

FINA
OPĆA PRAVILA PRUŽANJA USLUGA IZDAVANJA
KVALIFICIRANIH ELEKTRONIČKIH VREMENSKIH ŽIGOVA

Verzija 1.0

Datum stupanja na snagu: 22.05.2017.

OID Dokumenta: 1.3.124.1104.2.3.1.1.0

Informacije o dokumentu

| | |
|---------------------|--|
| Ime dokumenta: | Opća pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova |
| OID dokumenta: | 1.3.124.1104.2.3.1.1.0 |
| Tip dokumenta: | Opća pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova (<i>Time-Stamp Policy, TP</i>) |
| 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 |

SADRŽAJ:

| | |
|--|----|
| <i>REFERENTNE DOKUMENTIRANE INFORMACIJE</i> | 9 |
| Temeljni zakon | 9 |
| Podzakonski akti | 9 |
| Ostala zakonska regulativa | 9 |
| Normizacijski dokumenti..... | 9 |
| Finini dokumenti | 10 |
| 1. <i>Uvodne oznake i temeljni podaci</i> | 11 |
| 1.1. Pregled..... | 11 |
| 1.2. Naziv dokumenta i identifikacijski podaci..... | 12 |
| 1.3. Sudionici Fina QTSA 2017 servisa..... | 12 |
| 1.3.1. Pružatelj usluga izdavanja kvalificiranih elektroničkih vremenskih žigova | 12 |
| 1.3.2. Korisnici | 12 |
| 1.3.3. Registracijski uredi..... | 12 |
| 1.3.4. Pouzdajuće strane | 12 |
| 1.3.5. Ostali sudionici | 13 |
| 1.4. Primjerena uporaba vremenskih žigova | 13 |
| 1.4.1. Zabrane uporabe vremenskih žigova | 13 |
| 1.5. Administracija Općih pravila..... | 13 |
| 1.5.1. Organizacija odgovorna za održavanje dokumenta Opća pravila | 13 |
| 1.5.2. Kontakt podaci | 13 |
| 1.5.3. Tijelo koje utvrđuje usklađenost QTPS dokumenta s Općim pravilima | 13 |
| 1.5.4. Procedure odobravanja QTPS dokumenta..... | 14 |
| 1.6. Definicije i kratice..... | 14 |
| 1.7. Definicije | 14 |
| <i>Tablica 1.1. Definicije</i> | 19 |
| 1.8. Kratice | 19 |
| <i>Tablica 1.2. Kratice</i> | 19 |
| 2. <i>OBJAVE I ODGOVORNOSTI ZA REPOZITORIJ</i> | 20 |
| 2.1. Identifikacija tijela koje vodi repozitorij | 20 |
| 2.2. Objava informacija o izdavanju vremenskih žigova..... | 20 |
| 2.3. Vrijeme ili učestalost objavljivanja | 20 |
| 2.4. Kontrole pristupa repozitoriju..... | 20 |
| 3. <i>Identifikacija korisnika i izdavanje ELEKTRONIČKIH vremenskih žigova</i> | 21 |
| 3.1. Identifikacija Korisnika | 21 |
| 3.1.1. Inicijalno utvrđivanje identiteta Korisnika..... | 21 |
| 3.1.2. Način dostave pristupnice | 21 |
| 3.1.3. Sklapanje ugovora | 22 |
| 3.2. Identifikacija i autentikacija na Fina QTSA 2017 servis..... | 22 |
| 3.3. Certifikat jedinice za izradu vremenskog žiga | 22 |
| 3.4. Elektronički vremenski žig | 22 |
| 3.4.1. Zahtjev za izdavanje vremenskog žiga (<i>Time-Stamp Request</i>)..... | 23 |
| 3.4.2. Odgovor servisa za izdavanje elektroničkih vremenskih žigova (<i>Time-Stamp Response</i>) | 23 |
| 3.5. Profil vremenskog žiga | 23 |

| | | |
|--------|---|----|
| 3.6. | Točnost vremena u izdanim elektroničkim vremenskim žigovima | 24 |
| 3.7. | Sinkronizacija sata s UTC | 24 |
| 3.7.1. | Ljetno računanje vremena | 24 |
| 3.8. | Provjera valjanosti vremenskog žiga | 24 |
| 3.9. | Raspoloživost usluge | 25 |
| 3.10. | Izdavanje nekvalificiranih elektroničkih vremenskih žigova | 25 |
| 3.11. | Transportni protokol za uslugu izdavanja elektroničkih vremenskih žigova | 25 |
| 4. | OPERATIVNI ZAHTJEVI NA ŽIVOTNI CIKLUS CERTIFIKATA za Fina QTSA 2017 | 26 |
| 4.1. | Izdavanje certifikata | 26 |
| 4.2. | Opoziv i suspenzija certifikata | 26 |
| 4.2.1. | Razlozi za opoziv | 26 |
| 4.2.2. | Tko može tražiti opoziv | 26 |
| 4.2.3. | Profil CRL | 26 |
| 4.2.4. | Učestalost izdavanja CRL | 26 |
| 4.2.5. | Maksimalno kašnjenje za CRL | 26 |
| 4.2.6. | <i>Online</i> dostupnost provjere opozvanih certifikata/statusa certifikata | 27 |
| 4.2.7. | Drugi dostupni načini objave opozvanih certifikata | 27 |
| 5. | PROVJERA SUSTAVA, UPRAVLJANJA I RADNIH POSTUPAKA | 28 |
| 5.1. | Mjere fizičke zaštite | 28 |
| 5.1.1. | Lokacija objekta i konstrukcija | 28 |
| 5.1.2. | Fizički pristup | 28 |
| 5.1.3. | Sustavi za napajanje i klimatizaciju | 29 |
| 5.1.4. | Opasnost od poplave | 29 |
| 5.1.5. | Protupožarna zaštita | 29 |
| 5.1.6. | Pohrana medija | 29 |
| 5.1.7. | Zbrinjavanje otpada | 29 |
| 5.1.8. | Sigurnosne kopije na drugoj lokaciji | 29 |
| 5.2. | Organizacijske mjere zaštite | 29 |
| 5.2.1. | Povjerljive uloge | 29 |
| 5.2.2. | Broj osoba potrebnih za obavljanje aktivnosti | 30 |
| 5.2.3. | Identifikacija i potvrđivanje identiteta za svaku ulogu | 30 |
| 5.2.4. | Uloge koje zahtijevaju odvajanje dužnosti | 30 |
| 5.3. | Osoblje | 30 |
| 5.3.1. | Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja | 30 |
| 5.3.2. | Procedure provjere prikladnosti osoblja | 30 |
| 5.3.3. | Zahtjevi za školovanjem | 31 |
| 5.3.4. | Periodičko obnavljanje znanja i osvježavanje | 31 |
| 5.3.5. | Učestalost i slijed izmjene zaposlenika | 31 |
| 5.3.6. | Kazne za neovlaštene radnje | 31 |
| 5.3.7. | Zahtjevi na vanjske suradnike | 31 |
| 5.3.8. | Dokumentacija koja je dostupna osoblju | 31 |
| 5.4. | Postupci upravljanja revizijskim zapisima | 31 |
| 5.4.1. | Tipovi događaja koji se zapisuju | 31 |
| 5.4.2. | Učestalost obrade revizijskih zapisa | 32 |
| 5.4.3. | Vremenski period pohrane revizijskih zapisa | 32 |
| 5.4.4. | Zaštita revizijskih zapisa | 32 |
| 5.4.5. | Postupci izrade sigurnosnih kopija revizijskih zapisa | 32 |
| 5.4.6. | Sustav prikupljanja revizijskih zapisa (unutarnji ili vanjski) | 32 |
| 5.4.7. | Obavještanje subjekta uzročnika događaja | 32 |
| 5.4.8. | Procjena ranjivosti | 32 |

| | | |
|---------|--|-----------|
| 5.5. | Arhiviranje zapisa | 33 |
| 5.5.1. | Tipovi arhiviranih zapisa | 33 |
| 5.5.2. | Vremenski period arhiviranja..... | 33 |
| 5.5.3. | Zaštita arhive | 33 |
| 5.5.4. | Postupci izrade sigurnosnih kopija arhive | 33 |
| 5.5.5. | Zahtjevi na zaštitu zapisa vremenskim žigom | 33 |
| 5.5.6. | Sustav prikupljanja arhivskih zapisa (unutarnji ili vanjski) | 33 |
| 5.5.7. | Postupci dobivanja i provjere arhiviranih zapisa..... | 34 |
| 5.6. | Promjena TSU ključa | 34 |
| 5.7. | Oporavak od kompromitiranja ili nepogode | 34 |
| 5.7.1. | Postupci u slučaju incidenta ili kompromitiranja | 34 |
| 5.7.2. | Postupci u slučaju oštećenja u računalnim resursima, programima i/ili podacima | 34 |
| 5.7.3. | Postupci u slučaju kompromitiranja privatnog ključa ili ispada iz sinkroniziranosti s UTC vremenom | 34 |
| 5.7.4. | Mogućnost nastavka poslovanja nakon nepogode..... | 35 |
| 5.8. | Prestanak rada Fina QTSA 2017 servisa | 35 |
| 6. | TEHNIČKE MJERE ZAŠTITE | 37 |
| 6.1. | Generiranje i instalacija para ključeva | 37 |
| 6.1.1. | Generiranje para TSU ključeva | 37 |
| 6.1.2. | Dostava javnog TSU ključa pouzdajućim stranama | 37 |
| 6.1.3. | Duljine ključeva..... | 37 |
| 6.1.4. | Generiranje i provjera kvalitete parametara javnog ključa | 37 |
| 6.1.5. | Namjene ključeva | 37 |
| 6.2. | Zaštita privatnog ključa i tehnike upravljanja kriptografskim modulom..... | 38 |
| 6.2.1. | Norme i tehničke mjere zaštite kriptografskog modula | 38 |
| 6.2.2. | Upravljanje privatnim TSU ključem od strane više osoba (n od m)..... | 38 |
| 6.2.3. | Sigurno skladištenje privatnog ključa | 38 |
| 6.2.4. | Sigurnosno kopiranje privatnog ključa..... | 38 |
| 6.2.5. | Arhiviranje privatnog ključa | 38 |
| 6.2.6. | Prijenos privatnog ključa | 38 |
| 6.2.7. | Spremanje privatnog ključa u kriptografskom modulu | 38 |
| 6.2.8. | Metoda aktivacije privatnog TSU ključa | 39 |
| 6.2.9. | Metoda deaktivacije privatnog TSU ključa..... | 39 |
| 6.2.10. | Metoda uništavanja privatnog TSU ključa | 39 |
| 6.2.11. | Ocjena kriptografskog modula | 39 |
| 6.3. | Ostali vidovi upravljanja parom ključeva..... | 39 |
| 6.3.1. | Arhiviranje javnog ključa | 39 |
| 6.3.2. | Vremenski period važenja Fina QTSA 2017 certifikata i korištenja para TSU ključeva 39 | |
| 6.3.3. | Upravljanje životnim ciklusom kriptografskih modula | 40 |
| 6.4. | Aktivacijski podaci..... | 40 |
| 6.4.1. | Generiranje i instalacija aktivacijskih podataka | 40 |
| 6.4.2. | Zaštita aktivacijskih podataka | 40 |
| 6.5. | Upravljanje računalnom sigurnošću | 40 |
| 6.5.1. | Posebni tehnički zahtjevi na računalnu sigurnost..... | 40 |
| 6.5.2. | Ocjena računalne sigurnosti | 41 |
| 6.6. | Tehničke kontrole životnog ciklusa..... | 41 |
| 6.6.1. | Kontrole razvoja sustava..... | 41 |
| 6.6.2. | Kontrole upravljanja sigurnošću | 41 |

| | | |
|--------|---|-----------|
| 6.6.3. | Sigurnosne kontrole životnog ciklusa | 41 |
| 6.7. | Provjera mrežne sigurnosti | 42 |
| 6.8. | Uporaba vremenskog žiga | 42 |
| 7. | SADRŽAJ CERTIFIKATA, LISTA OPOZVANIH CERTIFIKATA I OCSP PROFILI | 43 |
| 7.1. | Profil certifikata Fina QTSA 2017 | 43 |
| 7.1.1. | Broj(evi) verzije | 43 |
| 7.1.2. | Ekstenzije certifikata | 43 |
| 7.1.3. | Identifikator objekta (OID) algoritama | 43 |
| 7.1.4. | Oblici naziva | 43 |
| 7.1.5. | Ograničenja u nazivima | 43 |
| 7.1.6. | Identifikator objekta (OID) općih pravila izdavanja elektroničkih vremenskih žigova | 43 |
| 7.1.7. | Uporaba ekstenzije <i>Policy Constraints</i> | 44 |
| 7.1.8. | Sintaksa i semantika kvalifikatora općih pravila | 44 |
| 7.1.9. | Procesne semantike za kritičnu ekstenziju <i>Certificate Policies</i> | 44 |
| 8. | PROVJERA SUKLADNOSTI | 45 |
| 8.1. | Učestalost ili okolnosti provjere sukladnosti | 45 |
| 8.1.1. | Vanjska provjera sukladnosti | 45 |
| 8.1.2. | Interna provjera sukladnosti | 45 |
| 8.2. | Identitet/kvalifikacije ocjenitelja | 45 |
| 8.3. | Odnos ocjenitelja s tijelom koje se ocjenjuje | 45 |
| 8.4. | Predmeti ocjenjivanja sukladnosti | 46 |
| 8.5. | Mjere u slučaju neusklađenosti | 46 |
| 8.6. | Priopćavanje rezultata | 46 |
| 9. | OSTALE POSLOVNE I PRAVNE ODREDBE | 47 |
| 9.1. | Naknada za usluge | 47 |
| 9.1.1. | Povrat naknada | 47 |
| 9.2. | Financijska odgovornost | 47 |
| 9.2.1. | Pokrivenost osiguranjem | 47 |
| 9.2.2. | Druga sredstva | 47 |
| 9.2.3. | Osiguranje ili garancije krajnjim korisnicima | 47 |
| 9.3. | Povjerljivost poslovnih podataka | 47 |
| 9.3.1. | Opseg povjerljivih poslovnih podataka | 47 |
| 9.3.2. | Podaci koji se ne smatraju povjerljivim poslovnim podacima | 48 |
| 9.3.3. | Odgovornost za zaštitu povjerljivih poslovnih podataka | 48 |
| 9.4. | Zaštita osobnih podataka | 48 |
| 9.4.1. | Plan zaštite osobnih podataka | 48 |
| 9.4.2. | Povjerljivi osobni podaci | 48 |
| 9.4.3. | Osobni podaci koji nisu povjerljivi | 48 |
| 9.4.4. | Odgovornost za zaštitu osobnih podataka | 49 |
| 9.4.5. | Ovlaštenje za korištenje osobnih podataka | 49 |
| 9.4.6. | Dostupnost podataka mjerodavnim tijelima | 49 |
| 9.4.7. | Ostale okolnosti objave podataka | 49 |
| | Nema odredbi | 49 |
| 9.5. | Prava intelektualnog vlasništva | 49 |
| 9.6. | Obveze Fina QTSA 2017 sudionika | 49 |

| | | |
|---------|---|----|
| 9.6.1. | Obveze Fine | 49 |
| 9.6.2. | Obveze RA | 50 |
| 9.6.3. | Obveze Korisnika..... | 50 |
| 9.6.4. | Obveze pouzdajućih strana | 51 |
| 9.7. | Odgovornosti sudionika Fina QTSA 2017 servisa | 51 |
| 9.7.1. | Odgovornosti Fine | 51 |
| 9.7.2. | Odgovornosti Korisnika..... | 51 |
| 9.7.3. | Odgovornosti pouzdajućih strana..... | 52 |
| 9.8. | Odricanje od odgovornosti Fina QTSA..... | 52 |
| 9.9. | Ograničenja odgovornosti | 52 |
| 9.10. | Naknada štete | 52 |
| 9.11. | Trajanje i prestanak važenja..... | 53 |
| 9.11.1. | Trajanje | 53 |
| 9.11.2. | Prestanak važenja | 53 |
| 9.11.3. | Posljedice prestanka važenja i nastavak djelovanja..... | 53 |
| 9.12. | Individualne obavijesti i komunikacija sa sudionicima | 53 |
| 9.13. | Izmjene i dopune | 54 |
| 9.13.1. | Procedure izmjena i dopuna | 54 |
| 9.13.2. | Mehanizmi obavještanja i vremenski periodi | 54 |
| 9.13.3. | Okolnosti pod kojima se mora mijenjati OID..... | 54 |
| 9.14. | Postupak rješavanja sporova | 54 |
| 9.15. | Važeći propisi..... | 55 |
| 9.16. | Usklađenost s primjenjivim propisima..... | 55 |
| 9.17. | Razne odredbe..... | 55 |

AUTORSKA PRAVA

Ova Opća pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova su Finino vlasništvo, administrirana su od strane Fina PMA te su podložna zaštiti autorskih prava prema zakonima u Republici Hrvatskoj.

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 elektroničkom potpisu (NN 10/2002)
- [3] Zakon o izmjenama i dopunama zakona o elektroničkom potpisu (NN 80/2008)
- [4] Zakon o izmjeni zakona o elektroničkom potpisu (NN 30/2014)

Podzakonski akti

- [5] Pravilnik o evidenciji davatelja usluga certificiranja u Republici Hrvatskoj (NN 107/2010)
- [6] Pravilnik o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN 107/2010)
- [7] Pravilnik o izmjenama i dopunama Pravilnika o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN 89/2013)

Ostala zakonska regulativa

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

Normizacijski dokumenti

- [9] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- [10] 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
- [11] ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
- [12] ETSI EN 319 411-1 V1.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- [13] ETSI EN 319 411-2 V2.1.1. (2016-02) – 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
- [14] 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

- [15] ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- [16] ETSI TS 119 312 V1.1.1. (2014-11) – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
- [17] IETF RFC 3161 (2001) Internet X.509: Public Key Infrastructure: Time Stamp Protocol (TSP)
- [18] IETF RFC 3739 - Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
- [19] IETF RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [20] IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (2013)
- [21] NIST FIPS PUB 140-2:2002 - Security Requirements for Cryptographic Modules
- [22] ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements
- [23] ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls

Finini dokumenti

- [24] Opća pravila pružanja usluga certificiranja i Pravilnik o postupcima certificiranja za Fina Root CA, CP/CPS_{ROOT}
- [25] Pravilnik o postupcima pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova, QTPS
- [26] Pravilnik o postupcima certificiranja za nekvalificirane certifikate, CPS_{NQC-eIDAS}

1. UVODNE OZNAKE I TEMELJNI PODACI

Fina je kao pružatelj usluga izdavanja kvalificiranih certifikata i vremenskih žigova upisana pod evidencijskim brojem HR-QC-2008-07-16-1 u Evidenciju davatelja usluga certificiranja u Republici Hrvatskoj koju vodi središnje tijelo državne uprave nadležno za poslove gospodarstva.

Finin servis izdavanja kvalificiranih vremenskih žigova pod nazivom Fina QTSA 2017 dio je postojeće Fina PKI produkcijske okoline.

Fina QTSA 2017 izdaje kvalificirane vremenske žigove koji se mogu koristiti zajedno s kvalificiranim certifikatima, a izdaju se na sustavu koji je po razini sigurnosti izjednačen sa sustavom za izdavanje kvalificiranih certifikata.

1.1. Pregled

Ovaj dokument Opća pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova (engl.: *Qualified Time-Stamp Policy*, QTP) sadrži Finina pravila za pružanje usluga izdavanja kvalificiranih elektroničkih vremenskih žigova.

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

Sadržaj ovih Općih pravila usklađen je s normizacijskim dokumentima:

- ETSI EN 319 401 [9],
- ETSI EN 319 421 [10],
- ETSI EN 319 422 [11],
- ETSI TS 119 312 [16].

Svrha ovih Općih pravila je definiranje i uređivanje pravila i načela prema kojima trebaju postupati Fina QTSA, korisnici usluge izdavanja kvalificiranih elektroničkih vremenskih žigova (u daljnjem tekstu: Korisnici) i pouzdajuće strane.

Za tumačenje odredaba ovih Općih pravila mjerodavne su odredbe Uredbe (EU) br. 910/2014 [1], Zakona o elektroničkom potpisu [2], [3] i [4], podzakonskih akata [5], [6] i [7] donesenih temeljem tog zakona te normizacijskih dokumenata i preporuka na koje isti upućuju.

Kvalificirani elektronički vremenski žigovi izdani prema ovim Općim pravilima usklađeni su sa zahtjevima norme ETSI EN 319 421 [10].

Fina kao pružatelj usluga izdavanja kvalificiranih elektroničkih vremenskih žigova uključuje svoj vlastiti OID u vremenske žigove koje izdaje. U Fininim kvalificiranim elektroničkim vremenskom žigovima nalazi se identifikator ovih Opća pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova (QTP OID: 1.3.124.1104.2.3.2.1.0).

Pružanje usluge izdavanja kvalificiranih elektroničkih vremenskih žigova sukladno je s ETSI općim pravilima najboljih standarda struke (engl.: *Best practices Time-Stamp Policy*, BTSP):

- ETSI EN 319 421[10]
BSTP: *Best practices Time-Stamp Policy*
OID: 0.4.0.2023.1.1

1.2. Naziv dokumenta i identifikacijski podaci

OID za Finu dodijeljen je od strane *British Standards Institution (BSI) International Code Designator (ICD)*. Na temelju tog OID-a Fina je za potrebe 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: Opća pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova
- Verzija: 1.0
- Datum stupanja na snagu: 22.05.2017.
- OID: 1.3.124.1104.2.3.1.1.0
- Internetska adresa na kojima je objavljena javna verzija ovih Opća pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova je:

<http://rdc.fina.hr/QTSA2017/FinaQTSA2017-QTP1-0-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 vremenskih žigova).

1.3.2. Korisnici

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

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

Pouzdanje strane su fizičke osobe ili poslovni subjekti koji su primatelji kvalificiranih elektroničkih vremenskih žigova i djeluju temeljem razumnog pouzdanja u vremenske žigove koje izdaje Fina QTSA 2017.

1.3.5. Ostali sudionici

Nema odredbi.

1.4. Primjerena uporaba vremenskih žigova

Kvalificirani 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 vremenskom žigu. Kvalificirani vremenski žigovi koje izdaje Fina QTSA 2017 koriste se i za očuvanje dugotrajnosti elektroničkih potpisa.

1.4.1. Zabrane uporabe vremenskih žigova

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

1.5. Administracija Općih pravila

1.5.1. Organizacija odgovorna za održavanje dokumenta Opća pravila

Za izradu i održavanje ovog dokumenta Općih pravila ovlaštena je i odgovorna Fina.

Ovlaštene osobe iz organizacijskih jedinica Fina koje sudjeluju u izradi, održavanju, implementaciji i odobravanju pravila i postupaka u Fina PKI koja se primjenjuju u pružanju usluga povjerenja u daljnjem tekstu nazivaju se zajedničkim nazivom Fina PMA.

Promjene sadržaja ovog dokumenta Općih pravila 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 ovih Općih pravila:

Poštanska adresa:

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

telefon: +385-1-6128-171

telefax: +385-1-6304-081

E-mail: pma@fina.hr

1.5.3. Tijelo koje utvrđuje usklađenost QTPS dokumenta s Općim pravilima

Usklađenost QTPS dokumenta [25] s ovim Općim pravilima utvrđuje Fina PMA.

1.5.4. Procedure odobravanja QTPS dokumenta

Izrada, odobravanje i stupanje na snagu QTPS dokumenta [25] kojom se potvrđuje njegova sukladnost s ovim Općim pravilima opisana je u točki 1.5.1. i 9.13.1. ovih Općih pravila.

1.6. Definicije i kratice

1.7. 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. |
| 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 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: <ol style="list-style-type: none"> 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 potpis | Podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje Potpisnik koristi za potpisivanje. |
| 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. <i>Trusted Third Party</i>). |
| Fina RA mreža | Mreža registracijskih ureda u Fini, a sastoji se od Središnjeg RA Fine i Fina LRA ureda. |

| POJAM | DEFINICIJA |
|--|--|
| Fizička osoba - građanin | Fizička osoba koja uslugu certificiranja traži sa svrhom korištenja certifikata 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 <i>online</i> 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. |
| Jedinica za izradu vremenskog žiga (TSU) | Hardver i softver združen u jednu cjelinu koja u danom trenutku ima samo jedan aktivan potpisni ključ za izradu vremenskog žiga. |
| Koordinirano svjetsko vrijeme (UTC) | Vremenska ljestvica koja se temelji na sekundi kako je definirana ITU-R preporukom TF.460-5. Za većinu primjena u praksi UTC je ekvivalentan srednjem sunčevom vremenu na nultom meridijanu (0°). Točnije, UTC je kompromis između vrlo stabilnog atomskog vremena (<i>Temps Atomique International</i> - 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: <ul style="list-style-type: none"> • 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 usluga 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 vremenski žig | Elektronički vremenski žig koji ispunjava sljedeće zahtjeve: <p>(a) povezuje datum i vrijeme s podacima na način kojim se u razumnoj mjeri isključuje mogućnost nezapažene promjene podataka;</p> <p>(b) temelji se na izvoru točnog vremena povezanom s koordiniranim svjetskim vremenom; i</p> <p>(c) potpisan je pomoću naprednog elektroničkog potpisa ili pečaćen pomoću naprednog elektroničkog pečata kvalificiranog pružatelja usluga povjerenja ili jednakovrijednom metodom.</p> |
| Kvalificirani pružatelj usluga povjerenja | Pružatelj usluga povjerenja koji pruža jednu ili više kvalificiranih usluga povjerenja i kojemu je nadzorno tijelo odobrilo kvalificirani status. |
| Lista opozvanih certifikata (CRL) | Potpisana lista u kojoj su naznačeni certifikati koje izdavatelj certifikata više ne smatra valjanim. |

| POJAM | DEFINICIJA |
|---|---|
| Napredan elektronički pečat | Elektronički pečat koji ispunjava sljedeće zahtjeve: (a) na nedvojbenu 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 nedvojbenu 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 usluge izdavanja vremenskih žigova - <i>Time-Stamp Policy (TP)</i> | Imenovani skup pravila koji ukazuje na primjenjivost vremenskog žiga za određenu skupinu i/ili klasu primjena sa zajedničkim zahtjevima na sigurnost. |
| Opoziv certifikata | Radnja koja certifikat nepovratno čini nevažećim od trenutka opoziva. |
| Par ključeva | Dva jedinstveno povezana kriptografska ključa, od kojih je jedan privatni ključ, a drugi javni ključ. |
| 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 verifikiranja potpisa. |

| POJAM | DEFINICIJA |
|--|---|
| Poslovni subjekt | <ol style="list-style-type: none"> 1. Pravne osobe, primjerice <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • tijela državne vlasti; • tijela državne uprave; • državne agencije i dr. 3. Fizičke osobe s registriranom djelatnošću, primjerice <ul style="list-style-type: none"> • obrtnici; • odvjetnici; • javni bilježnici i dr. |
| Potpisnik | Fizička osoba koja izrađuje elektronički potpis. |
| Pouzdanja strana | Fizička osoba ili poslovni subjekt koji se oslanja na elektroničku identifikaciju ili uslugu povjerenja. |
| Pouzdan popis | Popis države članice EU koji pruža informacije o statusu i povijesti statusa usluga povjerenja pružatelja usluga povjerenja u odnosu na usklađenost s važećim zahtjevima i odgovarajućim odredbama važećih propisa (engl. <i>Trusted List</i>). |
| Povjerljive uloge | Uloge o kojima ovisi sigurnost rada pružatelja usluga povjerenja. Povjerljive uloge (engl. <i>Trusted Roles</i>) 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. |
| Pripadajuća osoba | Fizička osoba zaposlena u Poslovnom subjektu ili na drugi način povezana s Poslovnim subjektom, a koja je od strane istog Poslovnog subjekta autorizirana za dobivanje certifikata. Takav certifikat identificira osobu i Poslovni subjekt te naznačuje da je ta osoba povezana s Poslovnim subjektom. |
| 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“. |
| 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 <i>mutatis mutandis</i> 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 | Radnja koja certifikat čini nevažećim od trenutka suspenzije. Suspendirani certifikat se reaktivacijom može ponovno učiniti važećim. |
| Sustav certificiranja | Sustav IT proizvoda i komponenti organiziranih za pružanje usluga certificiranja. |
| 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. <i>Policy Management Authority</i>) |
| TSA sustav | Sustav IT proizvoda i komponenti organiziranih za pružanje usluga izdavanja vremenskih žigova. |
| Usluga povjerenja | Elektronička usluga koja se u pravilu pruža uz naknadu i koja se sastoji od: (a) izrade, verifikacije i validacije elektroničkih potpisa, elektroničkih pečata ili elektroničkih vremenskih žigova, usluge elektroničke preporučene dostave i certifikata koji se odnose na te usluge; ili (b) izrade, verifikacije i validacije certifikata za autentikaciju mrežnih stranica; ili (c) čuvanja elektroničkih potpisa, pečata ili certifikata koji se odnose na te usluge. |
| 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. |

| POJAM | DEFINICIJA |
|-----------------------------|---|
| Verifikacija potpisa | Proces provjere kriptografske vrijednosti potpisa korištenjem podataka za verifikaciju potpisa. |

Tablica 1.1. Definicije

1.8. Kratice

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

Tablica 1.2. Kratice

2. OBJAVE I ODGOVORNOSTI ZA REPOZITORIJ

2.1. Identifikacija tijela koje vodi repozitorij

Fina PKI repozitorij vodi Fina kao kvalificirani pružatelj usluga povjerenja. Fina je odgovorna za rad Fina PKI 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 vremenskih žigova

Na Fina PKI repozitoriju javno su objavljeni dokumenti i informacije o pružanju usluga izdavanja vremenskih žigova:

- aktualna Opća pravila pružanja usluga izdavanja kvalificiranih vremenskih žigova;
- aktualni Pravilnik o postupcima pružanja usluga izdavanja kvalificiranih vremenskih žigova;
- prijašnje verzije Općih pravila pružanja usluga izdavanja kvalificiranih vremenskih žigova i Pravilnika o postupcima davanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova;
- 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 vremenskih žigova;
- cjenik usluga izdavanja vremenskih žigova;
- obrazac zahtjeva za pristupanje FINA Servisu vremenske ovjere;
- informacije o certifikatu za potpis vremenskog žiga;
- aktualne lokacije Fina RA/LRA ureda;
- Korisničke upute;
- obavijesti korisnicima vezane uz pružanje usluga izdavanja vremenskih žigova;
- ostale informacije vezane uz rad Fina QTSA.

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.

2.3. Vrijeme ili učestalost objavljivanja

Fina na godišnjoj razini i prema potrebi održava i ažurira Opća pravila pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova i Pravilnik o postupcima pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova 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 svim sudionicima Fina PKI.

Fina na repozitoriju ima uspostavljene kontrole pristupa u cilju sprječavanja neautoriziranog dodavanja, promjene ili brisanja informacija te zaštite njihove cjelovitosti i autentičnosti. 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 (u daljnjem tekstu: elektronički vremenski žig) samo registriranim korisnicima koji posjeduju Finin autentikacijski certifikat ili Finin aplikacijski certifikat.

Ako Korisnik već ima Finin digitalni certifikat kojim će pristupiti Fininom servisu za izdavanje elektroničkih vremenskih žigova treba popuniti i ovjeriti pristupnicu za Fininu uslugu izdavanja elektroničkih vremenskih žigova te je zajedno s dva primjerka ovjerenih ugovora o korištenju usluge izdavanja elektroničkih vremenskih žigova dostaviti u Fina LRA. Obrazac pristupnice i ugovora nalaze se na internetskim stranicama Fina <http://www.fina.hr/finadigicert>.

Ako Korisnik nema Finine digitalne certifikate, uz pristupnicu i ugovore za korištenje usluge vremenskog žiga treba zatražiti i izdavanje Fininog digitalnog certifikata kojim će pristupiti Fininjoj usluzi izdavanja elektroničkih vremenskih žigova.

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

3.1.1. Inicijalno utvrđivanje identiteta Korisnika

Fina prikuplja osobne podatke fizičkih osoba i podatke poslovnih subjekata isključivo za potrebe registracije u cilju izdavanja certifikata.

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-eIDAS} [27].

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

Za registrirane Korisnike Fininih digitalnih certifikata već je provedena identifikacija Korisnika pa za korištenje usluge izdavanja elektroničkih vremenskih žigova Korisnici u Fina LRA registracijski ured 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 naprednim elektroničkim potpisom uz korištenje kvalificiranog certifikata.

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 pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova i propisima koji uređuju pružanje usluge izdavanja elektroničkih vremenskih žigova, sklapaju Korisnici i Fina kao pružatelj usluge.

3.2. Identifikacija i autentikacija na Fina QTSA 2017 servis

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

Fina QTSA može Korisnicima koji posjeduju autentikacijski ili aplikacijski certifikat odobriti i drugi odgovarajući način autentikacije Korisnika (npr. korisničko ime i zaporka).

URL adrese za autentikaciju na Fina QTSA 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 vremenskih žigova temeljem IP adresnog područja za Finine korisnike.

3.3. Certifikat jedinice za izradu vremenskog žiga

Fina QTSA javno objavljuje javni ključ jedinice za izradu vremenskog žiga (TSU) kao sadržaj certifikata Fina QTSA 2017 na repozitoriju iz točke 2.2. ovih Općih pravila.

Certifikat za TSU izdaje Fina RDC 2015 CA sukladno zahtjevima normi ETSI EN 319 411-2 [13].

Prije početka izdavanja elektroničkih vremenskih žigova Fina QTSA 2017 učitava svoj certifikat za TSU. Pri dobivanju svojeg TSU certifikata Fina QTSA 2017 provjerava je li Fina RDC 2015 CA ispravno potpisao TSU certifikat.

3.4. Elektronički vremenski žig

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 ovih općih pravila po kojem je izdan (QTP OID);
- da ima jedinstveni identifikator;
- da se vrijeme korišteno u TSU može povezati sa stvarnim vremenom dostavljenim od pouzdanog izvora;
- da sadrži točan podatak o vremenu iz TSU u vrijeme izdavanja elektroničkog vremenskog žiga;
- da sadrži *hash* reprezentaciju elektroničkog zapisa za koji se izdaje elektronički vremenski žig;

- da je potpisan privatnim TSU ključem koji ima isključivu namjenu potpisivanja vremenskog žiga;
- identifikator države u kojoj je Fina QTSA ima sjedište;
- identifikator za Fina QTSA 2017;
- identifikator TSU koja je izdala elektronički vremenski žig.

Elektronički vremenski žig izdaje se sukladno preporuci ITF RFC 3161 [17] i normi ETSI EN 319 421 [10] te s profilom usklađenim s normom ETSI EN 319 422 [11].

Samo jedan privatni TSU ključ je istovremeno aktivan.

Fina QTSA 2017 servis za izdavanje elektroničkih vremenskih žigova podržava zahtjeve za izdavanje elektroničkih vremenskih žigova sukladno normi ETSI EN 319 422 [11] i preporuci IETF RFC 3161 [17].

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

Zahtjev za izdavanje elektroničkog vremenskog žiga u skladu je s normom ETSI EN 319 422 [11] i točkom 2.4.2. u dokumentu IETF RFC 3161 [17].

Podražana polja u zahtjevu za izdavanje elektroničkog vremenskog žiga opisana su u QTPS dokumentu [25].

Korisnik koji od Fina QTSA 2017 zahtijeva izdavanje vremenskog žiga mora ostvariti autenticiranu konekciju 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 vremenskog žiga, treba podržavati protokol za elektronički vremenski žig sukladan s preporukom IETF RFC 3161 [17].

3.4.2. Odgovor servisa za izdavanje elektroničkih vremenskih žigova (*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 [11] i točkom 2.4.2. u dokumentu IETF RFC 3161 [17].

Podražana polja odgovoru Fina QTSA 2017 servisa za izdavanje elektroničkih vremenskih žigova opisana su u QTPS dokumentu [25].

3.5. Profil vremenskog žiga

Osnovni podaci o profilu kvalificiranih 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: 1.3.124.1104.2.3.1.1.0 ETSI OID: 0.4.0.2023.1.1 |
| messageImprint | Podržani hash algoritmi: <ul style="list-style-type: none"> • hashAlgorithm: sha-256 (OID: 2.16.840.1.101.3.4.2.1) |

| Polje | Vrijednosti za kvalificirani elektronički vremenski žig kojeg izdaje Fina QTSA 2017 servis |
|--------------------|--|
| serialNumber | Cijeli broj |
| genTime | UTC vrijeme, razlučivost od razlučivost od 1 s |
| Nonce | Cijeli broj |
| signatureAlgorithm | sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) |

Tablica 3.1. Osnovni podaci o kvalificiranom elektroničkom vremenskom žigu kojeg izdaje Fina QTSA 2015 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 zajamčenu točnost 1 s.

3.7. Sinkronizacija sata s UTC

Fina QTSA osigurava da je vrijeme Fina QTSA 2017 sustava sinkronizirano s UTC vremenom, unutar preciznosti propisane u točki 3.6. ovih Općih pravila, 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 automatski prelazi na alternativni pouzdani izvor UTC vremena.

3.7.1. Ljetno računanje vremena

Fina QTSA 2017 servis u izdanim elektroničkim vremenskim žigovima upisuje 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 vremenskog žiga

Provjeru valjanosti elektroničkog potpisa Fina QTSA 2017 servisa u vremenskom žigu pouzdajuće strane trebaju provoditi prema zahtjevima normizacijskog dokumenta ETSI EN 319 102-1 [15].

Provjera valjanosti elektroničkog vremenskog žiga obuhvaća sljedeće provjere:

- provjeru da podaci za koje je tražen elektroničkim vremenski žig povezani s tim elektroničkim vremenskim žigom i TSU certifikatom Fina QTSA 2017 servisa;
- validaciju potpisa kojim je potpisa elektronički vremenski žig,
- provjeru da izdani elektronički vremenski žig ispunjava specifične zahtjeve u pogledu točnosti, pouzdanosti i odgovornosti Fina QTSA 2017 servisa, odnosno Fina kao kvalificiranog pružatelja usluga.

3.9. Raspoloživost usluge

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

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

Servis Fina QTSA 2017 koristi siguran HTTPS protokol (TLS) - uz klijentsku autentikaciju certifikatom – *two-way* TLS).

4. OPERATIVNI ZAHTEVI NA ŽIVOTNI CIKLUS CERTIFIKATA ZA FINA QTSA 2017

4.1. Izdavanje certifikata

Izdavanje Fina QTSA 2017 certifikata obavljaju ovlaštene osobe s povjerljivim ulogama u Fina PKI, pod dualnom kontrolom, u Fina PKI štíćenom prostoru.

4.2. Opoziv i suspenzija certifikata

Opoziv certifikata za Fina QTSA 2017 servis provodi se sukladno sukladni 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 nedosupnosti ili gubitka privatnog ključa;
- u slučaju zabranjene uporabe privatnog TSU ključa;
- ako Fina procjeni da Fina QTSA 2017 certifikat svojim tehničkim karakteristikama, profilom ili sadržajem ne pruža prikladnu razinu povjerenja pouzdajućim stranama;
- ako Fina QTSA 2017 prestaje s radom, a Fina nije u mogućnosti osigurati nastavak pružanja usluga kod drugog kvalificiranog pružatelja usluga;
- ako certifikat nije izdan sukladno zahtjevu ili odredbama ovih Općih pravila.

4.2.2. Tko može tražiti opoziv

Zahtjev za opoziv Fina QTSA 2017 certifikata može podnijeti ovlaštena osoba u Fina QTSA uz odobrenje odgovorne osobe Fina QTSA.

4.2.3. Profil CRL

Profil CRL sukladan je preporuci IETF RFC 5280 [19].

4.2.4. 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 prethodnog izdavanja CRL.

4.2.5. Maksimalno kašnjenje za CRL

Maksimalno kašnjenje CRL od trenutka njenog izdavanja do trenutka objave u redovitim uvjetima iznosi dvije minute.

4.2.6. *Online* dostupnost provjere opozvanih certifikata/statusa 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 [20].

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.

4.2.7. Drugi dostupni načini objave opozvanih certifikata

Nema odredbi.

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 izdavanja kvalificiranih certifikata i kvalificiranih elektroničkih vremenskih žigova primjenjuje mjere fizičke zaštite sustava certificiranja s ciljem minimiziranja rizika vezanih uz fizički zaštitu i u skladu s poslovnom politikom Fine, važećom zakonskom regulativom i međunarodnim preporukama.

5.1.1. Lokacija objekta i konstrukcija

Primarni produkcijski Fina QTSA 2017 sustav smješten je u zgradi Fine, u posebnom štíćenom prostoru izdvojenom za tu namjenu uz primjenu više razina fizičke i tehničke zaštite koje onemogućuju neovlašten fizički pristup sustavu i podacima i time sprječavaju kompromitiranje sustava i usluga. Fizička zaštita temeljena je na konceptu uporabe sigurnosnih zona te se razina zaštite povećava svakim prolaskom u sljedeću zonu. Fizička zaštita od upada ostvarena je sigurnosnim perimetrima koji razdvajaju zone postavljene oko sustava certificiranja.

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

Sigurni prostori i podprostori u kojima se nalaze komponente Fininog sustava certificiranja na primarnoj i sekundarnoj lokaciji u daljnjem tekstu nazivaju se zajedničkim nazivom Fina PKI štíćeni prostor.

5.1.2. Fizički pristup

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

Osobama koje nemaju ovlaštenje fizičkog pristupa sustavu certificiranja pristup je dozvoljen samo u pratnji ovlaštenih osoba i sukladno Fininim internim procedurama.

O svakom pristupu sustavima certificiranja vodi se evidencija.

Fizički pristup podacima registriranih korisnika koje prikuplja RA mreža imaju samo ovlašteni zaposlenici Fina PKI i ovlašteni zaposlenici Fina RA mreže koji osobne podatke o fizičkim

osobama prikupljaju, pohranjuju, koriste i brišu u skladu s odgovarajućim propisima o zaštiti osobnih podataka.

5.1.3. Sustavi za napajanje i klimatizaciju

Uređaji i prostor u kojem se nalazi Fina QTSA 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.

5.1.4. Opasnost od poplave

Lokacija na kojoj se nalazi Fina QTSA sustav, Fina RA sustav i repozitorij zaštićena je od poplave.

5.1.5. Protupožarna zaštita

Fina QTSA sustav, Fina RA sustav i repozitorij zaštićeni su sustavom za detekciju požara i sustavom za automatski gašenje požara sukladno važećoj zakonskoj regulativi.

5.1.6. Pohrana medija

Mediji na kojima se nalaze arhivske i sigurnosne kopije Fina PKI podataka u elektroničkom obliku, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na dvije odvojene štćene lokacije s uspostavljenom protupožarnom zaštitom i koje su osigurane od poplave. Ovi mediji zaštićeni su od oštećenja, krađe i neovlaštenog pristupa.

5.1.7. Zbrinjavanje otpada

Uređaji i mediji koji sadrže povjerljive informacije u elektroničkom obliku, a koji više nisu potrebni, sigurnosno se uništavaju tako da povjerljive informacije ne mogu više biti čitljive niti obnovljene. Uništavanje ovih uređaja i medija odvija se pod nadzorom ovlaštenih osoba u Fina PKI.

Papirnati dokumenti i materijali koji sadrže povjerljive informacije sigurnosno se uništavaju prije odlaganja u otpad.

5.1.8. Sigurnosne kopije na drugoj lokaciji

Sigurnosne kopije Fina QTSA i Fina RA sustava, arhivske ili sigurnosne kopije podataka, kopije sadržaja repozitorija te sigurnosne kopije programske opreme pohranjuju se na lokaciji sekundarnog sustava certificiranja koji je izdvojen od primarnog produkcijskog sustava certificiranja. Ove su sigurnosne kopije u odnosu na njihove originale zaštićene jednakom ili višom razinom mjera fizičke zaštite.

5.2. Organizacijske mjere zaštite

5.2.1. Povjerljive uloge

Poslovi upravljanja informacijskim i komunikacijskim sustavom, poslovi upravljanja izdavanjem elektroničkih vremenskih žigova, administriranje i implementacije sigurnosnih postupaka te poslovi nadzora djelovanja Fina PKI obavljaju se unutar odvojenih organizacijskih jedinica Fine.

Poslovi, obaveze i odgovornosti zaposlenika podijeljene su prema odgovarajućim povjerljivim ulogama. Povjerljive uloge čine temelj povjerenja u Fina PKI i dodjeljuju se ovlaštenim

zaposlenicima iz nadležnih organizacijskih jedinica Fine. Svaka povjerljiva uloga je dokumentirana s jasno definiranim opisom poslova i odgovornostima.

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

5.2.2. Broj osoba potrebnih za obavljanje aktivnosti

Poslove u Fina PKI obavljaju isključivo ovlaštene osobe. 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 Općih pravila.

Pristup i poslovi u Fina PKI štíćenom prostoru provode se isključivo uz istovremenu prisutnost najmanje dvije osobe s povjerljivim ulogama koje imaju dozvole pristupa tom sustavu.

Za obavljanje pojedinih sigurnosno osjetljivih zadataka u Fina PKI štíćenom prostoru zahtjeva se sudjelovanje propisanog broja osoba s određenim povjerljivim ulogama.

5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu

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.

5.2.4. Uloge koje zahtijevaju odvajanje dužnosti

Zbog sigurnosnih zahtjeva izdavanja kvalificiranih certifikata provodi se odvajanje sljedećih dužnosti:

- osobi kojoj je dodijeljena povjerljiva uloga Službenik za sigurnost ili Službenik za registraciju ne dodjeljuje se povjerljiva uloga Službenik za nadzor sustava;
- osobi kojoj je dodijeljena povjerljiva uloga Administrator sustava ne dodjeljuje se povjerljiva uloga Službenik za sigurnost ili Službenik za nadzor sustava.

5.3. Osoblje

5.3.1. Kvalifikacije, radno iskustvo i zahtjevi za provjerom osoblja

Prije početka rada na poslovima 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.

Zaposlenici koji rade na poslovima Fina PKI ne smiju biti u radnom, odnosno poslovnom odnosu s drugim pružateljima usluga povjerenja.

5.3.2. Procedure provjere prikladnosti osoblja

Prije početka rada na poslovima Fina PKI, Fina provodi odgovarajuće provjere kandidata u cilju procijene njihove stručnosti, sposobnosti i pouzdanosti u skladu s potrebama poslova Fina PKI.

5.3.3. Zahtjevi za školovanjem

Zaposlenicima koji obavljaju poslove unutar Fina PKI osigurava se školovanje i usavršavanje sukladno s njihovim povjerljivim ulogama.

5.3.4. Periodičko obnavljanje znanja i osvježavanje

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

Zaposlenici Fina PKI s povjerljivim ulogama u Fina PKI imaju obavezu stjecati i usavršavati svoje znanje.

Obnova znanja zaposlenika Fina RA mreže, a obzirom na poslove koje obavljaju, provodi se redovito, najmanje jednom u dvije godine.

5.3.5. Učestalost i slijed izmjene zaposlenika

Nema odredbi.

5.3.6. Kazne za neovlaštene radnje

Nepridržavanje propisanih mjera za ovlaštene osobe pri radu u Fina PKI podliježe povredi radne obveze prema Kolektivnom ugovoru, 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

Za ugovorene vanjske suradnike koji za Finu obavljaju dio usluga iz opsega usluga izdavanja kvalificiranih certifikata vrijede isti zahtjevi pri radu u Fina PKI kao i za interne zaposlenike.

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 sukladno dodijeljenoj povjerljivoj ulozi i pripadnim ovlaštenjima.

5.4. Postupci upravljanja revizijskim zapisima

5.4.1. Tipovi događaja koji se zapisuju

Revizijski zapisi Fina QTSA 2017 sustava sadrže zapise o događajima vezanim uz:

- upravljanje životnim ciklusom TSU ključeva Fina QTSA 2017 sustava;
- upravljanje životnim ciklusom TSU certifikata za Fina QTSA 2017 sustav;
- sinkronizaciju TSU sata s UTC;
- detekciju ispada iz sinkroniziranosti s UTC vremenom;

Revizijski zapisi sadrže i zapise o sigurnosnim događajima u Fina PKI vezanim uz promjene sigurnosnih politika, fizičku i tehničku zaštitu Fina PKI šticećenog prostora, pokretanje i zaustavljanje rada sustava, sistemске greške i kvarove hardvera, aktivnosti vatrozida i usmjerivača i dr.

5.4.2. Učestalost obrade revizijskih zapisa

Preglede revizijskih zapisa Fina QTS 2017 sustava obavlja Službenik za nadzor sustava. Pregledi revizijskih zapisa obavljaju se redovito, jednom dnevno radnim danima, te u slučaju izvanrednih situacija.

Postupak pregleda revizijskih zapisa obuhvaća:

- pregled stavki dnevnika sustava koje su stvorene nakon posljednje revizije;
- po potrebi, pripremu sažetog izvještaja koji sadrži objašnjenja važnih događaja.

5.4.3. Vremenski period pohrane revizijskih zapisa

Revizijski zapisi iz točke 5.4.1. ovih Općih pravila čuvaju se najmanje 10 godina od izdavanja elektroničkog vremenskog žiga na kojeg se zapisi odnose.

5.4.4. Zaštita revizijskih zapisa

Revizijski zapisi u Fina PKI zaštićeni su tijekom cijelog vremena čuvanja. Zaštita dnevnika sustava obuhvaća zaštitu zapisa od njihovog neovlaštenog čitanja i otkrivanja te očuvanje cjelovitosti zapisa.

Tako zaštićeni revizijski zapisi na zahtjev su raspoloživi samo ovlaštenim osobama, posebice u svrhu pružanja dokaza o vremenskom žigu za potrebe sudskih postupaka.

5.4.5. Postupci izrade sigurnosnih kopija revizijskih zapisa

Revizijski zapisi Fina PKI sustava arhiviraju se u dvije kopije na fizički odvojenim lokacijama.

Kopije revizijskih zapisa na sekundarnoj lokaciji zaštićuju se jednakom ili višom razinom zaštite u odnosu na revizijske zapise na primarnoj lokaciji (vidi točku 5.4.4.).

5.4.6. Sustav prikupljanja revizijskih zapisa (unutarnji ili vanjski)

Ovisno o vrsti podataka, revizijski zapisi prikupljaju se automatski ili ih prikuplja ovlaštena osoba.

Revizijski zapisi nastali u Fina PKI i Fina RA mreži prikupljaju se interno.

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.

5.5. Arhiviranje zapisa

5.5.1. Tipovi arhiviranih zapisa

Fina PKI 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. ovih Općih pravila;
- drugi Finini interni dokumenti.

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

5.5.2. Vremenski period arhiviranja

Sve arhivirane podatke i dokumentaciju Fina čuva najmanje 10 godina.

5.5.3. Zaštita arhive

Arhivirani podaci i dokumentacija zaštićuju se mehanizmima i postupcima propisane razine sigurnosti koje osiguravaju povjerljivost i cjelovitost arhive. Arhiva se štiti od neovlaštenog pregleda, modificiranja i brisanja podataka.

Tako zaštićeni arhivirani zapisi na zahtjev su raspoloživi samo ovlaštenim osobama, posebice u svrhu pružanja dokaza o izdanom vremenskom žigu za potrebe sudskih postupaka.

5.5.4. Postupci izrade sigurnosnih kopija arhive

Sigurnosna kopija arhiviranih podataka u elektroničkom obliku izrađuje se u Fina PKI štićenom prostoru te se čuva na siguran način na drugoj lokaciji izdvojeno od primarnog produkcijskog sustava certificiranja, sukladno točki 5.1.8. ovih Općih pravila.

5.5.5. Zahtjevi na zaštitu zapisa vremenskim žigom

Nema odredbi.

5.5.6. Sustav prikupljanja arhivskih zapisa (unutarnji ili vanjski)

Zapisi za arhiviranje prikupljaju se na način koji ovisi o vrsti zapisa.

Zapisi za arhiviranje nastali u Fina PKI i Fina RA mreži prikupljaju se i arhiviraju interno.

5.5.7. Postupci dobivanja i provjere arhiviranih zapisa

Pristup zapisima iz arhive imaju samo osobe ovlaštene za pristup tim podacima.

Verifikacija podataka iz arhive obavlja se provjerom njihove cjelovitosti.

5.6. Promjena TSU ključa

Fina osigurava da Fina QTSA 2017 kontinuirano pruža kvalificiranu uslugu povjerenja sa svojim validnim parom ključeva i pripadajućim TSU certifikatom za Fina QTSA 2017 sustav. Iz tog razloga Fina će prije isteka TSU certifikata, generirati novi par TSU ključeva. Također, Fina će generirati novi par TSU ključeva i u slučaju kada tu promjenu zahtjeva razina sigurnosti kriptografskog algoritma privatnog TSU ključa u uporabi. U oba slučaja za novi javni TSU ključ Fina RDC 2015 CA izdati će TSU certifikat za Fina QTSA 2017 servis.

Fina će o promjeni javnog TSU ključa i o novom TSU certifikatu za Fina QTSA 2017 sustav pravodobno obavijestiti sudionike Fina QTSA.

Novi pripadajući javni TSU ključ biti će dostupan sudionicima Fina QTSA na način na koji je to bio i prethodni javni TSU ključ, a sukladno opisu u točki 2.2. ovih Općih pravila.

Nakon generiranja novog para TSU ključeva elektronički vremenski žigovi potpisivat će se korištenjem novog privatnog TSU ključa.

Stari javni TSU ključ i stari pripadajući TSU certifikat za Fina QTSA 2017 servis se arhiviraju.

5.7. Oporavak od kompromitiranja ili nepogode

5.7.1. Postupci u slučaju incidenta ili kompromitiranja

Planom kontinuiteta poslovanja za Fina PKI regulirani su postupci u slučaju izbijanja incidenta ili kompromitiranja sustava, a koji obuhvaćaju postupke za oporavak sustava i uspostavu sigurnosnih uvjeta za pružanje usluga izdavanja elektroničkih vremenskih žigova.

Plan kontinuiteta poslovanja revidira se jednom godišnje.

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

Finin sustav certificiranja zasnovan je na pouzdanim hardverskim i softverskim komponentama, a kritične operacije sustava podržane su redundantnim komponentama.

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

Plan kontinuiteta poslovanja za Fina PKI regulira postupke oporavka sustava certificiranja u slučaju kvarova ili oštećenja opreme i mrežnih resursa te povrat podataka.

5.7.3. Postupci u slučaju kompromitiranja privatnog ključa ili ispada iz sinkroniziranosti s UTC vremenom

U slučaju kompromitiranja privatnog TSU ključa za Fina QTSA 2017 sustav pripadajući TSU certifikat biti će opozvan od strane Fina RDC 2015 CA.

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

Fina će za sve Korisnike i Pouzdajuće strane putem internetskih stranica Fina PKI repozitorija iz točke 2.2.1. ovog QTP 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 vremenskih žigova koji sadrže neispravne podatke.

Fina će o opozivu TSU certifikata za Fina QTSA 2017 sustav ili ispada iz sinkroniziranosti s UTC vremenom obavijestiti sudionike Fina QTSA:

- 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.

Fina će generirati novi par TSU ključeva. Fina RDC 2015 CA će za novi javni TSU ključ izdati novi TSU certifikat za Fina QTSA 2017 sustav.

Novi TSU certifikat za Fina QTSA 2017 sustav biti će dostupan sudionicima Fina QTSA na način na koji je bio dostupan i prethodni TSU certifikat, a sukladno opisu u točki 2.2. ovih Općih pravila.

5.7.4. Mogućnost nastavka poslovanja nakon nepogode

U Planu kontinuiteta poslovanja Fina PKI određeni su postupci za nastavak poslovanja nakon katastrofe. Ovisno o vrsti katastrofe Fina će pružanje usluge izdavanja elektroničkih vremenskih žigova nastaviti na svojem primarnom produkcijskom sustavu certificiranja ili će pružanje usluge nastaviti na svojem sekundarni sustavu certificiranja iz točke 5.1.1. ovih Općih pravila do oporavka svojeg primarnog produkcijskog sustava.

5.8. Prestanak rada Fina QTSA 2017 servisa

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 pripadajući Fina QTSA 2017 certifikat u slučaju da Fina iz bilo kojeg razloga ne bude u mogućnosti osigurati nastavak pružanja usluga

izdavanja elektroničkih vremenskih žigova kod drugog kvalificiranog pružatelja usluga povjerenja.

U slučaju prestanka pružanja usluga izdavanja elektroničkih vremenskih žigova Fina će arhivirati, zaštititi i čuvati zapise prema odredbama iz točke 5.5. ovih Opći pravila 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

Ovo poglavlje opisuje mjere zaštite koje se poduzimaju u cilju postizanja zahtijevane razine sigurnosti kriptografskih ključeva, aktivacijskih podataka, kritičnih sigurnosnih parametara, upravljanja ključevima i drugih mjera tehničke sigurnosti za Fina QTSA i za izdavanje elektroničkih vremenskih žigova.

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 koristeći kriptografske algoritme za generiranje ključeva koji su sukladni s normizacijskim dokumentom ETSI TS 119 312 [16].

Par TSU ključeva za Fina QTSA 2017 sustav generira se u HSM modulu koji zadovoljava zahtjeve iz točke 6.2.1. ovih Općih pravila.

Fina QTSA 2017 sustav s pripadajućim HSM modulom nalazi se tijekom i nakon postupka generiranja para TSU ključeva u Fina PKIštićenom prostoru iz točke 5.1.1. ovih Općih pravila, 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 sustav sudjeluju ovlaštene osobe s povjerljivim ulogama u Fina QTSA, uz minimalno dualnu kontrolu.

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

6.1.2. Dostava javnog TSU ključa pouzdajućim stranama

Javni TSU ključ Fina QTSA 2017 servisa služi za provjeru potpisa vremenskog žiga, a nalazi se u certifikatu za Fina QTSA 2017 servis koji je objavljen na LDAP imeničkom poslužitelju te na Fininim internetskim stranicama <http://www.fina.hr/finadigicert>.

6.1.3. Duljine ključeva

Duljina TSU ključeva za Fina QTSA 2017 servis i algoritmi za potpisivanje vremenskog žiga su:

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

6.1.4. Generiranje i provjera kvalitete parametara javnog ključa

Ključevi koje upotrebljava Fina QTSA 2017 generiraju se sukladno normizacijskom dokumentu ETSI TS 119 312 [16].

6.1.5. Namjene ključeva

Privatni TSU ključ za Fina QTSA 2017 koristi se samo za elektronički potpis 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 tehničke mjere zaštite kriptografskog modula

HSM modul kojim TSU obavlja potpisivanje vremenskog žiga zadovoljava zahtjeve prema FIPS 140-2 [21], 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 vremenskog žiga. Taj mehanizam sprječava jednu osobu da sama pristupi privatnom potpisnom TSU ključu.

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 štice 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 štice prostora na odvojenim lokacijama.

Fizički pristup sigurnosnim kopijama privatnih TSU ključeva Fina QTSA 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.

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 razinu 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 QTSA, uz dualnu kontrolu. Privatni TSU ključevi prenose se iz HSM modula isključivo u svrhe izrade sigurnosne kopije.

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 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. Svaka od ovih ovlaštenih osoba za aktivaciju HSM-a upotrebljava upravljačku karticu kriptografskog modula 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 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 važenja privatnog TSU ključa, zbog kompromitiranja ili opravdane sumnje u kompromitiranost privatnog ključa, ili zbog prestanka njegova korištenja, a provode ga ovlaštene osobe s povjerljivim ulogama u Fina QTSA uz minimalno dualnu kontrolu. Postupkom uništavanja privatnog Fina CA ključa trajno su onesposobljene i sve sigurnosne kopije tog privatnog ključa te ih više nije moguće upotrijebiti.

6.2.11. Ocjena kriptografskog modula

Ocjena HSM modula provodi se certificiranjem prema odgovarajućim normama za kriptografske module navedenim u točki 6.2.1. ovih Općih pravila.

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. ovih Općih pravila, a u arhivi se čuvaju na rok iz točke 5.5.2. ovih Općih pravila.

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 Fina QTSA 2017 certifikata nije duži od vremenskog perioda u kojem se korišteni kriptografski algoritmi i duljine ključeva smatraju sigurnim za primjenu.

Zbog osiguranja kriptografske zaštite izdanih elektroničkih vremenskih žigova period važenja privatnog TSU ključa mora biti manji od vremenskog perioda važenja pripadajućeg certifikata.

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

Privatni TSU ključevi Fina QTSA 2017 ne upotrebljavaju se nakon isteka roka važenja certifikata, nakon opoziva certifikata ili nakon isteka perioda važenja privatnog TSU ključa te se u tom slučaju zahtjevi za izdavanjem vremenskog žiga odbacuju.

6.3.3. Upravljanje životnim ciklusom kriptografskih modula

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

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

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

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

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 upravljačke kartice kriptografskog modula, a zaštićeni su 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.

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.

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 zloćudnog 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 [22].

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.

Softver koji se koristi za pružanje usluge izdavanja elektroničkih vremenskih žigova potječe iz pouzdanog izvora. 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

Fina provodi provjeru svih dijelova sustava za izdavanje elektroničkih vremenskih žigova u odnosu na sigurnost, pouzdanost i kvalitetu djelovanja, a u skladu s važećim propisima iz točke 9.15. ovih Općih pravila.

U slučaju povrede sigurnosti sustava certificiranja 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 osobe i poslovne subjekte 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 sustava za izdavanje elektroničkih vremenskih žigova i informacija štiti se antivirusnom zaštitom i uporabom autoriziranog softvera.

Provodi se praćenje raspoloživih kapaciteta Fina PKI 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 sustava 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. 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.

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

Fina QTSA 2017 sustav je sigurnosno podešen i očvršćen.

6.8. Uporaba 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

Profil certifikata za Fina QTSA 2015 sustav usklađen je s normama EN 319 411-2 [13] i ETSI EN 319 422 [11].

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

7.1.1. Broj(evi) verzije

Certifikati su sukladni verziji 3 prema X.509 specifikaciji.

7.1.2. Ekstenzije certifikata

Dokument s opisom profila certifikata dostupan je na internetskim stranicama Fina QTSA repozitorija iz točke 2.2. ovih Općih pravila. [_](#)

7.1.3. Identifikator objekta (OID) algoritama

Algoritmi s pripadajućim OID identifikatorima za sve certifikate koje izdaju subordinirani Fina CA-ovi 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 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 izdavanja elektroničkih vremenskih žigova

Ekstenzija *Certificate Policies* certifikata sadrži odgovarajući Finin OID ovih Općih pravila i ETSI OID općih pravila najboljih standarda struke (engl.: *best practices*, BTSP).

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 Pravilnika o postupcima pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova, QTPS [25] na hrvatskom i engleskom jeziku.

7.1.9. Procesne semantike za kritičnu ekstenziju *Certificate Policies*

Nema odredbi.

8. PROVJERA SUKLADNOSTI

Nadzor nad radom Fine kao kvalificiranog pružatelja usluga povjerenja reguliran je Uredbom (EU) br. 910/2014 [1] i Zakonom o elektroničkom potpisu [2] - [4], a provodi ga središnje tijelo državne uprave nadležno za poslove gospodarstva.

Nadzor nad radom kvalificiranog pružatelja usluga povjerenja u području prikupljanja, uporabe i zaštite osobnih podataka Potpisnika mogu provoditi i državna te druga tijela određena zakonom i drugim propisima koji uređuju zaštitu osobnih podataka.

Provjera sukladnosti obavlja se u cilju potvrđivanja da Fina kao kvalificirani pružatelj usluga povjerenja i usluge izdavanja kvalificiranih certifikata koje Fina pruža ispunjavaju zahtjeve utvrđene Uredbom (EU) br. 910/2014 [1], Zakonom o elektroničkom potpisu [2] - [4], podzakonskim propisima [5] -[7] donesenih temeljem Zakonom o elektroničkom potpisu [2] - [4] i normama ETSI EN 319 401 [9] i ETSI EN 319 421 [10].

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 [14].

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 [14].

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

- odredbi norme ETSI EN 319 421 [10];
- PKI područja, tehnologije vremenske ovjere te područja informacijske sigurnosti;
- zakonske regulative iz područja davanja 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 usluga povjerenja:

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

Opis predmetnog ocjenjivanja sukladnosti definiran je planom ocjenjivanja sukladnosti.

8.5. Mjere u slučaju neusklađenosti

Ako je u pružanju kvalificirane usluge povjerenja utvrđena nesukladnost Fina će poduzeti potrebne korake kako bi otklonila nesukladnost u roku koji je odredilo nadzorno tijelo.

8.6. Priopćavanje rezultata

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

U slučaju vanjske provjere sukladnosti Fina će dostaviti izvještaj vanjskog ocjenitelja o provjeri sukladnosti nadzornom tijelu unutar tri radna dana od primitka.

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 naplaćuje sukladno cjeniku Fine. Cjenik svih usluga koje se naplaćuju objavljen je na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila.

Fina zadržava pravo izmjene cjenika. Izmjene cjenika objavljuju se na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila.

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 certificiranja u skladu s ovim Općim pravilima.

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

Fina prikuplja podatke poslovnih subjekata isključivo za potrebe registracije u cilju izdavanja certifikata.

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 certificiranja, a koje sudionici označe

povjerljivim, ili određenom vrstom ili stupnjem tajnosti, ili koji su po prirodi povjerljivi jer bi njihovo neovlašteno otkrivanje moglo prouzročiti štetu sudioniku.

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 pružanja 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 obavezan je štititi povjerljive poslovne podatke iz točke 9.3.1. ovih Općih pravila, 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 prikuplja osobne podatke fizičkih osoba isključivo za potrebe registracije u cilju izdavanja certifikata.

Sklapanjem ugovora o pružanju usluga izdavanja kvalificiranih elektroničkih vremenskih žigova Korisnici su suglasni da Fina koristi i obrađuje njihove podatke prikupljene u postupku registracije sukladno važećoj zakonskoj regulativi te su suglasni da je Fina ovlaštena čuvati te podatke u trajanju od najmanje 10 godina.

9.4.1. Plan zaštite osobnih podataka

Fina provodi tehničke, kadrovske i organizacijske mjere zaštite osobnih podataka sukladno Zakonu o zaštiti osobnih podataka [8] u svrhu zaštite privatnosti osoba i zaštite podataka od moguće zlouporabe te očuvanja točnosti, potpunosti i ažurnosti osobnih podataka.

Mjere zaštite osobnih podataka primjenjuju se prilikom razmjene osobnih podataka Korisnika između Fina RA mreže i sustava za izdavanje 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 usluga izdavanja elektroničkih vremenskih žigova. Osobni podaci koje prikupi Fina i koji nisu sadržaj certifikata, koji se ne prikazuju u javnim evidencijama i/ili registrima koji se za potrebe davanja usluge certificiranja moraju propisano voditi, su povjerljivi osobni podaci koje Fina propisano štiti.

9.4.3. Osobni podaci koji nisu povjerljivi

Svi prikupljeni osobni podaci smatraju se povjerljivima.

9.4.4. Odgovornost za zaštitu osobnih podataka

Fina je odgovorna za zaštitu osobnih podataka prikupljenih u svrhu pružanja usluga izdavanja 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 usluga izdavanja kvalificiranih 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. ovih Općih pravila 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 dokument Općih pravila kao i druga Finina dokumentacija objavljena na internetskim stranicama repozitorija iz točke 2.2. 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 i pripadajući TSU certifikati za Fina QTSA 2017 sustav koji se koriste za potpisivanje elektroničkih vremenskih žigova vlasništvo su Fine.

9.6. Obveze Fina QTSA 2017 sudionika

9.6.1. Obveze Fine

Fina kao kvalificirani pružatelj usluga izdavanja kvalificiranih elektroničkih vremenskih žigova obvezuje se:

- provoditi pružanje usluga izdavanja elektroničkih vremenskih žigova u skladu s Uredbom (EU) br. 910/2014 [1], normizacijskim dokumenatima i preporukama, ovim Općim pravilima te drugim aktima Fine vezanim uz obavljanje usluga izdavanja elektroničkih vremenskih žigova;
- izdavati kvalificirane elektroničke vremenske žigove sukladno profilu određenom u točki 3.5. ovih Općih pravila;
- osigurati točnost vremena u izdanim elektroničkim vremenskim žigovima sukladno točki 3.6. ovih Općih pravila;
- provoditi potpisivanje vremenskog žiga na opremi koja udovoljava zahtjevima iz točke 6.2.1. ovih Općih pravila;

- 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 repozitorija iz točke 2.2. ovih Općih pravila;
- obavljati usluge izdavanja elektroničkih vremenskih žigova s pažnjom dobrog stručnjaka;
- primjenjivati u svom poslovanju organizacijske i tehničke mjere zaštite podataka prikupljenih od Korisnika pri ugovaranju korištenja ove usluge i te podatke čuvati kao poslovnu tajnu te ih koristiti isključivo za potrebe usluga izdavanja elektroničkih vremenskih žigova iz opsega ovih Općih pravila i dodatnih usluga certificiranja iz skupa Fina PKI usluga (npr. izdavanje certifikata);
- primjenjivati odredbe Zakona o zaštiti osobnih podataka [8] i drugih propisa kojima je uređena zaštita osobnih podataka te tajnost podataka u Republici Hrvatskoj;
- 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 Subjektima na daljnju obradu u Fina QTSA;
- čuvanje, arhiviranje i zaštita podataka i dokumentacije na period od najmanje 10 godina od isteka certifikata na kojeg se odnose;
- osiguravanje od gubitka ili povrede povjerljivosti, cjelovitosti i dostupnosti arhiviranih podataka Korisnika, na način propisan ovim QTPS dokumentom;
- obavještavanje podnositelja zahtjeva za izdavanje certifikata o javno objavljenim i dostupnim uvjetima pružanja usluga certificiranja i ovim QTPS dokumentom.

9.6.3. Obveze Korisnika

Korisnik je obvezan:

- prilikom predaje zahtjeva za korištenje usluga izdavanja elektroničkih vremenskih žigova u zahtjevu navesti točne i istinite osobne podatke te odmah obavijestiti Finu, kao pružatelja usluga, o svakoj promjeni tih podataka;
- validirati elektronički potpis Fina QTSA 2017 na zaprimljenom 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 elektroničkih vremenskih žigova;

- za korištenje usluge izdavanja vremenskog žiga plaćati Fini naknadu sukladno cjeniku Fina QTSA usluga iz točke 9.1. ovih Općih pravila.

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

Korisnik je, također obavezan s pažnjom dobrog domaćina, odnosno gospodarstvenika pravodobno na internetskim stranicama Fina QTSA repozitorija iz točke 2.2. ovih Općih pravila pratiti i upoznati se s objavljenim izmjenama i/ili dopunama ovih Općih pravila.

9.6.4. Obveze pouzdajućih strana

Prije pouzdanja u elektronički vremenski žig pouzdajuća strana mora:

- obaviti validaciju potpisa elektroničkog vremenskog žiga;
- provjeriti na važećoj listi opozvanih certifikata (CRL), ili korištenjem *online* Fininog OCSP servisa opozvanost Fina QTSA 2017 certifikata čijim je pripadnim privatnim TSU ključem potpisan elektronički vremenski žig.

U slučaju verificiranja vremenskog žiga nakon isteka vremena važenja Fina QTSA 2017 certifikata, pouzdajuća strana treba provjeriti na internetskim stranicama Fina QTSA repozitorija iz točke 2.2. ovih Općih pravila da li je 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.

Pouzdanja strana obvezna je pridržavati se odredbi ovih Općih pravila.

9.7. Odgovornosti sudionika Fina QTSA 2017 servisa

9.7.1. Odgovornosti Fine

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

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 ovih Općih pravila.

Ova Opća pravila sastavni su dio ugovora o pružanju usluga izdavanja elektroničkih vremenskih žigova kojeg sklapaju Korisnik i Fina kao pružatelj usluga izdavanja kvalificiranih elektroničkih vremenskih žigova.

9.7.2. Odgovornosti Korisnika

Korisnik je odgovoran za:

- sadržaj podataka, odnosno elektroničkog zapisa za koji traži izdavanje elektroničkog vremenskog žiga;
- korisničku aplikaciju koju koristi za ugradnju 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 zahtjevu 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. ovih Općih pravila.

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.

9.7.3. Odgovornosti pouzdajućih strana

Pouzdujuća strana koja se, ne poštujući odredbe iz ovih Općih pravila te protivno utvrđenim obvezama iz točke 9.6.3. ovih Općih pravila, pouzdaje u nevažeći elektronički vremenski žig, snosi sama sve rizike pouzdanja u takav elektronički vremenski žig.

Pouzdujuća 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 QTSA

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

Fina nije odgovorna za:

- štete prouzročene prijevernom ili nemarnom autentikacijom na Finin servis za izdavanje elektroničkih vremenskih žigova;
- štete nastale kao rezultat neispravnosti i pogrešaka u softveru i hardveru Korisnika i pouzdajuće strane.

9.9. Ograničenja odgovornosti

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

9.10. Naknada štete

Svaki sudionik odgovara oštećenom za štetu koju je počinio zbog nepoštivanja odredbi ovih Općih pravila i važećih relevantnih propisa.

Korisnik Finine usluge izdavanja kvalificiranih elektroničkih vremenskih žigova odgovora oštećenom, odnosno svakom drugom sudioniku ako koristi uslugu temeljem lažnog predstavljanja prilikom prijave na servis za izdavanje elektroničkih vremenskih žigova.

Pouzdanja strana odgovora oštećenom, odnosno svakom drugom sudioniku, ako se pouzda u izdani elektronički vremenski žig bez provjere njegove valjanosti ili ga koristi protivno svrhamu određenim u ovim Općim pravilima te općim pravilima pružanja usluga certificiranja prema kojima je certifikat izdan.

Fina je odgovorna osobi koja se pouzda u izdani elektronički vremenski žig i Fina QTSA 2017 certifikat samo ako je ta odgovornost jasno uspostavljena ugovorom ovim Općim pravilima, QTPS dokumentom [25] ili hrvatskom zakonskom regulativom.

9.11. Trajanje i prestanak važenja

9.11.1. Trajanje

Ovaj dokument Općih pravila važi do stupanja na snagu novog dokumenta Općih pravila ili do objave prestanka njegovog važenja. Nova verzija dokumenta ili objava prestanka važenja biti će objavljena na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila 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

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

9.11.3. Posljedice prestanka važenja i nastavak djelovanja

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

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

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 Fina

| | |
|-------------------|---|
| 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

Ova Opća pravila Fina PMA 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. ovih Općih pravila poslati dopis s prijedlogom za ispravke pogrešaka, prijedlog nadopuna ili izmjenu ovog 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.

9.13.2. Mehanizmi obavještanja i vremenski periodi

Sve izmjene i dopune dokumenta Općih pravila objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila.

Nove verzije Općih pravila s izmijenjenim OID-om Općih pravila objavljuju se u elektroničkom obliku na internetskim stranicama repozitorija iz točke 2.2. ovih Općih pravila.

Datum stupanja na snagu izmjena i dopuna ili novoobjavljenog dokumenta Općih pravila naznačeni su 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 dokumentu Općih pravila koje mogu utjecati na sudionike zahtijevaju i izmjenu OID-a Općih pravila. Novi OID za novu verziju 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 certificiranja uređene ovim Općim pravilima, 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. ovih Općih pravila.

9.15. Važeći propisi

Kvalificirane usluge povjerenja iz opsega ovog QTPS dokumenta Fina pruža sukladno odredbama Uredbe (EU) br. 910/2014 [1], provedbenih akata donesenih temeljem Uredbe (EU) br. 910/2014, Zakona [2], [3] i [4], podzakonskih akata donesenih temeljem tog zakona [5], [6] i [7], te normizacijskih dokumenata ETSI EN 319 401 [9] i ETSI EN 319 421 [10].

9.16. Usklađenost s primjenjivim propisima

Ova Opća pravila i pružanje usluga izdavanja kvalificiranih elektroničkih vremenskih žigova koje su obuhvaćene ovim Općim pravilima usklađeni su s propisima iz točke 9.15. ovih Općih pravila.

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

9.17. Razne odredbe

Fina javno objavljuje ova Opća pravila, 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 pružanju usluga izdavanja kvalificiranih elektroničkih vremenskih žigova Korisnici se informiraju o uvjetima pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova. Prihvatanje uvjeta pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova preduvjet je za izdavanje kvalificiranih elektroničkih vremenskih žigova.

Prije sklapanja ugovora o obavljanju usluga certificiranja korisnici se informiraju o uvjetima pružanja usluga izdavanja kvalificiranih elektroničkih vremenskih žigova.