UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Anže Starič

Implementacija odprtokodne rešitve časovnega žigosanja

SEMINARSKA NALOGA
pri predmetu
KRIPTOGRAFIJA IN TEORIJA KODIRANJA 2

Mentor: prof. dr. Aleksandar Jurišić

Povzetek

Časovno žigosanje nam omogoča dokazovanje, da smo si v nekem trenutku res lastili dokument. Po predstavitvi centralnih sistemov za časovno žigosanje sledi pregled priporočila za agencije za časovno žigosanje (RFC 3161) in priporočila za varnostne politike agencij za časovno žigosanje (RFC 3628). V nadaljevanju sledi analiza skladnosti dveh agencij s priporočili, v zaključku pa se dotaknemo dodane vrednosti agencije za časovno žigosanje na FRI. V okviru naloge sta nastala tudi patch za knjižnjico OpenTSA ter politika delovanja za agencijo za časovno žigosanje FriTSA.

1 Uvod

V mnogih primerih potrebujemo dokaz posedovanja nekega dokumenta oziroma v določenem času v preteklosti. Pri znanstvenih področjih, kjer je živa raziskovalna dejavnost, se srečamo s pojmom intelektualne lastnine. Pri tej je pomembno, kdaj je izumitelj prvič zapisal idejo, katero si lasti.

Sprejet analogni način za beleženje raziskav je uporaba laboratorijskega dnevnika. Poročilo raziskave je kronološko zapisani v poseben dnevnik, pri čemer nobena stran ne ostane prazna. Dnevnik ima zaporedno številčene skupaj sešite strani, kar močno oteži spreminjanje vsebine brez vidnih znakov. Če nato dnevnik še periodično pregledujejo in podpisujejo nadrejenu, je njegova pristnost še toliko bolj verjetna.

Težava vodenja takega dnevnika je, da ga je potrebno izpolnjevati ročno, verodostojnost nam jamčijo fizične lastnostni, saj bi bilo morebitno naknadno spreminjanje opazno na materialu iz katerega je dnevnik narejen. Opisana ideja pa nam ne pomaga, če dnevnik vodimo v digitalni obliki. Prednost digitalnih medijev je ravno v tem, da lahko podatke zapisujemo, spreminjamo in kopiramo, ne da bi pri tem vidno spremenili medij.

Za umeščanje digitalnih podatkov v tok časa si tako ne moremo pomagati z lastnosti medijev, na katerih so shranjeni, zato se je potrebno problema lotiti s kriptografskimi metodami. V projektu se bomo ukvarjali z implementacijo centralnega sistema za časovno žigosanje. V drugem poglavju si bomo ogledali kako deluje centralni sistem za časovno žigosanje, v tretjem pa z zahtevami, katerim mora zadostiti. V četrtem poglavju si bomo ogledali kaj mora vsebovati politika delovanja takega sistema.

V petem poglavju sledi analiza dveh agencij za časovno žigosanje. SI-TSA je obstoječa agencija za časovno žigosanje, ki deluje v okviru Ministrstva za javno upravo. FriTSA je agencija za časovno žigosanje, ki je bila implementirana v okviru tega projekta.

V zaključku se bomo dotaknili dodane vrednosti, ki jo nudi agencija za časovno žigosanje FriTSA za študente FRI, ter možnosti za izboljšave.

2 Centralni sistem za časovno žigosanje

Centralni sistem za izdajo časovnih žigov sta uvedla Haber in Stornetta [7]. V osnovni izvedbi ga sestavljajo Agencija za časovno žigosanje (Time-Stamping Authority - TSA) ter uporabniki. Uporabniki izstavljajo zahtevke za časovne žige dokumentov, na katere agencija odgovarja z veljavnimi časovnimi žigi. Preden začnemo s pregledom protokola časovnega žigosanja je prav, da povemo, kaj časovni žig sploh je.

Definicija 1. *Časovni žig je podpisana n-terica*

$$(izvleček, čas, politikaDelovanja),$$

kjer je

- *izvleček - izvležek narejen z zgoščevalno funkcijo, ki je krepko brez trčenj*
- *čas - podatek o času, podan v GMT s točnostjo ene sekunde*
- *politikaDelovanja - oznaka verzije politike delovanja, v okviru katere je časovni žig izdan*

Definicija 2. *Časovni žig zagotavlja, da je dokument obstajal v trenutku žigosanja.*

Prvo definicijo centralnega sistema za časovno žigosanje zasledimo leta 1991 v že omenjenem članku [7], kjer je predstavljena shema časovnega žigosanja ter shema za povezovanje časovnih žigov v verige. S povezovanjem žigov v verige želimo onemogočiti zagotoviti, da TSA ne more izdajati časovnih žigov, ki bi dokument datirali v preteklost oziroma v prihodnost.

Nadaljnje delo na področju časovnega žigosanja so predstavljale raziskave novih povezovalnih shem [4] ter definiranjem zahtev za sisteme za izdajo časovnih žigov [5]. Leta 2001 je bil objavljeno priporočilo RFC 3161 [3], ki predstavi storitev časovnega žigosanja kot del infrastrukture javnega ključa, leta 2003 pa še RFC 3628 [8], ki predlaga področja, ki naj bi jih pokrivala politika delovanja TSA. S slednjima se bomo bolj potrobno ukvarjali v sledečih poglavjih.

3 Protokol časovnega žigosanja

Časovno žigosanje je kot sestavni del kriptografije javnega ključa definirano v priporočilu RFC 3161 (Internet X.509 Public Key Infrastructure, Time-Stamp Protocol). Priporočilo določa tako tehnične vidike protokola (izgled zahtevka za časovni žig ter odgovora nanj) kot tudi zahteve, ki so potrebne zaradi zagotavljanja varnosti protokola. Slednje si bomo bolj podrobno pogledali v tem poglavju.

3.1 Zahteve za agencijo za časovno žigosanje

Agencija za časovno žigosanje naj

1. *ima zaupanja vreden vir točnega časa
2. vsak časovni žig izda z zaupanja vrednim podatkom o času
3. vsak časovni žig opremi z unikatno serijsko številko
4. za vsak veljaven zahtevek izda časovni žig, če je to le mogoče
5. vsak časovni žig opremi s podatkom o politiki delovanja, ki je bila uporabljena pri izdaji žiga
6. *časovno žigosa le izvlečke dokumentov, generirane z izbrano zgoščevalno funkcijo brez trčenj
7. preveri, če je dolžina izvlečka ustreza izbrani zgoščevalni funkciji
8. ne uporablja vsebine izvlečka razen za preverjanje dolžine
9. ne vključuje v časovni žig podatkov, ki bi identificirali pošiljatelja zahtevka
10. *za izdajo časovnih žigov uporablja ključ, ki je generiran izključno za ta namen

3.2 Analiza zahtev

Poglejmo si najprej zahteve, ki so pomembne s stališča varnosti protokola (v gornjem seznamu so označene z *).

Trditev 1. *TSA mora imeti zaupanja vreden vir točnega časa.*

Dokaz. Denimo, da TSA nima zaupanja vrednega vira točnega časa. To pomeni, da lahko napadalec vpliva na vir točnega časa tako, da ta kot trenutni čas oddaja čas drugačen od resničnega (bodisi oddaja čas v preteklosti, bodisi v prihodnosti). Ker TSA izdaja časovne žige s časom, ki ga prejme od vira točnega časa, bo tako izdala časovni žig, ki bo dokument datiral v preteklost oz. prihodnost, kar pa je v nasprotju z definicijo 2.

TSA mora torej imeti zaupanja vreden vir točnega časa. □

Trditev 2. *TSA mora za izdajo časovnih žigov uporabljati ključ, ki je generiran izključno za ta namen.*

Dokaz. Denimo, da TSA za izdajo časovnih žigov uporablja ključ, ki ga sicer uporablja še za podpisovanje sporočil. Vzemimo `LažniDokument` in izračunajmo njegov izvleček. Nato sestavimo sporočilo (izvleček, 0001-00-00 00:00:00), ter ga podpišemo. Označimo podpis s S. Dobljena trojka, (izvleček, 0001-00-00 00:00:00, S) je veljaven časovni žig, ki `LažniDokument` umešča v leto 1, kar pa je v nasprotju z definicijo 2.

Ključ, katerega TSA uporablja za izdajanje časovnih žigov se mora zato uporabljati izključno v ta namen. □

Trditev 3. *Izvleček v časovnem žigu mora biti generiran z zgoščevalno funkcijo brez trčenj.*

Dokaz. Denimo, da izvleček ni bil generiran z zgoščevalno funkcijo, ki je krepko brez trčenj.

Vzemimo `OriginalniDokument` ter ga časovno žigosajmo. Označimo dobljeni žig kot `OriginalniŽig`. Ker zgoščevalna funkcija ni krepko brez trčenj, lahko poiščemo še `LažniDokument`, ki ima enak izvleček kot `OriginalniDokument`, vendar pa je nastal kasneje. `LažniDokument` lahko z uporabo `OriginalnegaŽiga` umestimo v čas pred njegovim nastankom, kar pa je v nasprotju z definicijo 2.

Izvleček mora biti zato generiran z zgoščevalno funkcijo, ki je krepko brez trčenj. □

Ostale zahteve niso nujne s stališča varnosti samega protokola, vendar pa nam nudijo nekatere dodatne lastnosti.

Serijska številka na vsakem izdanem časovnem žigu nam omogoča, da vodimo arhiv izdanih časovnih žigov.

Oznaka politike delovanja na žigu nam omogoča, da je uporabnik seznanjen s politiko delovanja, ki je veljala ob izdaji žiga. Politika lahko npr. omejuje namene, za katere se lahko ta žig uporabi ali pa določa, koliko časa se podatki o izdanih žigih še hranijo v arhivu. Več o politikah delovanja agencij za časovno žigosanje si bomo pogledali v naslednjem poglavju.

Preverjanje dolžine izvlečka nam služi kot dodatna kontrola, da med prenosom zahteve ni prišlo do napak. Če izvleček ne ustreza izbrani funkciji lahko zahtevo takoj zavrnemo iz ne trošimo sistemskih virov za izdelavo neveljavnega časovnega žiga.

3.3 Postopek časovnega žigosanja

1. Uporabnik pošlje agenciji za časovno žigosanje
   - izvleček dokumenta
   - oznako zgoščevalne funkcije
   - veliko naključno število (opcijsko)
2. TSA preveri, če
   - je uporabljena zgoščevalna funkcija varna
   - izvleček ustreza izbrani zgoščevalni funkciji
3. TSA izvleček skupaj s trenutnim časom podpiše
4. TSA pošlje uporabniku

- časovni žig (definicija 1)
- svoj certifikat
- uporabnikovo veliko naključno število (če obstaja)

5. Uporabnik preveri, če
   - je izvleček enak njegovemu
   - je podpis veljaven
   - je certifikat TSA veljaven
   - je veliko naključno število enako kot pri zahtevku (če obstaja)

3.4 Analiza postopka

Postopek časovnega žigosanja je precej enostaven. Vsak komunikacija se zgodi v dveh sporočilih, zahtevi in odgovoru. Pomen posameznih vrednosti, ki se prenašajo je razložen v poglavju 3.2, na tem mestu pa si poglejmo bolj podrobno možnosti za napade na ta protokol v času izvajanja postopka 3.3.

3.4.1 Napad srednjega moža

Motiv napadalca v času izvajanja zahteve za časovni žig je uporabniku izdati žig, ki bo neuporaben, bodisi datiran v preteklost, bodisi prihodnost. Ker napadalec nima ključa, s katerimi TSA izdaja časovne žige, žigov ne more spreminjati, saj se v tem primeru podpis nebi ujemal, lahko pa izvede napad srednjega moža.

Denimo, da moramo nek dokument periodično časovno žigosati, da ohranjamo njegovo veljavnost. V tem primeru bodo zahteve za časovni žig, katere pošiljamo TSA, v primeru da se dokument ni spremenil, enake. Napadalec bi v tem primeru lahko posnel odgovor TSA, ter ga ponovno posredoval uporabniku. S tem uporabnik nebi prejel novega časovnega žiga, temveč starega, z datumom v preteklosti, s čimer nebi podaljšal veljavnosti dokumenta.

Kaj lahko stori uporabnik, da tak napad odkrije? Rešitev je preprosta, če uporabnik pozna točen čas mora le preveriti, da čas v časovnem žigu ne odstopa preveč. Kaj pa če uporabnik nima dostopa do ure? V tem primeru si pomaga z velikimi naključnimi števili (nonce). Preden pošlje zahtevo, ji doda še veliko naključno število. Ko TSA izda žig, to isto število priloži odgovoru. Če je število v odgovoru enako kot v zahtevi, uporabnik žig sprejme, sicer pa zavrne. S tem onemogočimo napad s ponovnim pošiljanjem.

4 Politika delovanja agencije za časovno žigosanje

Vsaka agencija za časovno žigosanje mora imeti definirano politiko delovanja, v okviru katere izdaja časovne žige. Področja, ki jih mora politika delovanja pokrivati so definirana v priporočilu RFC 3628 (Policy Requirements for Time-Stamping Authorities).

4.1 Obveznosti in odgovornosti

TSA naj v politiki delovanja določi obveznosti agencije, uporabnikov ter tretjih oseb, vključuje naj tudi obveznosti vseh zunanjih organizacij, od katerih je odvisno delovanje agencije. Politika naj bo na voljo uporabnikom in tretjim osebam skupaj z vso potrebno dokumentacijo, ki je potrebna za upoštevanje določil politike. Ta naj vključuje

1. kontaktne podatke agencije,
2. oznako vsaj ene zgoščevalne funkcije, ki se lahko uporabi za izdelavo izvlečka,
3. pričakovano življensko dobo izdanih časovnih žigov,
4. časovno natančnost, s katero se izdajajo časovni žigi,
5. morebitne omejitve uporabe,
6. informacijo, kako naj se zanesljivo preverja časovne žige.

4.2 Upravljanje s ključi

Politika delovanja agencije za časovno žigosanje naj določa, postopke za izdelavo, varovanje, obnavljanje in prenehanje uporabe zasebnih ključev za podpisovanje časovnih žigov. Določila morajo zagotavljati, da ostanejo zasebni ključi tajni, s čimer se zagotovi integriteta agencije. Izdelava varnostnih kopij zasebnega ključa ni priporočljiva, da se zmanjša možnost za zlorabo. V primeru, da se varnostne kopije zasebnih ključev vseeno izdelajo, naj politika določa postopke za kreiranje, hranjenje varnostnih kopij in obnovo ključa, ki zagotavljajo tajnost ključa.

Politika naj določa, kdo in kako nudi dostop do javnih ključev, s katerimi je možno preveriti veljavnost časovnih žigov. Certifikate agencije naj izdaja certifikatna agencija, ki je enako ali bolj zaupanja vredna kot agencija za časovno žigosanje. Veljavnost certifikatov (in s tem veljavnost časovnih žigov) naj ne bo daljša kot je pričakovani čas varnosti algoritmov in dolžin ključev uporabljenih pri generiranju časovnih žigov.

4.3 Časovno žigosanje

Določila politike naj zagotavljajo, da so časovni žigi izdani varno ter vključujejo točen čas. Politika naj torej določa način sinhronizacije ure z virom točnega časa, časovno natančnost, s katero se izdajajo časovni žigi ter postopke ob odkritju prevelikih odstopanj lokalne ure od referenčne.

Politika naj določa, da agencija za časovno žigosanje zagotavlja sinhronizacijo ure tudi v primeru uporabe prestopnih sekund ter vodi dnevnik, kdaj

so bile prestopne sekunde upoštevane. V primeru, da je odstopanje ure večje od predpisane natančnosti, naj agencija o tem obvesti uporabnike.

4.4 Upravljanje in organizacija

Politika naj določa, kako naj se varujejo prostori agencije za časovno žigosanje, kakšne omejitve dostopa so v veljavi in kakšen nadzor nad osebjem se izvaja. Določa naj zahteve za znanje in izobrazbo zaposlenih, ki skrbijo za delovanje agencije.

Določa naj tudi načine, kako se agencijo za časovno žigosanje varuje pred zunanjimi napadi (virusi, vdori, ...). Določa naj, kakšna je zaščita okolja, v katerem se nahaja agencija za časovno žigosanje, kako se varujejo prenosni mediji ter kakšni načini odkrivanja vdorov in poročanja o njih se uporabljajo.

Agencija za časovno žigosanje naj zajema tudi postopke, ki se izvedejo v primeru razkritja zasebnega ključa ali suma razkritja zasebnega ključa ali odkritja prevelikega odstopanja časovne točnosti, saj vsi ti dogodki vplivajo na zanesljivost izdanih časovnih žigov. Postopki naj vključujejo obveščanje uporabnikov o zlorabi, ki se je zgodila in prenehanje izdajanja časovnih žigov dokler se napaka ne odpravi.

4.5 Končne določbe

Politika naj določa postopke ob prenehanju delovanja agencije za časovno žigosanje, ki zagotavljajo, da je preverjanje izdanih časovnih žigov še naprej mogoče. Postopki naj vsebujejo

1. obveščanje uporabnikov o prenehanju delovanja agencije,
2. prekinitev sodelovanja z vsemi podizvajalci, ki so sodelovali pri izdaji ćasovnih žigov
3. prenos obveznosti na drugo zanesljivo organizacijo, katera naj hrani sistemski dnevnik ter dnevnik izdaje časovnih žigov ter skrbi za dosegljivost javnih ključev oziroma certifikatov dokler je to smiselno
4. uničenje zasebnih ključev, vključno z varnostnimi kopijami na način, ki zagotavlja trajno uničenje.

4.6 Skladnost z zakonodajo

Določila politike naj bodo skladna z evropsko in slovensko zakonodajo. To vključuje varovanje podatkov, preprečitev dostopa nepooblaščenim osebam, ter vodenje dnevnikov o delovanju agencije za časovno žigosanje.

5 Pregled rešitev

5.1 SI-TSA

SI-TSA je izdajatelj varnih časovnih žigov in je del infrastrukture javnih ključev overitelja na Ministrstvu za javno upravo. Na voljo je aplikacijam, katere uporabljajo institucije javne uprave ter poslovnim subjektom in drugim končnim uporabnikom s sklenjenim dogovorom.

5.1.1 Tehnični del [1]

SI-TSA sprejema izvlečke dokumentov, ki so izdelani z zgoščevalno funkcijo SHA-1 ali boljšo. Izvlečkov izdelanih z zgoščevalno funkcijo MD5 ne sprejema, saj ne veljajo več za dovolj varne. V primeru da ima zahtevek dodano veliko naključno število (nonce), ga agencija pripne odgovoru.

Za podpisovanje časovnih žigov agencija uporablja z RSA šifriran povzetek SHA-1 časovnega žiga. Dolžina ključa je 2048 bitov, veljavnost potrdil je pet let od izdaje, nova pa se generirajo vsaka tri leta. Njihovi podatki so javno objavljeni na spletni strani agencije.

Čas žigosanja je izražen v univerzalnem času (UTC), ki nima poletnega in zimskega časa, zato je pozimi eno uro, poleti pa dve uri za slovenskim. Časovni žigi so izdani z natančnostjo ene sekunde.

5.1.2 Politika delovanja [2]

Agencija za časovno žigosanje SI-TSA v svoji politiki delovanja ne omejuje rabe časovnih žigov, vendar mora biti le-ta v skladu s slovensko zakonodajo. Navodila za preverjanje veljavnosti časovnih žigov so javno objavljena na spletni strani agencije.

Ključi SI-TSA se generirajo v fizično in elektronsko varovanem okolju overovitelja, javni ključ SI-TSA je podpisal izdajatelj SIGOV-CA in mu izdal digitalno potrdilo. Algoritem in način generiranja sta v skladu z zahtevami SIGOV-CA in mednarodnimi priporočili. Zasebni ključ je varovan v strojnih kriptografskih modulih.

Javni ključ je objavljen in dostavljen v skladu s politiko SIGOV-CA v obliki digitalnega potrdila. Lastnosti in podatki o potrdilih so objavljeni tudi na spletni strani agencije. SI-TSA izjavlja, da ravna s ključi v skladu s potrdili, podrobni postopki so objavljeni v zasebnem delu politike.

Ura strežnikov SI-TSA se na varen način uskladi s časom UTC s strežnikom za sinhronizacijo časa po protokolu NTP, ki uporablja referenčno uro GPS ali DCF77 ali referenčni oscilator. Usklajenost ure strežnikov SI-TSA z referenčnim časom se stalno preverja in v primerih morebitnih odstopanj SI-TSA ustrezno ukrepa.

SI-TSA izjavlja, da so postopki za nadzor in varovanje prostorov agencije, nadzor nad osebjem, fizično varovanje in upravljanje infrastrukture v skladu s priporočili. Podrobnosti so napisane v zasebnem delu politike.

Overitelj na MJU in izdajatelj SI-TSA delujeta v skladu z:

1. ZEPEP,
2. Uredbo,

3. evropskimi direktivami,

4. priporočili RFC za časovno žigosanje: RFC 3161 “Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)”,

5. priporočili ETSI za časovne žige: ETSI TS 101 861 (v1.2.1) “Time stamping profile”,

6. in drugimi veljavnimi predpisi.

5.1.3 Cenik

Storitev	Način plačila	Cena v EUR
posamezni časovni žig	enkratni znesek	0,06
sveženj 1.000 žigov	enkratni znesek	47,99
sveženj 5.000 žigov	enkratni znesek	221,52
sveženj 10.000 žigov	enkratni znesek	406,11
sveženj 25.000 žigov	enkratni znesek	922,98
sveženj 50.000 žigov	enkratni znesek	1476,78
sveženj 100.000 žigov in več	enkratni znesek	1772,13

5.2 FriTSA

Agencija za časovno žigosanje FriTSA deluje v okviru Fakultete za računalništvo in informatiko UL. Na voljo je študentom in zaposlenim na fakulteti. Navodila za preverjanje žigov bodo javno objavljena na spletni strani agencije.

Za generiranje časovnih žigov skrbi odprtokodna implementacija priporočila RFC 3161 OpenTSA [6], ki je bila v okviru projekta posodobljena, tako da deluje z najnovešo verzijo knjižnjice OpenSSL.

5.2.1 Tehnični del

FriTSA sprejema izvlečke, ki so izdelani z zgoščevalno funkcijo SHA-1. Izvlečkov generiranih z zgoščevalno funkcijo MD5 ne sprejema, saj ne veljajo več za dovolj varne. V primeru, da ima zahtevek dodano veliko naključno število (nonce), ga agencija pripne odgovoru.

Za podpisovanje se uporablja z RSA šifriran povzetek pridobljen s SHA-1 zgoščevalno funkcijo. Dolžina ključa je 2048 bitov, veljavnost potrdila je 5 let od izdaje. Podatki potrdil bodo javno objavljeni na spletni strani agencije.

Čas žigosanja je izražen v univerzalnem času (UTC), ki nima poletnega in zimskega časa, zato je pozimi eno uro, poleti pa dve uri za slovenskim. Časovni žigi so izdani z natančnostjo ene sekunde.

5.2.2 Politika delovanja

Agencija za časovno žigosanje FriTSA v svoji politiki delovanja ne omejuje rabe časovnih žigov. Navodila za preverjanje veljavnosti časovnih žigov bodo javno objavljena na spletni strani.

Ključe FriTSA generira Certifikatna agencija @friCA. Le-ta mu generira zasebni in javni ključe ter ustrezno digitalno potrdilo. Algoritem in način generiranja ključa sta v skladu s politiko delovanja Certifikatne agencije @friCA.

Javni ključ je objavljen in dostavljen v skladu s politiko Certifikatne agencije @friCA v oblike digitalnega potrdila. Lastnosti in izvleček potrdila bodo objavljeni tudi na spletni strani.

Ura strežnika za časovno žigosanje se na varen način usklajuje s časom UTC s strežnikom za sinhronizacijo časa po protokolu NTP. Usklajenost ure strežnika se stalno preverja. V primeru morebitnih odstopanj FriTSA ustrezno ukrepa.

FriTSA izjavlja, da so postopki za nadzor in varovanje prostorov agencije, nadzor nad osebjem, fizično varovanje in upravljanje infrastrukture v skladu s priporočili. Podrobnosti so zapisane v zasebnem delu politike.

Agencija za časovno žigosanje FriTSA je agencija zaprtega tipa, zato določbe *Zakona o elektronskem poslovanju in elktronskem podpisu ZEPEP*, z izjemo določb 4. in 14. člena zanjo ne veljajo. Politika se ravna po zakonu čim bolj, tam kjer je to smiselno.

5.2.3 Cenik

Storitev je za uporabnike brezplačna.

6 Zaključek

6.1 Dodana vrednost

Agencija za časovno žigosanje FriTSA uporabnikom nudi možnost izdelave varnih časovnih žigov. Z njeno uporabo si lahko študentje pomagajo pri dokazovanju lastništva projektnih oziroma domačih nalog. V primeru, da namreč dva študenta oddata enako domačo nalogo bi namreč lahko časovni žig, ki bi dokazoval, da je en od študentov naredil nalogo pred drugim s tem dokazoval avtorstvo naloge.

V primeru nedosegljivostjo strežnika za oddajo domačih nalog, bi lahko s časovnim žigom dokazovali, da je bila naloga narejena še pred potekom roka, čeprav ni bila oddana pravočasno. Seveda bi za dejansko uporabnost agencije njene časovne žige morali sprejeti in razumeti tudi asistentje, ki preverjajo domače naloge.

V vsakem primeru pa agencija za časovno žigosanje FriTSA dopolni obstoječo Certifikatno agencijo @friCA, ter tako predstavlja naslednji korak k polni infrastrukturi javnega ključa. Njene storitve bi lahko uporabljali pri oddaji elektronskih vlog na študentski referat ter pri mnogih drugih elektronskih storitvah fakultete.

6.2 Možnosti za izboljšave

Implementirana agencija za časovno žigosanje je osnovna verzija agencije, ki ne uporablja metod za veriženje časovnih žigov. To pomeni, da ji mora uporabnik brezpogojno zaupati, da lahko trdimo, da uporablja varne časovne žige. Možnost za izboljšavo bi bila, da se doda še sistem veriženja časovnih žigov, kar bi bilo uporabno, če bi želeli storitev nuditi tudi ostalim fakultetam UL, saj pri njih ne moremo predpostaviti brezpogojnega zaupanja naši agenciji.

Druga omejitev sistema je, da uporabnik zahtevo za izdajo časovnega žiga pošilja neposredno strežniku, ki izdaja časovne žige. V primeru večjega števila uporabnikov bi to predstavljalo težavo, saj ne moremo transparentno dodajati novih strežnikov. Pomankljivost bi lahko odpravili tako, da bi agencijo poleg strežnikov, ki izdajajo časovne žige sestavljal se strežnik, ki bi sprejemal zahtevke in jih nato glede na obremenjenost pošiljal v obdelavo strežnikom za izdajo časovnih žigov.

Literatura

[1] SI-TSA. `http://www.si-tsa.si/`.

[2] Politika SI-TSA za izdajo varnih časovnih žigov, Javni del notranjih pravil overitelja na Ministrstvu za javno upravo, verzija 4.0. `http://www.si-tsa.si/dokumenti/SI-TSA-politika-za-casovni-zig-4.pdf`, 2007.

[3] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato. IETF RFC 3161 time-stamp protocol (tsp). Technical report, IETF Network Working Group, 2001.

[4] A. Buldas and P. Laud. New linking schemes for digital time-stamping. In *The 1st International Conference on Information Security and Cryptology*, pages 3–14. Citeseer, 1998.

[5] A. Buldas, P. Laud, H. Lipmaa, and J. Villemson. Time-stamping with binary linking schemes. In *Advances in Cryptology—CRYPTO'98*, pages 371–450. Springer, 1998.

[6] Zoltan Glozik. OpenTSA. `http://www.opentsa.org/`.

[7] S. Haber and W. Stornetta. How to time-stamp a digital document. *Advances in Cryptology-CRYPT0'90*, pages 437–455, 1991.

[8] D. Pinkas, N. Pope, and J. Ross. Policy Requirements for Time-Stamping Authorities. Technical report, RFC 3628. November 2003.