FINA

PRAVILNIK O POSTUPCIMA PRUŽANJA USLUGA IZDAVANJA KVALIFICIRANIH ELEKTRONIČKIH VREMENSKIH ŽIGOVA

Verzija 1.5

Datum stupanja na snagu: 10.05.2021.

OID Dokumenta: 1.3.124.1104.2.3.2.1.5

Informacije o dokumentu

Ime dokumenta:	Pravilnik o postupcima pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova
OID dokumenta:	1.3.124.1104.2.3.2.1.5
Tip dokumenta:	Pravilnik o postupcima pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova (*TSA practice statement*, TPS)
Oznaka distribucije	Javno
Vlasnik dokumenta	Financijska agencija, Fina
Kontakt	pma@fina.hr

Povijest izmjena

Verzija	Datum	Razlog izmjene
1.0	22.05.2017.	Inicijalna verzija
1.1	02.05.2018.	Ažuriranje referente liste zakonske regulative, proširenje prava pristupa usluzi izdavanja elektroničkih kvalificiranih vremenskih žigova i na certifikate drugih pružatelja usluga povjerenja, ispravljanje prepoznatih grešaka.
1.2	11.09.2018	Ažuriranje referente liste zakonske regulative, dodavanje izjave o usklađenosti strukture dokumenta s RFC 3647, dodavanje opisa CA certifikata, pojašnjenje o zaustavljanju Fina QTSA 2017 servisa nakon 1 sekunde netočnosti, dodavanje pravila o iznošenju TSA opreme iz štićenog prostora, dodavanje izjave o postupcima vezanim za upravljanje kritičnim ranjivostima i dodavanje izjave o dostupnosti usluga osobama s invaliditetom.
1.3	26.02.2019	Promjene u odgovoru servisa izdavanja kvalificiranih elektroničkih vremenskih žigova, dodavanje odredbe o arhiviranju ugovora o pružanju usluge izdavanja kvalificiranih elektroničkih vremenskih žigova i ispravljanje prepoznatih grešaka.
1.4	17.04.2020.	Dodane reference na Pravilnik o pružanju i korištenju usluga povjerenja i Uredbu (EU) 2016/679, u točki 3.1.2. dodane odredbe za elektroničko potpisivanje pristupnice, u točki 3.8. ispravljen i poboljšan opis zahtjeva za provjeru valjanosti elektroničkog vremenskog žiga, u točki 4.2.1. dopunjen opis razloga za opoziv Fina QTSA 2017 certifikata, u točki 4.2.4. skraćeno vrijeme maksimalnog kašnjenja za CRL, u točki 5.2.4. poboljšan opis zahtjeva za odvajanje dužnosti, u točki 6.6.2 poboljšan opis zahtjeva za transport HSM-ova, u poglavlju 8. dodan podatak o tijelu za provedbu nadzora iz područja zaštite osobnih podataka, u točki 8.1.1. poboljšan opis vanjske provjere sukladnosti, u točki 8.6. poboljšan i proširen opis dostave izvješća o ocjenjivanju sukladnosti te objave rezultata vanjskoj provjeri sukladnosti, u točki 9.4. ispravljene i dopunjene odredbe vezane uz zaštitu osobnih podataka, u točki 9.6.4. ispravke u tekstu obaveza Pouzdajućih strana, u točki 9.8. ispravke u tekstu odricanje od odgovornosti, u točki 9.10. ispravke u tekstu vezanog uz naknadu šteta, u točkama 9.11.2. i 9.11.3. dopuna odredbi vezanih uz prestanak i posljedice prestanka važenja ovog QTPS dokumenta te ispravljanje prepoznatih grešaka.

1.5	05.05.2021.	U točki 4.2.2. dodana mogućnost određivanja roka za opoziv TSU certifikata, u točki 5.2.3. dodana odgovornost Službenika za sigurnost i odredba o bilježenju aktivnosti prijavljene osobe, u točki 9.15. dodana je referenca na Pravilnik o pružanju i korištenju usluga povjerenja, u točkama 5.1., 5.1.7., 5.3.3., 5.5.3., 5.5.6., 6.1.1., 6.1.4, 6.2.2. i 9.4.3. poboljšan je i dopunjen tekst te ispravljanje prepoznatih grešaka u dokumentu.

SADRŽAJ:

AUTORSKA PRAVA

REFERENTNE DOKUMENTIRANE INFORMACIJE

Temeljni zakon

[1] Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ

[2] Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (NN 62/2017)

Podzakonski akti

[3] Pravilnik o pružanju i korištenju usluga povjerenja (NN 60/2019)

Ostala zakonska regulativa

[4] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)

[5] Zakon o provedbi Opće uredbe o zaštiti podataka (NN42/2018)

Normizacijski dokumenti

[6] ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[7] ETSI EN 319 421 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[8] ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

[9] ETSI EN 319 411-1 V1.2.2. (2018-04) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[10] ETSI EN 319 411-2 V2.2.2. (2018-04) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[11] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

[12] ETSI TS 119 312 V.1.3.1 (2019-02) – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

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

[14] IETF RFC 3739 - Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

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

[16] IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (2013)

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

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

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

[20] IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework

Finini dokumenti

[21] Opća pravila pružanja usluga certificiranja i Pravilnik o postupcima certificiranja za Fina Root CA, CP/CPS_{ROOT}

[22] Opća pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova, QTP

[23] Pravilnik o postupcima certificiranja za kvalificirane certifikate za elektroničke potpise i pečate, $CPS_{QC\text{-}eIDAS}$

[24] Pravilnik o postupcima certificiranja za nekvalificirane certifikate, $CPS_{NQC\text{-}eIDAS}$

1. UVODNE OZNAKE I TEMELJNI PODACI

Fina je kao kvalificirani pružatelj usluga povjerenja upisana u Pouzdani popis pružatelja usluga povjerenja u Republici Hrvatskoj kojeg vodi središnje tijelo državne uprave nadležno za poslove gospodarstva.

Finin servis izdavanja kvalificiranih elektroničkih vremenskih žigova je kao kvalificirana usluga povjerenja pod nazivom Fina QTSA 2017 upisan u Pouzdani popis pružatelja usluga povjerenja u Republici Hrvatskoj.

Fina QTSA 2017 je dio Fina PKI produkcijske okoline, a kvalificirani elektronički vremenski žigovi koje izdaje mogu se koristiti zajedno s kvalificiranim certifikatima koje izdaje Fina.

1.1. Pregled

Ovaj Pravilnik o postupcima pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova (u daljnjem tekstu: QTPS dokument) opisuje postupke i procedure koje Fina PKI primjenjuje pri pružanju usluga izdavanja kvalificiranih elektroničkih vremenskih žigova, a sukladno odredbama Općih pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova [22].

Primijenjena tehnologija kvalificiranih elektroničkih vremenskih žigova zasniva se na kriptografiji javnog ključa, X.509 certifikatima i pouzdanim servisima točnog vremena.

Sadržaj ovog QTPS dokumenta usklađen je s normizacijskim dokumentima:

- ETSI EN 319 401 [6],
- ETSI EN 319 421 [7],
- ETSI EN 319 422 [8],
- ETSI TS 119 312 [12].

Svrha ovog QTPS dokumenta je definiranje i uređivanje postupaka iz opsega ovog dokumenta prema kojima trebaju postupati Fina QTSA 2017 servis, korisnici usluge izdavanja kvalificiranih elektroničkih vremenskih žigova (u daljnjem tekstu: Korisnici) i Pouzdajuće strane.

Za tumačenje odredbi ovog QTPS dokumenta mjerodavne su odredbe Uredbe (EU) br. 910/2014 [1], Zakona o provedbi Uredbe (EU) br. 910/2014 [2], normizacijskih dokumenata i preporuka na koje isti upućuju, te odredbe Općih pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova [22].

Kvalificirani elektronički vremenski žigovi izdani prema postupcima definiranim ovim QTPS dokumentom usklađeni su sa zahtjevima norme ETSI EN 319 421 [7].

Fina kao pružatelj usluga izdavanja kvalificiranih elektroničkih vremenskih žigova uključuje svoj vlastiti QTP OID: 1.3.124.1104.2.3.1.1.5 u kvalificirane elektroničke vremenske žigove koje izdaje.

Pružanje usluge izdavanja kvalificiranih elektroničkih vremenskih žigova sukladno je s ETSI EN 319 421 [7] BTSP (Best practices Time-Stamp Policy): opća pravila najbolje prakse za elektroničke vremenske žigove, OID: 0.4.0.2023.1.1.

Struktura ovog dokumenta temelji se na normizacijskom dokumentu IETF RFC 3647 [20].

1.2. Naziv dokumenta i identifikacijski podaci

Ovaj QTPS dokument sadrži Finina postupke za pružanje usluga izdavanja kvalificiranih elektroničkih vremenskih žigova.

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

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

- Naziv: Pravilnik o postupcima pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova
- Verzija: 1.5
- Datum stupanja na snagu: 10.05.2021.
- OID: 1.3.124.1104.2.3.2.1.5
- Internetska adresa na kojima je objavljen ovaj QTPS dokument je: http://rdc.fina.hr/QTSA2017/FinaQTSA2017-QTPS1-5-hr.pdf.

1.3. Sudionici Fina QTSA 2017 servisa

1.3.1. Pružatelj usluga izdavanja kvalificiranih elektroničkih vremenskih žigova

Fina preko servisa Fina QTSA 2017 pruža uslugu izdavanja kvalificiranih elektroničkih vremenskih žigova (u daljnjem tekstu: usluga izdavanja elektroničkih vremenskih žigova).

1.3.1.1. Fina Root CA

Fina Root CA je izdao samopotpisani Fina Root CA certifikat te CA certifikat za njemu subordinirani Fina RDC 2015 CA. Fina Root CA ne izdaje certifikate Korisnicima.

Osnovni podaci o Fina Root CA certifikatu dani su u Tablici 1.1.

Polje	Atribut	Vrijednost
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	*Vrijeme izdavanja certifikata*
	notAfter	*Vrijeme izdavanja certifikata + 20 godina*
Subject	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
SHA-1 *fingerprint*: 62:02:bf:16:9a:f2:7f:a6:7e:d0:ce:c6:6b:78:2b:83:22:61:26:e9		
SHA-256 *fingerprint*:5a:b4:fc:db:18:0b:5b:6a:f0:d2:62:a2:37:5a:2c:77:d2:56:02:01:5d:96:64:87:56:61:1e:2e:78:c5:3a:d3		

Tablica 1.1. Osnovni podaci o Fina Root CA certifikatu

Fina Root CA certifikat dostupan je na sljedećoj internetskoj adresi: http://rdc.fina.hr/Root/FinaRootCA.cer.

1.3.1.2. Fina RDC 2015 CA

Fina RDC 2015 CA izdaje certifikate za TSU.

Osnovni podaci o Fina RDC 2015 CA certifikatu dani su u Tablici 1.2.

Polje	Atribut	Vrijednost
Issuer	commonName	Fina Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	*Vrijeme izdavanja certifikata*
	notAfter	*Vrijeme izdavanja certifikata + 10 godina*
Subject	commonName	Fina RDC 2015
	organizationName	Financijska agencija
	countryName	HR
SHA-1 *fingerprint*: d8:86:43:90:c7:6c:9b:71:f0:40:4f:f3:76:fc:38:fd:73:78:7d:08		
SHA-256 *fingerprint*: 85:7b:fc:e4:3b:1b:b4:60:1f:f4:54:3b:46:d3:fb:2e:21:3b:f9:b4:fe:eb:6f:13:be:9e:f4:5c:04:ff:6f:8b		

Tablica 1.2. Osnovni podaci o Fina RDC 2015 CA certifikatu

Fina RDC 2015 CA certifikat dostupan je na sljedećoj internetskoj adresi: http://rdc.fina.hr/RDC2015/FinaRDCCA2015.cer.

1.3.2. Korisnici

Korisnici servisa Fina QTSA 2017 su fizičke osobe - građani ili poslovni subjekti koji s Finom ugovaraju korištenje usluga izdavanja elektroničkih vremenskih žigova.

Korisnici Fininog servisa za izdavanje kvalificiranih elektroničkih vremenskih žigova su i Finini interni korisnici.

1.3.3. Registracijski uredi

Poslovi registracije Korisnika za korištenje Fina QTSA 2017 servisa obavljaju se u registracijskim uredima Fine. Fina ima organiziranu mrežu registracijskih ureda (u daljnjem tekstu: Fina RA mreža) koja obavlja poslove registracije Korisnika za Fina QTSA 2017 servis.

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 Službenici za registraciju. Poslovima registracije u Fina RA mreži koordinira Središnji Fina RA koji je središnja komunikacijska točka Fina RA mreže.

Fina može odrediti i drugi odgovarajući način registracije Korisnika.

1.3.4. Pouzdajuće strane

Pouzdajuće strane su fizičke osobe ili poslovni subjekti koji su primatelji kvalificiranih elektroničkih vremenskih žigova (u daljnjem tekstu: elektronički vremenski žig) i djeluju temeljem razumnog pouzdanja u elektroničke vremenske žigove koje izdaje Fina QTSA 2017 servis.

1.3.5. Ostali sudionici

Nema odredbi.

1.4. Uporaba elektroničkih vremenskih žigova

1.4.1. Primjerena uporaba elektroničkih vremenskih žigova

Kvalificirani elektronički vremenski žigovi koje izdaje Finin servis Fina QTSA 2017 mogu se koristiti za bilo koju primjenu koja zahtjeva dokazivanje postojanja podataka u elektroničkom obliku u vremenu koje je navedeno u izdanom elektroničkom vremenskom žigu. Kvalificirani elektronički vremenski žigovi koje izdaje Fina QTSA 2017 servis koriste se i za očuvanje dugotrajnosti elektroničkih potpisa.

1.4.2. Zabrane uporabe elektroničkih vremenskih žigova

Nije dozvoljena uporaba kvalificiranih elektroničkih vremenskih žigova za one podatke, odnosno elektroničke zapise čiji je sadržaj protivan Ustavu Republike Hrvatske, prisilnim propisima ili moralu društva.

1.5. Administracija dokumenta Opća pravila

1.5.1. Organizacija odgovorna za održavanje dokumenta Opća pravila

Za izradu i održavanje dokumenta Općih pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova [22] (u daljnjem tekstu: Opća pravila) i ovog QTPS dokumenta odgovorna je Fina.

Ovlaštene osobe iz organizacijskih jedinica Fine koje sudjeluju u razvoju, održavanju, implementaciji i odobravanju općih pravila i pravilnika pružanja usluga povjerenja u Fina PKI u daljnjem tekstu nazivaju se zajedničkim nazivom Fina PMA.

Promjene sadržaja dokumenta obavljaju se na temelju internih prijedloga i zahtjeva za usklađivanjem sa zakonskom regulativom i mjerodavnim normama.

1.5.2. Kontakt podaci

Kontakt podaci za administraciju i sadržaj ovog QTPS dokumenta:

Poštanska adresa:

Fina
Sektor komercijalnih digitalnih rješenja
Ured za upravljanje politikama e-poslovanja
Koturaška cesta 43
10000 Zagreb
Hrvatska

telefon: +385-1-6128-171
telefax: +385-1-6304-081
E-mail: pma@fina.hr

1.5.3. Tijelo koje utvrđuje usklađenost QTPS dokumenta s Općim pravilima

Usklađenost ovog QTPS dokumenta s Općim pravilima [22] utvrđuje Fina PMA.

Fina PMA odgovoran je za usklađenost ovog dokumenta s Općim pravilima [22].

1.5.4. Procedure odobravanja QTPS dokumenta

Izrada, odobravanje i stupanje na snagu ovog QTPS dokumenta kojom se potvrđuje njegova sukladnost s Općim pravilima [22] opisana je u točki 9.13.1 ovog QTPS dokumenta.

1.6. Definicije i kratice

1.6.1. 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.
Autentikacija	Elektronički postupak koji omogućava da elektronička identifikacija fizičke ili pravne osobe, ili izvornost i cjelovitost podataka u elektroničkom obliku budu potvrđeni.
Autor pečata	Pravna osoba koja izrađuje elektronički pečat.
CA certifikat	Certifikat javnog ključa za CA kojeg je izdao drugi CA ili kojeg je izdao isti CA.
Certifikat	Vidi pojam „certifikat javnog ključa“.
Certifikat za elektronički pečat	Elektronička potvrda koja povezuje podatke za validaciju elektroničkog pečata s pravnom osobom i potvrđuje naziv te osobe.
Certifikat za elektronički potpis	Elektronička potvrda koja povezuje podatke za validaciju elektroničkog potpisa s fizičkom osobom i potvrđuje barem ime ili pseudonim te osobe.
Certifikat javnog ključa	Javni ključ Subjekta koji je zajedno s drugim informacijama zaštićen od krivotvorenja digitalnim potpisom izrađenim privatnim ključem certifikacijskog tijela koje je izdalo certifikat.
Certifikacijsko tijelo (CA)	Tijelo koje izrađuje i dodjeljuje certifikate javnog ključa, a kojem vjeruje jedan ili više korisnika. Certifikacijsko tijelo može biti: 1. pružatelj usluga povjerenja koji izrađuje i dodjeljuje certifikate javnog ključa, ili 2. tehnički servis izrade certifikata kojeg upotrebljava pružatelj usluga certificiranja koji izrađuje i dodjeljuje certifikate javnog ključa.
Elektronički pečat	Podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka.
Elektronički potpis	Podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje Potpisnik koristi za potpisivanje.

POJAM	DEFINICIJA
Elektronički vremenski žig	Podaci u elektroničkom obliku koji povezuju druge podatke u elektroničkom obliku s određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme.
Fina LRA	Lokalni registracijski ured u Fina poslovnoj mreži.
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 RA Fine i Fina LRA ureda.
Fizička osoba – građanin	Fizička osoba koja uslugu izdavanja elektroničkih vremenskih žigova 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).
Infrastruktura javnog ključa (PKI)	Infrastruktura za upravljanje javnim ključevima koji podržavaju usluge autentikacije, enkripcije, cjelovitosti i neporecivosti.
Javni imenik	Informatički sustav koji služi za *online* objavu informacija vezanih uz certifikate, uključujući i informacije o opozvanosti certifikata.
Javni ključ	U kriptografskom sustavu javnog ključa, javno poznati ključ iz Subjektovog para ključeva.
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	Poslovni subjekt ili fizička osoba koja je sklapanjem ugovora s pružateljem usluga povjerenja preuzela ugovorne obveze Korisnika.
Kriptografski modul	Softver ili uređaj određene razine sigurnosti koji: • generira par ključeva, i/ili • štiti kriptografske informacije, i/ili • obavlja kriptografske funkcije.
Kvalificirani certifikat za elektronički pečat	Certifikat za elektronički pečat koji izdaje kvalificirani pružatelj usluge povjerenja i koji ispunjava zahtjeve određene u Prilogu III. Uredbe (EU) br. 910/2014 [1].
Kvalificirani certifikat za elektronički potpis	Certifikat za elektroničke potpise koji izdaje kvalificirani pružatelj usluga povjerenja i koji ispunjava zahtjeve utvrđene u Prilogu I. Uredbe (EU) br. 910/2014 [1].
Kvalificirani elektronički pečat	Napredan elektronički pečat koji je izrađen pomoću sredstava za izradu kvalificiranog elektroničkog pečata i temelji se na kvalificiranom certifikatu za elektronički pečat.
Kvalificirani elektronički potpis	Napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i temelji se na kvalificiranom certifikatu za elektroničke potpise.

POJAM	DEFINICIJA
Kvalificirani elektronički vremenski žig	Elektronički vremenski žig koji ispunjava sljedeće zahtjeve: (a) povezuje datum i vrijeme s podacima na način kojim se u razumnoj mjeri isključuje mogućnost nezapažene promjene podataka, (b) temelji se na izvoru točnog vremena povezanom s koordiniranim svjetskim vremenom, i (c) potpisan je pomoću naprednog elektroničkog potpisa ili pečaćen pomoću naprednog elektroničkog pečata kvalificiranog pružatelja usluga povjerenja ili jednakovrijednom metodom.
Kvalificirani pružatelj usluga povjerenja	Pružatelj usluga povjerenja koji pruža jednu ili više kvalificiranih usluga povjerenja i kojemu je nadzorno tijelo odobrilo kvalificirani status.
Kvalificirano sredstvo za izradu elektroničkog potpisa	Sredstvo za izradu elektroničkog potpisa koje ispunjava zahtjeve utvrđene u Prilogu II Uredbe (EU) br. 910/2014 [1].
Lista opozvanih certifikata *(*CRL*)*	Potpisana lista u kojoj su naznačeni certifikati koje je opozvao izdavatelj certifikata.
Napredan elektronički pečat	Elektronički pečat koji ispunjava sljedeće zahtjeve: (a) na nedvojben način je povezan s Autorom pečata, (b) omogućava identificiranje Autora pečata, (c) izrađen je korištenjem podacima za izradu elektroničkog pečata koje Autor pečata može, uz visoku razinu pouzdanja i pod svojom kontrolom, koristiti za izradu elektroničkog pečata, i (d) povezan je s podacima na koje se odnosi na takav način da se može otkriti bilo koja naknadna izmjena podataka.
Napredan elektronički potpis	Elektronički potpis koji ispunjava sljedeće zahtjeve: (a) na nedvojben način je povezan s Potpisnikom, (b) omogućava identificiranje Potpisnika, (c) izrađen je korištenjem podacima za izradu elektroničkog potpisa koje Potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom, i (d) povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka.
Opća pravila pružanja usluga 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 pružanja usluga izdavanja vremenskih žigova - *Time-Stamp Policy* (TP)	Imenovani skup pravila koji ukazuje na primjenjivost elektroničkog vremenskog žiga za određenu skupinu i/ili klasu primjena sa zajedničkim zahtjevima na sigurnost.
Opoziv certifikata	Trajni prestanak valjanosti certifikata prije isteka roka važenja navedenog u certifikatu.
Par ključeva	Dva jedinstveno povezana kriptografska ključa, od kojih je jedan privatni ključ, a drugi javni ključ.
Podaci za izradu elektroničkog pečata	Jedinstveni podaci koje Autor elektroničkog pečata koristi za izradu elektroničkog pečata.

POJAM	DEFINICIJA
Podaci za izradu elektroničkog potpisa	Jedinstveni podaci koje Potpisnik koristi za izradu elektroničkog potpisa
Podaci za validaciju	Podaci koji se koriste za validaciju elektroničkog potpisa ili elektroničkog pečata.
Podaci za verifikaciju potpisa	Podaci, poput kodova ili javnih kriptografskih ključeva koji se koriste u svrhu verificiranja potpisa.
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.
Potpisnik	Fizička osoba koja izrađuje elektronički potpis.
Pouzdajuća strana	Fizička osoba ili poslovni subjekt koji se oslanja na elektroničku identifikaciju ili uslugu povjerenja.
Povjerljive uloge	Uloge o kojima ovisi sigurnost rada pružatelja usluga povjerenja. Povjerljive uloge (engl. *Trusted Roles*) i pripadajuće odgovornosti pružatelj usluga povjerenja jasno opisuje u opisu posla djelatnika.
Pravilnik o postupcima certificiranja (CPS)	Pravilnik operativnih postupaka koje certifikacijsko tijelo provodi u izdavanju, upravljanju, opozivu ili obnovi certifikata.
Privatni ključ	U kriptografskom sustavu javnog ključa, ključ iz Subjektovog para ključeva koji je poznat samo Subjektu.
Pružatelj usluga povjerenja	Fizička ili pravna osoba koja pruža jednu ili više usluga povjerenja bilo kao kvalificirani ili nekvalificirani pružatelj usluga povjerenja.
QSCD uređaj	Kvalificirano sredstvo za izradu elektroničkog potpisa/pečata (vidi pojam „kvalificirano sredstvo za izradu elektroničkog potpisa“, odnosno „sredstvo za izradu kvalificiranog elektroničkog pečata“.
QTSA sustav	Sustav IT proizvoda i komponenti organiziranih za pružanje usluga izdavanja kvalificiranih elektroničkih vremenskih žigova.
RA mreža	Cjelokupna mreža registracijskih tijela, a sastoji se od Fina RA mreže te od vanjskih ugovorenih RA s kojima Fina ima sklopljen ugovor o obavljanju poslova registracije.

POJAM	DEFINICIJA
Registracijski ured (RA)	Tijelo odgovorno za identifikaciju i autentikaciju subjekata certificiranja, kao i drugih osoba ili organizacija.
Root CA	Certifikacijsko tijelo najviše razine unutar domene pružatelja usluga povjerenja i koje potpisuje certifikate subordiniranih CA-ova.
Root CA certifikat	CA certifikat kojeg je samom sebi izdao root CA.
Službenik za registraciju	Osoba odgovorna za potvrđivanje podataka koji su potrebni za izdavanje certifikata i za odobravanje zahtjeva za izdavanje certifikata.
Središnji RA	Središnji registracijski ured koji je primarno je zadužen za koordiniranje cjelokupne RA mreže, ali može i izravno obavljati registriranje Korisnika
Sredstvo za izradu elektroničkog pečata	Konfigurirani softver ili hardver koji se koristi za izradu elektroničkog pečata.
Sredstvo za izradu elektroničkog potpisa	Konfigurirani softver ili hardver koji se koristi za izradu elektroničkog potpisa.
Sredstvo za izradu kvalificiranog elektroničkog pečata	Sredstvo za izradu elektroničkog pečata koje *mutatis mutandis* ispunjava zahtjeve određene u Prilogu II. Uredbe (EU) br. 910/2014 [1].
Subjekt	Entitet identificiran u certifikatu kao nositelj privatnog ključa koji je povezan s javnim ključem sadržanim u certifikatu.
Suspenzija certifikata	Privremeni prestanak valjanosti certifikata prije isteka roka važenja navedenog u certifikatu. Suspendirani certifikat se reaktivacijom može ponovno učiniti valjanim.
Tijelo za ocjenjivanje sukladnosti	Tijelo u smislu članka 2. točke 13. Uredbe (EZ) br. 765/2008 koje je u skladu s tom Uredbom ovlašteno kao nadležno za provedbu ocjenjivanja sukladnosti kvalificiranog pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža.
Tijelo za upravljanje pravilima certificiranja (PMA)	Tijelo s konačnom ovlašću i odgovornošću za određivanje i odobravanje pravila pružanja usluga povjerenja (engl. *Policy Management Authority*)
Usluge certificiranja	Usluge izdavanja i upravljanja životnom ciklusom certifikata.
Validacija	Postupak verifikacije i potvrđivanja da su elektronički potpis ili pečat valjani.
Validacija certifikata	Postupak verificiranja i potvrđivanja da je certifikat valjan.
Verifikacija potpisa	Proces provjere kriptografske vrijednosti potpisa korištenjem podataka za verifikaciju potpisa.

Tablica 1.3. Definicije

1.6.2. Kratice

KRATICA	PUNI NAZIV	ZNAČENJE
CA	*Certification Authority*	Certifikacijsko tijelo
CP	*Certificate Policy*	Opća pravila pružanja usluga certificiranja
$CP_{QC\text{-}eIDAS}$	*Certificate Policy for Qualified Certificates for Electronic Signatures and Seals*	Opća pravila pružanja usluga certificiranja za kvalificirane certifikate za elektroničke potpise i pečate
CPS	*Certification Practice Statement*	Pravilnik o postupcima certificiranja
$CPS_{QC\text{-}eIDAS}$	*Certification Practice Statement for Qualified Certificates and Seals*	Pravilnik o postupcima certificiranja za kvalificirane certifikate za elektroničke potpise i pečate
CRL	*Certificate Revocation List*	Lista opozvanih certifikata
HSM	*Hardware Security Module*	Hardverski kriptografski modul
LDAP	*Lightweight Directory Access Protocol*	Protokol za pristup informacijskim direktorijima
LRA	*Local Registration Authority*	Lokalni registracijski ured
OCSP	*Online Certificate Status Protocol*	Protokol *on-line* provjere statusa certifikata
OID	*Object Identifier*	Identifikator objekta
PIN	*Personal Identification Number*	Osobni tajni broj za aktivaciju smart kartice, USB tokena ili sličnog uređaja
PKI	*Public Key Infrastructure*	Infrastruktura javnog ključa
PMA	*Policy Management Authority*	Tijelo za upravljanje pravilima certificiranja
QSCD	*Qualified electronic Signature/Seal Creation Device*	Kvalificirano sredstvo za izradu elektroničkog potpisa/pečeta
QTP	*Qualified Time-Stamp Policy*	Opća pravila pružanja usluga izdavanja kvalificiranih vremenskih žigova
QTPS	*Qualified TSA Practice Statement*	Pravilnik o postupcima pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova
QTSA	*Qualified Time-Stamping Authority*	Pružatelj usluga izdavanja kvalificiranih elektroničkih vremenskih žigova
RA	*Registration Authority*	Registracijsko tijelo
TAI	*International Atomic Time*	Međunarodno atomsko vrijeme
TLS	*Transport Layer Security*	Kriptografski protokol za sigurnu razmjenu podataka putem Interneta
TSU	*Time-Stamping Unit*	Jedinica za izradu elektroničkih vremenskih žigova
UTC	*Coordinated Universal Time*	Koordinirano svjetsko vrijeme

Tablica 1.4. Kratice

2. OBJAVE I ODGOVORNOSTI ZA REPOZITORIJ

2.1. Identifikacija tijela koje vodi repozitorij

Fina QTSA repozitorij vodi Fina kao kvalificirani pružatelj usluga povjerenja. Fina je odgovorna za rad Fina QTSA repozitorija te za objavu dokumenata i informacija na repozitoriju.

Fina osigurava dostupnost repozitorija na internetskim stranicama uz raspoloživost 24 sata na dan, 7 dana u tjednu.

2.2. Objava informacija o izdavanju elektroničkih vremenskih žigova

Na Fina QTSA repozitoriju javno su objavljeni dokumenti i informacije o pružanju usluga izdavanja kvalificiranih elektroničkih vremenskih žigova.

2.2.1. Sadržaj repozitorija

Na internetskim stranicama Fina QTSA repozitorija javno se objavljuju sljedeći dokumenti i informacije:

- aktualna Opća pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova,
- aktualni QTPS dokument,
- prijašnje verzije Općih pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova i QTPS dokumenta,
- uvjeti pružanja usluga izdavanja elektroničkih vremenskih žigova i izjava o pružanju usluga izdavanja elektroničkih vremenskih žigova,
- certifikat TSU kojeg Fina QTSA 2017 servis koristi pri potpisivanju elektroničkih vremenskih žigova,
- cjenik usluga izdavanja elektroničkih vremenskih žigova,
- obrazac pristupnice za korištenje Fina QTSA 2017 servisa,
- aktualne lokacije Fina RA/LRA ureda,
- korisničke upute,
- obavijesti Korisnicima vezane uz pružanje usluga izdavanja elektroničkih vremenskih žigova,
- ostale informacije vezane uz rad Fina QTSA 2017 servisa.

Javno objavljeni sadržaj Fina QTSA repozitorija, koji je sastavni dio Fina PKI repozitorija, dostupan je s internetske adrese http://www.fina.hr/finadigicert.

U Fina PKI repozitoriju ne objavljuju se povjerljivi podaci.

2.2.2. Postupci objave sadržaja i upravljanja repozitorijom

Objavu dokumenata na repozitoriju po odobrenju obavlja ovlaštena osoba zadužena za upravljanje sadržajem internetskog dijela repozitorija.

Obavijesti Korisnicima i informacije o zakonskim aktima objavljuju se po početku primjene u Fina PKI. Objavu informacija i dokumenata odobrava Fina PMA.

Certifikati Fina CA-ova, certifikat Fina QTSA 2017 servisa i pripadajuće informacije objavljuju se po njihovu izdavanju.

Objavu dokumenata uvjeta pružanja usluga, korisničkih uputa, obrazaca pristupnice , ugovora i punomoći odobrava Fina PMA. Objava ovih dokumenata se obavlja bez prethodne najave, a starije verzije dokumenata brišu se iz repozitorija.

Fina CA automatski objavljuje pripadajuće CRL na javnom imeniku i na internetskim stranicama repozitorija nakon njihova izdavanja.

Objavu nove verzije cjenika odobrava Fina PMA.

Obavijesti i informacije Korisnicima mogu se objaviti na internetskim stranicama repozitorija i bez odobrenja Fina PMA, ali Fina PMA mora biti pravodobno obaviješten o svakoj objavi obavijesti i informacija.

2.3. Vrijeme ili učestalost objavljivanja

Fina na godišnjoj razini i prema potrebi održava i ažurira Opća pravila [22] i ovaj QTPS dokument te ih nakon odobrenja objavljuje. Drugi Fina PKI dokumenti i ostale relevantne informacije objavljuju se prema potrebi, nakon odobrenja.

2.4. Kontrole pristupa repozitoriju

Dokumenti i informacije objavljene na Fina PKI repozitoriju su besplatne i javno dostupne.

Fina na repozitoriju ima uspostavljene kontrole pristupa u cilju sprječavanja neautoriziranog dodavanja, promjene ili brisanja informacija te zaštite njihove cjelovitosti i autentičnosti. Pristup objavljenim dokumentima i informacijama na repozitoriju omogućen je samo za čitanje.

Pravo dodavanja, promjene ili brisanja informacija na Fina PKI repozitoriju imaju ovlaštene osobe Fine.

3. IDENTIFIKACIJA KORISNIKA I IZDAVANJE ELEKTRONIČKIH VREMENSKIH ŽIGOVA

3.1. Identifikacija Korisnika

Fina QTSA 2017 pruža uslugu izdavanja kvalificiranih elektroničkih vremenskih žigova samo registriranim Korisnicima.

Ako Korisnik već ima validni digitalni certifikat izdan od Fine ili od pružatelja usluga povjerenja koje Fina odobri i kojim će pristupati Fininom servisu za izdavanje elektroničkih vremenskih žigova treba popuniti i ovjeriti pristupnicu za korištenje Finine usluge izdavanja elektroničkih vremenskih žigova te je dostaviti u Fina LRA. Obrazac pristupnice nalazi se na internetskim stranicama repozitorija iz točke 2.2. ovog QTPS dokumenta.

Ako Korisnik nema odgovarajući digitalni certifikat može zatražiti i izdavanje Fininog digitalnog certifikata kojim će pristupati Fininoj usluzi izdavanja elektroničkih vremenskih žigova.

Ako korisnička aplikacija ne podržava autentikaciju certifikatom, Korisnik može poslati upit vezan uz korištenje usluge na e-mail adresu: info.rdc@fina.hr gdje će dobiti odgovor o mogućnosti ugovaranja Finine usluge izdavanja elektroničkih vremenskih žigova za Korisnikov specifičan scenarij.

Nakon registracije Korisnik s Finom sklapa ugovor o korištenju Finine usluge izdavanja elektroničkih vremenskih žigova.

3.1.1. Inicijalno potvrđivanje identiteta Korisnika

Provjeru podataka koji se prikupljaju u postupku registracije Korisnika Fina provodi njihovom usporedbom s podacima iz dostavljene dokumentacije te ukoliko je primjenjivo korištenjem komunikacijskih kanala sukladno važećoj zakonskoj regulativi.

Postupak identifikacije podnositelja zahtjeva za izdavanje Fininog autentikacijskog certifikata ili Fininog aplikacijskog certifikata opisan je u Fininom Pravilniku o postupcima certificiranja za nekvalificirane certifikate ($CPS_{NQC\text{-}eIDAS}$) [24].

Za korištenje usluge izdavanja elektroničkih vremenskih žigova korisnici digitalnih certifikata podnose pravilno ispunjenu i potpisanu pristupnicu.

Za registrirane Korisnike Fininih digitalnih certifikata već je provedena identifikacija Korisnika pa za korištenje usluge izdavanja kvalificiranih elektroničkih vremenskih žigova Korisnici dostavljaju samo pristupnicu prema točki 3.1.2 ovog QTPS dokumenta.

3.1.2. Način dostave pristupnice

Pristupnica se može dostaviti na sljedeće načine:

- osobno podnošenje u Fina LRA registracijskom uredu,
- poštanskom dostavom ili preko dostavljača u Fina LRA registracijskom uredu,
- elektroničkom dostavom pristupnice, potpisane kvalificiranim elektroničkim potpisom ili naprednim elektroničkim potpisom koji se temelji na kvalificiranom certifikatu kojeg je izdao kvalificirani pružatelj usluga povjerenja ili na certifikatu kojeg je izdao Fina CA, ili se autentikacija podnositelja Pristupnice i cjelovitost podataka u Pristupnici osiguravaju drugim

sigurnim metodama, na e-mail adresu iz točke 9.12. ovog QTPS dokumenta ili putem drugog podržanog elektroničkog kanala.

3.1.3. Sklapanje ugovora

Ugovor o pružanju usluga izdavanja elektroničkih vremenskih žigova je ugovor koji sukladno Uvjetima o pružanju usluge izdavanja kvalificiranih elektroničkih vremenskih žigova, općim propisima obveznog prava, Općih pravila [22] i propisima koji uređuju pružanje usluge izdavanja elektroničkih vremenskih žigova, sklapaju Korisnici i Fina kao pružatelj usluge.

3.2. Autentikacija na Fina QTSA 2017 servis

Registrirani Korisnici pristupaju usluzi izdavanja elektroničkih vremenskih žigova uz autentikaciju autentikacijskim ili aplikacijskim certifikatom kojeg je izdala Fina.

Registrirani Korisnici mogu pristupiti usluzi izdavanja elektroničkih vremenskih žigova i uz autentikaciju certifikatom izdanim od drugih pružatelja usluga povjerenja koje Fina prihvati.

Fina može Korisnicima odobriti i drugi odgovarajući način autentikacije Korisnika (npr. korisničko ime i zaporka).

URL adrese za autentikaciju na Fina QTSA 2017 servis, ovisno o metodi autentikacije su:

- autentikacija certifikatom: https://tsa.fina.hr/ts-rfc3161
- autentikacija korisničkim imenom i zaporkom: https://tsa.fina.hr:3443/ts-rfc3161.

Finini interni Korisnici pristupaju Fininom servisu za izdavanje elektroničkih vremenskih žigova temeljem IP adresnog područja za Finine Korisnike. Internim Fininim Korisnicima ne naplaćuje se usluga izdavanja elektroničkih vremenskih žigova.

3.3. Certifikat jedinice za izradu elektroničkog vremenskog žiga

Fina QTSA javno objavljuje javni ključ jedinice za izradu elektroničkog vremenskog žiga (TSU) kao sadržaj certifikata Fina QTSA 2017 na repozitoriju iz točke 2.2. ovog QTPS dokumenta.

Fina QTSA 2017 certifikat za TSU izdaje Fina RDC 2015 CA sukladno zahtjevima normi ETSI EN 319 411-2 [10].

Fina QTSA 2017 servis započinje s izdavanjem elektroničkih vremenskih žigova korištenjem novog privatnog TSU ključa nakon ispunjenja sljedećih uvjeta:

- certifikat koji odgovara privatnom TSU ključu izdan je i javno je objavljen na repozitoriju iz točke 2.2. ovog QTPS dokumenta,
- Fina QTSA 2017 servis provjerio je potpis izdavatelja Fina QTSA 2017 certifikata, uključujući provjeru je li Fina QTSA 2017 certifikat ispravno potpisan od strane Fina RDC 2015 CA te uključujući provjeru pune certifikacijske staze do Fina Root CA.

Profil Fina QTSA 2017 certifikata opisan je u točki 7.1 ovog QTPS dokumenta.

3.4. Elektronički vremenski žig

Finini elektronički vremenski žigovi potpisuju se RSA privatnim ključem Fina QTSA 2017 servisa, duljine 2048 bitova uz korištenje kriptografskih algoritama SHA-256 i RSA.

Fina QTSA 2017 osigurava da se elektronički vremenski žigovi izdaju na siguran način i s točnom oznakom vremena.

Za svaki elektronički vremenski žig osigurava se:

- da sadrži OID pripadajućih Općih pravila [22] (QTP OID),
- da ima jedinstveni identifikator u vidu serijskog broja (maksimalne duljine do 18 okteta),
- da se podatak o vremenu koji je korišten u TSU može povezati sa stvarnim vremenom dostavljenim od pouzdanog izvora,
- da sadrži točan podatak o vremenu iz TSU u vrijeme izdavanja elektroničkog vremenskog žiga,
- da sadrži *hash* reprezentaciju podataka za koji se izdaje elektronički vremenski žig,
- da je potpisan privatnim TSU ključem koji ima isključivu namjenu potpisivanja elektroničkih vremenskih žigova,
- identifikator države u kojoj je Fina QTSA 2017 ima sjedište,
- identifikator za Fina QTSA 2017,
- identifikator TSU koja je izdala elektronički vremenski žig.

Elektronički vremenski žig izdaje se sukladno preporuci ITF RFC 3161 [13] i normi ETSI EN 319 421 [7] te prema profilu usklađenim s normom ETSI EN 319 422 [8].

3.4.1. Zahtjev za izdavanje elektroničkog vremenskog žiga (*Time-Stamp Request*)

Fina QTSA 2017 servis za izdavanje elektroničkih vremenskih žigova podržava zahtjeve klijentskih aplikacija za izdavanje elektroničkih vremenskih žigova sukladno normi ETSI EN 319 422 [8] i preporuci IETF RFC 3161 [13], uključujući korištenje sljedećih polja u zahtjevu:

- *reqPolicy,*
- *nonce,*
- *certReq.*

Finin servis za izdavanje elektroničkih vremenskih žigova ne podržava korištenje sljedećeg polja:

- *extensions.*

Fina QTSA 2017 servis za izdavanje elektroničkih vremenskih žigova u zahtjevu za izdavanje elektroničkog vremenskog žiga prihvaća sljedeći *hash* algoritam (*hashAlgorithm*):

- sha-256 (OID: 2.16.840.1.101.3.4.2.1)

Korisnik koji se na Fina QTSA 2017 servis prijavljuje korištenjem Fininog digitalnog certifikata ili korištenjem korisničkog imena i zaporke mora ostvariti autenticiranu vezu s komunikacijskim poslužiteljem Fina QTSA 2017 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 elektroničkog vremenskog žiga, treba podržavati protokol za elektronički vremenski žig sukladan s preporukom IETF RFC 3161 [13].

Fina QTSA ne definira fiksan vremenski rok za obradu zahtjeva za izdavanje elektroničkog vremenskog žiga.

3.4.1.1. Profil zahtjeva za izdavanje elektroničkog vremenskog žiga

Opis osnovnih polja i ekstenzija u profilu zahtjeva za izdavanje elektroničkih vremenskih žigova:

- *Version*

  Format zahtjeva odgovara verziji „v1“ specificiranoj u normi ETSI EN 319 422 [8] i preporuci IETF RFC 3161 [13], tako da ovo polje sadrži vrijednost „1“.

- *MessageImprint*

  Podaci koji se označavaju elektroničkim vremenskim žigom, a sastoji se od dva dijela:

  - *Hash* algoritam (*hashAlgorithm*)
    OID *hash* algoritma kojim je izrađen sažetak dokumeta/podataka (*hash),*
  - Sažetak *(hash, odnosno hashedMessage).*
    Sam sažetak dokumenta/podataka koji se označavaju elektroničkim vremenskim žigom. Duljina podataka ovisi o korištenom hash algoritmu.

- *Identifikator politike izdavanja elektroničkih vremenskih žigova (reqPolicy)*
  - opcionalno polje

  Specificira politiku izdavanja elektroničkih vremenskih žigova prema kojoj se zahtijeva izdavanje elektroničkog vremenskog žiga.

- *Nonce*
  - opcionalno polje

  Cijeli broj, duljine 64 bita, kojim se osigurava da izdani elektronički vremenski žig odgovara zahtjevu Korisnika za njegovim izdavanjem. U slučaju da zahtjev za izdavanje elektroničkog vremenskog žiga sadrži vrijednost za *nonce* tada odgovor servisa za izdavanje elektroničkih vremenskih žigova mora sadržavati istu vrijednost.

- *Zahtjev za dostavom certifikata (certReq)*

  Podrazumijevana (*deafault*) vrijednost je "FALSE".

  Ukoliko zahtjev sadrži vrijednost „TRUE“, tada certifikat TSU jedinice referenciran u polju *SigningCertificate attribute* mora biti uključen u odgovoru servisa za izdavanje elektroničkih vremenskih žigova.

- *Ekstenzije (extensions)*

  Fina QTSA 2017 servis za izdavanje elektroničkih vremenskih žigova ne podržava korištenje ovog polja. Ukoliko Finin servis primi zahtjev koji sadrži ovo polje tada elektronički vremenski žig neće biti izdan, a servis će na zahtjev odgovoriti porukom o greški "unacceptedExtension".

3.4.2. Odgovor Fina QTSA 2017 servisa (*Time-Stamp Response*)

Odgovor Fina QTSA 2017 servisa za izdavanje elektroničkih vremenskih žigova na zahtjev za izdavanje elektroničkog vremenskog žiga u skladu je s normom ETSI EN 319 422 [8] i s točkom 2.4.2. u dokumentu IETF RFC 3161 [13], a podržane su sljedeće ekstenzije:

- *accuracy,*
- *nonce.*

U slučaju da zahtjev za izdavanje elektroničkog vremenskog žiga sadrži vrijednost za *nonce* tada i odgovor servisa za izdavanje elektroničkih vremenskih žigova mora sadržavati istu vrijednost.

Fina QTSA 2017 servis za izdavanje elektroničkih vremenskih žigova podržava sljedeći *hash* algoritam (*hashAlgorithm*):

- sha-256 (OID: 2.16.840.1.101.3.4.2.1)

TSU u Fina QTSA 2017 servisu ima u određenom vremensku aktivan samo jedan potpisni ključ kojim potpisuje izdane elektroničke vremenske žigove.

3.4.2.1. Profil odgovora Fina QTSA 2017 servisa

- Status *(PKIStatusInfo)*

  Informacija o statusu uspješnosti izdavanja elektroničkog vremenskog žiga, sukladno točki 2.4.2. u dokumentu IETF RFC 3161 [13].

- Token elektroničkog vremenskog žiga (*TimeStampToken*)
  - opcionalno polje

  Ovo polje sadrži token elektroničkog vremenskog žiga u slučaju kad polje Status (*PKIStatusInfo*) ima vrijednost „0“ ili „1“. U slučajevima kad je u polju Status (*PKIStatusInfo*) sadržana neka druga vrijednost polje Token elektroničkog vremenskog žiga (*TimeStampToken*) nije sadržano u odgovoru servisa.

3.5. Profil elektroničkog vremenskog žiga

Osnovni podaci o profilu elektroničkih vremenskih žigova koje izdaje Fina QTSA 2017 servis dani su u Tablici 3.1.

Polje	Vrijednosti za kvalificirani elektronički vremenski žig kojeg izdaje Fina QTSA 2017 servis
Version	V1, vrijednost=“1“
Policy OID	Fina OID: 1.3.124.1104.2.3.1.1.5
messageImprint	Podržani hash algoritam: sha-256 (OID: 2.16.840.1.101.3.4.2.1)
serialNumber	Cijeli broj
genTime	UTC vrijeme, razlučivost od 1 s
Ordering	FALSE
Nonce	Cijeli broj
signatureAlgorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)

Tablica 3.1. Osnovni podaci o kvalificiranom elektroničkom vremenskog žigu kojeg izdaje Fina QTSA 2017 servis

3.6. Točnost vremena u izdanim elektroničkim vremenskim žigovima

Fina kao pružatelj usluga izdavanja kvalificiranih elektroničkih vremenskih žigova obvezuje se na točnost podataka o vremenu ugrađenom u elektronički vremenski žig. Podatak o UTC vremenu koji se ugrađuje u svaki pojedini elektronički vremenski žig ima odstupanje manje od +/- 1 s.

Elektronički vremenski žig kojeg izdaje Fina QTSA 2017 sadrži datum i vrijeme koje je u skladu sa stvarnim UTC vremenom. Podatak o točnom vremenu dobiva se od Fininih satelitskih prijamnika.

Fina QTSA 2017 će prestati izdavati elektroničke vremenske žigove ako se ustanovi da je vrijeme koje koristi Fina QTSA 2017 TSU izvan deklarirane točnosti.

3.7. Sinkronizacija sata s UTC

Fina posjeduje satelitske prijamnike signala točnog UTC vremena distribuiranog s jednog od UTC(k) laboratorija koje se preuzima putem GPS satelitskog sustava. Fina QTSA 2017 sustav se automatski sinkronizira s ovim satelitskim prijemnicima.

Fina QTSA osigurava da je vrijeme Fina QTSA 2017 sustava sinkronizirano s UTC vremenom, unutar preciznosti propisane u točki 3.6. ovog QTPS dokumenta, a posebno:

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

Primarni izvor pouzdanog UTC vremena u Fina QTSA 2017 sustavu je satelitski GPS signal.

Kao alternativni pouzdani izvor UTC vremena Fina QTSA 2017 sustav koristi podatak o UTC vremenu dobiven od strane ovlaštenog referentnog laboratorija putem internetske veze korištenjem NTP protokola.

U slučaju ispada primarnog izvora pouzdanog UTC vremena Fina QTSA 2017 sustav automatski prelazi na alternativni pouzdani izvor UTC vremena.

3.7.1. Ljetno računanje vremena

Fina QTSA 2017 servis u izdanim elektroničkim vremenskim žigovima upisuje točno vrijeme u UTC formatu.

Preporuka je Korisnicima i Pouzdajućim stranama da provjere na koji način klijentska aplikacija prikazuje vrijeme u izdanim elektroničkim vremenskim žigovima te da obrate pozornost na prikazivanje lokalnog vremena u različitim vremenskim zonama, a naročito u vrijeme prelaska na ljetno računanje vremena.

3.8. Provjera valjanosti elektroničkog vremenskog žiga

Prije pouzdanja u kvalificirani elektronički vremenski žig Pouzdajuća strana obvezna je obaviti provjeru valjanosti elektroničkog vremenskog žiga.

Provjera valjanosti elektroničkog vremenskog žiga obuhvaća sljedeće provjere:

- je li elektronički vremenski žig ispravno potpisan i da privatni ključ koji se koristi za potpisivanje elektroničkog vremenskog žiga nije bio kompromitiran do trenutka provjere,

- provjeru da izdani elektronički vremenski žig ispunjava specifične zahtjeve u pogledu točnosti, pouzdanosti i odgovornosti Fina QTSA 2017 servisa, odnosno Fine kao kvalificiranog pružatelja usluga,
- provjeru ograničenja uporabe elektroničkog vremenskog žiga navedenih u točki 1.4.2. ovog QTPS dokumenta te uzimanje u obzir svih ostalih mjera opreza propisanih u ugovoru i uvjetima pružanja usluge izdavanja elektroničkih vremenskih žigova.

Provjera potpisa Fina QTSA 2017 na zaprimljenom kvalificiranom elektroničkom vremenskom žigu obuhvaća i provjeru valjanosti Fina QTSA 2017 certifikata kojim je elektronički vremenski žig potpisan. Provjera statusa certifikata može se obaviti korištenjem Finog OCSP servisa za online provjeru statusa certifikata čija je internetska adresa navedena u *Authority Information Access* ekstenziji Fina QTSA 2017 certifikata. Opozvanost Fina QTSA 2017 certifikata može se provjeriti i putem CRL koja se objavljuje na LDAP imeničkom poslužitelju kao i na web poslužitelju. Internetske adrese na kojima se objavljuju CRL za provjeru opozvanost Fina QTSA 2017 certifikata navedene su u *CRL Distribution Points* ekstenziji Fina QTSA 2017 certifikata.

U slučaju provjere valjanosti elektroničkog vremenskog žiga nakon isteka vremena važenja Fina QTSA 2017 certifikata, Pouzdajuća strana treba na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovog QTPS dokumenta provjeriti je li privatni TSU ključ bio kompromitiran i da li se kriptografski hash algoritam te potpisni kriptografski algoritam i duljina potpisnog TSU ključa kojima je potpisan elektronički vremenski žig još uvijek smatraju sigurnim.

3.9. Raspoloživost usluge

Fina kao pružatelj usluga izdavanja kvalificiranih elektroničkih vremenskih žigova jamči kontinuiranu dostupnost usluge izdavanja elektroničkih vremenskih žigova i javno objavljenih uvjeta pružanja usluge.

U slučaju ispada, odnosno nedostupnosti produkcijskog Fina QTSA 2017 servisa na primarnoj lokaciji, maksimalno vrijeme za oporavak Fina QTSA 2017 servisa na sekundarnoj lokaciji je u skladu s planom kontinuiteta poslovanja.

3.10. Izdavanje nekvalificiranih elektroničkih vremenskih žigova

TSU jedinice Fina QTSA 2017 servisa za izdavanje kvalificiranih elektroničkih vremenskih žigova izdaju samo kvalificirane elektroničke vremenske žigove.

3.11. Transportni protokol za uslugu izdavanja elektroničkih vremenskih žigova

Fina QTSA 2017 servis koristi siguran HTTPS protokol (TLS).

4. OPERATIVNI ZAHTJEVI NA ŽIVOTNI CIKLUS CERTIFIKATA Fina QTSA 2017

4.1. Izdavanje certifikata

Zahtjev za inicijalno generiranje para TSU ključeva i izdavanje pripadajućeg TSU certifikata za Fina QTSA 2017 servis podnosi ovlaštena osoba u Fina PKI. Zahtjev odobrava ovlaštena osoba u Fina PMA.

Zahtjev za obnovu TSU certifikata za Fina QTSA 2017 servis s generiranjem novog para TSU ključeva podnosi ovlaštena osoba u Fina PKI. Zahtjev odobrava ovlaštena osoba u Fina PMA.

Izdavanje Fina QTSA 2017 certifikata obavljaju ovlaštene osobe Fina PKI s povjerljivim ulogama, sukladno Tablici 5.2. u točki 5.2.2. ovog QTPS dokumenta, pod minimalno dualnom kontrolom u Fina PKI štićenom prostoru opisanom u točki 5.1.1. ovog QTPS dokumenta.

Fina objavljuje izdani TSU certifikat za Fina QTSA 2017 servis na internetskim stranicama Fina QTSA repozitorija iz točke 2.2. ovog QTPS dokumenta.

4.2. Opoziv i suspenzija certifikata

Opoziv certifikata za Fina QTSA 2017 servis provodi se sukladno niže navedenim točkama.

Suspenzija certifikata za Fina QTSA 2017 servis nije dozvoljena.

4.2.1. Razlozi za opoziv

Fina QTSA 2017 certifikat opoziva se iz sljedećih razloga:

- u slučaju kompromitiranja privatnog ključa ili ako se pojavi osnovana sumnja da je privatni ključ kompromitiran,
- ako neka od informacija sadržanih u certifikatu postane netočna,
- u slučaju trajne nedostupnosti ili gubitka privatnog ključa,
- u slučaju zabranjene uporabe privatnog TSU ključa,
- u slučaju da certifikat više nije sukladan s općim pravilima ili QTPS dokumentom prema kojima je bio izdan,
- ako certifikat nije izdan sukladno zahtjevu,
- ako Fina procjeni da Fina QTSA 2017 certifikat svojim tehničkim karakteristikama, profilom ili sadržajem ne pruža prikladnu razinu povjerenja Pouzdajućim stranama,
- u slučaju da korišteni kriptografski algoritmi i parametri prestanu pružati zahtijevanu sigurnost i zaštitu,
- ako Fina QTSA 2017 prestaje s radom, a Fina nije u mogućnosti osigurati nastavak pružanja QTS usluga kod drugog kvalificiranog pružatelja usluga,
- u slučajevima kada to nalaže zakon ili drugi propis.

4.2.2. Tko može tražiti opoziv

Zahtjev za opoziv Fina QTSA 2017 certifikata podnosi ovlaštena osoba u Fina PKI. Zahtjev odobrava ovlaštena osoba u Fina PMA.

Zahtjev za opoziv Fina QTSA 2017 certifikata u slučaju kompromitiranja privatnog TSU ključa, katastrofe ili prestanka pružanja usluga izdavanja elektroničkih vremenskih žigova podnosi ovlaštena osoba u Fina PKI. Odobrenje zahtjeva za opozivom daje Fina PMA.

Nakon odobrenja zahtjeva za opozivom Fina QTSA 2017 certifikata ovlaštene osobe s povjerljivim ulogama u Fina PKI sukladno Tablici 5.2. iz točke 5.2.2. u Fina PKI štićenom prostoru iz točke 5.1.1. ovog QTPS dokumenta obavljaju opoziv TSU certifikata za Fina QTSA servis.

Fina će opozivati TSU certifikat za Fina QTSA servis u roku navedenom u zahtjevu za opoziv certifikata. Ako takav rok u zahtjevu nije naveden Fina će certifikat opozvati u najkraćem razumnom roku, a najkasnije u roku od 24 sata od primitka odobrenog zahtjeva za opoziv.

4.2.3. Učestalost izdavanja CRL

Fina RDC 2015 CA izdaje i potpisuje Fina RDC 2015 CRL.

CRL se objavljuje odmah po opozivu certifikata te svakih šest sati od zadnjeg izdavanja CRL. Vrijeme u kojem najkasnije mora biti izdana sljedeća CRL (vrijednost polja *Next Update*) je 24 sata od zadnjeg izdavanja CRL.

4.2.4. Maksimalno kašnjenje za CRL

Maksimalno kašnjenje CRL od trenutka njenog izdavanja do trenutka objave u redovitim uvjetima iznosi manje od 30 sekundi.

4.2.5. Zahtjevi za *online* provjeru statusa opozvanosti certifikata

Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi podržavaju *online* provjeru statusa opozvanosti izdanih certifikata putem Fina OCSP servisa čiji je rad usklađen s preporukom IETF RFC 6960 [16].

Informacija o statusu opozvanosti certifikata korištenjem Fina OCSP servisa dostupna je u realnom vremenu.

Adresa Fina OCSP servisa je http://ocsp.fina.hr, a upisuje se u ekstenziji *Authority Information Access* svakog certifikata koje izdaju CA-ovi navedeni u ovoj točki.

Za korištenje Fina OCSP servisa Pouzdajuća strana treba imati aplikacijsko rješenje koje može koristiti OCSP servis, sukladan s preporukom IETF RFC 6960 [16], uporabom GET i POST metode.

4.2.6. Drugi dostupni načini objave opozvanih certifikata

Nema odredbi.

4.2.7. Dostupnost usluga

Dostupnost CRL i OCSP servisa je 24 sata na dan, 7 dana u tjednu. U slučaju ispada sustava, nastanka okolnosti koje su izvan kontrole Fine ili uslijed utjecaja više sile, usluge će biti dostupne u skladu s planom kontinuiteta poslovanja.

4.3. Kraj korištenja

Sukladno Uvjetima pružanja usluga izdavanja elektroničkih vremenskih žigova Korisnici sklapaju s Finom Ugovor o pružanju usluga izdavanja elektroničkih vremenskih žigova na neodređeno vrijeme. Ugovor može prestati otkazom, raskidom, sporazumom ili istekom, opozivom ili suspenzijom i posljednjeg certifikata temeljem kojeg je Korisnik pristupao Fina QTSA 2017 servisu.

5. PROVJERA SUSTAVA, UPRAVLJANJA I RADNIH POSTUPAKA

Fina osigurava primjerenu zaštitu imovine koja se upotrebljava za pružanje usluga izdavanja elektroničkih vremenskih žigova te u tu svrhu vodi cjelokupni popis te imovine s pripadajućom klasifikacijom koja je sukladna procjeni rizika.

Mjere fizičke zaštite, postupci koje Fina primjenjuje u zaštiti sustava za izdavanje elektroničkih vremenskih žigova kao i postupci provjere tog sustava, upravljanja i radnih postupaka u Fina PKI interne su prirode te se njihovi detalji ne objavljuju javno.

5.1. Mjere fizičke zaštite

Fina kao pružatelj usluga povjerenja primjenjuje mjere fizičke zaštite Fina QTSA 2017 sustava s ciljem minimiziranja rizika vezanih uz fizički zaštitu i u skladu s poslovnom politikom Fine, važećom zakonskom regulativom i međunarodnim preporukama.

Fina primjenjuje mjere fizičke zaštite sustava izdavanja kvalificiranih elektroničkih vremenskih žigova zbog ograničavanja pristupa hardverskim i softverskim komponentama sustava kao i zbog ograničavanja pristupa povjerljivim podacima.

5.1.1. Lokacija objekta i njegova konstrukcija

Primarni produkcijski Fina QTSA 2017 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 Fina QTSA 2017 sustav namijenjen je za preuzimanje funkcija primarnog produkcijskog Fina QTSA 2017 sustava u slučaju prestanka rada primarnog produkcijskog sustava do njegovog oporavka te ponovnog uspostavljanja njegovih servisa. Sekundarni Fina QTSA 2017 sustav smješten je na izdvojenoj udaljenoj lokaciji Fine i u odnosu na primarni sustav udovoljava jednakim ili višim sigurnosnim zahtjevima.

Fina PKI štićeni prostor interno je podijeljen na sigurnosne zone.

Sigurnosne zone u kojima se nalaze komponente Fina QTSA 2017 sustava na primarnoj i sekundarnoj lokaciji u daljnjem tekstu nazivaju se zajedničkim nazivom Fina PKI štićeni prostor.

5.1.2. Fizički pristup

Fizički pristup Fina QTSA 2017 sustavu u Fina PKI štićenom prostoru i pripadnim sigurnosnim zonama unutar tog prostora ostvaruje se uz dualnu kontrolu ovlaštenih osoba Fina PKI, a u skladu s njihovim ulogama i ovlastima.

Osobama koje nemaju ovlaštenje fizičkog pristupa sustavima u Fina PKI štićenom prostoru pristup je dozvoljen samo u pratnji i uz cjelovremeni nadzor ovlaštenih osoba Fina PKI uz njihovu dualnu kontrolu, a u skladu s Fininim internim procedurama. Za vrijeme boravka osoba koje nemaju ovlaštenje fizičkog pristupa sustavima u Fina PKI štićenom prostoru ne provode se postupci koji bi tim osobama mogli otkriti povjerljive informacije.

O svakom pristupu Fina QTSA 2017 sustavu vodi se evidencija.

Oprema, informacije, mediji i softver iz Fina PKI štićenog prostora iznosi se isključivo uz sudjelovanje i minimalno dualnu kontrolu ovlaštenih osoba u Fina PKI kojima su dodijeljene

odgovarajuće povjerljive uloge, i uz prethodno ovlaštenje. Pri tome se vodi računa o propisnoj zaštiti ili uništavanju podataka prije njihova iznošenja, a sukladno internim procedurama.

Fizički pristup Fina QTSA 2017 sustavu u Fina PKI štićenom prostoru može se ostvariti jedino prolaskom kroz pristupne zone.

Pristup arhivskom prostoru u kojem se arhivira papirnata dokumentacija Fina PKI imaju samo ovlaštene osobe Fine. Arhivski prostor Fine opremljen je sustavom video nadzora i pod stalnim je nadzorom zaštitarske tvrtke.

5.1.3. Sustavi za napajanje i klimatizaciju

Uređaji i prostor u kojem se nalazi Fina QTSA 2017 sustav, Fina RA sustav i repozitorij te sustavi tehničke zaštite opskrbljeni su neprekidnim napajanjem električnom energijom i klimatizacijom koja je dimenzionirana na način koji osigurava odgovarajuće radne uvjete i u slučaju prekida vanjskog napajanja.

Rezervno napajanje električnom energijom osigurano je uređajem za neprekidno napajanje u kombinaciji s dizel agregatom koje omogućuje neprekidan i pouzdani rad Fina QTSA 2017 sustava do ponovne uspostave primarnog napajanja.

U svim prostorijama u kojima se nalazi oprema Fina QTSA 2017 sustava postavljeni su klima uređaji za održavanje propisanog radnog okruženja.

5.1.4. Opasnost od poplave

Oprema Fina QTSA 2017 sustava smještena je na lokacijama koje su osigurane od poplave i smještena je na povišenim podovima.

5.1.5. Protupožarna zaštita

Automatski sustav za detekciju i zaštitu od požara unutar Fina PKI štićenog prostora instaliran je u skladu s pravilima protupožarne zaštite. Automatski sustav koristi sredstva za gašenje koja su primjenjiva za gašenje požara na električnim instalacijama i IT opremi. Fina PKI štićeni prostor ima stabilni sustav za dojavu požara i detektore požara.

Prostori u Fina RA mreži štite se u skladu s odredbama Fininog internog pravilnika o zaštiti od požara.

Arhivski prostor Fine u kojem se čuva papirnata arhiva Fina PKI opremljen je vatrodojavnim sustavom i štiti se u skladu s odredbama Fininog internog pravilnika o zaštiti od požara.

5.1.6. Pohrana medija

Mediji na kojima se nalaze arhivske i sigurnosne kopije Fina QTSA 2017 podataka u elektroničkom obliku, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na dvije odvojene štićene lokacije na siguran način kako bi se zaštitili od oštećenja, otuđenja ili neovlaštenog pristupa. Mediji s podacima se pohranjuju u Fina PKI štićenom prostoru primarnog produkcijskog sustava te na pričuvnoj lokaciji.

Za rad sa sigurnosnim kopijama podataka ovlaštene su osobe s povjerljivim ulogama Operater sustava.

5.1.7. Zbrinjavanje otpada

Dokumenti i podaci u papirnatom i elektroničkom obliku koji se nalaze u Fina PKI štićenom prostoru ili sadržavaju povjerljive informacije, 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 Fina PKI.

Svi se povjerljivi dokumenti i podaci prije odlaganja u otpad na mjestu nastanka fizički uništavaju na način da se ovako uništene informacije ne mogu rekonstruirati.

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

Uništavanje medija na kojima se nalaze povjerljivi podaci te uništavanje podataka i ključeva povezanih s HSM modulima provodi se sukladno Fininim internim procedurama. Takvo brisanje i uništavanje podataka HSM modula provodi se i prije njihovog eventualnog slanja na servis ili popravak.

Fina zbrinjava sve vrste otpada koji nastaje unutar prostorija i poslovnih prostora Fine u skladu s internim radnim uputama i procedurama za ekološko zbrinjavanje otpada.

5.1.8. Sigurnosne kopije na drugoj lokaciji

Sigurnosne kopije Fina QTSA 2017 sustava, središnjeg Fina RA sustava, sadržaja repozitorija i arhive u elektroničkom obliku, sigurnosne kopije programske opreme pohranjuju se na sekundarnoj lokaciji iz točke 5.1.1. ovog QTPS dokumenta.

Sigurnosne kopije koje se pohranjuju u Fina PKI štićenom prostoru na pričuvnoj lokaciji se, u odnosu na njihove izvornike, čuvaju uz primjenu jednake ili više razine sigurnosti primijenjenih mjera fizičke zaštite.

5.2. Organizacijske mjere zaštite

5.2.1. Povjerljive uloge

Upravljanje informacijskim i komunikacijskim sustavom, sustavom izdavanja elektroničkih vremenskih žigova, administriranje i implementacije sigurnosnih postupaka te nadzor djelovanja Fina QTSA obavlja se u unutar odvojenih organizacijskih dijelova Fine.

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

Povjerljive uloge dodjeljuju se ovlaštenim osobama po pravilima koja osiguravaju da jedna osoba sama ne može zaobići sigurnosne mjere ili ugroziti sigurnost i pouzdanost Fina QTSA 2017 sustava.

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

Opis povjerljivih uloga te pripadni opis poslova, ovlasti i odgovornosti koje obavlja pojedina uloga opisani su u internim dokumentima Fine. U pripadajućim popisima za svaku ulogu navedeni su djelatnici Fine kojima je ta uloga dodijeljena.

5.2.2. Broj osoba potrebnih za obavljanje aktivnosti

Fina ima stalno zaposlen dovoljan broj stručnih osoba sa znanjem, iskustvom i kvalifikacijama koji je potreban u Fina PKI za pružanje usluga iz opsega ovih ovog QTPS dokumenta.

Pristup i rad u štićenom Fina PKI prostoru provodi se isključivo uz istovremenu prisutnost najmanje dvije ovlaštene osobe Fina PKI koje imaju dozvole pristupa sustavu smještenom u štićenom Fina PKI prostoru.

Potreban broj djelatnika s pripadnim povjerljivim ulogama za obavljanje pojedinih zadataka na Fina QTSA 2017 sustavu naveden je u odgovarajućoj internoj dokumentaciji Fine.

5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu

Prilikom prijave na kritične aplikacije i servise unutar Fina PKI provodi se identifikacija i potvrda identiteta osobe koja pristupa aplikaciji ili servisu. Identifikacija i potvrda identiteta osobe provodi se odgovarajućom metodom autentikacije. Pristup i korištenje aplikacija i servisa unutar Fina PKI omogućen je samo ovlaštenim osobama sukladno povjerljivoj ulozi koju obnašaju.

Identifikacija ovlaštenih osoba Fina PKI i određivanje prava pristupa za obavljanje pojedinih zadataka u Fina PKI provodi se kroz sigurnosne procedure i postupke provjere.

Ovlaštene osobe s povjerljivim ulogama u Fina PKI moraju se autenticirati prije bilo kojeg pristupa Fina CA, Fina QTSA i/ili Fina RA sustavu. U tu svrhu ovlaštene osobe Fina PKI dobivaju odgovarajuća sredstva za autentikaciju. Prije dobivanja sredstva za autentikaciju navedeno osoblje mora zadovoljiti zahtjeve navedene u točki 5.3. ovog QTPS dokumenta.

Sredstva za autentikaciju su:

- kartice kontrole prolaza za ulazak u Fina PKI štićene sigurnosne zone iz točke 5.1.1. ovog QTPS dokumenta,
- certifikati na sigurnim kriptografskim ili QSCD uređajima,
- korisničko ime i zaporka ili digitalni certifikat na sigurnom kriptografskom ili QSCD uređaju za prijavu na operacijske sustave Fina QTSA 2017 sustava,
- upravljačke kartice kriptografskog modula koje smiju dobiti samo ovlaštene osobe u Fini s povjerljivim ulogama u Fina PKI, sukladno ulogama iz točke 5.2.1. ovog QTPS dokumenta.

Svako od navedenih sredstava za autentikaciju posebno je personalizirano za određenu ovlaštenu osobu. Uporaba navedenih sredstava za autentikaciju je ograničena na zadatke i sustav za koje je autorizirana određena povjerljiva uloga.

Službenik za sigurnost odgovoran je za utvrđivanje valjanosti identiteta djelatnika s povjerljivom ulogom u Fina PKI.

Tijekom korištenja kritičnih aplikacija i servisa aktivnosti prijavljene osobe propisno se bilježe, spremaju i čuvaju.

5.2.4. Uloge koje zahtijevaju odvajanje dužnosti

Opis poslova ovlaštenog osoblja s povjerljivim ulogama na Fina QTSA 2017 sustavima temelji se na načelu odvajanja dužnosti i dodjele minimalnih korisničkih prava koja omogućuju nesmetano obavljanje dodijeljenih poslova.

Kod odvajanja uloga primjenjuju se sljedeća pravila:

- Službeniku za sigurnost i Službeniku za registraciju ne smije biti dodijeljena povjerljiva uloga Službenika za nadzor sustava,
- Administrator sustava ne smije biti dodijeljena uloga Službenika za sigurnost ili povjerljiva uloga Službenika za nadzor sustava.

5.3. Osoblje

5.3.1. Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

Pri zapošljavanju osoblja na poslovima u Fina PKI uzimaju se u obzir zahtjevi za odgovarajućom stručnom spremom za svaku povjerljivu ulogu.

Prije početka rada u Fina PKI kandidati moraju posjedovati odgovarajuća stručna znanja, iskustvo, kvalifikacije i edukacije u radu s kriptografskim tehnologijama, zaštitom računalnih sustava, informacijskom sigurnošću te zaštitom osobnih podataka u domeni vlastitog djelokruga rada u okviru poslova Fina PKI.

Prilikom zapošljavanja novih djelatnika, Fina provodi testiranje u cilju procjene njihove kvalitete i kompetencija za obavljanje povjerljivih uloga u Fina PKI sustavu.

Fina PKI osoblje s povjerljivim ulogama ne smije biti ni u kakvom sukobu interesa koji bi ugrozio rad Fina PKI sustava.

5.3.2. Procedure provjere prikladnosti osoblja

Prije zapošljavanja kandidata na poslovima Fina PKI, Fina provodi psihološko testiranje osoblja kako bi se ocijenila njihova primjerenost u skladu s potrebama poslova koje će obavljati.

Fina PKI osoblje prije zaposlenja u Fina PKI dostavlja uvjerenje o nekažnjavanju izdano od nadležnog Općinskog suda kojim se potvrđuje da se protiv fizičke osobe ne vodi kazneni postupak, da nije doneseno rješenje o istrazi, nije podignuta optužnica koja je stala na pravnu snagu, nije donesena nepravomoćna presuda po optužnom prijedlogu i nije izdan kazneni nalog.

Svaki zaposlenik Fine potpisivanjem ugovora o radu obvezuje se na čuvanje poslove tajne.

5.3.3. Zahtjevi za školovanjem

Osoblje u Fina PKI prije početka obavljanja poslova u Fina PKI, prolaze edukaciju sukladno poslovima koje će obavljati.

Fina PKI osoblju s povjerljivim ulogama u radu na Fina QTSA 2017 sustavu osigurava se edukacija i usavršavanje sukladno njihovim povjerljivim ulogama.

Edukacija i usavršavanje osoblja s povjerljivim ulogama u radu na Fina QTSA sustavu obuhvaća:

- Fina QTSA, Fina CA i Fina RA sigurnosni principi i mehanizmi,

- svjesnost o sigurnosti,
- QTSA softver koji je u uporabi u Fina QTSA 2017 sustavu,
- zadaci povezani s povjerljivim ulogama koje će obavljati na Fina QTSA 2017 sustavu,
- postupci oporavka od nezgode i nastavka poslovanja.

Edukacija Službenika za registraciju u Središnjem Fina RA i Službenika za registraciju u Fina LRA uključuje:

- osnovno o certifikatima i elektroničkim vremenskim žigovima,
- načini registracije Korisnika,
- uobičajene prijetnje u procesu provjere informacija,
- ako je primjenjivo, rad u Fina RA i Fina CMS aplikacijama,
- svjesnost o sigurnosti,
- zaštita osobnih podataka,
- informacije s kojima je potrebno upoznati Korisnike.

5.3.4. Periodičko obnavljanje znanja i osvješćivanje

Osvješćivanje o informacijskoj sigurnosti provodi se jednom godišnje za sve zaposlenike Fina PKI.

Osobe s povjerljivim ulogama u Fina PKI su odgovorne usavršavati svoje vještine i stjecati nova znanja iz svog područja rada samostalnom edukacijom ili organiziranim internim i vanjskim edukacijama, a o čemu se vodi evidencija.

Obnova znanja osoblja Fina RA mreže, a obzirom na poslove koje obavljaju, provodi se redovito, najmanje jednom godišnje.

5.3.5. Učestalost i slijed izmjene zaposlenika

Ne primjenjuje se.

5.3.6. Kazne za neovlaštene radnje

Nepridržavanje propisanih mjera za ovlaštene osobe pri radu u Fina PKI podliježe povredi radne obveze, a eventualne kaznene mjere određuju se disciplinskim postupkom.

U slučaju neovlaštenih radnji od strane ugovornih partnera primijenit će se odredbe definirane ugovorom s ugovornim partnerom.

5.3.7. Zahtjevi na vanjske suradnike

Zahtjevi za dobavljače roba i usluga za Fina PKI regulirani su internim dokumentima o radu s dobavljačima. Pristup vanjskih suradnika informacijskoj imovini u Fina PKI odobrava se isključivo temeljem ugovora za samo onu informacijsku imovinu koja je predmet ugovora i samo za aktivnosti navedene u ugovoru.

5.3.8. Dokumentacija koja je dostupna osoblju

Svakom zaposleniku dostupna je dokumentacija potrebna za obavljanje njegovih radnih zadataka, koja uključuje interne i vanjske materijale za edukaciju, te radne upute i procedure za obavljanje pojedinih poslova u Fina PKI, sukladno dodijeljenoj povjerljivoj ulozi i pripadnim ovlaštenjima.

5.4. Postupci upravljanja revizijskim zapisima

5.4.1. Tipovi događaja koji se zapisuju

Svi važni događaji u Fina QTSA 2017 sustavu zapisuju se kao revizijski zapisi u elektroničkom ili papirnatom obliku. Revizijski zapisi sadrže podatak o vrsti događaja, datum i vrijeme događaja te podatak o uspješnosti ili neuspješnosti događaja kojeg se prati.

Podatak o datumu i vremenu u revizijskim zapisima događaja u elektroničkom obliku Fina PKI usklađen je s NTP poslužiteljem koji je sinkroniziran s izvorom točnog vremena te ima odstupanje manje od +/- 1 s u odnosu na UTC vrijeme.

Za Fina QTSA 2017 sustav u Fina PKI zapisuju se u elektroničkom ili papirnatom obliku revizijski zapisi događaja vezanih uz:

- upravljanje životnim ciklusom TSU ključeva,
- upravljanje životnim ciklusom TSU certifikata,
- upravljanje životnim ciklusom HSM modula kojim je zaštićeni privatni TSU ključ Fina QTSA 2017,
- sinkronizaciju TSU sata s UTC vremenom,
- detekciju ispada iz sinkroniziranosti s UTC vremenom,
- registraciju fizičke osobe i poslovnog subjekta,
- izdavanje elektroničkih vremenskih žigova,
- sigurnosne događaje, uključujući događaje podizanja i spuštanja sustava, ispada sustava i kvara hardvera te izmjene sigurnosnih postavki sustava.

Podaci i događaji koji se zapisuju u dnevnicima Fina PKI sustava detaljnije su navedeni i opisani u internim dokumentima Fine.

5.4.2. Učestalost obrade revizijskih zapisa

Postupak pregleda revizijskih zapisa Fina QTSA 2017 sustava obuhvaća:

- pregled revizijskih zapisa koji su stvoreni nakon posljednje revizije,
- po potrebi, pripremu sažetog izvještaja koji sadrži objašnjenja važnih događaja.

Ovi pregledi uključuju provjeru oštećenosti revizijskih zapisa i kratku kontrolu zapisa, s podrobnijim istraživanjem neregularnih evidentiranih događaja.

Preglede revizijskih zapisa Fina QTSA 2017 sustava i pripadajućeg HSM modula obavlja Službenik za nadzor sustava. Pregledi revizijskih zapisa Fina QTSA 2017 sustava i pripadajućeg HSM modula obavljaju se redovito, jednom dnevno radnim danima, te u slučaju izvanrednih situacija. O obavljenom pregledu ovih revizijski zapisa vodi se evidencija u papirnatom ili elektroničkom obliku, a vodi je osoba s povjerljivom ulogom Službenik za nadzor sustava.

Analiza ostalih revizijskih zapisa obavlja se po potrebi, a provodi je ovlašteno osoblje Fina PKI.

U slučaju detektiranja nepravilnosti ili pogreške koje se odnose na sigurnost, ovlaštena osoba za pregled revizijskih zapisa sustav izrađuje izvještaj o analizi revizijskih zapisa i daljnjim potrebnim aktivnostima. U slučaju otkrivanja neautorizirane aktivnosti, postupa se u skladu s Fininim internim procedurama.

Sve radnje poduzete na osnovi analize revizijskih zapisa moraju se dokumentirati.

5.4.3. Vremenski period pohrane revizijskih zapisa

Revizijski zapisi Fina QTSA 2017 sustava iz točke 5.4.1. ovog QTPS dokumenta čuvaju se najmanje 10 godina od izdavanja elektroničkog vremenskog žiga na kojeg se zapisi odnose.

5.4.4. Zaštita revizijskih zapisa

Revizijski zapisi Fina QTSA 2017 sustava zaštićuju se mehanizmima i postupcima koji osiguravaju povjerljivost i cjelovitost zapisa te ne dozvoljavaju njihovu izmjenu, kao ni jednostavno brisanje ili uništenje zapisa.

Povjerljivost revizijskih zapisa Fina QTSA 2017 sustava osigurava se kontrolom pristupa sustavu i pravom za čitanje zapisa.

Pristup revizijskim zapisima ograničen je na ovlašteno Fina PKI osoblje, odnosno na osobe s povjerljivim ulogama, s kombinacijom kontrola fizičkog pristupa Fina PKI štićenom prostoru i sigurnosnih kontrola pristupa podacima sustava.

Revizijski zapisi svih sustava u Fina PKI koji sadrže podatke navedene u točki 5.4.1. ovog QTPS dokumenta se, nakon perioda čuvanja na sustavima gdje su nastali, arhiviraju i štite sukladno postupcima opisanim u točki 5.5.3. ovog QTPS dokumenta.

Revizijski zapisi koji se vode u papirnatom obliku štite se od neovlaštenog pregleda, brisanja, izmjene ili uništenja korištenjem uobičajenim metoda za zaštitu papirnate dokumentacije.

Revizijski zapisi koji se vode u papirnatom obliku, kao što je Evidencija za praćenje ulazaka i izlazaka iz Fina PKI štićenog prostora, štite se od neovlaštenog pregleda, brisanja, izmjene ili uništenja korištenjem uobičajenim metoda za zaštitu papirnate dokumentacije.

5.4.5. Postupci izrade sigurnosnih kopija revizijskih zapisa

Novonastali revizijski zapisi kopiraju se na dnevnoj razini te se njihove kopije pohranjuju i čuvaju unutar primarnog produkcijskog Fina PKI štićenog prostora. Dodatno, kopije datoteka revizijskih zapisa u Fina PKI se na medijima za pohranu podataka pohranjuju u sekundarni štićeni prostor na pričuvnoj lokaciji, sukladno točki 5.1.8. ovog QTPS dokumenta.

Postupci izrade sigurnosnih kopija revizijskih zapisa detaljnije su opisani u internim dokumentima Fine.

5.4.6. Sustav prikupljanja revizijskih zapisa (unutarnji ili vanjski)

Sustav prikupljanja revizijskih zapisa svih sustava u Fina PKI je interni sustav na kojem se revizijski zapisi prikupljaju kombinacijom automatskih i manualnih procesa koji se izvode na Fina PKI poslužiteljima i koje pokreće, odnosno nadgleda Fina PKI osoblje s povjerljivim ulogama.

Manualni procesi prikupljanja dnevnika sustava odnose se na vođenje Evidencije za praćenje ulazaka i izlazaka iz Fina PKI štićenog prostora.

5.4.7. Obavještavanje subjekta uzročnika događaja

U slučaju uočavanja zapisa o značajnom događaju u radu Fina PKI koji je povezan s određenim subjektom Fina zadržava pravo odlučiti o obavještavanju subjekta ili Korisnika koji je taj događaj uzrokovao.

5.4.8. Procjena ranjivosti

Fina obavlja redovitu procjenu rizika informacijske imovine, procjenu ranjivosti za prepoznate javne i privatne adrese te penetracijsko testiranje.

Procjena rizika informacijske imovine provodi se jednom godišnje. Procjena ranjivosti sustava za prepoznate javne i privatne adrese Fina PKI provodi se kvartalno. Penetracijski test provodi se jednom godišnje. Procjene rizika i ranjivosti te penetracijski test provode se i nakon značajnih promjena.

Svaku novu kritičnu ranjivost Fina će razmotriti i za svaku takvu ranjivost, za koju se utvrdi potencijalni utjecaj, Fina će u roku od 48 sati od njezina saznanja postupiti na jedan od sljedećih načina:

- ukloniti ranjivost, ili
- ako uklanjanje ranjivosti u roku od 48 sati od njezina saznanja nije moguće, izraditi i provesti plan uklanjanja ranjivosti, ili
- dokumentirati činjeničnu osnovu na temelju koje je utvrđeno da ranjivost ne zahtijeva uvođenje dodatnih mjera za njeno uklanjanje.

5.5. Arhiviranje zapisa

5.5.1. Tipovi arhiviranih zapisa

Fina QTSA 2017 arhivira niže navedene podatke koji, ovisno o tipu, mogu biti u elektroničkom i/ili papirnatom obliku:

- opća pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova,
- pravilnici o postupcima izdavanja kvalificiranih elektroničkih vremenskih žigova,
- uvjeti pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova,
- pristupnice za servis izdavanja kvalificiranih elektroničkih vremenskih žigova,
- podaci i pripadajuća dokumentacija prikupljena postupkom registracije fizičkih osoba i poslovnih subjekata,
- revizijski zapisi Fina QTSA 2017 sustava iz točke 5.4.1. ovog QTPS dokumenta,
- drugi Finini interni dokumenti.

Ugovor o pružanju usluge izdavanja kvalificiranih elektroničkih vremenskih žigova sastoji se od pristupnice za servis izdavanja kvalificiranih elektroničkih vremenskih žigova, Uvjeta pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova i općih pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova. Arhiviranje ovog ugovora ostvaruje se arhiviranjem dokumenata od kojih se on sastoji.

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

Detaljnije odredbe koje se odnose na tipove arhiviranih zapisa nalaze se u internoj dokumentaciji Fine.

5.5.2. Vremenski period arhiviranja

Sve arhivirane podatke i dokumentaciju Fina čuva najmanje 10 godina od izdavanja elektroničkog vremenskog žiga na kojeg se odnose.

5.5.3. Zaštita arhive

Arhivirana dokumentacija Fina QTSA 2017 sustava u papirnatom obliku čuva se u Fina PKI štićenom prostoru koji je opisan u točki 5.1.1. ovog QTPS dokumenta. Arhivirani zapisi su na zahtjev raspoloživi samo ovlaštenim osobama Fina PKI, uz dualnu kontrolu.

Arhivirana dokumentacija u papirnatom obliku koja je prikupljena u postupku registracije fizičkih osoba i poslovnih subjekata čuva se u štićenom arhivskom prostoru Fine koji je pod stalnim nadzorom službe tjelesne zaštite, a pristup arhiviranoj dokumentaciji omogućen je samo ovlaštenim osobama Fina PKI i djelatnicima zaduženim za arhivu Fine. Na ovaj način arhiva se štiti od neovlaštenog pregleda, izmjene i brisanja.

Arhivirani zapisi u elektroničkom obliku iz točke 5.5.1. ovog QTPS dokumenta čuvaju se na odgovarajućim medijima za arhiviranje podataka u Fina PKI štićenom prostoru koji je opisan u točki 5.1.1. Arhivirani zapisi štite se mehanizmima i postupcima koji osiguravaju povjerljivost i cjelovitost zapisa te ne dozvoljavaju izmjenu zapisa, kao ni jednostavno brisanje ili uništenje zapisa. Povjerljivost arhiviranih zapisa u elektroničkom obliku štiti se enkripcijom, a cjelovitost zapisa štiti se digitalnim potpisom. Arhivirani zapisi su na zahtjev raspoloživi samo ovlaštenim osobama Fina PKI, uz dualnu kontrolu. Minimalno jednom godišnje Fina PKI osoblje provjerava integritet arhive, te ako je arhiva oštećena, ona se obnavlja pomoću sigurnosne kopije.

Arhivirani Fina PKI dokumenti dostupni su ovlaštenim osobama, a na zahtjev su raspoloživi za potrebe pravnih postupaka u svrhu pružanja dokaza o ispravnom pružanju usluga.

5.5.4. Postupci izrade sigurnosnih kopija arhive

Sigurnosne kopije arhiviranih zapisa u elektroničkom obliku iz točke 5.5.1. ovog QTPS dokumenta čuvaju se u sekundarnom Fina PKI štićenom prostoru na pričuvnoj lokaciji iz točke 5.1.1. ovog QTPS dokumenta koji ima jednaku ili višu razinu zaštite u odnosu na Fina PKI štićeni prostor na primarnoj lokaciji.

Pristup sigurnosnim kopijama arhiviranih zapisa u elektroničkom obliku ima samo ovlašteno osoblje Fina PKI, uz dualnu kontrolu.

5.5.5. Zahtjevi na zaštitu zapisa elektroničkim vremenskim žigom

Nema odredbi.

5.5.6. Sustav prikupljanja arhivskih zapisa (unutarnji ili vanjski)

Arhivirani zapisi prikupljaju se na način koji ovisi o vrsti podataka i dokumenata.

Dokumentacija Fina QTSA 2017 sustava u papirnatom obliku prikuplja se manualno i arhivira se interno.

Zapisi u elektroničkom obliku iz točke 5.5.1. ovog QTPS dokumenta prikupljaju se automatski te se arhiviraju interno u Fina PKI štićenom prostoru na primarnoj lokaciji te u sekundarnom štićenom prostoru na pričuvnoj lokaciji iz točke 5.1.1. ovog QTPS dokumenta.

5.5.7. Postupci dobivanja i provjere arhiviranih zapisa

Pristup zapisima iz arhive imaju samo osobe ovlaštene za pristup podacima iz arhive. Pristup podacima arhiviranim u štićenim prostorima iz točke 5.1.1. ovog QTPS dokumenta imaju samo ovlaštene osobe Fina PKI, uz dualnu kontrolu.

Verifikacija podataka iz arhive obavlja se provjerom njihove cjelovitosti, npr. verifikacijom digitalnog potpisa kojim su arhivirani podaci potpisani.

Arhivirani podaci u elektroničkom obliku se po potrebi uspoređuju s pripadnom kopijom.

5.6. Promjena TSU ključa

Fina će dovoljno vremena prije isteka perioda važenja privatnog TSU ključa generirati novi par TSU ključeva za Fina QTSA 2017 sukladno točki 6.3.2. ovog QTPS dokumenta iz razloga očuvanja razine sigurnosti kriptografskog algoritma privatnog TSU ključa u uporabi.

Novi par TSU ključeva generira se na način opisan u točki 6.3.3. ovog QTPS dokumenta.

Novi TSU certifikat Fina QTSA 2017 s novo generiranim javnim ključem potpisuje se privatnim ključem Fina RDC 2015 CA.

O planiranoj promjeni TSU ključa Fina će pravovremeno obavijestiti sudionike Fina PKI objavom informacija na stranicama Fina PKI repozitorija iz točke 2.2. ovog QTPS dokumenta. Novi TSU certifikat za Fina QTSA 2017 dostupan je sudionicima Fina PKI putem javnog imenika i internetskih stranica repozitorija.

5.7. Oporavak od kompromitiranja ili nepogode

5.7.1. Postupci u slučaju incidenta ili kompromitiranja

Fina ima plan kontinuiteta poslovanja Fina PKI, a kojim su regulirani postupci u slučajevima:

- prirodnih katastrofa,
- napada, pljački ili blokade zgrade,
- uništenja IT infrastrukture na primarnoj produkcijskoj lokaciji,
- nedostupnost IT infrastrukture na primarnoj produkcijskoj lokaciji uslijed kvara hardvera ili softvera većih razmjera,
- nedostupnosti radnika,
- prekida usluga dobavljača,
- za događaje gubitka ili kompromitiranja ili sumnje u kompromitiranost privatnog TSU ključa za Fina QTSA 2017.

Internim planovima obuhvaćeni su i postupci koje treba poduzeti u cilju oporavka i uspostave prvotnih sigurnosnih prilika RA sustava, arhive i repozitorija.

Obavještavanje u slučaju gore navedenih nepogoda opisano je u odgovarajućim postupcima za slučajeve nepogoda.

Obavještavanje u slučaju kompromitiranja ili sumnje u kompromitiranost privatnog TSU ključa za Fina QTSA 2017 opisano je u točki 5.7.3. ovog QTPS dokumenta.

Plan kontinuiteta poslovanja revidira se jednom godišnje.

5.7.2. Postupci u slučaju oštećenja u računalnim resursima, programima i/ili podacima

Fina QTSA 2017 sustav zasnovan je na pouzdanim hardverskim i softverskim komponentama, a kritične operacije sustava podržane su redundantnim komponentama.

Funkcionalnost, ispravnost rada i pravovremeno otklanjanje oštećenja komponenti Fina QTSA 2017 sustava osigurano je kroz ugovore o podršci i održavanju s dobavljačima opreme.

Plan kontinuiteta poslovanja za Fina PKI regulira postupke oporavka FINA QTSA 2017 sustava u slučaju kvarova ili oštećenja opreme te povrat podataka.

Sigurnosne kopije elektroničkih zapisa nastalih u radu Fina PKI sustava izrađuju se na dnevnoj razini te se periodički dostavljaju u štićeni prostor na pričuvnoj lokaciji.

5.7.3. Postupci u slučaju kompromitiranja privatnog ključa i/ili gubitka kalibracije

U slučaju kompromitiranja privatnog TSU ključa Fina QTSA 2017 sustava Fina će odmah po saznanju prekinuti s uporabom kompromitiranog privatnog TSU ključa za Fina QTSA 2017 sustav te će ispitati okolnosti kompromitiranja ključa. Fina će obavijestiti sudionike da se u takvom slučaju podacima o opozvanosti ne mora nužno vjerovati.

Ako se potvrdi kompromitiranje ključa Fina PMA donosi odluku o opozivu Fina QTSA 2017 certifikata povezanog s kompromitiranim ključem.

O opozivu Fina QTSA 2017 certifikata Fina će obavijestiti sljedeće sudionike:

- Fina RA mrežu,
- Korisnike,
- Pouzdajuće strane.

Nakon ustanovljavanja i otklanjanja uzroka koji su prouzročili kompromitiranje TSU ključa, Fina će, ako je primjenjivo, poduzeti mjere za sprječavanje ponavljanja takvog događaja. Ovisno o utvrđenim uzrocima kompromitiranja TSU ključa Fina može donijeti odluku o privremenom prelasku na produkciju sa sekundarne lokacije.

Fina će za TSU čiji je privatni ključ kompromitiran provesti postupak generiranja novog para TSU ključeva te će Finino certifikacijsko tijelo Fina RDC 2015 CA za novi javni TSU ključ izdati novi Fina QTSA 2017 certifikat.

U slučaju da korišteni kriptografski algoritmi i parametri prestanu pružati zahtijevanu sigurnost i zaštitu Fina će, ukoliko je to moguće, pravodobno o tome obavijestiti:

- Fina RA mrežu,
- Korisnike,
- Pouzdajuće strane.

Fina će razmotriti mogućnost korištenja drugih odgovarajućih preporučenih sigurnijih kriptografskih algoritama te će, ukoliko to bude moguće, donijeti odluku o korištenju drugog algoritma. Fina će izraditi konkretne planove i postupke te će o njima i rokovima obavijestiti Korisnike i Pouzdajuće strane te će provest odgovarajuće aktivnosti u cilju nastavka pružanja usluge Korisnicima.

U slučaju nedostupnosti signala pouzdanog izvora UTC vremena distribuiranog iz referentnog UTC laboratorija, iz bilo kojeg razloga, Fina QTSA 2017 servis prestat će s izdavanjem elektroničkih vremenskih žigova sve do ponovne uspostave sinkronizacije putem satelitskog signala ili drugog adekvatnog načina sinkronizacije.

Fina će za sve Korisnike i Pouzdajuće strane putem internetskih stranica Fina PKI repozitorija iz točke 2.2. ovog QTPS dokumenta objaviti opis kompromitiranja ili gubitka kalibracije.

U slučaju većeg kompromitiranja rada QTSA 2017 ili gubitka kalibracije Fina će putem internetskih stranica Fina PKI repozitorija za sve Korisnike i Pouzdajuće strane objaviti informacije za jasnu identifikaciju izdanih elektroničkih vremenskih žigova koji sadrže neispravne podatke.

5.7.4. Mogućnost nastavka poslovanja nakon nepogode

U planu kontinuiteta poslovanja određeni su postupci za nastavak poslovanja nakon nepogode. Ovisno o vrsti nepogode Fina će pružanje usluge izdavanja elektroničkih vremenskih žigova nastaviti na svojem primarnom produkcijskom sustav ili će pružanje usluge nastaviti na svojem sekundarnom sustavu do oporavka svojeg primarnog produkcijskog sustava.

Strategijom kontinuiteta poslovanja regulirani su uvjeti i prijelaz pružanja usluga povjerenja na sekundarni Fina QTSA 2017 sustav iz točke 5.1.1. ovog QTPS dokumenta.

5.8. Prestanak rada Fina QTSA 2017

O planiranom prestanku pružanja usluga izdavanja elektroničkih vremenskih žigova Fina će:

- obavijestiti sve Korisnike usluge, Pouzdajuće strane i središnje tijelo državne uprave nadležno za poslove gospodarstva najmanje tri mjeseca prije planiranog prestanka pružanja usluga izdavanja elektroničkih vremenskih žigova,
- uložiti sav napor da kod drugog kvalificiranog pružatelja usluga povjerenja osigura nastavak pružanja usluga izdavanja elektroničkih vremenskih žigova te će tom pružatelju usluga dostaviti svu dokumentaciju prikupljenu u postupku registracije Korisnika kao i svu dokumentaciju o izdanim elektroničkim vremenskim žigovima,
- uništiti aktualni privatni ključ TSU i opozvati sve važeće Fina QTSA 2017 certifikate.

U slučaju prestanka pružanja usluga izdavanja elektroničkih vremenskih žigova Fina će arhivirati, zaštititi i čuvati zapise prema odredbama iz točke 5.5. ovog QTPS dokumenta kako bi ti zapisi bili raspoloživi za pružanje dokaza u sudskim, upravnim i drugim postupcima u skladu s važećim odredbama zakonske regulative, ili će Fina s drugim poslovnim subjektom ugovoriti takvo arhiviranje, zaštitu i čuvanje zapisa.

6. TEHNIČKE MJERE ZAŠTITE

6.1. Generiranje i instalacija para ključeva

6.1.1. Generiranje para TSU ključeva

Fina provodi generiranje para TSU ključeva za Fina QTSA 2017 sustav za izdavanje elektroničkih vremenskih žigova koristeći kriptografske algoritme za generiranje ključeva koji su sukladni s normizacijskim dokumentom ETSI TS 119 312 [12].

Kriptografski algoritmi koji se koristi za generiranje ključeva, kao i duljina ključeva za Fina QTSA 2017 odabrani su sukladno normizacijskom dokumentu ETSI TS 119 312 [12] tako da budu prikladni za cijelo vrijeme važenja Fina QTSA 2017 certifikata.

Par TSU ključeva za Fina QTSA 2017 sustav generira se u HSM modulu koji zadovoljava zahtjeve iz točke 6.2.1. ovog QTPS dokumenta.

Fina QTS sustav s pripadajućim HSM modulom nalazi se tijekom i nakon postupka generiranja para TSU ključeva u Fina PKI štićenom prostoru iz točke 5.1.1. ovog QTPS dokumenta, a pristup Fina QTSA 2017 sustavu dopušten je ovlaštenim osobama Fina PKI s povjerljivim ulogama, uz minimalno dualnu kontrolu.

U postupku generiranja para TSU ključeva za Fina QTSA 2017 servis sudjeluju ovlaštene osobe s povjerljivim ulogama u Fina QTSA sukladno tablici 5.4. u ovom QTPS dokumentu.

O provedenom generiranju TSU ključeva za Fina QTSA 2017 vodi se zapisnik.

6.1.2. Dostava javnog ključa CA-u

Javni TSU ključ Fina QTSA 2017 servisa internom se procedurom dostavlja u Fina RDC 2015 CA.

Javni TSU ključ dostavlja se na certifikaciju u Fina RDC 2015 CA na način koji osigurava provjeru cjelovitosti i izvornosti javnog ključa.

Postupak dostave javnog TSU ključa provode ovlaštene osobe s povjerljivim ulogama u Fina PKI unutar Fina PKI štićenog prostora, uz minimalno dualnu kontrolu.

6.1.3. Dostava javnog TSU ključa Pouzdajućim stranama

Javni TSU ključ Fina QTSA 2017 servisa sastavni je dio Fina QTSA 2017 certifikata koji je objavljen na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovog QTPS dokumenta.

6.1.4. Duljine ključeva

Subordinirani Fina RDC 2015 CA upotrebljava sha256WithRSA algoritam s ključem duljine 4096 bita.

Fina QTSA 2017 servis upotrebljava sha256WithRSA algoritam s ključem duljine 2048 bita.

6.1.5. Generiranje i provjera kvalitete parametara javnog ključa

TSU par ključeva kojeg upotrebljava Fina QTSA 2017 servis generira se sukladno normizacijskom dokumentu ETSI TS 119 312 [12].

6.1.6. Namjene ključeva

Privatni TSU ključ za Fina QTSA 2017 koristi se samo za potpis kvalificiranih elektroničkih vremenskih žigova.

Certifikat za Fina QTSA 2017 u ekstenziji *Key Usage* ima postavljene vrijednosti *digitalSignature* i *nonRepudiation* te u ekstenziji *extKeyUsage* ima postavljenu vrijednost *timeStamping.*

6.2. Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom

6.2.1. Norme i upravljačke funkcije kriptografskog modula

HSM modul kojim TSU obavlja potpisivanje kvalificiranih elektroničkih vremenskih žigova zadovoljava zahtjeve prema FIPS 140-2 [17], razina 3.

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

Upravljanje privatnim TSU ključem od strane više osoba sigurnosni je mjera koja zahtijeva autorizaciju više ovlaštenih osoba za pristup privatnom TSU ključu za potpis elektroničkog vremenskog žiga. Taj mehanizam sprječava jednu osobu da sama pristupi privatnom potpisnom TSU ključu Fina QTSA 2017 servisa.

Upravljanje privatnim TSU ključem Fina QTSA 2017 provodi se fizičkim pristupom HSM-u uz minimalno dualnu kontrolu te autorizacijom dvije ovlaštene osobe s povjerljivim ulogama u Fina QTSA. Pri upravljanju privatnim ključevima Fina QTSA 2017 ovlaštene osobe s povjerljivim ulogama koriste pripadajuće upravljačke kartice kriptografskog modula na principu n od m.

6.2.3. Sigurno skladištenje privatnog ključa

Nije dozvoljeno skladištenje privatnih TSU ključeva za Fina QTSA 2017.

6.2.4. Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje privatnih TSU ključeva Fina QTSA 2017 sustava provodi se uz dualnu kontrolu ovlaštenih osoba s povjerljivim ulogama u Fina QTSA, u prostoru najviše razine sigurnosti unutar Fina PKI štićenog prostora. Privatni TSU ključ dohvaća se iz HSM modula isključivo u enkriptiranom obliku te se u tom obliku kopira i čuva u sigurnom prostoru najviše razine sigurnosti unutar Fina PKI štićenih prostora na odvojenim lokacijama.

Fizički pristup sigurnosnim kopijama privatnih TSU ključeva Fina QTSA 2017 sustava imaju isključivo ovlaštene osobe s povjerljivim ulogama u Fina QTSA uz dualnu kontrolu.

6.2.5. Arhiviranje privatnog ključa

Nije dozvoljeno arhiviranje privatnih TSU ključeva Fina QTSA 2017.

6.2.6. Prijenos privatnog ključa

Za vrijeme dok je izvan HSM modula privatni TSU ključ je zaštićen enkriptiranjem. Enkriptiranje privatnog ključa provodi se strogim pridržavanjem zahtjeva navedenih u certifikacijskoj dokumentaciji HSM modula te se time osigurava jednaka razina sigurnosti zaštite privatnog ključa kao i kad se ključ nalazi u HSM modulu.

Prijenos privatnog ključa provode samo ovlaštene osobe s povjerljivim ulogama u Fina PKI, uz dualnu kontrolu unutar Fina PKI štićenog prostora.

Kod prijenosa privatnog TSU ključa iz jednog HSM modula u drugi HSM privatni ključ se smije prenositi samo u HSM jednake ili više razine sigurnosti u odnosu na HSM iz kojega se privatni ključ prenosi.

6.2.7. Spremanje privatnog ključa u kriptografskom modulu

Privatni TSU ključevi Fina QTSA 2017 zaštićeni su HSM modulima i mogu se koristiti jedino ako su propisno aktivirani.

Nema ograničenja obzirom na format u kojem su privatni TSU ključevi spremljeni u HSM modulima.

6.2.8. Metoda aktivacije privatnog TSU ključa

Aktivacija privatnih TSU ključeva za Fina QTSA 2017 provodi se pod dualnom kontrolom ovlaštenih osoba s povjerljivom ulogom Administrator sustava u Fina QTSA 2017. Svaka od ovih ovlaštenih osoba za aktivaciju HSM-a upotrebljava hardversko sredstvo za aktivaciju (OCS kartica) i pripadajući tajni PIN.

Jednom aktiviran, privatni ključ ostaje aktiviran bez vremenskog ograničenja.

6.2.9. Metoda deaktivacije privatnog TSU ključa

Deaktivacija privatnog TSU ključa Fina QTSA 2017 provodi se prema postupcima i uz zadovoljenje zahtjeva određenih u certifikacijskom dokumentu upotrijebljenog HSM modula, pod dualnom kontrolom ovlaštenih osoba s povjerljivom ulogom Administrator sustava u Fina QTSA.

Deaktivacija privatnih TSU ključeva provodi se kada postoji neposredan zahtjev za privremenim obustavljanjem aktivnosti sustava, u slučajevima isteka perioda valjanosti privatnog ključa te u slučaju opoziva pripadajućeg certifikata.

Privatni TSU ključevi Fina QTSA 2017 sustava deaktiviraju se:

- zaustavljanjem Fina QTSA 2017 serverskog procesa,
- isključenjem HSM-a,
- isključenjem servera povezanog s HSM-om.

Privatni TSU ključ mora se čuvati u zaštićenom obliku kad je deaktiviran.

6.2.10. Metoda uništavanja privatnog TSU ključa

Postupak uništavanja privatnog TSU ključa provodi se nakon isteka perioda valjanosti privatnog ključa, zbog kompromitiranja ili sumnje u kompromitiranost privatnog ključa, ili zbog prestanka njegova korištenja, a provode ga ovlaštene osobe s povjerljivim ulogama u Fina PKI. Postupkom

uništavanja privatnog Fina CA ključa trajno su onesposobljene i sve sigurnosne kopije tog privatnog ključa te ih više nije moguće upotrijebiti.

Uništavanje privatnog TSU ključa provodi se sukladno Fininim internim dokumentima i uz strogo pridržavanje zahtjeva navedenih u certifikacijskim dokumentima HSM modula. Fina QTSA 2017 TSU privatni ključ se uništava uz prisutnost osoba s povjerljivim ulogama u Fina PKI. O uništavanju TSU privatnog ključa vodi se zapisnik.

6.2.11. Ocjena kriptografskog modula

Ocjena HSM modula provodi se certificiranjem prema odgovarajućim normama za kriptografske module navedenim u točki 6.2.1. ovog QTPS dokumenta.

6.3. Ostali vidovi upravljanja parom ključeva

6.3.1. Arhiviranje javnog ključa

Javni ključevi Fina QTSA 2017 arhiviraju se u svrhu pružanja dokaza o izdanim elektroničkim vremenskim žigovima u sudskim, upravnim i drugim postupcima.

Javni TSU ključevi Fina QTSA 2017 sustava sastavni su dio pripadajućih Fina QTSA 2017 certifikata koji se arhiviraju sukladno točkama 5.5.3. i 5.5.4. ovog QTPS dokumenta, a u arhivi se čuvaju na rok iz točke 5.5.2. ovog QTPS dokumenta.

6.3.2. Vremenski period važenja Fina QTSA 2017 certifikata i korištenja para TSU ključeva

Fina QTSA 2017 certifikat ima period važenja od 4 godine.

Period važenja privatnog TSU ključa Fina QTSA 2017 servisa definiran ekstenzijom *PrivateKeyUsagePeriod* u Fina QTSA 2017 certifikatu je 12 mjeseci.

Period važenja privatnih TSU ključeva i TSU certifikata za Fina QTSA 2017 naveden je u ekstenziji *PrivateKeyUsagePeriod* u TSU certifikatu za Fina QTSA 2017.

Nakon isteka vremena važenja privatnog TSU ključa Fina QTSA 2017 odbacuje svaki zahtjev za izdavanje elektroničkog vremenskog žiga.

Po isteku važenja privatni TSU ključevi i njihove kopije sigurno se onesposobljuju tako da ne postoji niti jedna njihova kopija te iste nije moguće ponovo koristiti.

Period važenja TSU certifikata za Fina QTSA 2017 naveden je u polju *Validity* u TSU certifikatu za Fina QTSA 2017.

TSU certifikat za Fina QTSA 2017 Pouzdajuće strane mogu upotrebljavati za validaciju potpisa TSU u izdanim elektroničkim vremenskim žigovima i nakon isteka perioda važenja TSU certifikata ukoliko korišteni kriptografski algoritmi pružaju zahtijevanu razinu sigurnosti.

6.4. Aktivacijski podaci

6.4.1. Generiranje i instalacija aktivacijskih podataka

Aktivacijski podaci povezani s privatnim TSU ključem za Fina QTSA 2017 generiraju se i instaliraju prilikom postupka generiranja pripadajućeg privatnog ključa.

6.4.2. Zaštita aktivacijskih podataka

Aktivacijski podaci povezani s privatnim TSU ključem za Fina QTSA 2017 podijeljeni su na hardverska sredstva za aktivaciju koja se zaštićena pripadajućim PIN-ovima te se na siguran način čuvaju u Fina PKI štićenom prostoru.

6.5. Upravljanje računalnom sigurnošću

6.5.1. Posebni tehnički zahtjevi na računalnu sigurnost

Pristup IT sustavu i aplikacijama u Fina PKI imaju isključivo ovlaštene osobe nakon autentikacije. Kontrola pristupa operacijskim sustavima Fina QTSA 2017 poslužitelja dopušta pristup samo ovlaštenom osoblju s povjerljivim ulogama u Fina QTSA, sukladno točki 5.2.1. ovog QTPS dokumenta.

Fina provodi odvajanje dužnosti i odgovornosti za povjerljive uloge osoblja u Fina QTSA, sukladno točki 5.2.4. ovog QTPS dokumenta.

Identifikacija i potvrđivanje identiteta za svaku povjerljivu ulogu u Fina QTSA provodi se korištenjem odgovarajućih sredstava za autentikaciju sukladno točki 5.2.3. ovog QTPS dokumenta.

Fina PKI sustav provodi kontinuirano praćenje i posjeduje alarmni sustav u svrhu detektiranja, bilježenja i pravovremenog reagiranja na pokušaje nedozvoljenog pristupa resursima sustava.

Implementiran je sustava zaštite od zlоćudnog koda te je zabranjeno korištenja neautoriziranog softvera.

6.5.2. Ocjena računalne sigurnosti

U cilju sigurnosti i kvalitete pružanja kvalificiranih usluga povjerenja Fina ima uspostavljen sustav upravljanja informacijskom sigurnošću sukladan normi ISO/IEC 27001 [18]. Sukladnost se potvrđuje certifikatom izdanim od strane neovisnog certifikacijskog tijela.

6.6. Tehničke kontrole životnog ciklusa

6.6.1. Kontrole razvoja sustava

Pri nabavi razvoja softvera od vanjskog izvođača, Fina ugovorom s dobavljačem osigurava sigurnosne principe razvoja sustava.

Analiza sigurnosnih zahtjeva provodi se u fazi dizajna i specifikacije bilo kojeg projekta razvoja Fina PKI sustava kako bi se osiguralo da je sigurnost ugrađena u informacijske tehnologije u Fina PKI sustavima.

Nove verzije softvera testiraju se u testnom okruženju.

Implementacija softvera u produkciji provodi se u skladu s dokumentiranim postupcima upravljanja promjenama.

Plan za upravljanje konfiguracijom Fina PKI sustava sadrži jasan prikaz trenutnog stanja, popis dokumentacije nastale u sklopu izrade informacijskog sustava, mjere za osiguranje kvalitete, procjenu ranjivosti, softverski dizajn, sistemski test i definicije kontrolnih mehanizama.

6.6.2. Kontrole upravljanja sigurnošću

HSM-ovi za Fina QTSA se prilikom transporta u nabavi štite mjerama od proboja i neovlaštene izmjene koje osigurava proizvođač. Prilikom isporuke HSM-ovi se provjeravaju obzirom na proboj te se provjerava njihov integritet. Transfer HSM-a kojeg obavlja Fina reguliran je posebnom internom procedurom.

Instalaciju i aktivaciju HSM kriptografskih modula u Fina PKI štićenom prostoru provodi ovlašteno osoblje s povjerljivim ulogama u Fina PKI, uz minimalno dulanu kontrolu.

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

Pri pokretanju HSM modula provodi se automatska provjera njihovog integriteta.

Prilikom instalacije softvera i njegovih zakrpi u Fina PKI provode se mjere za provjeru autentičnosti i cjelovitosti softvera koji se instalira.

Ovlašteno osoblje Fine provodi kontrolu i nadzor postavki Fina PKI sustava.

Fina provodi provjeru sustava za izdavanje elektroničkih vremenskih žigova u odnosu na sigurnost, pouzdanost i kvalitetu djelovanja, a u skladu s važećim propisima iz točke 9.14. ovog QTPS dokumenta.

U slučaju povrede sigurnosti Fina QTA 2017 sustava ili gubitka njegovog integriteta koji može imati značajan utjecaj na pružanje usluge povjerenja ili na zaštitu osobnih podataka Fina će u roku od 24 sata o istome obavijestiti središnje tijelo državne uprave nadležno za poslove gospodarstva kao tijelo nadležno za nadzor kvalificiranih pružatelja usluga povjerenja te prema potrebi, druga nadležna tijela. U slučaju da gubitak integriteta može imati negativni utjecaj na korisnike Fininih usluga povjerenja Fina će o istome bez odgode obavijestiti sve fizičke i pravne osobe na koje povreda sigurnosti može utjecati.

6.6.3. Sigurnosne kontrole životnog ciklusa

Fina provodi upravljanje promjenama u Fina PKI kako bi se promjene izvodile iz opravdanog razloga te na kontrolirani i formalizirani način.

Integritet Fina QTSA 2017 sustava štiti se antivirusnom zaštitom i uporabom autoriziranog softvera.

Provodi se praćenje raspoloživih kapaciteta Fina QTSA 2017 sustava te se procjenjuje zadovoljenje postojećih kapaciteta za buduće potrebe sustava kako bi se pravodobno planiralo njihovo proširenje.

6.7. Provjera mrežne sigurnosti

Sigurnost računalne mreže Fina PKI zasnovana je na konceptu odjeljivanja mreže na mrežne zone različitih razina. Mrežne zone odjeljuju se vatrozidovima koji propuštaju samo nužan mrežni promet. Na sve sustave locirane unutar jedne mrežne zone primjenjuju se jednake sigurnosne mjere. Pristup i komunikacija između zona je ograničen na autorizirano osoblje s povjerljivim ulogama nužno za pružanje usluge.

Oprema za zaštitu računalne mreže bilježi tijek prometa i pokušaje pristupa Fininim PKI servisima. Samo ovlašteno osoblje u Fina PKI ima administratorske ovlasti za podešavanje i upravljanje

opremom za zaštitu računalne mreže. Udaljeno podešavanje opreme za zaštitu računalne mreže nije dozvoljeno.

Nepotrebne komunikacije, računi, portovi, protokoli i servisi su eksplicitno zabranjeni ili deaktivirani.

Interna računalna mreža Fina PKI zaštićena je od neovlaštenog pristupa, uključujući pristup Korisnika i trećih strana.

Kritičnim sustavima u Fina PKI štićenom prostoru onemogućen je mrežni pristup izvan tog prostora.

Fina QTSA 2017 sustav je sigurnosno podešen i očvršćen.

Interna računalna mreža Fina PKI zaštićena je od neovlaštenog pristupa, uključujući pristup Korisnika i trećih strana.

Svi sustavi kritični za pružanje usluga povjerenja smješteni su u Fina PKI štićenom prostoru.

Mrežne komponente Fina PKI sustava čuvaju se u fizički i logički sigurnom okruženju i usklađenost njihove konfiguracije periodički se provjerava.

6.8. Uporaba elektroničkog vremenskog žiga

Vrijeme u Fina PKI sustavu usklađeno je s UTC točnim vremenom. Revizijski zapisi Fina QTSA 2017 sustava sadrže točan podatak o datumu i vremenu njihovog nastanka, uz odstupanje manje od +/- 1 s.

7. SADRŽAJ CERTIFIKATA, LISTA OPOZVANIH CERTIFIKATA I OCSP PROFILI

7.1. Profil certifikata Fina QTSA 2017

Dokument s opisom profila TSU certifikata za Fina QTSA 2017 dostupan je na internetskim stranicama repozitorija iz točke 2.2. ovog QTPS dokumenta.

Certifikat za Fina QTSA 2017 servis izdaje Fina RDC 2015 CA.

7.1.1. Broj(evi) verzije

- *Version*

  Certifikat Fina QTSA 2017 sukladan je verziji 3 prema X.509 specifikaciji.

7.1.2. Osnovna polja i ekstenzije certifikata

7.1.2.1. Osnovna polja certifikata Fina QTSA 2017

U ovoj točki opisana su osnovna polja certifikata TSU jedinice Fininog servisa Fina QTSA 2017 za izdavanje elektroničkih vremenskih žigova.

- *Serial Number*

  Jedinstveni identifikator Fina QTSA 2017 certifikata generiran od Fina RDC 2015 CA.

  Duljina serijskog broja je 16 ili 17 okteta što osigurava 64 bita entropije.

- *Algorithm Identifier*

  Kriptografski algoritam. Fina kao pružatelj usluga povjerenja za potpis certifikata za Fina QTSA 2017 servis izdavanja elektroničkih vremenskih žigova koristi kriptografski algoritam: sha256WithRSAEncryption.

- *Signature*

  Potpis izdavatelja certifikata za Fina QTSA 2017 servis.

- *Issuer*

  Naziv izdavatelja certifikata po normi X.520. Izdavatelj certifikata za Finin servis Fina QTSA 2017 je Finino certifikacijsko tijelo (CA): Fina RDC 2015.

- *Validity*

  Polje Validity određuje period važenja certifikata. Vrijeme je u UTC formatu, a sadržaj polja kodiran je u skladu s IETF RFC 5280 [15]. Period važenja Fina QTSA 2017 certifikata je 4 godine.

- *Subject*

  Polje Subject sadrži jedinstveni naziv izdavatelja elektroničkih vremenskih žigov sukladan normi X.520.

- *Subject Public Key*

  Atribut subjectPublicKey sadrži javni ključ koji odgovara privatnom TSU ključu kojim Finin servis Fina QTSA 2017 za izdavanje elektroničkih vremenskih žigova potpisuje izdane elektroničke vremenske žigove.

7.1.2.2. Ekstenzije certifikata Fina QTSA 2017

U ovoj točki opisane su ekstenzije certifikata TSU jedinice Fininog servisa Fina QTSA 2017 za izdavanje elektroničkih vremenskih žigova.

- *Key Usage* – kritična ekstenzija

  U certifikatu izdanom TSU jedinici u Fina QTSA 2017 servisu dopuštene su samo sljedeće vrijednosti atributa za ovu ekstenziju: "digitalSignature" i "nonRepudiation".

- *Subject Directory Attributes* – nije kritična ekstenzija

  OID = 1.2.840.113533.7.68, interna vrijednost=18.

- *Private Key Usage Period* – nije kritična ekstenzija

  Private Key Usage Period polje definira vremenski period važenja privatnog TSU ključa Fina QTSA 2017 servisa. Vrijeme je u UTC formatu, a sadržaj polja kodiran je u skladu s IETF RFC 5280 [15]. Ovaj period postavljen je na 12 mjeseci.

- *Extended Key Usage* – kritična ekstenzija

  Atribut u ekstenziji *extKeyUsage* pobliže definira dopušteno korištenje privatnog ključa TSU jedinice Fininog servisa Fina QTSA 2017 za izdavanje elektroničkih vremenskih žigova.

  U certifikatu izdanom TSU jedinici Fininog servisa Fina QTSA 2017 za izdavanje elektroničkih vremenskih žigova ova ekstenzija sadrži atribut: „*timeStamping*“ čija je vrijednost: OID: 1.3.6.1.5.5.7.3.8.

- *Certificate Policies* – nije kritična ekstenzija

  Atributi u ovoj ekstenziji sadrže Finin identifikator (OID) pravila po kojima je izdan certifikat za TSU jedinicu u Fininom servisu Fina QTSA 2017 za izdavanje elektroničkih vremenskih žigova.

  Ova ekstenzija sadrži i URL za aktualni QTPS dokument koji se primjenjuje u Fininom servisu Fina QTSA 2017 za izdavanje elektroničkih vremenskih žigova.

- *CRL Distribution Points* – nije kritična ekstenzija

  Vrijednosti atributa ove ekstenzije sadrže adrese preko kojih je dostupna CRL korištenjem *HTTP* i *LDAP* protokola.

- *Authority Key Identifier* – nije kritična ekstenzija

  Sadržaj atributa ove ekstenzije je jedinstveni identifikator javnog ključa čijim je pripadajućim privatnim ključem potpisan TSU certifikat Fininog servisa Fina QTSA 2017.

  Vrijednost atributa je SHA-1 sažetak javnog ključa Fininog certifikacijskog tijela (CA) Fina RDC 2015, duljine 160 bita.

- *Subject Key Identifier* – nije kritična ekstenzija

  Sadržaj atributa ove ekstenzije je jedinstveni identifikator javnog TSU ključa Fininog servisa Fina QTSA 2017.

  Vrijednost atributa je SHA-1 sažetak javnog TSU ključa Fininog servisa Fina QTSA 2017, duljine 160 bita.

- *Basic Constraints* – nije kritična ekstenzija

  Vrijedosti za ovu ekstenziju su:

  cA=*FALSE*

  pathLenConstraint=None

- *Authority Information Access* – nije kritična ekstenzija

  Unos vrijednosti za atribute u ovoj ekstenzije je obvezan, ali ova ekstenzija certifikata ne smije biti kritična. Vrijednosti sadržane u atributima ove ekstenzije su:

  - adresa Fininog OCSP servisa za *online* provjeru statusa opozvanosti certifikata Fina QTSA 2017 servisa,
  - adresa preko koje se, za provjeru certifikacijske staze, može pristupiti certifikatu Fininog certifikacijskog tijela (CA) koje je izdalo certifikat za Finin servis Fina QTSA 2017.

- *Qualified Certificate Statements* – nije kritična ekstenzija

  esi4-qtstStatement-1

  esi4-qtstStatement-5 sadrži internetske adrese dokumenta Uvjeti pružanja usluge izdavanja kvalificiranih elektroničkih vremenskih žigova na engleskom i hrvatskom jeziku:

  - https://rdc.fina.hr/pds/PDSqts-en.pdf, en
  - https://rdc.fina.hr/pds/PDSqts-hr.pdf, hr

7.1.3. Identifikator objekta (OID) algoritama

Algoritmi s pripadajućim OID identifikatorima za certifikat TSU jedinice Fina QTSA 2017 servisa prikazani su u Tablici 7.1.

Algoritam	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

Tablica 7.1. Algoritmi s pripadajućim OID identifikatorima

7.1.4. Oblici naziva

Oblici naziva za polje Subject u certifikatu Fina QTSA 2017 sustava:

commonName (CN): Fina QTSA 2017 *<redni broj izdanog certifikata>*

organizationIdentifier: VATHR-85821130368

organizationName (O): Financijska agencija

countryName (C): HR

7.1.5. Ograničenja u nazivima

Ekstenzija *Name Constraints* se ne koristi.

7.1.6. Identifikator objekta (OID) općih pravila TSU certifikata

Ekstenzija Certificate Policies certifikata sadrži odgovarajući Finin OID: 1.3.124.1104.5.12.52.

7.1.7. Uporaba ekstenzije *Policy Constraints*

Ekstenzija *Policy Constraints* se ne koristi.

7.1.8. Sintaksa i semantika kvalifikatora općih pravila

Kvalifikator općih pravila u ekstenziji Certificate Policies sadrži dva pokazivača u URI formatu koji sadrže internetsku adresu web stranice na kojoj je objavljen ovaj QTPS dokument na hrvatskom i engleskom jeziku.

7.1.9. Procesne semantike za kritičnu ekstenziju *Certificate Policies*

Nema odredbi.

7.2. Profil CRL

Profil CRL koju izdaje subordinirani Fina RDC 2015 CA sukladan je preporuci IETF RFC 5280 [15].

7.2.1. Broj(evi) verzije

CRL su sukladne verziji 2 prema X.509 specifikaciji.

7.2.2. CRL i ekstenzije unosa u CRL

Ekstenzije CRL koje se koriste u CRL listama i u elementima unosa CRL lista koje izdaju Fina CA-ovi definirane su u tablici 7.2.

Ekstenzije	Kritično	Vrijednost
crlExtensions		
cRLNumber	NE	Jednolično rastući serijski broj CRL duljine do 20 okteta.
AuthorityKeyIdentifier	NE	SHA-1 hash vrijednost duljine 160 bita
ExpiredCertsOnCRL	NE	11.05.2017 02:00:00 GMT
crlEntryExtensions		
reasonCode	NE	Kod razloga opoziva certifikata

Tablica 7.2. Ekstenzije CRL liste i elemenata unosa CRL listi koje izdaju Fina CA-ovi

7.3. OCSP profil

Profil odgovora Fina OCSP servisa usklađen je s preporukom IETF RFC 6960 [16].

7.3.1. Broj(evi) verzije

Profil odgovora Fina OCSP servisa sukladan je verziji 1 prema IETF RFC 6960 [16].

7.3.2. OCSP ekstenzije

Ekstenzije odgovora Fina OCSP servisa prikazane su u tablici 7.3.

Ekstenzije	Kritično	Vrijednost
Nonce	*NE*	*Vrijednost Nonce iz zahtijeva za status certifikata.*
Extended Revoked Definition	NE	Kod razloga opoziva certifikata (*Reason code*)

Tablica 7.3. Ekstenzije odgovora Fina OCSP servisa

8. PROVJERA SUKLADNOSTI

Nadzor nad radom Fine kao kvalificiranog pružatelja usluga povjerenja reguliran je Uredbom (EU) br. 910/2014 [1] i Zakonom o provedbi Uredbe (EU) br. 910/2014 [2], a provodi ga središnje tijelo državne uprave nadležno za poslove gospodarstva.

Nadzor nad radom Fine kao kvalificiranog pružatelja usluga povjerenja u području praćenja provedbe propisa o zaštititi osobnih podataka provodi Agencija za zaštitu osobnih podataka.

Provjera sukladnosti obavlja se u cilju potvrđivanja da Fina kao kvalificirani pružatelj usluga povjerenja pruža usluge izdavanja kvalificiranih elektroničkih vremenskih žigova sukladno zahtjevima utvrđenim Uredbom (EU) br. 910/2014 [1], Zakonom o provedbi Uredbe (EU) br. 910/2014 [2] te normama ETSI EN 319 421 [7] i ETSI EN 319 401 [6].

Fina ima implementiran sustav upravljanja kvalitetom prema normi ISO 9001 te se nalazi u certifikacijskom ciklusu čime dokazuje da ispunjava zahtjeve te norme, da ima dokumentiran sustav, definirane ovlasti, odgovornosti te opisane procese.

Također, Fina ima uspostavljen, kontinuirano nadziran, certificiran i prema poslovnim potrebama unaprjeđivan vlastiti sustav informacijske sigurnosti u skladu s normom ISO/IEC 27001 [18].

8.1. Učestalost ili okolnosti provjere sukladnosti

Provjere sukladnosti u radu Fina PKI su vanjske provjere sukladnosti i interne provjere sukladnosti.

8.1.1. Vanjska provjera sukladnosti

Vanjska provjera sukladnosti provodi se najmanje svaka 24 mjeseca, sukladno zahtjevima Uredbe (EU) br. 910/2014 [1] i norme ETSI EN 319 403 [11]. Vanjski nadzorni audit (vanjska nadzorna provjera sukladnosti) provodi se na godišnjoj razini između potpunih vanjskih provjera sukladnosti, sukladno normi ETSI EN 319 403 [11]. Vanjska provjera sukladnosti i nadzorni audit provode se prema zahtjevima norme ETSI EN 319 421 [7] koja uključuje normativnu referencu na normu ETSI EN 319 401 [6].

8.1.2. Interna provjera sukladnosti

Interna provjera sukladnosti provodi se prije početka pružanja nove kvalificirane usluge povjerenja, periodično najmanje svakih 12 mjeseci te nakon značajnijih promjena u radu Fina PKI.

8.2. Identitet/kvalifikacije ocjenitelja

Vanjsku provjeru sukladnosti provodi tijelo za ocjenjivanje sukladnosti. Osposobljenost tijela za ocjenjivanje sukladnosti i osposobljenost pripadajućih ocjenitelja osigurana je akreditacijom tijela za ocjenjivanje sukladnosti prema normi ETSI EN 319 403 [11].

Internu provjeru sukladnosti provode interni ocjenitelji sukladnosti koji zajedno raspolažu znanjima i razumijevanjem:

- odredbi norme ETSI EN 319 421 [7],
- PKI područja, tehnologije vremenskog žiga te područja informacijske sigurnosti,
- zakonske regulative iz područja pružanja usluga povjerenja.

8.3. Odnos ocjenitelja s tijelom koje se ocjenjuje

Tijelo za ocjenjivanje sukladnosti i pripadajući ocjenitelji neovisni su od Fine i Fininih sustava ocjenjivanja.

Interni ocjenitelji sukladnosti ne ocjenjuju sukladnost iz vlastitog djelokruga odgovornosti.

8.4. Predmeti ocjenjivanja sukladnosti

Predmeti ocjenjivanja sukladnosti obuhvaćaju slijedeća područja pružanja kvalificiranih usluga povjerenja:

- cjelovitost i točnost dokumentacije,
- implementiranost zahtjeva za kvalificirane usluge povjerenja,
- organizacijski procesi i procedure,
- tehničke procese i procedure,
- implementirane mjere informacijske sigurnosti,
- vjerodostojne sustave,
- fizičku sigurnost predmetnih lokacija.

Opis predmeta ocjenjivanja sukladnosti definiran je planom ocjenjivanja sukladnosti.

Fina će ocjenitelju sukladnosti na zahtjev omogućiti pristup svim prostorima Fina PKI sustava, pristup izvješćima internih i vanjskih provjera sukladnosti te drugim izvješćima i zapisima iz djelokruga pružanja usluga povjerenja. Fina će također ocjenitelju sukladnosti omogućiti pristup zapisima i ugovorima vezanim uz treće strane, interna, vanjska i upravljačka izvješća i sl. iz djelokruga pružanja usluga povjerenja.

8.5. Mjere u slučaju nesukladnosti

U ovisnosti o značaju otkrivene nesukladnosti vanjski ocjenitelj sukladnosti u izvješću navodi koju nesukladnost Fina mora otkloniti.

U slučaju značajne nesukladnosti Fina će što prije formirati plan otklanjanja značajne nesukladnosti i uz konzultaciju sa vanjskim ocjeniteljem sukladnosti što prije otkloniti značajne nesukladnosti.

Ako je u pružanju usluga povjerenja utvrđena manja nesukladnost koja kroz kraći vremenski rok nije otklonjiva Fina će poduzeti potrebne korake kako bi otklonila nesukladnost i ako je moguće u roku koji je odredilo nadzorno tijelo.

Preporuke vanjskih ocjenitelja, Fina će, uz konzultaciju sa vanjskim ocjeniteljem, primijeniti do slijedeće ocjene sukladnosti.

Vanjski ocjenitelj može predložiti i savjetovati izmjenu kojom se poboljšava pružanje usluga povjerenja. U tom slučaju Fina zadržava pravo prihvaćanja prijedloga.

Fina vodi interni dnevnik vremenskih razdoblja u kojima Fina QTSA 2017 servis nije radio u skladu s ovim QTPS dokumentom u kojem se navode i razlozi nesukladnosti.

8.6. Priopćavanje rezultata

Rezultati interne provjere sukladnosti povjerljive su prirode i Fina ih ne objavljuje javno.

Svi dokumenti interne provjere usklađenosti su na zahtjev dostupni vanjskim ocjeniteljima koji provode provjeru usklađenosti Fina PKI sustava.

Izvješće o ocjenjivanju sukladnosti koje zaprimi od tijela za ocjenjivanje sukladnosti Fina će dostaviti nadzornom tijelu u roku od tri radna dana od njegova primitka.

Fina na mrežnim stranicama repozitorija iz točke 2.2 ovog dokumenta javno objavljuje sažetak izvješća ili potvrdu o provedenoj vanjskoj provjeri sukladnosti. Nesukladnosti utvrđene tijekom provjere sukladnosti se smatraju povjerljivim informacijama i one se ne objavljuju.

9. OSTALE POSLOVNE I PRAVNE ODREDBE

9.1. Naknada za usluge

Fina, sukladno uvjetima iz sklopljenog ugovora o pružanju usluge izdavanja elektroničkih vremenskih žigova obavještava Korisnike i Pouzdajuće strane o naplati usluge. Ukoliko posebnim ugovorom nije drugačije određeno, usluga se naplaćuju sukladno cjeniku Fine. Cjenik svih usluga koje se naplaćuju objavljen je na internetskim stranicama repozitorija iz točke 2.2. ovog QTPS dokumenta.

Fina zadržava pravo izmjene cjenika. Izmjene cjenika objavljuju se na internetskim stranicama repozitorija iz točke 2.2. ovog QTPS dokumenta.

Ovisno o specifičnom Korisničkom zahtjevu cijena usluge može biti definirana posebnim ugovorom.

9.1.1. Povrat naknada

Povrat naknade Fina Korisnicima isplaćuje u slučaju pogrešne uplate ili preplate.

9.2. Financijska odgovornost

Fina kao pružatelj usluga povjerenja posjeduje financijsku stabilnost te raspolaže dostatnim financijskim sredstvima koja osiguravaju nesmetano pružanje usluga izdavanja elektroničkih vremenskih žigova u skladu s ovim QTPS dokumentom.

9.2.1. Pokrivenost osiguranjem

Fina kao pružatelj usluga povjerenja ima osiguran rizik od odgovornosti za štete koje nastanu obavljanjem usluga izdavanja elektroničkih vremenskih žigova.

Fina dodatno osigurava imovinu policom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda, poplava, eksplozija, udar vozila, pad ili udar letjelice, demonstracija, osiguranje opreme, strojne opreme, elektroničkih i komunikacijskih uređaja, instalacija i sl.

9.2.2. Druga sredstva

Nema odredbi.

9.2.3. Osiguranje ili garancije krajnjim korisnicima

Vidi točku 9.2.1.

9.3. Povjerljivost poslovnih podataka

9.3.1. 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 izdavanja elektroničkih vremenskih

žigova, 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 2017 sustavu.

Sve informacije koje se odnose na način kojim Fina QTSA upravlja TSU ključevima i Fina QTSA 2017 sustavom 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.

9.3.2. 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 pružanjem usluga izdavanja elektroničkih vremenskih žigova, 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.

9.3.3. Odgovornost za zaštitu povjerljivih poslovnih podataka

Svaki sudionik obvezan je štititi povjerljive poslovne podatke iz točke 9.3.1. ovog QTPS 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.

9.4. Zaštita osobnih podataka

Fina posvećuje pažnju zaštiti osobnih podataka koje prikuplja, pohranjuje i upotrebljava u svrhu pružanja usluge izdavanja kvalificiranih elektroničkih vremenskih žigova te s osobnim podacima postupa sukladno Uredbi (EU) 2016/679 [4] i Zakonu o provedbi Opće uredbe o zaštiti podataka [5].

Podnošenjem pristupnice za korištenje Fina QTSA 2017 servisa i sklapanjem ugovora o pružanju usluga izdavanja kvalificiranih elektroničkih vremenskih žigova Korisnici daju Fini suglasnost za korištenje i obradu njihovih osobnih podataka prikupljenih u postupku registracije sukladno važećoj zakonskoj regulativi te suglasnost za čuvanje tih podataka u trajanju od najmanje 10 godina.

9.4.1. Plan zaštite osobnih podataka

Fina ima i provodi Politiku zaštite osobnih podataka kojom se utvrđuju načela obrade osobnih podataka fizičkih osoba te kojom se izražava svijest, znanje i predanost za poštivanje prava i sloboda pojedinaca pri obradi osobnih podataka, a kojih se Fina mora pridržavati u svojem poslovanju. Osobne podatke prikupljene za potrebe pružanja usluge izdavanja kvalificiranih

elektroničkih vremenskih žigova Fina obrađuje u opsegu koji je primjeren, relevantan i ograničen samo za pružanje te usluge.

Fina stručnim znanjem, pouzdanošću, resursima, poštivanjem propisanih tehničkih, organizacijskih i sigurnosnih mjera jamči obradu osobnih podataka sukladno Uredbi (EU) 2016/679 [4] i Zakonu o provedbi Opće uredbe o zaštiti podataka [5].

Mjere zaštite povjerljivosti i cjelovitosti osobnih podataka primjenjuju se prilikom razmjene osobnih podataka Korisnika između Fina RA mreže i sustava izdavanja elektroničkih vremenskih žigova te prilikom čuvanja i arhiviranja osobnih podataka Korisnika do njihovog izlučivanja iz arhive i uništavanja.

9.4.2. Povjerljivi osobni podaci

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 pružanje usluge izdavanja elektroničkih vremenskih žigova. Osobni podaci koje prikupi Fina za potrebe pružanja usluge izdavanja elektroničkih vremenskih žigova su povjerljivi osobni podaci koje Fina propisano štiti.

9.4.3. Osobni podaci koji nisu povjerljivi

Svi osobni podaci prikupljeni u svrhu korištenja usluge izdavanja kvalificiranih elektroničkih vremenskih žigova smatraju se povjerljivim osobnim podacima.

9.4.4. Odgovornost za zaštitu osobnih podataka

Fina je odgovorna su za zaštitu osobnih podatka prikupljenih u svrhu pružanja usluge izdavanja kvalificiranih elektroničkih vremenskih žigova.

9.4.5. Ovlaštenje za korištenje osobnih podataka

Fina je ovlaštena, osim za potrebe ispunjenja zakonskih obveza, odnosno ugovornih obveza po ugovoru o pružanju usluge izdavanja elektroničkih vremenskih žigova, koristiti ili objavljivati osobne podatke samo temeljem pisane suglasnosti Korisnika.

9.4.6. Dostupnost podataka mjerodavnim tijelima

Fina neće činiti dostupnima podatke iz točaka 9.3.1. i 9.4.2. ovog QTPS dokumenta osim u slučajevima propisanim zakonom ili kada to pisano zahtjeva mjerodavni sud, upravno ili neko drugo mjerodavno državno tijelo.

9.4.7. Ostale okolnosti objave podataka

Nema odredbi.

9.5. Prava intelektualnog vlasništva

Ovaj QTPS dokument kao i druga Finina dokumentacija objavljena na internetskim stranicama repozitorija iz točke 2.2. ovog QTPS dokumenta je intelektualno vlasništvo Fine.

Fina ne polaže pravo intelektualnog vlasništva na softver koji se koriste u Fina PKI, a koji je u vlasništvu trećih osoba.

Privatni TSU ključevi Fina QTSA 2017 i pripadajući TSU certifikati koji se koriste za potpisivanje elektroničkih vremenskih žigova vlasništvo su Fine.

9.6. Obveze

9.6.1. Obveze Fine

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

Fina, također ima obvezu:

- provoditi pružanje usluga izdavanja elektroničkih vremenskih žigova u skladu s Uredbom (EU) br. 910/2014 [1], Zakonom o provedbi Uredbe (EU) br. 910/2014 [2] te normizacijskih dokumenata i preporuka na koje isti upućuju, Općim pravilima [22], ovim QTPS dokumentom te drugim aktima Fine vezanim uz pružanje usluga izdavanja elektroničkih vremenskih žigova,
- provoditi izdavanje elektroničkih vremenskih žigova na opremi koja udovoljava zahtjevima iz točke 6.2.1. ovog QTPS dokumenta,
- provoditi zahtijevane sigurnosne mjere za zaštitu prostora i opreme sustava za izdavanje elektroničkih vremenskih žigova,
- osigurati nesmetan rad i maksimalnu raspoloživost usluga izdavanja elektroničkih vremenskih žigova sukladno najboljoj poslovnoj praksi,
- objaviti akte, koji mogu biti javno dostupni, na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovog QTPS dokumenta
- obavljati usluge izdavanja elektroničkih vremenskih žigova s pažnjom dobrog stručnjaka,
- primjenjivati u svom poslovanju organizacijske i tehničke mjere zaštite osobnih podataka prikupljenih od Korisnika i prikupljene podatke čuvati povjerljivima te ih koristiti isključivo za potrebe usluga iz opsega ovog QTPS dokumenta i dodatnih usluga certificiranja iz skupa Fina PKI usluga,
- primjenjivati odredbe Zakona o zaštiti osobnih podataka [8] i drugih propisa kojima je uređena zaštita osobnih podataka te tajnost podataka u Republici Hrvatskoj,
- poštovati intelektualno vlasništvo, licenčna i druga prava,
- rješavati zastoje i greške u radu sustava za izdavanje elektroničkih vremenskih žigova u najkraćem mogućem roku,
- planirati održavanje i daljnji razvoj sustava za izdavanje elektroničkih vremenskih žigova sukladno važećim normama i razvoju tehnologije.

9.6.2. Obveze RA

Obveze Fina RA mreže:

- provođenje postupka registracije i identifikacije fizičkih osoba i poslovnih subjekata na način propisan ovim QTPS dokumentom,
- prosljeđivanje cjelovitih, točnih i provjerenih podataka o Korisnicima na daljnju obradu u Fina QTSA,

- čuvanje, arhiviranje i zaštita podataka i dokumentacije na period od najmanje 10 godina,
- osiguravanje od gubitka ili povrede povjerljivosti, cjelovitosti i dostupnosti arhiviranih podataka Korisnika, na način propisan ovim QTPS dokumentom,
- obavještavanje podnositelja pristupnice za Fina QTSA 2017 servis o javno objavljenim i dostupnim uvjetima pružanja usluge izdavanja kvalificiranih elektroničkih vremenskih žigova i ovim QTPS dokumentom.

9.6.3. Obveze korisnika

Korisnik je dužan:

- prilikom predaje pristupnice za korištenje usluga izdavanja elektroničkih vremenskih žigova u pristupnici navesti točne i istinite osobne podatke te odmah obavijestiti Finu, kao pružatelja usluga, o svakoj promjeni tih podataka,
- validirati potpis Fina QTSA 2017 na zaprimljenom elektroničkom vremenskom žigu i provjeriti važenje Fina QTSA 2017 certifikata,
- čuvati privatni ključ i pripadajuće aktivacijske podatke koji se odnose na certifikat kojim pristupa usluzi izdavanja elektronički vremenskih žigova,
- za korištenje usluge izdavanja elektroničkog vremenskog žiga plaćati Fini naknadu sukladno cjeniku Fina QTSA usluga iz točke 9.1. ovog QTPS dokumenta.

Korisnik se obvezuje da neće zahtijevati izdavanje elektroničkog 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, također obvezan s pažnjom dobrog domaćina, odnosno gospodarstvenika pravodobno na internetskim stranicama Fina PKI repozitorija iz točke 2.2. ovog QTPS dokumenta pratiti i upoznati se s objavljenim izmjenama i/ili dopunama ovog QTPS dokumenta.

9.6.4. Obveze Pouzdajućih strana

Prije pouzdanja u elektronički vremenski žig Pouzdajuća strana mora obaviti provjeru valjanosti elektroničkog vremenskog žiga sukladno točki 3.8 ovog QTPS dokumenta.

Pouzdajuća strana obvezna je pridržavati se odredbi ovog QTPS dokumenta.

9.7. Odgovornosti sudionika

9.7.1. Odgovornosti Fine

Fina kao pružatelj usluga izdavanja kvalificiranih elektroničkih vremenskih žigova ima punu odgovornost za pružanje usluga izdavanja elektroničkih vremenskih žigova i za ispunjenje svih zahtjeva propisanih ovim QTPS dokumentom.

Fina je odgovorna za:

- korištenje privatnih TSU ključeva za Fina QTSA 2017 servis odredbama iz ovog QTSA dokumenta,
- propisnu zaštitu privatnih TSU ključeva za Fina QTSA 2017 servis,

- trenutni prekid uporabe privatnog TSU ključa za Fina QTSA 2017 servis postupanje sukladno točki 5.7.3. ovog QTSA dokumenta u slučaju kompromitiranja privatnog TSU ključa.

Fina ima odgovornost da svi zahtjevi koji se odnose na pružanje usluga izdavanja elektroničkih vremenskih žigova, što uključuje postupke koje se odnose na izdavanje elektroničkih vremenskih žigova, nadzor sustava i sigurnosne kontrole, budu u skladu s odredbama ovog QTPS dokumenta.

9.7.2. Odgovornosti RA

Fina RA mreža je odgovorna za:

- prosljeđivanje cjelovitih, točnih i provjerenih podataka o Korisnicima na daljnju obradu u Fina QTSA,
- čuvanje, arhiviranje i zaštita podataka i dokumentacije na period od najmanje 10 godina,
- osiguravanje od gubitka ili povrede povjerljivosti, cjelovitosti i dostupnosti arhiviranih podataka Korisnika, na način propisan ovim QTPS dokumentom.

9.7.3. Odgovornosti Korisnika

Korisnik je odgovoran za:

- sadržaj podataka, odnosno elektroničkog zapisa za koji traži izdavanje elektroničkog vremenskog žiga,
- korisničku aplikaciju koju koristi za ugradnju elektroničkog vremenskog žiga te da osigura njenu potpunu interoperabilnost s Fina QTSA 2017 sustavom,
- za štetu koju prouzroči otkrivanjem svojeg privatnog ključa i/ili pripadajućih aktivacijskih podataka koji se odnose na certifikat kojim pristupa usluzi izdavanja elektroničkih vremenskih žigova,
- potpunost i točnost, odnosno istinitost svih podataka koje je naveo u pristupnici za korištenje usluga izdavanja elektroničkih vremenskih žigova na temelju kojeg je ugovorio korištenje usluge,
- nepravilnosti koje su nastale zbog neispunjavanja obveza utvrđenih u točki 9.6.2. ovog QTPS dokumenta.

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

9.7.4. Odgovornosti Pouzdajućih strana

Pouzdajuća strana koja se, ne poštujući odredbe iz ovog QTPS dokumenta te protivno utvrđenim obvezama iz točke 9.6.4. ovog QTPS dokumenta, pouzdaje u nevažeći elektronički vremenski žig, snosi sama sve rizike pouzdanja u takav elektronički vremenski žig.

Pouzdajuća strana koja namjerava ostvariti pouzdanje u elektroničke vremenske žigove koje izdaje Fina QTSA 2017 servis treba:

- voditi računa o primjerenoj uporabi i zabrani uporabe javnog ključa i certifikata opisanim u ovom QTPS dokumentu,
- obaviti provjeru roka važenja svih certifikata u certifikacijskom lancu te provesti provjeru certifikata prema postupcima za validaciju certifikacijske staze,

- obaviti provjeru statusa opozvanosti TSU certifikata za Fina QTSA 2017.

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

9.8. Odricanje od odgovornosti

Fina nije odgovorna za štete, uključujući i indirektne, kao i za bilo koji gubitak dobiti, gubitak podataka ili druge indirektne štete u sljedećim slučajevima:

- štete prouzročene prijevarnim ili nemarnim korištenjem usluge izdavanja elektroničkih vremenskih žigova,
- štete nastale kao rezultat neispravnosti i pogrešaka u softveru i hardveru Korisnika i Pouzdajuće strane,
- kad je šteta nastala kao rezultat prijevarnog davanja podataka i prijevarnog predstavljanja poslovnog subjekta ili fizičke osobe tijekom procesa identifikacije i potvrde identiteta, ako je identifikaciju i provjeru podataka RA mreža provodila u skladu sa zahtjevima iz ovog dokumenta i radnim uputama.

9.9. Ograničenja odgovornosti

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

9.10. Naknada štete

Svaki sudionik odgovara oštećenom za štetu koju je počinio zbog nepoštivanja odredbi ovog QTPS dokumenta, Općih pravila [22] i važećih relevantnih propisa.

Korisnik usluge izdavanja elektroničkih vremenskih žigova odgovora oštećenom, odnosno svakom drugom sudioniku ako koristi uslugu temeljem prijevarnog predstavljanja prilikom prijave na servis.

Pouzdajuća strana odgovora oštećenom, odnosno svakom drugom sudioniku, ako se pouzda u izdani elektronički vremenski žig bez provjere njegove valjanosti ili ga koristi protivno odredbama Općih pravila [22] i ovog QTPS dokumenta.

9.11. Trajanje i prestanak važenja

9.11.1. Trajanje

Ovaj QTPS dokument važi do stupanja na snagu novog QTPS dokumenta ili do objave prestanka njegovog važenja. Nova verzija dokumenta ili objava prestanka važenja biti će objavljena na internetskim stranicama repozitorija iz točke 2.2. ovog QTPS dokumenta s naznačenim danom stupanja na snagu. Novom dokumentu biti će dodijeljena nova verzija i novi OID te će u njemu biti naznačene obavljene izmjene.

9.11.2. Prestanak važenja

Stupanjem na snagu nove verzije QTPS dokumenta za sve elektroničke vremenske žigove izdane prema ovom dokumentu ostaju važiti one odredbe iz ovog dokumenta koje se ne mogu smisleno zamijeniti odredbama nove verzije QTPS dokumenta.

Prestanak važenja ovog QTPS dokumenta nije vezan i ne utječe na važenje elektroničkih vremenskih žigova izdanih primjenom ovog dokumenta.

Fina može za pojedine odredbe važećeg QTPS dokumenta izraditi izmjene i dopune kao što je to navedeno u točki 9.13. ovog QTPS dokumenta.

9.11.3. Posljedice prestanka važenja i nastavak djelovanja

Stupanjem na snagu nove verzije QTPS dokumenta na sve se elektroničke vremenske žigove izdane od tog dana primjenjuju odredbe iz tog dokumenta.

Novi QTPS dokument ne utječe na važenje elektroničkih vremenskih žigova koji su izdani primjenom prethodnih QTPS dokumenata.

9.12. Individualne obavijesti i komunikacija sa sudionicima

Individualna komunikacija sa sudionicima primarno se provodi preko Finine službe za odnose s korisnicima:

- besplatni telefon: 0800 0080

Individualne obavijesti i druga službena komunikacija u pisanom obliku provodi se korištenjem sljedećih kontaktnih podataka:

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

9.13. Izmjene i dopune

9.13.1. Procedure izmjena i dopuna

Ovaj QTPS dokument se revidira po potrebi.

Fina može bez obavijesti unositi tipografske ispravke, promjene kontakt podataka te druge manje ispravke koji ne utječu bitno na sudionike.

Svi sudionici mogu na kontakt adresu Fina PMA iz točke 1.5.2. ovog QTPS dokumenta poslati dopis s prijedlogom za ispravke pogrešaka, prijedlog nadopuna ili izmjenu ovog QTPS dokumenta. U dopisu se navode kontakt podaci osobe koja je poslala prijedlog promjene. Fina PMA može prihvatiti, prilagoditi ili odbiti predložene promjene nakon razmatranja istih.

Izradu novog ili izmjenu i dopunu postojećeg QTPS dokumenta odobrava i provodi Fina PMA, a sukladno poslovnim zahtjevima Fine i zahtjevima zakonske regulative i propisa iz točke 9.15. ovog dokumenta.

9.13.2. Mehanizmi obavještavanja i vremenski periodi

Sve izmjene i dopune QTPS dokumenta objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2. ovog QTPS dokumenta.

Nove verzije QTPS dokumenta s izmijenjenim OID-om QTPS dokumenta objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2. ovog QTPS dokumenta.

Datum stupanja na snagu izmjena i dopuna ili novoobjavljenog QTPS dokumenta naznačen je na njegovoj naslovnoj strani kao i na internetskim stranicama na kojima je objavljen.

9.13.3. Okolnosti pod kojima se mora mijenjati OID

Veće izmjene u QTPS dokumentu koje mogu utjecati na sudionike zahtijevaju i izmjenu OID-a QTPS dokumenta. Novi OID za novu verziju QTPS dokumenta određuje Fina PMA.

9.14. Postupak rješavanja sporova

U slučaju spora ili neslaganja između Fine i drugih sudionika povodom radnji i/ili postupaka glede pružanja usluge izdavanja elektroničkih vremenskih žigova uređene ovim QTPS 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.

Sudionici mogu Fini uputiti prigovor ako smatraju postoji odstupanje sadržaja usluge u odnosu na objavljene uvjete pružanja usluga. Fina će povodom prigovora odgovoriti podnositelju prigovora. Prigovor i odgovor na prigovor upućuju se pisano u papirnatom ili elektroničkom obliku na način opisan u točki 9.12. ovog QTPS dokumenta.

9.15. Važeći propisi

Kvalificirane usluge povjerenja iz opsega ovog QTPS dokumenta Fina pruža sukladno odredbama Uredbe (EU) br. 910/2014 [1], Zakona o provedbi Uredbe (EU) br. 910/2014 [2], Pravilnika o pružanju i korištenju usluga povjerenja [3] te normizacijskih dokumenata ETSI EN 319 421 [7] i ETSI EN 319 401 [6].

9.16. Usklađenost s primjenjivim propisima

Opća pravila [22], ovaj QTPS dokument i pružanje usluga koje su obuhvaćene ovim QTPS dokumentom usklađeni su s propisima iz točke 9.15. ovog QTPS dokumenta.

Svi sudionici suglasni su s primjenom hrvatskog prava u tumačenju primijenjenih odredbi.

9.17. Ostale odredbe

Gdje je to moguće, Fina omogućuje da usluga izdavanja kvalificiranih elektroničkih vremenskih žigova i proizvodi za krajnjeg korisnika koji se koriste pri pružanju ove usluge budu dostupni osobama s invaliditetom.

Ako podnositelj pristupnice ima neku vrstu invaliditeta, Fina pomaže podnositelju pri predaji pristupnice i registraciji.

Fina javno objavljuje Opća pravila [22], ovaj QTPS dokument i uvjete pružanja usluga izdavanja elektroničkih vremenskih žigova.

Uvjeti pružanja usluga izdavanja elektroničkih vremenskih žigova komuniciraju se dokumentom u papirnatom obliku ili dokumentom u elektroničkom obliku čija je cjelovitost zaštićena.

Prije sklapanja ugovora o pružanju usluga izdavanja elektroničkih vremenskih žigova Fina obavještava Korisnike o uvjetima pružanja usluga. Prihvaćanje uvjeta pružanja usluge preduvjet je za izdavanje elektroničkih vremenskih žigova.