA
Kontakt	pma@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
1.1.	1.12.2010.	
1.2.	31.10.2013.	Usklađivanje s pravilnikom [5], Popisom normizacijskih dokumenata [6] te normizacijskim dokumentom HRS ETSI/TS 102 023 [12].

SADRŽAJ:

1. UVODNE OZNAKE I TEMELJNI PODACI 8
1.1. Opis usluga 8
1.2. Naziv dokumenta i identifikacijski podaci 9
1.3. Korisnici i područje primjene usluga 9
1.4. Adresni podaci 11
1.5. Definicije i kratice 11
1.5.1. Definicije 11
1.5.2. Kratice 14
2. OPĆE ODREDBE 15
2.1. Obveze davatelja usluga, korisnika i pouzdajuće strane 15
2.1.1. Obveze davatelja usluga 15
2.1.2. Obveze korisnika 15
2.1.3. Obveze pouzdajuće strane 16
2.2. Odgovornost 16
2.2.1. Odgovornosti davatelja usluga 16
2.2.2. Odgovornosti korisnika 16
2.2.3. Odgovornosti pouzdajuće strane 17
2.3. Financijska odgovornost 17
2.4. Ograničenje odgovornosti 17
2.4.1. Ograničenje odgovornosti 17
2.4.2. Odricanje od odgovornosti 17
2.5. Usklađenost sa zakonom 18
2.6. Naknada za usluge 18
2.7. Provjera usklađenosti 18
2.7.1. Predmeti provjera 19
2.7.2. Mjere u slučaju neusklađenosti 19
2.7.3. Priopćavanje rezultata 19
2.8. Povjerljivost i tajnost 19
2.9. Zaštita intelektualnog vlasništva 19
3. OSNOVNI ZAHTJEVI U RADU 20
3.1. Postupci provjere sigurnosnih mjera 20
3.2. Arhiviranje podataka 20
3.3. Postupci otklanjanja posljedica šteta i nezgoda 21
3.4. Prestanak rada TSA 21
4. KONTROLA SIGURNOSTI OPREME, POSTUPAKA I OSOBLJA 23
4.1. Kontrola prostora, opreme i sredstava 23
4.2. Kontrola postupaka i provedbe radnih zadaća 24
4.3. Kontrola osoblja – broj, stručnost i ovlaštenja 24
5. KONTROLA TEHNIČKE SIGURNOSTI RADA DAVATELJA USLUGA VREMENSKOG ŽIGA 25
5.1. Zaštita podataka za izradu vlastitog elektroničkog potpisa 25
5.1.1. Norme za kriptografske module 25
5.1.2. Kontrola privatnog TSU ključa od strane više osoba 25
5.1.3. Upis privatnog TSU ključa u kriptografski modul 25
5.1.4. Metoda aktiviranja privatnog TSU ključa 25
5.1.5. Metoda uništenja privatnog TSU ključa 25
5.2. Upravljanje podacima za izradu vlastitog elektroničkog potpisa 26

5.2.1. Generiranje TSA ključa ... 26
5.2.2. Sigurnosno kopiranje privatnog TSU ključa ... 26
5.2.3. Distribucija javnog TSU ključa ... 26
5.2.4. Generiranje novog TSU ključa ... 26
5.2.5. Kraj životnog vijeka TSU ključeva ... 27
5.3. Kontrola sigurnosti računalnog sustava ... 27
5.4. Kontrola sigurnosti radnog vijeka sustava ... 27
5.5. Kontrola sigurnosti mrežnog sustava ... 28
5.6. Kontrola sigurnosti kriptografskih modula ... 28
5.7. Izdavanje vremenskog žiga ... 28
5.7.1. Izjava o davanju usluga izdavanja vremenskog žiga ... 28
5.8. Usluga vremenskog žiga ... 29
5.8.1. Vremenski žig ... 29
5.8.2. Sinkronizacija sata s UTC ... 29
6. SADRŽAJ CERTIFIKATA ... 30
7. POSTUPCI S DOKUMENTACIJOM ... 32
7.1. Postupci kod promjene sadržaja dokumentacije ... 32
7.2. Objavljivanje dokumentacije ... 32
7.3. Postupci prihvaćanja/odobravanja dokumentacije ... 32

AUTORSKA PRAVA

REFERENCE

Temeljni zakon

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

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

Podzakonski akti

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

[4] 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)

[5] 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)

[6] 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)

Ostali zakoni

[7] Zakon o zaštiti osobnih podataka (NN 106/2012)

Direktive Europskog parlamenta

[8] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

Normizacijski dokumenti

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

[10] 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)

[11] 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)

[12] 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)

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

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

[15] HRN ISO/IEC 15408:2013 (dijelovi 1 do 3) Informacijska tehnologija – Sigurnosne tehnike – Kriteriji za vrednovanje sigurnosti IT – 1. dio: Uvod i opći model, – 2. Dio: Funkcionalni zahtjevi za sigurnost, – 3. Dio: Jamstveni zahtjevi za sigurnost (ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008)

[16] NIST FIPS PUB 140-1:1994 – Security Requirements for Cryptographic Modules

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

FININI dokumenti

[18] FINA PKI – Opća pravila davanja usluga certificiranja

[19] FINA PKI – 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.

Ovaj dokument FINA PKI – Opća pravila davanja usluga izdavanja vremenskog žiga (u daljnjem tekstu: TP) odgovara dokumentu „Opća pravila davanja usluga ugradnje vremenskog žiga“ definiranom u Pravilniku o evidenciji davatelja usluga certificiranja [3] te sadrži temeljna pravila i skup načela za davanje usluga izdavanja vremenskih žigova koja su usklađene sa zakonskom regulativom o elektroničkom potpisu u Republici Hrvatskoj. Opseg ovog TP dokumenta je davanje usluge izdavanja vremenskog žiga kroz „FINA Servis vremenske ovjere“ (u daljnjem tekstu: usluga izdavanja vremenskog žiga) koju obavlja FINA kao davatelj usluga izdavanja vremenskog žiga (*Time Stamping Authority*, TSA, u daljnjem tekstu: FINA TSA). Detaljni opis pravila i postupaka iz opsega ovog TP dokumenta nalazi se u dokumentu FINA PKI – Pravilnik o postupcima certificiranja za nekvalificirane certifikate [19] (u daljnjem tekstu: CPS_{NQC}). Sadržaj ovog TP dokumenta usklađen je s normizacijskim dokumentom HRS ETSI/TS 102 023 [12].

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

1.1. Opis usluga

FININA usluga izdavanja vremenskog žiga je usluga koja temeljem zahtjeva korisniku usluge izdaje vremenski žig.

Usluga izdavanja vremenskog žiga sastoji se od dva dijela:

- izdavanje vremenskog žiga;
- upravljanje izdavanjem vremenskog žiga.

Izdavanje vremenskog žiga obuhvaća aktivnosti vezane uz izradu vremenskog žiga, a upravljanje izdavanjem vremenskog žiga obuhvaća nadzor i upravljanje nad radom usluga na način propisan ovim TP dokumentom.

FINA TSA snosi punu odgovornost za davanje usluga izdavanja vremenskog žiga i odgovoran je za siguran i ispravan rad jedne ili više TSU jedinica koje izrađuju vremenski žig. FINA TSA ima obvezu izdavati vremenske žigove koje je naknadno moguće pravilno identificirati sukladno točki 1.2. ovog TP dokumenta.

Privatni ključevi koje koriste TSU jedinice za potpisivanje vremenskih žigova smatraju se vlasništvom FINA TSA.

FINA TSA 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. Svaku TSU jedinicu treba se moći pravilno identificirati.

Zaključno, FINA TSA je davatelj usluga izdavanja vremenskog žiga koji vremenske žigove izdaje sukladno Zakonu o elektroničkom potpisu [1], Zakonu o izmjenama i dopunama zakona o elektroničkom potpisu [2] i europskoj Direktivi o elektroničkim potpisima [8]**.**

1.2. 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 vremenskog žiga dodijelila OID: 1.3.124.1104.2.

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

- Naziv: FINA PKI – Opća pravila davanja usluge izdavanja vremenskog žiga
- Verzija: 1.2
- Datum objave: 31.10.2013.
- Datum stupanja na snagu: 7.11.2013.
- OID: 1.3.124.1104.2.1.1.1.2
- Web adresa stranice na kojoj je dokument objavljen: http://tsa.fina.hr

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

1.3. 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. Kako izdavatelj certifikata nije obavezan davati informaciju o vremenu opoziva već isteklog certifikata nastaje problem pouzdane verifikacije elektroničkog potpisa nakon isteka potpisnog certifikata. 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.

FININA usluga izdavanja vremenskog žiga 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.

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

FINA TSA pruža uslugu izdavanja vremenskog žiga samo registriranim korisnicima.

Korisnici usluge izdavanja vremenskog žiga mogu biti:

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

Registraciju korisnika provodi FINA RA mreža koju čini mreža lokalnih registracijskih ureda FINE.

FINA TSA može odrediti i drugi odgovarajući način registracije korisnika.

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.

Registrirani korisnici pristupaju usluzi izdavanja vremenskog žiga uz obveznu autentifikaciju autentifikacijskim certifikatom kojeg je izdao FINA RDC CA ili FINA RDC-TDU CA.

FINA TSA može odobriti i drugi odgovarajući način autentifikacije korisnika.

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.

1.4. Adresni podaci

Kontakt podaci za administraciju i sadržaj ovog TP dokumenta navedeni su u nastavku.

Poštanska adresa:

FINA
Sektor usluga za financijsku industriju i korporativne klijente
Odjel upravljanja politikom ePoslovanja
Koturaška cesta 43
10000 Zagreb
Hrvatska

Telefon: +385-1-6128-171

Telefax: +385-1-6304-081

E-mail: pma@fina.hr

1.5. Definicije i kratice

1.5.1. 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 je li 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.

POJAM	DEFINICIJA
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.
FINA RA mreža	Mreža registracijskih ureda u FINI, a sastoji se od središnjeg FINA RA i FINA LRA ureda.
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).
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.
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 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.
Lista opozvanih certifikata (CRL)	Potpisana lista koja ukazuje na skup certifikata koji se od strane izdavatelja certifikata više ne smatraju važećim.
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.

POJAM	DEFINICIJA
Pouzdajuća strana	Primatelj vremenskog žiga koji se pouzdaje u taj vremenski žig.
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.
Registracijski ured (RA)	Pravna ili fizička osoba koju ovlašćuje TSA, a koja je zadužena za registraciju korisnika.
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.
TSA sustav	Sustav IT komponenti koje osiguravaju izvedbu servisa 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*.
Vremenski žig	Elektronički potpisana potvrda izdavatelja koja potvrđuje sadržaj podataka na koje se odnosi u navedenom vremenu.

1.5.2. Kratice

KRATICA	PUNI NAZIV	ZNAČENJE
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
LRA	*Local Registration Authority*	Lokalni registracijski ured
OID	*Object Identifier*	Identifikator objekta
PMA	*Policy Management Authority*	Tijelo za upravljanje pravilima certificiranja
RA	*Registration Authority*	Registracijski ured
TP	*Time-Stamp Policy*	Opća pravila davanja usluge izdavanja vremenskog žiga
TSA	*Time-Stamping Authority*	Davatelj usluga izdavanja vremenskog žiga
TSU	*Time-Stamping Unit*	Jedinica za izradu vremenskog žiga
UTC	*Coordinated Universal Time*	Koordinirano svjetsko vrijeme

2. OPĆE ODREDBE

2.1. Obveze davatelja usluga, korisnika i pouzdajuće strane

2.1.1. Obveze davatelja usluga

FINA TSA obvezuje se na točnost podatka o vremenu ugrađenom u vremenski žig. Podatak o UTC vremenu koji se ugrađuje u svaki pojedini vremenski žig ima odstupanje manje od +/- 1 s.

FINA TSA također ima obvezu:

- provoditi davanje usluga izdavanja vremenskog žiga u skladu sa Zakonom o elektroničkom potpisu [1] i [2], podzakonskim propisima [3], [4], [5] i [6] donesenim temeljem Zakona [1] i [2], međunarodnim normama i preporukama, ovim TP dokumentom te drugim aktima FINA TSA za obavljanje usluga izdavanja vremenskog žiga;
- provoditi izdavanje vremenskog žiga na vjerodostojnom sustavu, a potpisivanje vremenskog žiga na opremi koja udovoljava zahtjevima iz točke 5.1.1. 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 vremenskog žiga sukladno najboljoj poslovnoj praksi;
- objaviti akte koji mogu biti javno dostupni na web stranicama http://tsa.fina.hr;
- 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 [7] 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 normama i razvoju tehnologije.

2.1.2. 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 FINA TSA o svakoj promjeni tih podataka.

Korisnik kojem se izdaje vremenski žig treba verificirati elektronički potpis FINA TSA na zaprimljenom vremenskom žigu i provjeriti valjanost FINA TSA certifikata. Opozvanost FINA TSA certifikata provjerava se putem CRL koju izdaje FINA RDC CA i koja se objavljuje na LDAP imeničkom poslužitelju kao i na web poslužitelju. Adrese na kojima se objavljuje CRL za provjeru opozvanost FINA TSA certifikata navedene su u CRL *Distribution Points* ekstenziji FINA TSA

certifikata sukladno profilu Certifikata za vremenski žig (NCP+) opisanom u točki 6. ovog TP dokumenta.

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 usluzi.

Korisnik je obvezan s pažnjom dobrog domaćina odnosno gospodarstvenika pravodobno na web stranicama http://tsa.fina.hr 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 TSA usluga iz točke 2.6. ovog TP dokumenta.

2.1.3. Obveze pouzdajuće strane

Prije pouzdanja u vremenski žig pouzdajuća strana mora:

- obaviti verifikaciju potpisa vremenskog žiga;
- provjeriti na važećoj listi opozvanih certifikata (CRL) opozvanost FINA TSA certifikata čijim je pripadnim privatnim ključem TSU potpisao vremenski žig.

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

Pouzdajuća strana obvezna je pridržavati se odredbi ovog TP dokumenta.

2.2. Odgovornost

2.2.1. Odgovornosti davatelja usluga

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 usklađivanja svih zahtjeva koji se odnose na davanje usluga izdavanja vremenskog žiga, što uključuje postupke koje se odnose na izdavanje vremenskog žiga, nadgledanje sustava i sigurnosne kontrole, s propisima danim u poglavlju 5. 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.

2.2.2. Odgovornosti korisnika

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

Korisnik je odgovoran osigurati potpunu interoperabilnost korisničke aplikacije, koju koristi za ugradnju vremenskog žiga, s FINA TSA 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 2.1.2. 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 koja su proizašla iz ugovora o pružanju usluga izdavanja vremenskog žiga.

2.2.3. Odgovornosti pouzdajuće strane

Pouzdajuća strana koja se, ne poštujući odredbe iz ovog TP dokumenta te protivno utvrđenim obvezama iz točke 2.1.3., 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.

2.3. Financijska odgovornost

FINA kao davatelj usluga izdavanja vremenskog žiga raspolaže financijskim sredstvima koja osiguravaju nesmetano pružanje usluga neovisno o broju korisnika usluga i za cijelo vrijeme obavljanja usluga izdavanja vremenskog žiga.

2.4. Ograničenje odgovornosti

2.4.1. Ograničenje odgovornosti

FININA maksimalna financijska odgovornost prema korisniku i pouzdajućoj strani, koja se razumno pouzdaje u vremenski žig, iznosi najviše 20.000,00 kuna po transakciji.

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.

2.4.2. Odricanje od odgovornosti

Osim onog što je za FINA TSA izričito navedeno u točkama 2.1.1. i 2.2.1. ovog TP dokumenta i točki 9.6. Općih pravila davanja usluga certificiranja [18], FINA TSA ne odgovora ni za koje drugo jamstvo ili odgovornost, a posebno ne u slučaju ako bi do odgovornosti FINA TSA prema danim jamstvima došlo zbog povrede jamstava i odgovornosti drugih sudionika navedenih u točkama 2.1. i 2.2. ovog TP dokumenta.

FINA TSA nije odgovorna za štete, uključujući indirektne i specijalne štete, štete za slučaj nezgode, štete 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:

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

2.5. Usklađenost sa zakonom

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

Ovaj TP dokument i davanje usluga izdavanja vremenskog žiga obuhvaćenih ovim TP dokumentom usklađeni su s propisima navedenim u ovoj točki.

2.6. Naknada za usluge

FINA TSA, 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 TSA usluga.

Cjenik FINA TSA usluga i njegove izmjene objavljuju se na web stranici http://tsa.fina.hr.

FINA zadržava pravo izmjene cjenika.

2.7. Provjera usklađenosti

Inspekcijski nadzor nad radom FINA TSA reguliran je Zakonom o elektroničkom potpisu [1] i [2], a provodi ga ministarstvo nadležno za gospodarstvo te Državni inspektorat prema odredbama posebnog zakona.

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 TSA i provedbu unutarnjeg procesa odobravanja rada FINA TSA 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 [12].

2.7.1. Predmeti provjera

Pri provjeri usklađenosti ocjenitelji provjeravaju postupa li FINA TSA prema ovom TP dokumentu, internom CPS_{NQC} [19] dokumentu te ostaloj mjerodavnoj internoj dokumentaciji.

2.7.2. Mjere u slučaju neusklađenosti

U slučaju neusklađenosti u radu FINA TSA, 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 TSA ne provede akcije za otklanjanje neusklađenosti, FINA PMA može donijeti odluke o akcijama koje će biti primjerene težini neusklađenosti.

FINA TSA mora voditi interni dnevnik vremenskih razdoblja u kojima nije radio u skladu s ovim TP dokumentom s navedenim razlozima neusklađenosti.

2.7.3. Priopćavanje rezultata

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

Rezultate vanjske provjere usklađenosti FINA može javno objaviti na web stranicama http://tsa.fina.hr.

2.8. Povjerljivost i tajnost

FINA TSA privatni potpisni ključevi kojima TSU-ovi potpisuju vremenske žigove su osjetljive i tajne informacije te se oni stoga moraju držati u najstrožoj tajnosti. Ne smiju postojati mogućnosti u kojima bi se privatni TSU ključevi mogli pojaviti nezaštićeni izvan kriptografskog modula.

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 TSA sustavu.

Pristup tajnim informacijama ograničava se na ovlaštene osobe kojima su te informacije potrebne za obavljanje dodijeljenih im dužnosti. Sve informacije koje se odnose na način kojim FINA TSA upravlja ključevima TSU jedinica i sustavom smatraju se tajnim informacijama.

2.9. Zaštita intelektualnog vlasništva

3. OSNOVNI ZAHTJEVI U RADU

3.1. Postupci provjere sigurnosnih mjera

FINA TSA u svojim dnevnicima sustava bilježi sve važne događaje povezane s radom FINA TSA sustava. Informacije o događajima koji se bilježe automatski se prikupljaju. Tipovi događaja koji se bilježe u dnevnicima sustava FINA TSA navedeni su u točki 5.4.1. CPS_{NQC} dokumenta [19]. Kopije dnevnika sustava izrađuju se na dnevnoj osnovi.

Informacije o događajima čuvaju se na FINA TSA opremi dok ne budu prenesene u prikladnu arhivu. Gdjegod je to moguće, premještanje dnevnika sustava iz FINA TSA 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 3.2. ovog TP dokumenta.

FINA TSA nije obavezan slati obavijest osobi, poslovnom subjektu, uređaju ili aplikaciji koja je prouzročila događaj zabilježen na FINA TSA opremi.

Zabilježeni događaji mogu se analizirati u cilju procjene mogućnosti povrede FINA TSA sustava.

3.2. Arhiviranje podataka

FINA TSA 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 TSA sustava;
- zapisi koji se odnose na događaje povezane s životnim ciklusom TSU ključeva i pripadnih certifikata;
- zapisnici;
- drugi dokumenti FINA TSA sukladno važećim propisima.

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

Detaljan opis arhiviranih podataka i dokumentacije nalazi se u točki 5.5.1. CPS_{NQC} [19] dokumenta.

U svrhu čuvanja zapisa izrađuju se i sigurnosne kopije koje se čuvaju na drugoj lokaciji, izdvojenoj od FINA TSA sustava u upotrebi.

Svi arhivirani podaci i dokumentacija čuvaju se najmanje 10 godina.

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 TSA sustava, zaštićuju se jednakom ili višom razinom zaštite.

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

Od trenutka isteka javni TSU ključevi arhiviraju se na period od najmanje 10 godina radi omogućavanja provjere vremenskih žigova izdanih za vrijeme važenja TSU ključeva. Arhiviranje javnog TSU ključa opisano je poglavlju 6.3.1. CPS_{NQC} [19] dokumenta.

3.3. Postupci otklanjanja posljedica šteta i nezgoda

FINA TSA na odgovarajući način reagira na incident, koordinirano, pravovremeno i u najkraćem mogućem vremenu na način definiran u točki 5.7. CPS_{NQC} [19] dokumenta. Sve dostupne informacije o incidentima bilježe se u dnevnicima sustava. Ovi događaji u najkraćem mogućem roku dojavljuju se odgovornim osobama, u prvom redu voditelju zaduženom za rad FINA TSA.

U slučaju događaja koji bi ugrozili sigurnost i pouzdanje u uslugu izdavanja vremenskog žiga, uključujući i gubitak povjerenja u FINA TSA privatni TSU ključ ili ispad iz sinkronizacije sata izvan propisanog odstupanja, FINA TSA je obvezan na odgovarajući način o tome izvijestiti korisnike i pouzdajuće strane.

U slučaju ugroze ili sumnje na ugrozu usluge izdavanja vremenskog žiga ili ispada iz sinkronizacije TSU sata, FINA TSA će svim korisnicima i pouzdajućim stranama dati kratki opis i objašnjenje događaja.

U slučaju detekcije gubitka privatnog ključa ili kalibracije, FINA TSA 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 TSA će objaviti dodatne informacije s kojima je moguće identificirati one vremenske žigove koji su bili kompromitirani.

3.4. Prestanak rada TSA

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 TSA, te će mu dostaviti svu dokumentaciju u svezi s obavljanjem usluga izdavanja vremenskog žiga za FINA TSA koji prestaje s radom.

FINA će osigurati ili prenijeti drugom pouzdanom poslovnom subjektu obvezu održavanja dostupnosti FINA TSA 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 TSA će osigurati sve potrebne korake, kojima će biti opozvani i objavljen opoziv svih TSU certifikata FINA TSA.

4. KONTROLA SIGURNOSTI OPREME, POSTUPAKA I OSOBLJA

4.1. Kontrola prostora, opreme i sredstava

FINA TSA 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 povjerljivim ulogama kako je opisano u točkama 4.2 i 4.3. ovog TP dokumenta. Pristup se kontrolira sustavom za kontrolu pristupa. Stalnu kontrolu pristupa provodi zaduženo osoblje ili se ona provodi elektronički.

FINA TSA osigurava punu fizičku kontrolu pristupa kritičnim servisima TSA u cilju onemogućavanja neautoriziranog fizičkog pristupa.

Za izvođenje i upravljanje servisima izdavanja vremenskog žiga:

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

Kontrola pristupa kriptografskim modulima zadovoljava zahtjeve za sigurnost kriptografskih modula kako je to definirano u točkama 5.2. i 5.6.

Svaki vremenski žig kojeg izdaje FINA TSA sadrži TP OID – jedinstveni identifikator ovog TP dokumenta. Vremenski žig kojeg izdaje FINA TSA 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 TSA automatski sinkronizira.

U slučaju nedostupnosti satelitskog signala iz bilo kojeg razloga, FINA TSA 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.

Vremenski žig je potpisan ključem čiji pripadajući certifikat ima sadržaj opisan u poglavlju 6.

Upravljanje FINA TSA 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 TSA. Fizičke i sigurnosne kontrole štite resurse FINA TSA.

4.2. Kontrola postupaka i provedbe radnih zadaća

Za rad na FINA TSA zapošljavaju se osobe koje imaju adekvatna stručna zvanja, iskustvo i kvalifikaciju, uz poželjnu stručnu certifikaciju.

Povjerljive uloge, ovlaštenja i odgovornosti navedene su u točki 5.2.1. CPS_{NQC} [19] dokumenta i u opisu poslova onih djelatnika kojima su dodijeljene povjerljive uloge. Prilikom dodjeljivanja uloga i zadaća, ostvareno je i propisano razdvajanje uloga. Sukladno njihovoj osjetljivosti, uloge se dodjeljuju djelatnicima koji su dokazali svoju stručnosti i koji poznaju dodijeljeno područje rada. Prije nego što započnu obnašati povjerljive uloge u FINA TSA, djelatnici FINA TSA moraju savladati znanja i vještine za provedbu administrativnih i upravljačkih funkcija.

Djelatnici koji obnašaju povjerljive uloge u FINA TSA trebaju poznavati tehnologije vremenske ovjere, tehnologiju elektroničkog potpisivanja, mehanizme kalibracije i sinkroniziranja FINA TSA satova s UTC, sigurnosne postupke kod obnašanja povjerljivih uloga te trebaju imati iskustvo u provedbi mjera sigurnosti u informatičkim sustavima.

Djelatnici kojima su povjerene povjerljive uloge ne smiju biti izloženi sukobu interesa, jer bi to moglo utjecati na odluke u FINA TSA.

Djelatnicima koji su počinili teži prekršaj ili težu povredu radnih obaveza, ne mogu biti dodijeljene povjerljive uloge u FINA TSA sustavu.

4.3. Kontrola osoblja – broj, stručnost i ovlaštenja

Pristup i poslovi u štićenom FINA TSA sustavu provode se isključivo uz istovremeno prisustvo najmanje dvije ovlaštene osobe koje imaju dozvole pristupa tom sustavu.

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

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

U slučaju izvođenja neovlaštene ili zlonamjerne radnje koju je izvela ovlaštena osoba u FINA TSA primjenjuju se odredbe važeće zakonske regulative i internih pravilnika FINE. Takvoj osobi bit će zabranjen daljnji rad na poslovima FINA TSA.

Detaljniji opis odabira, provjere, identifikacije i potvrđivanja identiteta ovlaštenih zaposlenika te način njihova uključenja na pristupne liste pojedinih FINA TSA resursa nalazi se u točkama 5.2. i 5.3. CPS_{NQC} [19] dokumenta.

5. KONTROLA TEHNIČKE SIGURNOSTI RADA DAVATELJA USLUGA VREMENSKOG ŽIGA

5.1. Zaštita podataka za izradu vlastitog elektroničkog potpisa

5.1.1. Norme za kriptografske module

Kriptografski modul kojim TSU obavljaju potpisivanje vremenskog žiga mora:

- zadovoljavati zahtjeve prema FIPS 140-1 [16] ili FIPS 140-2 [17], razina 3 ili viša ili
- zadovoljavati zahtjeve prema CWA 14167-2 [14] ili
- predstavljati vjerodostojan sustav osiguran razinom EAL 4 ili višom u skladu s ISO 15408 normom [15] ili primjenom jednako vrijednih sigurnosnih kriterija.

5.1.2. Kontrola privatnog TSU ključa od strane više osoba

Kontrola od strane više osoba sigurnosni je mehanizam koji zahtijeva višestruke autorizacije za pristup privatnom ključu za potpis vremenskog žiga. Taj mehanizam sprečava samostalan pristup jedne osobe FINA TSA privatnom potpisnom ključu.

Privatni TSU ključ FINA TSA za potpis vremenskog žiga pohranjuje se u kriptografskom modulu pod kontrolom najmanje dvije osobe. Osobe koje sudjeluju u toj kontroli moraju biti ovlaštene za ovu operaciju.

5.1.3. Upis privatnog TSU ključa u kriptografski modul

Privatni TSU ključevi FINA TSA moraju biti generirani u kriptografskom modulu. Ako privatni ključ treba prenijeti iz jednoga kriptografskog modula u drugi, privatni ključ mora biti enkriptiran tijekom prijenosa i ne smije se ni u jednom trenutku pojaviti nezaštićen dok je izvan kriptografskog modula.

5.1.4. Metoda aktiviranja privatnog TSU ključa

Prije aktiviranja privatnog TSU ključa ovlaštene osobe moraju se autentificirati na kriptografski modul. Privatni TSU ključ mora se čuvati u zaštićenom obliku kada je deaktiviran.

5.1.5. Metoda uništenja privatnog TSU ključa

Privatni TSU ključ FINA TSA mora se uništiti nakon prestanka potrebe za njegovim korištenjem, odnosno na kraju njegovog životnog ciklusa. Uništenje privatnog TSU ključa mora se obaviti na način koji osigurava nemogućnost oporavka privatnog ključa nakon njegovog uništenja. Privatni TSU ključ uništava se mehanizmima definiranim u zahtjevima koje moraju ispunjavati kriptografski moduli iz mjerodavne norme iz točke 5.1.1. ovog TP dokumenta. Taj postupak izvodi se od strane ovlaštenog osoblja pod njihovom minimalno dualnom kontrolom. Postupak se dokumentira i arhivira.

Postupak za uništenje FINA TSA ključeva opisan je u poglavlju 6.2.10. CPS_{NQC} [19] dokumenta.

5.2. Upravljanje podacima za izradu vlastitog elektroničkog potpisa

5.2.1. Generiranje TSA ključa

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

TSU par ključeva FINA TSA sustava izrađuje se i pohranjuje u kriptografskom modulu. Postupak generiranja ovih ključeva provodi stručno ovlašteno osoblje s povjerljivim ulogama uz minimalno dualnu kontrolu. Opis zahtjeva za izbor osoblja opisan je u poglavlju 5.3. CPS_{NQC} [19] dokumenta.

U postupku izrade kriptografskih ključeva za FINA TSA osigurana je njihova kontrola, posebno:

- generiranje TSU ključeva za potpisivanje vremenskih žigova FINA TSA izvode ovlaštene osobe s povjerljivim ulogama u FINA TSA sustavu, a postupak se izvodi u štićenom okruženju;
- generiranje TSU ključeva za potpisivanje FINA TSA vremenskih žigova obavlja se unutar zaštićenog kriptografskog modula koji zadovoljava zahtjeve navedene u točki 5.1.1 ovog TP dokumenta;
- duljina TSU ključeva FINA TSA i algoritmi za potpisivanje vremenskog žiga su:
    - RSA kriptografski algoritam s dužinom ključa od 2048 bita;
    - *hash* algoritam SHA-1.

Privatni TSU ključ za FINA TSA čuva se u zaštićenom kriptografskom modulu koji zadovoljava zahtjeve navedene u točki 5.1.1 ovog TP dokumenta.

Generiranje para TSU ključeva detaljnije je opisano u točki 6.1.1. CPS_{NQC} [19] dokumenta.

5.2.2. Sigurnosno kopiranje privatnog TSU ključa

Sigurnosno kopiranje privatnog TSU ključa izvodi se pod dualnom kontrolom i samo od strane ovlaštenog osoblja FINA TSA. Privatni TSU ključ kopira se i dohvaća iz kriptografskog modula isključivo u enkriptiranom obliku. Sigurnosne kopije privatnog TSU ključa čuvaju se u najmanje dva primjerka na odvojenim i adekvatno štićenim lokacijama.

Sigurnosno kopiranje privatnog TSU ključa detaljnije je opisano u točki 6.2.4. CPS_{NQC} [19] dokumenta.

5.2.3. Distribucija javnog TSU ključa

Javni TSU ključ FINA TSA služi za provjeru potpisa vremenskog žiga, a nalazi se u certifikatu „SERVIS VREMENSKE OVJERE TSA1“ koji je objavljen na LDAP imeničkom poslužitelju rdc-ldap.fina.hr te na web stranicama http://tsa.fina.hr. FINA TSA certifikat izdaje FINA RDC CA sukladno Općim pravilima davanja usluga certificiranja [18] i CPS_{NQC} [19] dokumentu.

5.2.4. Generiranje novog TSU ključa

Generiranje novog TSU ključa i njegova uspostava za FINA TSA provodi se pravovremeno prije isteka perioda valjanosti FINA TSA certifikata. Generiranje se provodi na način koji je opisan u točki 5.2.1. ovog TP dokumenta.

5.2.5. Kraj životnog vijeka TSU ključeva

Privatni TSU ključ FINA TSA ne smije se koristiti po isteku perioda važenja FINA TSA certifikata „SERVIS VREMENSKE OVJERE TSA1“. FINA TSA ne smije biti u mogućnosti izdavati vremenske žigove nakon isteka važenja FINA TSA certifikata.

FINA TSA provodi operativne postupke prema kojima se osigurava pravovremeno generiranje novih TSU ključeva prije isteka valjanosti postojećih ključeva. Po isteku valjanosti, privatni TSU ključevi i njihove kopije sigurno se uništavaju sukladno točki 5.1.5. ovog TP dokumenta, tako da ne postoji niti jedna njihova kopija te iste nije moguće ponovo koristiti.

5.3. Kontrola sigurnosti računalnog sustava

FINA TSA osigurava sigurno i ispravno davanje usluge izdavanja vremenskog žiga. Integritet komponenti i podataka u sustavu FINA TSA adekvatno je zaštićen od napada virusa, neprijateljskog koda i djelovanja neautoriziranih programskih sustava. Mediji za pohranu podataka FINA TSA 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 TSA sustav zadovoljava niže navedene uvjete zaštite:

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

5.4. Kontrola sigurnosti radnog vijeka sustava

FINA TSA sustav koristi autentične i vjerodostojne sustave i proizvode. Prije uspostave FINA TSA sustava, oprema (hardver i softver) treba biti zaštićeno pakirana i isporučena povjerljivom metodom. Oprema ne smije sadržavati nikakve druge aplikacije koje nisu dio FINA TSA 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 TSA softver mora biti isporučen u originalnom pakiranju i mora imati metodu verifikacije kojom se utvrđuje da:

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

FINA TSA mora osigurati mehanizam za periodičnu provjeru integriteta softvera.

5.5. Kontrola sigurnosti mrežnog sustava

Sve lokalne mrežne komponente moraju biti smještene na fizički zaštićenim mjestima.

Mrežni promet mora biti filtriran i nadziran. Treba osigurati da je FINA TSA oprema zaštićena od svih poznatih oblika napada koji dolaze putem računalne mreže. Svi mrežni portovi i servisi koji se ne upotrebljavaju trebaju biti isključeni. Na FINA TSA opremi treba biti instaliran i pokrenut samo mrežni softver koji je potreban za obavljanje davanja usluge certificiranja.

5.6. Kontrola sigurnosti kriptografskih modula

FINA TSA mora osigurati da kriptografski moduli nisu mijenjani tijekom transporta ili tijekom skladištenja.

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

FINA TSA mora kontinuirano provjeravati i osigurati ispravnost rada kriptografskog modula.

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

Postupak za rukovanje kriptografskim modulima opisan je u točki 6.2. CPS_{NQC} [19] dokumenta.

5.7. Izdavanje vremenskog žiga

FINA TSA 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.

Postupci vezani uz izdavanje vremenskog žiga opisani su u CPS_{NQC} [19] dokumentu.

FINA TSA obavještava sve korisnike i pouzdajuće strane o uvjetima korištenja usluga izdavanja vremenskog žiga kroz dokument Uvjeti pružanja usluga vremenske ovjere.

Sadržaj i odobravanje CPS_{NQC} [19] dokumenta provodi FINA PMA kao nadzorno tijelo.

U slučaju promjena ovog dokumenta i CPS_{NQC} [19] dokumenta, FINA PMA će nakon odobrenja objaviti na web stranicama http://tsa.fina.hr nove verzije dokumenata i vrijeme od kada isti počinju važiti.

5.7.1. Izjava o davanju usluga izdavanja vremenskog žiga

FINA TSA objavljuje izjavu o davanju usluga izdavanja vremenskog žiga na web stranicama http://tsa.fina.hr.

Ova izjava sadrži:

- kontakt podatke za FINA TSA;
- 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 TSA, 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 TSA sustava;
- primijenjena regulativa i izjava o zadovoljenju zakonskih zahtjeva;
- ograničenja odgovornosti;
- procedure u slučaju spora;
- informacije o provjeri FINA TSA od nezavisnog tijela o zadovoljenju zahtjeva propisanih ovim dokumentom, ukoliko je provjera obavljena.

5.8. Usluga vremenskog žiga

5.8.1. Vremenski žig

FINA TSA osigurava izdavanje vremenskih žigova na siguran način i s točnom oznakom vremena. Svaki vremenski žig:

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

Vremenski žig mora biti izdan sukladno preporuci ITF RFC 3161 [9] s profilom usklađenim s normizacijskim dokumentom HRS ETSI/TS 101 861 [10].

Profil vremenskog žiga detaljno je definiran u poglavlju 7.1. CPS_{NQC} [19] dokumenta.

5.8.2. Sinkronizacija sata s UTC

FINA TSA mora osigurati sinkroniziranost FINA TSA vremena s UTC vremenom unutar preciznosti propisane ovim dokumentom u točki 2.1.1., a posebno:

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

6. SADRŽAJ CERTIFIKATA

U tablici 6.1. opisan je profil Certifikat za vremenski žig (NCP+) koji se koristi u izdavanju certifikata za potpis vremenskog žiga:

Polje	Atribut	Opis/Vrijednost
Osnovna polja		
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	32-bitni neponovljivi cijeli broj: 3f 1c 8a 93
signatureAlgorithm	AlgorithmIdentifier	sha1RSA (sha1 sa RSA enkripcijom) OID: 1.2.840.113549.1.1.5
signatureValue		Vrijednost potpisa izdavatelja certifikata
Issuer	organizationalUnit	RDC
	organizationName	FINA
	countryName	HR
Validity	notBefore	Vrijeme izdavanja certifikata: 08. lipnja 2006. 11:33:09
	notAfter	Vrijeme izdavanja certifikata + 120 mjeseci (valjanost 10 godina): 08. lipnja 2016. 12:03:09
Subject	commonName	Naziv usluge izdavanja vremenskog žiga: SERVIS VREMENSKE OVJERE TSA1
	organizationName	Skraćeni naziv poslovnog subjekta i matični broj: FINA 00332852
	countryName	HR
SubjectPublicKeyInfo	AlgorithmIdentifier	RSA (2048 bit)
	subjectPublicKey	Javni ključ TSA1

Polje	Atribut		Opis/Vrijednost
Ekstenzije	**CE**	**Atribut**	**Vrijednost**
SubjectAltName	NE	URIName	Opcionalno. Sadrži URL adresu TSA: URL=http://tsa.fina.hr
PrivateKeyUsagePeriod	NE	notBefore	Vrijeme izdavanja certifikata
		notAfter	Vrijeme izdavanja certifikata + 120 mjeseci (valjanost 10 godina)
CertificatePolicies	NE	policyIdentifier	Visoka razina sigurnosti OID: 1.3.124.1104.5.11.52.4.3
		policyQualifiers	CPS: http://rdc.fina.hr/cp/

Polje	Atribut		Opis/Vrijednost
Ekstenzije	**CE**	**Atribut**	**Vrijednost**
CRLDistributionPoints	NE	DistributionPoint	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL20 OU=RDC O=FINA C=HR [2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://rdc-ldap.fina.hr/ou=RDC,o=FINA,c=HR?certificateRevocationList%3Bbinary URL=http://rdc.fina.hr/crls/rdc.crl
AuthorityKeyIdentifier	NE	keyIdentifier	60-bitna SHA-1 *hash* vrijednost ključa s vodećim 0100 bitovima (po RFC 5280): KeyID=47 45 00 6e f0 57 a6 c0
SubjectKeyIdentifier	NE	keyIdentifier	60-bitna SHA-1 *hash* vrijednost ključa s vodećim 0100 bitovima (po RFC 5280): 49 b9 41 ee f4 c4 63 e8
BasicConstraints	NE	cA	CA: FALSE: Subject Type=End Entity Path Length Constraint=None
keyUsage	DA	digitalSignature	Digital Signature, Non-Repudiation (c0)
		nonRepudiation	
extKeyUsage	DA	timeStamping	OID: 1.3.6.1.5.5.7.3.8

Tablica 6.1. Profil Certifikata za vremenski žig (NCP+)

7. POSTUPCI S DOKUMENTACIJOM

7.1. 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 1.4 ovog TP dokumenta. Odluke o prihvaćanju primjedbi su diskreciono pravo FINE.

7.2. Objavljivanje dokumentacije

Ovaj dokument javno je objavljen na web stranici http://tsa.fina.hr.

7.3. Postupci prihvaćanja/odobravanja dokumentacije

Promjene u FINA TSA dokumentaciji prihvaća i odobrava FINA PMA.