FINA RDC

OPĆA PRAVILA DAVANJA USLUGA UGRADNJE VREMENSKOG ŽIGA

Verzija 1.1

Datum 1.12.2010.

AUTORSKA PRAVA

PODACI ZA KONTAKT

Upiti u vezi sa uvođenjem i administriranjem ovog dokumenta mogu se uputiti:

pma@fina.hr

PREGLED PROMJENA

Redni broj	Verzija	Točka	Opis promjene	Datum promjene

SADRŽAJ:

1. UVODNE OZNAKE I TEMELJNI PODACI

Dokument Opća pravila davanja usluga ugradnje vremenskog žiga (dalje u tekstu TSP) navodi zahtjeve koje mora ispunjavati FININ servis usluga vremenskog žiga (Time Stamping Authority - dalje u tekstu TSA) kod izdavanja tokena koji sadrže potpisanu vremensku ovjeru (vremenski žig). Dokument TSP definira sudionike procesa, navodi njihova prava i odgovornosti. Detaljni opis pravila i postupaka nalazi se u FININOM Pravilniku o postupcima certificiranja (dalje u tekstu CPS). Struktura i sadržaj ovog dokumenta kompatibilni su s ETSI pravilima.

Za izradu elektroničke transakcije i njezinu neporecivost u vremenu, nužno je pouzdano i neporecivo povezati vrijeme njene izrade sa njenim sadržajem.

Tipična transakcija vremenskog žiga je elektronički potpisani dokument. Kako bi se u potpunosti otklonila mogućnost naknadnog potpisivanja dokumenta i potpisivanje dokumenta sa nevažećim ključevima, potrebno je dokazati da je ključ sa kojim je dokument ili poruka bila potpisana, bio valjan u trenutku njezinog potpisivanja. Valjanost ključa se može provjeriti pomoću statusa njemu pridruženog certifikata. Kako bi se utvrdila valjanost certifikata u trenutku kada je izveden elektronički potpis, potrebno je imati pouzdan zapis o točnom vremenu izvedbe elektroničkog potpisa. U tu svrhu može poslužiti vremenski žig.

Da bi se dokazala valjanost elektroničkog potpisa, potrebno je dokazati da je potpisnik/subjekt potpisao dokument u vrijeme valjanosti certifikata. Ovo je potrebno u dvjema okolnostima:

1. u periodu važenja potpisnikova/ subjektova certifikata, jer korisnikov privatni ključ može biti kompromitiran i prema tome opozvan;
2. nakon perioda važenja certifikata potpisnika/subjekta.

Uporaba vremenskog žiga rješava ovaj problem. Vremenski žig omogućuje dokaz da je određeni podatak postojao prije određenog vremena. Ova tehnika omogućuje dokazivanje da je potpis izrađen prije podatka sadržanog u vremenskom žigu.

Usluga davanja vremenskog žiga omogućuju pouzdanje u elektronički potpis i poslije isteka valjanosti/opoziva certifikata potpisnika/subjekta. Vremenski žig izdan u skladu s ovim općim pravilima može se koristiti za zaštitu dugotrajnih elektroničkih potpisa.

Ova opća pravila su namijenjena za provedbu servisa vremenskog žiga, koji treba biti podrška za pravno valjanju upotrebu elektroničkog potpisa. Ovi servisi se mogu primijeniti u bilo kojoj aplikaciji koja zahtjeva dokaz da je određeni podatak postojao prije nekog određenog vremena.

Opća pravila davanja usluga ugradnje vremenskog žiga se baziraju na kriptografiji javnog ključa, X.509 certifikatima i pouzdanim servisima točnog vremena.

Postojeći dokument specificira zahtjeve koji se odnose na davanje usluge vremenskog žiga koja rezultira izdavanjem vremenskih žigova, a koji sadrže podatak o vremenu usklađen sa koordiniranim svjetskim vremenom (Coordinated universal time - UTC).

Ovaj dokument mogu koristiti pouzdajuće strane i potpisnici.

1.1. Reference

1.1.1. Temeljni zakon i podzakonski akti - pravilnici

[1] Zakon o elektroničkom potpisu (NN 10/02 i 80/08)

[2] Pravilnik o evidenciji davatelja usluga certificiranja u Republici Hrvatskoj (NN 107/10)

[3] Pravilnik o izradi elektroničkog potpisa, uporabi sredstva za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN 107/10)

1.1.2. Smjernice Europskog parlamenta

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

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

1.1.3. Standardi

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

[7] IETF RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

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

[9] ETSI TS 101 733: Electronic signature formats

[10] ETSI TS 101 861: Time stamping profile

[11] ITU–R Recommendation TF 536-1 (1998): Time scale notations

1.1.4. FINA PKI pravilnici

[12] Pravilnik o postupcima certificiranja (CPS) Verzija 3.2

1.2. Kratice

Za potrebe ovog dokumenta, koriste se slijedeće kratice:

KRATICA	ZNAČENJE – engl	ZNAČENJE - hrv
TSA	Time-Stamping Authority	Davatelj usluga izdavanja vremenskog žiga
TSU	Time-Stamping Unit	Jedinica za izradu vremenske ovjere
TST	Time-Stamp token	Vremenski žig
GMT	Greenwich Mean Time	Vrijeme po Greenwichu
UTC	Coordinated Universal Time	Koordinirano svjetsko vrijeme

1.3. Definicije

Za svrhu ovog dokumenta, dane su slijedeće definicije pojmova:

POJAM	DEFINICIJA
Pouzdajuća strana	primatelj vremenskog žiga , strana koja se pouzdaje u vremenski žig.
Potpisnik/subjekt	strana koja ima potrebu za servisima koje omogućuje TSA i koja prihvaća uvjetime izdavanja vremenskog žiga
Vremenski žig	elektronički potpisana potvrda izdavatelja koja potvrđuje sadržaj podataka na koje se odnosi u navedenom vremenu.
TSA izjava o politici	izjava o TSA politici i postupcima, koje se želi posebno naglasiti ili koje treba objaviti potpisnicima/subjektima i pouzdajućim stranama
TSA izjava o postupcima	izjava o postupcima koje provodi TSA, kada izdaje tokene vremenske ovjere
TSA sustav	Sustav IT komponenti koje osiguravaju izvedbu servisa vremenskog žiga
Opća pravila davanja usluga ugradnje vremenskog žiga	skup pravila koji naznačuje uporabu vremenskog žiga za pojedinu skupinu i/ili za neku klasu aplikacija, koje imaju slične sigurnosne zahtjeve.
TSU - jedinica za izradu tokena vremenske ovjere	sklopovlje i programska podrška združena u jednu jedinicu i koja u danom trenutku ima samo jedan aktivan ključ za elektroničko potpisivanje tokena vremenske ovjere.
UTC - Koordinirano svjetsko vrijeme	Mjerenje vremena na bazi sekunde, kako je to definirano prema ITU-R (International Telecommunications Radio Committee) preporuci (ITU-R Recommendation TF.460-5).

1.4. Opis usluga

FININA usluga izdavanja vremenskog žiga (TSA) je servis koji svojim korisnicima i pouzdajućim stranama povezanim s ovjeroviteljima u domeni FINA PKI (FINA RDC i FINA RDC-TDU) kao i drugim davateljima usluga certificiranja izdaje potvrde o vremenu neke transakcije (vremenski žig).

TSA snosi punu odgovornost za davanje usluga izdavanja vremenskog žiga i odgovoran je za siguran i ispravan rad jedne ili više TSU jedinica s kojima elektronički potpisuje zahtjeve za izdavanjem vremenskog žiga. TSA ima obavezu izdavati vremenske žigove koje je naknadno moguće pravilno identificirati sukladno točki 1.5.).

TSU privatni ključevi koji se koriste za potpisivanje tokena vremenske ovjere smatraju se vlasništvom TSA. TSA ima punu odgovornost za održavanje svih obveza prema ovoj politici u svezi TSU privatnih ključeva.

TSA može svoje servise izvoditi sa više TSU jedinica. Svaka jedinica u tom slučaju posjeduje vlastiti ključ s kojim se potpisuju tokeni. Svaku jedinicu treba biti moguće pravilno identificirati.

Zaključno, TSA je davatelj usluga izdavanja vremenskog žiga, koja izdaje pouzdajuće potvrde o vremenu neke transakcije sukladno Zakonu o elektroničkom potpisu i smjernici EU o elektroničkim potpisima.

1.5. Identifikacijski podaci i identifikator tipa objekta (OID oznaka)

OID (Objekt-Identifikator) za ova Opća pravila davanja usluga ugradnje vremenskog žiga (TSA politika):

OID polje	Atribut	Kod	Opis
ID	FINA OID	1.3.124.1104	FINA objekti
TSA ID	TSA OID	2	Identifikacija usluge
TSA policy	TSA TSP	1	TSA politika v.1.1

Identifikator politike TSA, koji provodi servise u okviru FININE infrastrukture javnog ključa nalazi se u svakom vremenskom žigu. Ova opća pravila su dostupna pouzdajućim stranama, ovjeroviteljima i njihovim klijentima u skladu s pravilima opisanim u poglavlju 6.1.

1.6. Korisnici i područje primjene usluga

Ova opća pravila namijenjena su prvenstveno za izdavanje vremenskih žigova koji se ugrađuju u elektroničke potpise, za njihovu dugotrajnu valjanost. Vremenski žig je moguće koristiti i za druge aplikacije koje imaju slične ili iste zahtjeve.

TSA može pružati javne servise za elektroničke transakcije, obrasce, arhivirane podatke, itd. Ova opća pravila se mogu koristiti za otvorene servise davanja usluge ugradnje vremenskog žiga ili servise koji za zatvorenu korisničku skupinu u FINA PKI.

Korisnik može biti poslovni subjekt koji ima više krajnjih korisnika (pojedinačnih subjekata), ili krajnji korisnik kao pojedinačni subjekt.

Subjekti su korisnici opisani u Općim pravilima pružanja usluga certificiranja.

1.7. Adresni podaci

Financijska agencija posluje na adresi

Vrtni put 3

10000 Zagreb

Tel: +385 1 6127 111

Telefax: +385 1 6128 089

e-mail: pma@fina.hr

2. OPĆE ODREDBE

2.1. Obveze davatelja usluga, potpisnika i pouzdajuće strane

2.1.1. Obveze davatelja usluga

FINA jamči točnost podatke o vremenu ugrađenog u vremenski žig. Podatak o UTC vremenu koje se ugrađuje u vremenski žig ima razinu točnosti od +/- 100 ms.

FINA također jamči slijedeće:

- Da se njezina komercijalna aktivnost provodi na pouzdanom hardware-u i software-u, u skladu sa zahtjevima opisanim u mjerodavnim CWA dokumentima,
- Aktivnost i servisi na koje se odnose ova Opća pravila davanja usluga ugradnje vremenskog žiga su u skladu sa zakonom i ne povređuju intelektualno vlasništvo, licenčna i druga prava,
- Servisi koje pruža su u skladu s opće prihvaćenim normama iz područja davanja usluga izdavanja vremenskog žiga.
- Dodatne informacije koje definiraju FININE obveze opisane su u poglavlju poglavlju 2.1. Pravilnika o postupcima certificiranja (CPS).

2.1.2. Obveze potpisnika

Subjekt koji dobiva vremenski žig, treba verificirati elektronički potpis TSA,i provjeriti CRL za certifikat TSA. Tekuća CRL se objavljuje na LDAP imeničkom poslužitelju rdc-ldap.fina.hr i na web stranici FINE http://rdc.fina.hr.

Ostale obveze subjekata opisane su u poglavlju 2.1. Pravilnika o postupcima certificiranja (CPS).

2.1.3. Obveze pouzdajuće strane

Prije pouzdanja u vremenski žig pouzdajuća strana mora:

- obaviti verifikaciju potpisa vremenskog žiga
- provjeriti na važećoj listi opozvanih certifikata (CRL) važenje TSA certifikata čijim pripadnim privatnim ključem je potpisan žig vremenske ovjere.

U slučaju da se verificira vremenski token poslije isteka vremena važenja TSA certifikata, pouzdajuća strana treba učiniti slijedeće:

- provjeriti je li još uvjek pouzdana kriptografska hash funkcija koja je korištena za taj token
- provjeriti jesu li duljina kriptografskog ključa TSA-a i pripadajući algoritam još uvjek smatrani sigurnim.

Ova Opća pravila davanja usluga ugradnje vremenskog žiga ne specificiraju nikakva dodatna ograničenja u odnosu na uporabu vremenskog žiga, osim uvjeta postavljenih u ugovoru. Ostali zahtjevi prema pouzdajućim stranama opisani su u poglavlju 2.1. Pravilnika o postupcima certificiranja (CPS).

2.2. Odgovornost

FININI ugovori sa potpisnicima i subjektima opisuju uzajamne obveze i odgovornosti.

FININA Opća pravila pružanja usluga certificiranja i ova Opća pravila davanja usluga ugradnje vremenskog žiga su integralni dijelovi ugovora potpisanih između FINE i potpisnika/subjekta.

FINA jamči da su svi zahtjevi, koji se odnose na TSA, što uključuje procedure koje se odnose na izdavanje vremenskog žiga, nadgledanje sustava i sigurnosne kontrole, u skladu s propisima danim u poglavlju 5. ovog dokumenta.

Dodatne obveze TSA, subjekata i pouzdajućih strana opisane su u poglavlju 2.1 Pravilnika o postupcima certificiranja (CPS).

2.3. Financijska odgovornost

Ako nije na drugi način određeno, tj. posebnim ugovorom, FININA ukupna financijska odgovornost za vremenski žig izdan sukladno ovim općim pravilima i za transakcije obavljene na temelju pouzdanja u tako izdane vremenske žigove iznosi do 40.000 kuna.

Ostale odgovornosti opisane su u u poglavlju 2.2. Pravilnika o postupcima certificiranja (CPS).

2.4. Ograničenje odgovornosti

Ovoj dokument ne specificira dodatna ograničenja odgovornosti TSA.

Sukladno ovim općim pravilima, TSA može ograničiti svoju odgovornosti do razine koja nije suprotna zakonima u RH.

2.5. Usklađenost sa zakonom

FINA je davatelj usluga izdavanja vremenskog žiga, koja izdaje pouzdajuće potvrde o vremenu neke transakcije sukladno Zakonu o elektroničkom potpisu i podzakonskim propisima.

2.6. Naknada za usluge

FINA izdaje tokene vremenskog žiga svakoj zainteresiranoj strani. Cijene usluge izdavanja vremenskog žiga nalaze u FININOM cjeniku, a objavljena je i na web stranici http://rdc.fina.hr.

2.7. Provjera usklađenosti

TSA sukladno ovim općim pravilima u vremenski žig ugrađuje pripadni identifikator općih pravila, sukladno točki 1.5. ovog dokumenta. Na zahtjev potpisnika/subjekta ili pouzdajuće strane TSA daje dokaz o usklađenosti sa ovim općim pravilima.

TSA mora pokazati da:

1. ispunjava sve zahtjeve prema poglavlju 2.2 ovog dokumenta;

2. da je ugradio sve kontrole s kojima se ostvaruju zahtjevi specificirani u poglavlju 5. ovog dokumenta.

2.8. Povjerljivost i tajnost

Privatni potpisni TSA ključ je osjetljiva i tajna informacije, te se on stoga mora držati u najstrožoj tajnosti. Ne smije postojati mogućnost u kojima bi se privatni ključ pojavio nešifriran izvan kriptografskog modula.

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

Pristup tajnim informacijama ograničava se na službene osobe, kojima su te informacije potrebne radi obavljanja njihovih službenih dužnosti. Sve informacije koje se odnose na način kojim TSA upravlja svojim ključevima i sustavom smatraju se tajnim informacijama.

2.9. Zaštita intelektualnog vlasništva

Ovaj dokument Opća pravila davanja usluga ugradnje vremenskog žiga je vlasništvo FINE i nije dopušteno njegovo neovlašteno mijenjanje ili korištenje njegovih dijelova bez prethodne dozvole vlasnika.

Privatni potpisni TSA kriptografski ključ isključivo vlasništvo FINE.

3. OSNOVNI ZAHTJEVI U RADU

3.1. Postupci provjere sigurnosnih mjera

TSA oprema bilježi događaje na razini operativnog sustava, servisa i aplikacija. Informacije koje se bilježe minimalno sadrže tip događaja i vrijeme nastanka. Gdje je to moguće, podaci za nadzor se automatski prikupljaju. Vodi se evidencija rada s datotekama i upravljanja korisničkim računima. Ti se događaji također bilježe u opremi TSA. Najmanje jednom mjesečno se rade pričuvne kopije revizijskih logova na trake.

Generirane Informacije o događajima na TSA opremi se na njoj čuvaju dok ne budu prenesene u prikladnu arhivu. Premještanje revizijskog loga iz CA opreme izvodi ovlaštena osoba. Revizijski logovi se zadržavaju kao arhivski slogovi u skladu sa 5.5.2.

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

Zabilježeni događaji se mogu analizirati u cilju procjene mogućnosti povrede TSA sustava. Time TSA osigurava da se procjene mogućnosti povrede sustava provedu, nadgledaju i obnove istraživanjem zabilježenih događaja.

3.2. Arhiviranje podataka

TSA osigurava pohranu zapisa o izvedenim transakcijama vremenske ovjere za određeni protekli period vremena.

Zapisi koji se odnose na izdavanje tokena vremenske ovjere, arhiviraju se kompletno i štite od neautoriziranog pristupa te im je osigurana tajnost. TSA zapisuje vremena važnih događaja u TSA. Arhivirani zapisi koji se odnose na vremenske ovjere će biti dostupni i po isteku važenja TSA privatnog ključa.

Informacije o potpisnicima/subjektima koje se zapisuju i arhiviraju smatraju se povjerljivima te su adekvatno zaštićene.

Pohranjuju se i zapisi koji se odnose na događaje povezane s životnim ciklusom TSA ključeva i pripadnih certifikata te zapisi koji se odnose na događaje povezane s ciklusom TSA certifikata.

3.3. Postupci otklanjanja posljedica šteta i nezgoda

TSA na odgovarajući način reagira na incident, koordinirano, pravovremeno i u najkraćem mogućem vremenu. Sve dostupne informacije o incidentima bilježe se u sistemskim zapisima. Ovi događaji se u najkraćem mogućem roku dojavljuju odgovornim osobama, u prvom redu voditelju zaduženom za rad TSA.

U slučaju događaja koji bi ugrozili sigurnost i pouzdanje u TSA servise, uključujući gubitak povjerenja u TSA privatni ključ ili detektirani gubitak kalibracije, TSA je obvezan na odgovarajući način o tim događajima izvijestiti svoje potpisnike/subjekte i pouzdajuće strane.

U slučaju kompromitiranja servisa, TSA će svim potpisnicima/subjektima i pouzdajućim stranama dati kratki opis i objašnjenje događaja.

U slučaju detekcije gubitka privatnog ključa ili kalibracije, TSA će zaustaviti izdavanje vremenskog žiga, dok se u potpunosti ne provedu postupci obnove pouzdanja u sustav.

U slučaju kompromitiranja sustava kroz duži vremenski period, TSA će objaviti dodatne informacije, s kojima je moguće identificirati one tokene vremenske ovjere koji su bili kompromitirani.

3.4. Prestanak rada/davanja usluge

U slučaju prestanka davanja usluge vremenskog žiga (ukidanje usluge), FINA će učiniti sve što je u njenoj moći kako bi se minimalizirao utjecaj prestanka rada servisa na poslovni proces potpisnika/subjekta ili pouzdajuće strane. FINA će osigurati nastavak održavanja svoje baze podataka, koja je nužna za verifikaciju ispravnosti tokena vremenske ovjere.

U slučaju prestanka davanja usluge vremenskog žiga FINA će na prikladan način izvijestiti pouzdajuće strane o svojoj odluci o prestanku davanja usluge .

TSA će osigurati sve potrebne korake, kojima će biti opozvani i objavljen opoziv svih TSA certifikata.

4. KONTROLA SIGURNOSTI OPREME, POSTUPAKA I OSOBLJA

4.1. Kontrola prostora, opreme i sredstava

TSA je implementirao odgovarajuću fizičku sigurnost radi ograničavanja pristupa informatičkoj opremi (hardveru i softveru) koja se upotrebljava za davanje usluge vremenskog žiga. Pristup ovoj informatičkoj opremi je ograničen na osobe koje obavljaju povjerljive poslove, kako je opisano u točki 4.3. ovog dokumenta. Pristup se kontrolira sustavom za kontrolu pristupa. Stalnu kontrolu pristupa provodi osoblje ili se ona provodi elektronički.

TSA osigurava punu fizičku kontrolu pristupa kritičnim servisima TSA u cilju smanjenja rizika od neautoriziranog fizičkog pristupa.

Za izvođenje i upravljanje servisima izdavanja vremenskog žiga:

- Ograničen je fizički pristup resursima TSA svim neautoriziranim osobama;
- Ugrađene su potrebne kontrole koje minimaliziraju i rizike: gubitka, oštećenja i kompromitiranja vlasništva poslovnog sustava.
- Ugrađene su kontrole koje onemogućavaju kompromitiranje TSA sustava zbog krađe podataka ili djelova informatičkih sustava za obradu podataka

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

Svaki vremenski žig kojeg izdaje TSA sadrži jedinstveni identifikator Općih pravila davanja usluga ugradnje vremenskog žiga. Vremenski žig kojeg izdaje TSA sadrži datum i vrijeme koje je u skladu s stvarnim UCT vremenom. Podatak o točnom vremenu dobiva se od satelitskog prijemnika. TSA posjeduje i pomoćni izvor podatak o točnom vremenu za slučaju kvara na satelitskom sustavu. Podešavanje sata se aktivira automatski nakon otkrivanja razlike između UCT vremena i glavnog sata, koja je veća od +/-250 ns.

U slučaju pogrešnog rada ili dekalibracije glavnog izvora podatka o točnom vremenu, TSA sustav dobiva podatak o točnom vremenu iz pomoćnog izvora. TST je potpisan ključem, čiji certifikat ima sadržaj opisan u poglavlju 6.

Upravljanje sa TSA sustavom izvodi se iz fizički štićenog okruženja, kako bi se ti resursi zaštitili od neautoriziranog pristupa podacima i sustavu upravljanja. Fizička zaštita izvedena je na način da je određeno fizičko sigurnosno okružje oko upravljačkih resursa TSA. Fizičke i sigurnosne kontrole štite resurse TSA.

4.2. Kontrola postupaka i provedbe radnih zadaća

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

Samo funkcije koje nisu sigurnosno osjetljive mogu obavljati osobe koje nužno nemaju naveden uvjete. Uloge, ovlaštenja i odgovornosti su dokumentirane u opisu poslova onih djelatnika koji obavljaju sigurnosne zadaće. Prilikom dodjeljivanja uloga i zadaća, ostvareno je i adekvatno razdvajanje uloga. Sukladno njihovoj osjetljivosti, uloge se dodjeljuju djelatnicima koji u dokazali svoju stručnosti i koji poznaju dodijeljeno područje rada. Djelatnici TSA prije nego što započnu obnašati odgovorne uloge u TSA, moraju savladati znanja i vještine za provedbu administrativnih i upravljačkih funkcija.

Djelatnici koji obnašaju uloge u TSA trebaju poznavati tehnologije vremenske ovjere, tehnologiju elektroničkog potpisivanja, mehanizma kalibracije i sinkroniziranja TSA satova s UTC, poznavanje sigurnosnih postupaka kod obnašanja sigurnosnih uloga i iskustvo u provedbi sigurnosti u informatičkim sustavima.

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

Djelatnici koje su počinile teži prekršaj ili težu povredu radnih obaveza, ne mogu se delegirati za obnašanje povjerljivih zadatka u TSA sustavu.

Karakteristike osoblja, kao i povjerljive uloge koje one provode opisane su u poglavlju 5.3. Pravilnika o postupcima certificiranja (CPS).

4.3. Kontrola osoblja – broj, stručnost i ovlaštenja

TSA osigurava da se zapošljavanje i rad djelatnika obavlja na način koji omogućuje povjerljivosti rada. TSA provodi komercijalno razumnu praksu da se osigura da osoba koja radi sama ne može biti izvan sustava zaštite.

Pri zapošljavanju djelatnika za rad u TSA provode se odgovarajuće provjere kako bi osobe mogle stručno obavljati povjerljive korisničke uloge Osoblje koje ne uspije zadovoljiti uvjete pri inicijalnom ili periodičnoj provjeri, neće moći obavljati ili nastaviti obavljati povjerljive korisničke uloge.

U slučaju neautorizirane akcije ili sumnje na neautoriziranu akciju koju je izvela osoba koja obavlja dužnosti u TSA, toj osobi će biti suspendiran pristup TSA sustavu.

5. KONTROLA TEHNIČKE SIGURNOSTI RADA DAVATELJA USLUGA VREMENSKOG ŽIGA

5.1. Zaštita podataka za izradu vlastitog elektroničkog potpisa

5.1.1. Standardi za kriptografske module

Kriptografski moduli kojima se obavlja potpisivanje vremenskog žiga moraju zadovoljavati sigurnosne kriterije sukladno obrascu za sigurnost kriptografskih modula FIPS 140-1, minimalno razina 3 ili FIPS 140-2, minimalno razina 3. Iznimno se može primijeniti i drugi priznati ekvivalentni standard za validaciju, certificiranje i provjeru kriptografskog modula.

5.1.2. Kontrola privatnog ključa od strane više osoba

Kontrola od strane više osoba sigurnosni je mehanizam koji zahtijeva višestruke autorizacije za pristup privatnom ključu za potpis vremenskog žiga. Taj mehanizam sprječava jednu osobu da sama pristupi TSA privatnom ključu za potpis.

TSA privatni ključ za potpis može se pohraniti samo pod kontrolom dviju ili više osoba. Osobe koje sudjeluju u toj kontroli trebaju biti ovlaštene za ovu operaciju.

5.1.3. Upis privatnog ključa u kriptografski modul

Ključevi davatelja usluga izdavanja vremenskog žiga trebaju biti generirani u kriptografskom modulu. Ako privatni ključ treba prenijeti iz jednoga kriptografskog modula u drugi, privatni ključ mora biti enkriptiran tijekom prijenosa i ne smije se ni u jednom pojaviti nezaštićen dok je izvan kriptografskog modula..

5.1.4. Metoda aktiviranja privatnog ključa

Prije aktiviranja privatnog ključa korisnici se moraju autenticirati kriptografskom modulu unošenjem PIN-a. Ta autentikacija može biti u obliku lozinke. Privatni ključevi moraju se čuvati u šifriranu obliku kad su deaktivirani.

5.1.5. Metoda uništenja privatnog ključa

Ukoliko je potrebno, privatni ključ TSA sustava se uništava 'zeroize' komandom. Fizičko uništenje kriptografskog modula tada nije potrebno.

5.2. Upravljanje podacima za izradu vlastitog elektroničkog potpisa

5.2.1. Generiranje TSA ključa

Par ključeva za TSA sustav mora biti generiran na takav način da privatni ključ ne može ni na koji način nikome biti poznat.

Kriptografski ključevi TSA sustava se izrađuju i pohranjuju u kriptografskom modulu. Postupak izrade ovih ključeva provodi stručno ovlašteno osoblje. Opis zahtjeva za izbor osoblja opisan je u poglavlju 5.3. Pravilnika o postupcima certificiranja (CPS).

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

- Generiranje TSA ključeva za potpisivanje vremenskih žigova izvode ovlaštene osobe kojima su povjerene upravljačke uloge u TSA sustavu, a postupak se izvodi u zaštićenom okruženju. Postupak izrade ključeva izvode najmanje dvije ovlaštene osobe, koji i autoriziraju potrebne operacije. Generiranje TSA ključeva za potpisivanje vremenskih žigova obavlja se unutar zaštićenog kriptografskog modula, koji je usklađen koji je u skladu s NIST FIPS 140-1 level 3 specifikacijom.
- Sukladno razini sigurnosti koju TSA treba osigurati bira se algoritam za izradu ključeva, duljina rezultirajućih ključeva i algoritmi za potpisivanje vremenskog žiga:
    - Za potpisivanje tokena vremenske ovjere koristiti se RSA algoritam s dužinom ključa od 2048 bit-a
    - Kao hash algoritam koristiti se SHA-1 algoritam.

5.2.2. Distribucija TSA javnog ključa

Javni ključ TSA služi za provjeru potpisa u vremenskom žigu, a nalazi se u certifikatu „SERVIS VREMENSKE OVJERE TSA1“ koji je objavljen na LDAP imeničkom poslužitelju rdc-ldap.fina.hr. TSA certifikat u FINA PKI domeni izdaje ovjerovitelj FINA RDC.

5.2.3. Obnavljanje TSA ključa

Vremenski period pouzdanja u TSA certifikat ne smije biti duži od vremena koje se smatra sigurnim za izabrani algoritam i izabranu dužinu tajnog ključa.

Dodatno treba uzeti u obzir da se sukladno točki 3.1., nadzorni zapisi za servise vremenskog žiga čuvaju se najmanje godinu dana po isteku valjanosti TSA ključa. Što je duži period važenja TSA certifikata, to će nadzorni podaci koje treba čuvati biti većeg volumena.

Obnavljanje TSA ključeva provodi se nakon isteka perioda valjanosti TSA certifikata. Istekli ključevi se arhiviraju na period od 10 godina. Nakon tog vremena ključevi se uništavaju. TSA javni ključ se čuva narednih 10 godina radi omogućavanja provjere vremenskih tokena izdanih u prošlosti. Arhiviranje ključeva opisano je poglavlju 6.2.5. Pravilnika o postupcima certificiranja (CPS).

5.2.4. Kraj životnog vijeka ključeva

Privatni ključ TSA se ne smije koristiti po isteku perioda njihovog važenja certifikata „SERVIS VREMENSKE OVJERE TSA1“.

Posebno:

a. TSA ima ostvarene sve tehničke uvjete i operativne postupke, prema kojima se osigurava pravovremeno obnavljanje ključeva TSA, prije isteka njihove valjanosti.
b. Po isteku valjanosti, privatni ključevi TSA se moraju sigurno uništiti, tako da ne postoji niti jedna njihova kopija te iste nije moguće ponovo koristiti.
c. Sustav koji generira vremenske žigove, po isteku valjanosti privatnih ključeva, ne smije omogućiti izdavanje novih tokena.

Procedure za uništenje TSA ključa opisane su u poglavlju 6.2.9. Pravilnika o postupcima certificiranja (CPS). Sustav za izdavanje tokena vremenske ovjere, koji radi u domeni FINA PKI odbija svaki zahtjev koji koristi istekli ključ.

5.3. Kontrola sigurnosti računalnog sustava

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

TSA poslužitelji zadovoljavaju niže navedene uvjete zaštite:

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

5.4. Kontrola sigurnosti radnog vijeka sustava

Sustav za davanje usluga izdavanja vremenskog žiga koristi autentične i povjerljive sustave i proizvode. Prije uspostave TSA sustava (hardver i softver) treba biti zaštićeno pakirana i isporučena povjerljivom metodom. Oprema ne smije sadržavati nikakve druge aplikacije koje nisu dio TSA konfiguracije. Nadogradnja opreme treba biti nabavljena na isti način kao uspostava primarne opreme i treba biti instalirana na definirani način od povjerljive i stručne osobe.

TSA softver mora biti isporučen u originalnom pakiranju i mora imati metodu verifikacije kojom se utvrđuje da je softver koji je na sustavu:

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

TSA mora osigurati mehanizam za periodičnu provjeru integriteta SW-a.

5.5. Kontrola sigurnosti mrežnog sustava

Sve lokalne mrežne komponente su smještene na fizički zaštićenim mjestima.

TSA oprema može biti istovremeno povezana na najviše dva mrežna segmenta. Mrežni promet je filtriran i nadziran. Treba osigurati da je TSA oprema zaštićena od svih poznatih oblika koji dolaze putem računalne mreže. Svi mrežni portovi i servisi koji se ne upotrebljavaju trebaju biti isključeni. Na TSA opremi treba biti instalirani upogonjen samo mrežni softver koji je potreban za obavljanje davanja usluge vremenskog žiga.

5.6. Kontrola sigurnosti kriptografskih modula

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

FINA RDC ima posebne procedure za rukovanje kriptografskim modulima.

6. SADRŽAJ CERTIFIKATA

U sljedećoj tablici opisan je profil certifikata za potpis vremenskog žiga

FINA RDC certifikat vremenskog žiga			
Atributi osnovnih politika		**vrijednost/sadržaj**	**opis/komentar**
Namjena		Potpis vremenskog žiga	certifikat za javni servis vremenske ovjere
Razina sigurnosti		Visoka	
X.509 - CERTIFIKAT		**vrijednost/sadržaj**	**opis/komentar**
1. Version		X.509 verzija 3.	Format; cijeli broj
2. serialNumber		10. znamenkasti neponovljivi cijeli broj	format; cijeli broj (2^{32}) - bez vodećih nula
3. signatureAlgorithm		1.2.840.113549.1.1.5.	sha1RSA
4. issuer			
organizationalUnit		RDC	ovjerovitelj (CA)
organizationName		FINA	naziv poslovnog subjekta koji pruža usluge certificiranja (CSP)
countryName		HR	zemlja sjedišta poslovnog subjekta koji pruža usluge certificiranja (CSP)
5. validity			
Valid from (not before)		vrijeme izdavanja	format; YYMMDDhhmmssZ (UTCTime)
Valid to (not after)		vrijeme izdavanja+120 mjeseci	format; YYMMDDhhmmssZ (UTCTime)
6. subject		X.500 DN subjekta	format; niz znakova UTF8
commonName		SERVIS VREMENSKE OVJERE TSA1	
organizationName		FINA	
countryName		HR	oznaka države prema ISO 3166
7. Public key		RSA-1024 javni ključ subjekta	prema RFC 3279
X.509 EKSTENZIJE	**kritično**	**vrijednost/sadržaj**	**opis/komentar**
8. authorityKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
9. subjectKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
10. keyUsage	NE	digitalSignature& Non-Repudiation	
11. Enhanced Key Usage	DA	Time Stamping (1.3.6.1.5.5.7.3.8)	

X.509 EKSTENZIJE	kritično	vrijednost/sadržaj	opis/komentar
12. certificatePolicies	NE		
PolicyIdentifier=		1.3.124.1104.5.11.52.4.3	FINA RDC poslovni autentifikacijski certifikat (srednja razina sigurnosti)
URL na CP		http://rdc.fina.hr/cp/	
13. basicConstrains	NE		
subjectType=		End Entity	
pathLengthConstraint =		None	
14. CRL Distribution Point	NE		
(1) CRL distribuirana; LDAP		CRLn	
ou=		RDC	
o=		FINA	
c=		HR	
(2) CRL kombinirana; LDAP		ldap://rdc-ldap.fina.hr/ou=RDC,o=FINA, c=HR?certificateRevocationList%3Bbinary	
(3) CRL kombinirana; HTTP		URL=http://rdc.fina.hr/crls/rdc.crl	
15. subjectAltName	NE	URL=http://tsa.fina.hr	format; RFC 822 Name
16. Private Key Usage Period	NE	100 %	Relativni period valjanosti privatnog ključa subjekta u odnosu na certifikat

7. POSTUPCI S DOKUMENTACIJOM

7.1. Postupci kod promjene sadržaja dokumentacije

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

Napisane i potpisane primjedbe na ovaj dokument se mogu uputiti u organizacijsku jedinicu FINE koja je zadužena za upravljanje politikama izdavanja certifikata i vremenskih žigova ili na e-mail adresu pma@fina.hr. Odluke o prihvaćanju primjedbi su diskreciono pravo FINE.

7.2. Objavljivanje dokumentacije

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

7.3. Postupci prihvaćanja/odobravanja dokumentacije

Promjene u dokumentaciji prihvaća tijelo zaduženo za upravljanje politikama izdavanja certifikata i vremenskih žigova.