Študent: Ivan Štajduhar
Vpisna št.: 63960309

Digitalni dokumenti

Projekt pri predmetu
"Kriptografija in računalniška varnost"

Ljubljana, 01.07. 2002

Kazalo

1. Uvod

V dobi informacijske družbe in elektronskega poslovanja se vedno več informacij pojavlja v elektronski obliki in vedno več papirnatih dokumentov prevzema novo podobo in obliko. Danes so v večini primerov dokumenti v elektronski obliki že ob samem nastajanju, kajti pisalni stroji in magnetni zvočni in video zapisi se uporabljajo vse manj. Ob razcvetu interneta in njegove najpopularnejše storitve elektronske pošte se vsi ti dokumenti vedno pogosteje tudi prenašajo po elektronski poti. Elektronsko poslovanje in elektronsko bančništvo sta vedno bolj vsakdanja. Zaradi vse bolj uveljavljenega mednarodnega poslovanja je prenos dokumentov na dolge razdalje postal vsakdanje opravilo in pojem geografske lokacije postaja vse manj pomemben.
Mnogi od elektronskih dokumentov (na primer pomembne poslovne pogodbe) so lahko vir tožb in pravd na sodiščih, podobno kot v tradicionalnih okoljih. Seveda elektronski dokumenti niso verodostojni sami po sebi, saj jih je enostavno kopirati in spreminjati brez možnosti razkritja takih posegov. Sami znaki so med seboj enaki in iz njih ni možno spoznati pisca, kot pri lastnoročnem pisanju na papir. Tudi podpis dokumenta (odtipkana ime in priimek na koncu dokumenta) ni prepoznaven, predvsem pa ni fizično povezan z vsebino dokumenta (medtem ko lastnoročni podpis obstaja na istem papirju kot tekst in je s tem z njim neločljivo povezan). Zato v preteklosti elektronski dokumenti niso imeli neke splošno veljavne zakonske podpore. Vendar se zaradi mnogih prednosti dokumentov v elektronski obliki, kot na primer fleksibilnost in hitrost prenosa, tudi zakonska podpora pojavlja v vedno več državah sveta.
Da je določen dokument pravno zaščiten, mora biti dokazljivo verodostojen. V primeru mednarodne pogodbe lahko eden od podpisnikov kasneje na sodišču dokazuje veljavnost podpisane pogodbe na podlagi partnerjevega podpisa na sami pogodbi. Poznani sta dve vrsti verodostojnosti:

(a) verodostojnost podatkov, ki je podobna žigosanju papirnatega dokumenta na način, ki preprečuje vsako nadaljnje spreminjanje vsebine in

(b) verodostojnost izvora podatkov, ki na primer povezuje konkretno osebo s samim dokumentom. Pri tradicionalni obliki dokumentov je verodostojnost izvora realizirana s pomočjo lastnoročnega podpisa dokumenta. Ker vsaka oseba podpiše v svojem življenju precej dokumentov, postane lastnoročni podpis del njegove identifikacije, ki je ni enostavno (vendar vseeno možno) ponarediti.

Elektronski dokument ali kakršenkoli drug zapis podatkov v elektronski obliki (v nadaljevanju dokument) je enostavno kopirati ali spreminjati, ne da bi to lahko opazili (v elektronskem svetu kopij ni, so samo originali). Digitalna informacija ni povezana z nosilcem informacije in ji hkrati manjka osebnostna nota (shranjena datoteka je lahko enostavno spremenjena in ponovno shranjena s strani vsakogar, ki ima do nje dostop). Torej enostavno dodajanje podpisa na konec dokumenta na tradicionalen način ni prava metoda.
Med najpomembnejšimi zahtevami v zvezi z rokovanjem z dokumenti sta torej varnost in zaščita. Danes je doseganje varnosti v računalniških okoljih še bolj zahtevno, saj so:

- računalniki med seboj bolj povezani in s tem bolj ranljivi,
- vedno več ljudi je računalniško pismenih, tudi takih s slabimi nameni,

- dostop do tehnologije za uničevanje "varnostnih pregrad" je enostaven,
- vedno več informacij se pretaka po omrežjih in vse je težko ustrezno zaščititi,
- podatki so veliko vredni in s tem bolj mamljivi za nepridiprave.

Tako se na področju elektronskega poslovanja vedno bolj uveljavljata pojma enkripcije in elektronskega podpisa, pojavljajo se različne programske in strojne rešitve, kot tudi ustrezna infrastruktura. Ena trenutno najatraktivnejših je Infrastruktura javnih ključev (IJK) z uporabo asimetrične kriptografije javnih ključev.
Večina teh rešitev zadošča potrebnim varnostnim zahtevam, vendar v nekaterih primerih niso zadostne. Trenutno še ne tako pereča pomanjkljivost IJK je zagotavljanje dolgoročnega varovanja. Prvi problem se nanaša na varnost ključa uporabljenega v kriptografiji. Dokler je ključ varno shranjen in dokler je dolžina ključa taka, da pri obstoječi strojni opremi in matematičnem znanju zagotavlja varnost, se lahko mirno spi. Vendar bo v prihodnosti mirnega spanca slej ko prej konec in takrat bo potrebno imeti pripravljene ustrezne nove rešitve. Drugi problem je veljavnost digitalnega potrdila, ki tako kot veljavnost potnega lista s časom poteče.

2. Osnovni pojmi digitalnih dokumentov

Da se boljše seznanimo z uporabo digitalnih dokumentov, potrebno je najprej definirati nekaj osnovnih pojmov in sicer arbitrirane protokole, digitalno podpisovanje in časovno žigosanje. Primere bom predstavil z imaginarnimi osebami (dramatis personae): Roko[?], Cicibela[?], Pepina[?], ostali.

Arbitrirani protokol (ang. arbitrated protocol): Kako delamo, ko imamo potrebo za nepristrano osebo, ki bi kontrolirala potek protokola?
Arbitrator je nezainteresirana tretja oseba, ki ji je poverjeno da izvede arbitrirani protokol. Nezainteresirana pomeni, da nima nobenega interesa v protokolu in nobene pristrankosti za interese določene strani v protokolu. Vse osebe vključene v protokol verjamejo da je vse, kaj arbitrator pove, točno, da je vse kaj naredi pravilno in da bo opravil svoj del protokola.
V svetu se, kot arbitratori, običajno pojavljajo pravniki. Na primer, Cicibela prodaja avto Roku, ki ga ne pozna. Roko bi rad plačal z čekom, ampak Cicibela ne zna če je ček vnovčljiv. Cicibela želi preveriti da je ček v redu preden prepiše lastništvo nad avtom na Roka. Roko, ki ne verjame Ani ne želi dati čeka, preden se na njega prepiše lastništvo. Če oba verjameta pravniku (arbitratoru) se zgodi naslednje:

1. Cicibela prepiše lastništvo na pravnika
2. Roko da ček Ani
3. Cicibela z čekom dvigne denar
4. Če je prejšnja operacija uspela, pravnik prepiše lastništvo na Roka

Digitalni podpis (ang. digital signature): Kdo je ustvaril digitalni dokument?
Še pomembnejše od šifriranja so v elektronskem poslovanju kriptografske metode za prepoznavanje subjektov, s katerimi komuniciramo, in preverjanje pristnosti elektronskih podatkov. Ne glede na to, ali so dokumenti v elektronski obliki zaupni ali ne, moramo imeti na voljo mehanizem, s katerim nadomestimo lastnoročni podpis in preprečimo nepooblaščeno spreminjanje podatkov. Preverjanju pristnosti podatkov in identifikaciji podpisnika v elektronskem poslovanju so namenjeni elektronski podpisi.
Za elektronsko podpisovanje obstaja več metod. Primeri zelo enostavnih so vključevanje slike lastnoročnega podpisa v dokument, podpisovanje z elektronskim peresom ali metode na podlagi simetričnih kriptografskih algoritmov, na primer MAC (Message Authentication Code). Enostavne metode žal, razen v strogo nadzorovanem okolju, ne zagotavljajo zadostne stopnje varnosti in zanesljivosti. Veliko primernejša metoda za elektronsko poslovanje je digitalno podpisovanje, ki temelji na asimetrični kriptografiji. Pri digitalnem podpisovanju podpisujemo z zasebnim ključem, podpise pa preverjamo s podpisnikovim javnim ključem.

Časovno žigosanje (ang. timestamping): Kako določiti v katerem času je dokument nastal?
Dokumentu se ob nastanku ali spremembi vsebine poleg podpisa pripne še časovni žig in s tem nepopravljivo zapiše datum in čas. Kasneje se lahko ob preverjanju tak žig prebere in ugotovi, da je bil dokument časovno žigosan v določenem trenutku, torej je nastal ob ali pred tem trenutkom. Dodatno pa se lahko iz zapisa časa ugotovi, ali je čas, zapisan v časovnem žigu, v časovnem okviru veljavnosti potrdila za podpisovanje, torej po začetku in pred koncem veljavnosti oz. pred preklicem. S tem obstaja zagotovilo, da je bil dokument podpisan v času, ko je bilo potrdilo veljavno. Lahko pa je preverjanje veljavnosti zaupano kar organizaciji, ki pripne (izdela) časovni žig (torej ji je potrebno zaupati) in je v potrdilu (dodatno) zapisano, da je bilo potrdilo v času kreiranja časovnega žiga in hkrati preverjanja podpisa uporabnika s strani te organizacije veljavno (elektronsko overjanje podpisa). Ker časovni žig, ki je posebna oblika podpisa, zagotavlja tudi celovitost podpisanih podatkov, se lahko podpisane dokumente, ki so v nekem trenutku zaradi napredka tehnologije varnostno ogroženi, naknadno časovno žigosa z bolj naprednimi in varnejšimi postopki in s tem ohrani veljavnost podpisa. Vendar sama omenjena ideja o rešitvi s časovnim žigosanjem ni dovolj. Potrebno je izdelati potrebno organizacijsko in infrastrukturno podporo in nenazadnje zakonsko podlago, ki bo rešitvi dala pravno veljavo.

3. Arbitraža

3.1. Arbitrirani protokoli

Koncept arbitraže obstaja od kadar obstaja svet. Vedno so bili ljudje ? vodje, svečeniki itn. ? ki so imeli avtoritet, da se obnašajo pravično. Arbitratorji imajo določeno družbeno vlogo in mesto v družbi; če bi izdali zaupanje družbe ogrozili bi svojo vlogo in mesto. Ideal arbitratorjev se da prenesti

na svet računalništva, ampak obstajajo določeni problemi:

- Enostavneje je najti tretjo neutralno stran, če jo poznaš in ji vidiš obraz. Dve strani, ki se medsebojno sumijo bodo verjetno sumive tudi do arbitratora, ki ga ne vidijo in ki je nekje drugje na omrežju
- Računalniško omrežje mora plačati za uzdrževanje arbitratorja. Če se spomnimo koliko pravniki računajo za svoje usluge, vprašanje je koliko bi denarja morali odšteti za omrežnega arbitratorja?
- V vsakem arbitriranem protokolu vedno obstaja zakasnitveni čas
- Arbitrator se mora ukvarjati z vsako transakcijo in zato predstavlja ozko grlo veliko-razsežnih implementacij kakršnegakoli protokola. Če povečamo število arbitratorjev v implementaciji se problem ozkega grla zmanjša, ampak se stroški dvignejo.
- Ker vsi na omrežju morajo verjeti arbitratorju, on predstavlja šibko točko v sistemu vsakomu, ki želi podrediti omrežje

3.2. Sodniški protokoli

Zaradi velikega stroška angažiranja arbitratorja, arbitrirane protokole lahko razdelimo na dva podprotokola nižjega nivoja. Eden je nearbitrirani podprotokol, ki je izveden vsakič, ko vključene strani želijo dokončati protokol. Drugi je arbitrirani podprotokol, ki se izvede samo v posebnih slučajih ? kadar obstaja konflikt - tako obliko arbitratorja imenujemo *sodnik* (ang. adjudicator).

Sodnik je, enako kot arbitrator, nepristrana tretja stran kateri vsi verjamejo. Za razliko od arbitratorja, sodnik ni neposredno vključen v vsaki protokol. Sodnik se vključi v protokol le, da preveri če je protokol pravilno opravljen. Predstavil bom primer protokola z sodnikom:
Nearbitrirani podprotokol:

1. Cicibela in Roko se zmenita v zvezi s pogodbo
2. Cicibela podpiše pogodbo
3. Roko podpiše pogodbo

Arbitrirani podprotokol (v primeru konflikta):

1. Cicibela in Roko prikličejo sodnika
2. Cicibela pokaže svoje dokaze
3. Roko pokaže svoje dokaze
4. Sodnik presodi na osnovi dokazov

Razlika med sodnikom in arbitratorom je ta, da sodnik ni vedno nujan. V primeru konflikta, sodnik je priklican da presodi (kar ni vedno nujno).

Sodniški protokoli (ang. adjudicated protocols) obstajajo v računalniškem svetu. Taki protokoli bazirajo na poštenosti vključenih strani; v primeru ko obstaja sum, da nekdo goljufa, obstaja dovolj podatkov da tretja stran preveri kdo je goljufal; ali vsaj da ugotovi če je nekdo goljufal, tako da lahko postopek razveljavi. Namesto da preprečijo goljufanje, sodniški protokoli jo edino lahko ugotavljajo ? to je dovolj da ljudje, ki bi goljufali, zgubijo pogum da to tudi naredijo.

3.3. Ostalo

Kaj je alternativa arbitraži? Obstajajo usiljivi protokoli (ang. self-enforcing protocols), ki predstavljajo najboljše tipe protokolov. Sam protokol garantira pravilnost in ne potrebuje nobenega arbitratorja da rešuje konflikte. Protokol je sestavljen tako da konflikt ni možen. Če ena stran poskuša goljufati, druga stran takoj izve za to in ustavi protokol in goljufija ne uspe. Če bi bilo možno, vsak protokol bi bil somonamečuči*. Žal, ne obstajajo taki protokoli za vsak problem ? takrat uporabljamo arbitražo.

4. Digitalni podpis

Lastnoročni podpisi se že nekaj časa uporabljajo kot dokaz o avtorstvu dokumenta ali dokaz o strinjanju z vsebino dokumenta. Kaj je toliko zanimivo v podpisu?

- Podpis je izvoran. Podpis prepriča prejemnika dokumenta da je podpisnik dokumenta zavestno in nameroma podpisal dokument.
- Podpisa se ne da ponarediti. Podpis je dokaz, da je podpisnik (noben drug) nameroma podpisal dokument.
- Podpisa se ne da nanovo uporabiti. Podpis je del dokumenta; nobena oseba ne more premaknuti podpis na drug dokument.
- Podpisani dokument je nespremenljiv. Enkrat ko je dokument podpisan, ne da se ga spreminjeti.
- Podpisa se ne da zanikati. Podpis in dokument so fizične stvari. Podpisnik ne more kasneje trditi da dokumenta ni podpisal.

V praksi, nobena od zgoraj navedenih izjav ni popolnoma resnična. Podpise je možno ponarediti, možno jih je prenesti z enega dokumenta na drugi in možno jih je spremeniti tudi po podpisovanju. Zakaj potem podpise sploh uporabljamo? Zato, ker je vse to zelo težko narediti in je verjetnost ugotavljanja goljufije zelo velika. Želeli bi podpise prenesti na računalnike in tukaj obstaja več problemov. Računalniške datoteke je enostavno kopirati. Četudi je težko ponarediti lastoročni podpis, zelo je enostavno izkopirati podpis (sliko podpisa) z drugega dokumenta. Poleg tega je dokumente, ki so na računalniku, zelo enostavno spreminjati tudi po podpisovanju, brez da je sprememba očitna. Predstavil bom nekaj možnosti.

4.1. Podpisovanje dokumentov z simetričnimi kriptosistemi in arbitratorjem

Cicibela želi podpisati digitalno sporočilo in ga poslati Roku. To bo možno z pomočjo simetričnega kriptosistema in arbitratorja. Vzamimo da arbitrator lahko komunicira z Cicibelo in z Rokom. Z Cicibelo deli tajni ključ K_A, z Rokom pa različen tajni ključ K_B (omenjeni ključi obstajao že kar nekaj časa in se lahko uporabljajo večkrat).

1. Cicibela šifrira svoje sporočilo za Roka z ključem K_A in ga pošlje arbitratorju.
2. Arbitrator dešifrira sporočilo z ključem K_A.
3. Arbitrator dešifriranemu sporočilu doda izjavo da ga je prejel od Cicibele (to seveda ve, ker edino Cicibela ima ključ K_A).
4. Arbitrator šifrira sestavljeno sporočilo z ključem K_B in ga pošlje Roku.
5. Roko dešifrira sporočilo z ključem K_B. Zdaj lahko prebere sporočilo od Cicibele in certifikat arbitratorja, da je sporočilo res napisala Cicibela.

Če Roko želi Pepini pokazati dokument, ki ga je podpisala Cicibela, ne sme ji oddati svoj tajni ključ. Lahko gre spet preko arbitratorja:

1. Roko vzame sporočilo in arbitratorjevo izjavo da je sporočilo prišlo od Cicibele, šifrira vse skupaj z ključem K_B in vse pošlje nazaj arbitratorju.
2. Arbitrator dešifrira prejeto pošto z ključem K_B in preveri če je originalno sporočilo res prišlo od Cicibele.
3. Arbitrator nanovo šifrira kopico tajnim ključem, ki ga deli z Pepino, K_C. Šifrirano sporočilo pošlje Pepini.
4. Pepina dešifrira kopico z ključem K_C. Zdaj lahko prebere Cicibelino sporočilo in potrdilo arbitratorja da je sporočilo res poslala ona.

Pomanjkljivost takih protokolov je ta, da preveč porabljajo čas arbitratorja. Arbitrator mora ves čas šifrirati in dešifrirati sporočila med vsakim parom ljudi ki želijo pošiljati šifrirane dokumente eni drugim. Arbitrator je ozko grlo takega sistema - preveč uporabnikov bo zadušilo celo komunikacijo. Kaj je z varnostjo? Če eni osebi uspe uzpostavitev kontrole nad arbitratorjem (svet: korupcija; računalniki: exploit), cel sistem bo postal nevaren. Obstajajo veliko boljše metode.

4.2. Podpisovanje dokumentov z kriptografijo javnih ključev

Obstajajo algoritmi javnih ključev, ki se dajo uporabiti za digitalne podpise. V nekaterih algoritmih (npr. RSA) se za šifriranje uporablja ali privatni ključ ali pa javni. Če podpišemo dokument z svojim privatnim ključem, imamo varen digitalni podpis. V ostalih primerih (npr. DSA) obstaja samostojni algoritam za digitalne podpise, ki ga se ne da uporabiti za šifriranje. Osnovni protokol je enostaven:

1. Cicibela šifrira dokument svojim privatnim ključem (torej, podpiše dokument) in ga pošlje Roku.
2. Roko dešifrira dokument z Cicibelinim javnim ključem in tako verificira podpis

Opisan protokol je veliko boljši od prejšnjega. Arbitratora ne potrebujemo da podpisuje ali verificira podpise, tudi ne da razrešuje konflikte - če Roko ne more prebrati dokument v koraku (2), potem ve da je podpis neveljaven. Protokol zadovoljuje vse pogoje vezane za lastoročni podpis, opisane na začetku poglavja.

4.2.1. Podpisovanje dokumentov in časovno žigosanje

Obstajajo neke nevarnosti. Roko lahko prelisiči Cicibelo v nekaterih okoliščinah. Roko lahko uporabi dokument, skupaj z podpisom od Cicibele. To seveda ni problem če je podpisani dokument neka pogodba - akj pomeni ena ali več kopij pogodbe, ampak postaja problem kadar je dokument digitalni ček. Vzamimo da je Cicibela napisala en ček na Roka v znesku 100$. Roko vzame ček (dokument), shrani eno kopijo na strano, gre z čekom na banko, banka verificira podpis, in prenese

denar na svoj bančni račun. Naslednji teden vzame kopijo in je spet nese na banko (recimo neko drugo banko) , banka verificira podpis in prenese denar na Rokov bančni račun. Roko lahko ponavlja celoten postopek kolikokrat želi. Kot posledica, digitalni podpisi pogosto vsebujejo časovni žig. Datum in čas podpisa sta shranjena na dokumentu. Banka shrani datum in čas v bazo podatkov. Ko Roko poskuša vnovčiti ček drugič, banka primerja časovni žig z časovnimi žigi v bazi podatkov (ker ga najde, pokliče policijo).

4.2.2. Podpisovanje dokumentov z uporabo enosmernih zgoščevalnih funkcij

V praktičnih implementacijah so kriptosistemi javnih ključev neučinkoviti (počasni) pri podpisovanju dolgih dokumentov. Da bi skrajšali potreben čas, protokoli za digitalno podpisovanje pogosto uporabljajo podpisovanje enosmernih zgostitev dokumenta.

1. Cicibela naredi enosmerno zgostitev dokumenta in je šifrira svojim privatnim ključem (podpiše dokument)
2. Cicibela pošlje dokument in podpisano zgostitev Roku
3. Roko naredi enosmerno zgostitev prejetega dokumenta in istočasno dešifrira prejeto zgostitev dokumenta z Cicibelinim javnim ključem. Če sta zgostitvi enaki je podpis veljaven.

Z uporabo zgostitev se potreben čas veliko skrajša. Zgostitve morajo seveda biti enosmerne - sicer bi lahko sami generirali več dokumentov ki bi se zgostili v isto vrednost in bi lahko z podpisom enega dokumenta podpisali tudi ostale.

Ostale prednosti? Podpis lahko držimo posebej (ni nujno de je na dokumentu). Prejemnikove zahteve po prostoru so veliko manjše - namesto dokumentov ima samo podpisane zgostitve dokumentov. Če želimo imati en centraliziran arhiv dokumentov, dovolj je da v njem shranimo samo zgostitve dokumentov (recimo skupaj z časovnimi žigi). Na tak način lahko patentiramo neko skrivnost - dokaz da smo nek dokument napisali je shranjen v arhivu, ampak noben ne pozna vsebine tega dokumenta, dokler je ne prezentiramo.

4.3. Skupinsko podpisovanje

Kako bi Roko in Cicibela skupaj podpisali isti digitalni dokument? Če ne uporabljamo enosmerne zgoščevalne funkcije, obstajajo dve možnosti. Ena je da Roko in Cicibela podpišeta vsak svojo kopijo dokumenta - rezultat je podpisani dokument, ki je dvakrat večji od originala. Druga možnost je da prvo Cicibela podpiše dokument in na to Roko podpiše podpisani dokument - to sicer deluje, ampak ne obstaja možnost verificiranja Cicibelinega podpisa brez da verificiramo tudi Rokov podpis.

Z uporabo enosmernih zgoščevalnih funkcij postopek poteka na naslednji način:

1. Cicibela podpiše zgostitev dokumenta
2. Roko podpiše zgostitev dokumenta
3. Roko pošlje svoj podpis Cicibeli
4. Cicibela pošlje dokument, svoj podpis in Rokov podpis Pepini
5. Pepina verificira Cicibelin in Rokov podpis

Roko in Cicibela lahko izvajajo koraka (1) in (2) istočasno. V koraku (5) Pepina lahko preveri en podpis brez potrebe da preveri tudi drugega.

4.4. Zanikanje digitalnega podpisa

Recimo da želimo goljufati. Prvo podpišemo nek dokument in potem rečemo da ga nismo podpisali. To naredimo tako da anonimno objavimo naš privatni ključ na internetu, ali ga prikladno izgubimo na javnemu mestu ali nekaj podobnega. Potem se lahko pretvarjamo da je nekdo drug podpisal dokument in ne mi. Kakšna zaščita obstaja od tega?

Časovni žigi lahko omejijo efekte takega načina goljufanja, ampak nekdo bi lahko trdil da je njen ključ bil ogrožen pred tem. Obstaja en protokol, ki uporablja podobno logiko:

1. Cicibela podpiše dokument
2. Cicibela generira glavo dokumenta, ki vsebuje identifikacijske informacije. Doda glavo na podpisan dokument, podpiše vse skupaj in pošlje arbitratorju
3. Arbitrator preveri zunanji podpis in potrdi identifikacijske informacije (glavo). Potem doda časovni žig na glavo+dokument, podpiše vse skupaj in pošlje Cicibeli in Roku.
4. Roko preveri arbitratorjev podpis, identifikacijske informacije in Cicibelin podpis.
5. Cicibela preveri sporočilo, ki ga je arbitrator poslal Roku. Če ona ni avtor tega sporočila, potem se hitro oglasi.

4.5. Simultano podpisovanje

4.5.1. Simultano podpisovanje dokumenta z pomočjo arbitratora

Roko in Cicibela želita skleniti pogodbo. Zmenila sta se v zvezi z besedilom pogodbe, ampak noben ne želi podpisati dokumenta preden ga drugi podpiše. En način kako rešiti ta problem je z pomočjo arbitratora:

1. Cicibela podpiše kopijo pogodbe in je pošlje arbitratorju
2. Roko podpiše kopijo pogodbe in je pošlje arbitratorju
3. Arbitrator pošlje sporočilo Roku in Cicibeli, da je drug podpisal
4. Cicibela podpiše dve kopije dokumenta in jih pošlje Roku
5. Roko podpiše obe prejeti kopiji, eno obdrži, drugo pa pošlje nazaj Cicibeli
6. Roko in Cicibela obvestita arbitratorja da vsak ima svojo kopijo pogodbe z oba podpisa
7. Arbitrator uniči kopije dokumenta z samo enim podpisom

Arbitrator preprečuje goljufanje - če bi katerakoli stran, v korakih (4)-(5) odločila da ne bo podpisala pogodbe, še vedno ostane ena kopija podpisane pogodbe pri arbitratorju. Iz že znanih razlogov se poskušamo izogniti uporabi arbitraže.

4.5.2. Simultano podpisovanje dokumenta brez arbitratorja

Roko podpiše prvo črko svojega imena, Cicibela podpiše prvo črko svojega imena, Roko podpiše drugo črko svojega imena, Cicibela podpiše drugo črko svojega imena, Roko...

V opisanem protokolu, Roko in Cicibela izmenjata vrsto sporočil oblike: "Strinjam se, da sam vezan na pogodbo z verjetnostjo *p*." Prejemnik takega sporočila lahko to sporočilo nese sodniku, ki z verjetnostjo p odloči če je dokument podpisan.

1. Roko in Cicibela odločita katerega datuma bo končalo podpisovanje. Odločita se tudi za

maksimalno verjetnostno razliko. Npr., Cicibela je odločila da ne bo vezana na dokument z verjetnostjo, ki je 2% večja od Rokove verjetnosti. Naj bo Cicibelina verjetnostna razlika *a* in naj bo Rokova verjetnostna razlika *b*.

2. Cicibela pošlje Roku dokument podpisan z $p=a$
3. Roko poršlje Cicibeli dokument podpisan z $p=a+b$
4. Naj bo p verjetnost sporočila, ki ga je Cicibela prejela od Roka v prejšnjem koraku. Cicibela pošlje Roku podpisano sporočilo z $p'=p+a$ (ali $p'=1$, če je vrednost $p+a$ večja od 1).
5. Naj bo p verjetnost sporočila, ki ga je Roko prejel od Cicibela v prejšnjem koraku. Roko pošlje Cicibeli podpisano sporočilo z $p'=p+b$ (ali $p'=1$, če je vrednost $p+b$ večja od 1).
6. Roko in Cicibela ponavljata koraka (4) in (5) vse dokler oba ne dobita sporočila z verjetnostjo $p=1$, ali do poteka datuma, zakazanega v koraku (1).

Z vsakim korakom je vezanost podpisnika dokumenta, na dokument, vse večja. Če se podpisovanje dokumenta konča v zakazanemu roku je vse v redu. Sicer, katerakoli oseba lahko nese dokument sodniku skupaj z zadnjim podpisanim "nasprotnikovim" sporočilom. Preden pogleda sporočilo, sodnik naključno izbere eno število med 0 in 1. Če je vrednost tega števila manjša od verjetnosti sporočila, obe strani sta vezani z dokumentom, če je vrednost večja, obe strani nista vezani na dokument.

4.5.3. Simultano podpisovanje dokumenta brez arbitratorja, z uporabo kriptografije

Kriptografski protokol uporablja enak pristop, kot je opisano v 4.5.2. DES, ki je predstavljen v opisu bi lahko zamenjali z katerimkoli simetričnim algoritmom.

1. Roko in Cicibela naključno izbereta $2n$ DES ključev, grupirane v parih (za potrebe protokola).
2. Roko in Cicbela generirata n parov sporočil, L_i in R_i oblike: "To je leva stran mojega i-tega podpisa" in "To je desna stran mojega i-tega podpisa", npr. Vsako sporočilo bo verjetno vsebovalo tudi digitalni podpis pogodbe in časovni žig. Predpostavimo da je pogodba podpisana, če ena od strani pokaže obe polovici, L_i in R_i, enega para podpisa.
3. Roko in Cicibela šifrirajo svoje pare sporočil z vsakim od $2n$ DES ključev, levo stran sporočila z levim ključem v paru in desno z desnim.
4. Roko in Cicibela pošljejo drugi drugemu kopice $2n$ šifriranih sporočil, levo in desno polovico posebej.
5. Roko in Cicibela pošljejo drugi drugemu vse pare ključev, vsaki par posebej na naslednji način, npr. Cicibela pošlje Roku ključ, ki se uporablja za šifriranje levega sporočila ali ključ, ki se uporablja za šifriranje desnega sporočila, neodvisno, za vsak od n parov. Po končani izmenjavi ključev Roko in CIcibela imata po en ključ od vsakega para ključev, ampak noben ne zna katero stran ima, levo ali desno.
6. Roko in Cicibela dešifrirata polovice sporočil, ki jih lako dešifrirata, z uporabo ključev, ki sta jih prejela. Preverita, da so dešifrirana sporočila veljavna.
7. Drugi drugemu pošljeta nekaj prvih bitov vsakega od $2n$ DES ključev. Ta korak ponavljata vse dokler ne izmenjata vse bite ključev.
8. Roko in Cicibela dešifrirata polovico sporočil, ki je ostala in pogodba je zdaj podpisana.
9. Roko in Cicibela izmenjata privatne ključe, ki sta jih uporabila za izbiro strani v koraku (5). Vsak preveri da drugi ni goljufal.

4.6. Uporaba digitalnih podpisov

Eden od prvih predlogov za uporabo digitalnih podpisov je bil implementacija preverjanja sporazuma o prepovedi nuklearnih testiranj. ZDA in SS so se zmenile da eni drugim postave seizmometre* v zemljo, ki bi lahko detektirali možna nuklearna testiranja. Problem je bil v tem da se je vsaka država morala prepričati, da druga država, domačin, ne bo spreminjala podatke iz seizmometrov*. Istočasno se je država domačin morala prepričati da merilni instrumenti pošiljajo le podatke potrebne za ta nadzor (zaščita od dodatnega vohunjenja).
Konvencionalne metode lahko obdelajo prvi problem. Edino digitalni podpisi lahko obdelajo oba problema.

5. Časovno žigosanje

Včasih ljudje potrebujejo potrdilo, da je dokument nastal določenega datuma. En primer bi bilo nesoglasje v zvezi z copyright-om ali patentom. Pri papirnatih dokumentih, notarji se podpišejo in nato pravniki shranijo kopije dokumenta. V digitalnem svetu je stvar bolj komplicirana. Kako ugotoviti če je nekdo spremenil vsebino dokumenta? Podobno, kako ugotoviti če je nekdo spremenil časovni žig, ki je dodan na konec dokumenta? Haber in Stornetta predlagata naslednje lastnosti protokola za časovno žigosanje:

- Podatki sami morajo biti žigosani, ne glede na medij na katerem so.
- Naj bi bilo nemogoče spremeniti kateregakoli bita dokumenta brezopazno.
- Naj bo nemogoče časovno žigosati dokument z datumom in časom različnim od sedanjeg.

Rešitev je več, predstavil bom le najbolj pomembne.

Arbitrirana rešitev (ang. arbitrated solution): Naj bo Janez lastnik servisa za časovno žigosanje.

1. Cicibela pošlje kopijo dokumenta Janezu
2. Janez zabeleži datum in čas prejema dokumenta (doda žig na dokument) in obdrži eno kopijo, kot dokaz
3. Če nekdo sumi Cicibelino trditev, da je dokument nastal takrat, potem Cicibela lahko prezentira dokaz z pomočjo Janeza.

Protokol deluje, ampak ima veliko slabosti:

- Ne obstaja privatnost. Če nekdo vohuni po komunikacijskem kanalu lahko izve celotno vsebino dokumenta.
- Baza podatkov (repozitorij časovno ožigosanih dokumentov) mora biti velika. Tudi hitrost komunikacijskih kanalov nekaj pomeni.
- Napaka pri prenosu dokumenta, napaka pri shranjevanju dokumenta ali vdor nepridipravih v bazo podatkov

◦. Obstaja možnost da lastnik servisa za časovno žigosanje ni pošten. Kako ga nadzorujemo?

Izboljšana arbitrirana rešitev (ang. improved arbitrated solution): Dodana je uporaba enosmerne zgoščevalne (ang. hash) funkcije in digitalnega podpisa. Naj bo Janez spet lastnik servisa za časovno žigosanje.

1. Cicibela generira enosmerno zgostitev dokumenta
2. Cicibela pošlje zgostitev dokumenta Janezu
3. Janez pripne datum in čas prejema zgostitve dokumenta, potem L_i in R_im digitalno podpiše celo stvar
4. Janez pošlje podpisano žigosano zgostitev nazaj Cicibeli

Tak pristop reši vse probleme iz prejšnjega protokola razen zadnjega.

Povezovalni protokol (ang. linking protocol): En način da se reši omenjeni problem je ta, da časovno žigosano zgostitev dokumenta povežemo z časovno zgostitvijo naslednjega dokumenta. Verjetno bodo prej ali slej obstajale tudi druge osebe, poleg Cicibele, ki bodo zahtevale časovni žig na svojih dokumentih. Naj bo H_n zgostitev dokumenta, naj bo A Cicibelina identifikacija in naj bo T_{n-1} prejšnji časovni žig.

1. Cicibela pošlje Janezu H_n in A
2. Janez pošlje nazaj Cicibeli T_n, kjer je T_n sestavljen iz (zgoščenih) naslednjih podatkov: $S_K(n,A,H_n,T_n,I_{n-1},H_{n-1},T_{n-1},L_n)$. S_K pomeni da je sporočilo podpisano z Janozovim javnim ključem. Cicibelino ime identificira osebo, ki je dala zahtevo za postopkom. Parameter n predstavlja redno številko časovnega žiga ? pred tekočim, Janez je izdal n-1 žigov. Parameter T_n predstavlja tekoči čas. Ostale informacije so identifikacija, izvirna zgostitev dokumenta, čas in zgoščen časovni žig dokumenta n-1.
3. Ko Janez doda časovni žig na dokument n+1, pošlje Cicibeli identifikacijo osebe, ki je zahtevala žigosanje dokumenta, I_{n+1}

Če nekdo sumi Cicibelin časovni žig, ona pokliče lastnike dokumentov n-1 in n+1. Če nekdo spet sumi njihove dokumente, lahko se preverijo lastniki dokumentov n-2 in n+2, itn. Na tak način je zelo težko goljufati in žigosati dokument z datumom, ki je različen od tekočega. Janez ne more zapisati datuma v prihodnosti, ker bi potreboval znanje o tem kateri dokument bo tik pred določenim datumom. Ne more zapisati datuma v preteklosti, ker bi dokaz o temu dokumentu moral biti zapisan v dokumentu tik po določenemu datumu. Edino kaj Janez lahko naredi je da izmisli verigo fiktivnih dokumentov pred in po izmišljenemu datumu, dovolj dolg da nekomur, ki bi preverjal pravilnost tega časovnega žiga, postane dolgčas.

Distribuiran protokol (ang. distributed protocol): Ljudje umirajo, časovni žigi se zgubljajo- Veliko stvari se lahko zgodi, ki otežavajo ugotavljanje pravilnosti žiga. Ta problem bi rešili tako, da namesto ene osebe (lastnika časovno žigosanega dokumenta) prej in ene osebe po vzamemo več (recimo 10) oseb prej in oseb po žigosanje našega dokumenta. Tako je veliko (10-krat) veča verjetnost, da nam bo uspelo preveriti pravilnost časovnega žiga. V distribuiranemu protokolu naredimo prav to ? izberemo k oseb, pa se še izognemo uporabi arbitratorja.

1. Z uporabo H_n kot vhoda, Cicibela generira zaporedje naključnih vrednosti, z uporabo pseudo-naključnega generatorja števil: $V_1,V_2,...,V_K$.

2. Cicibela interpretira vsako od teh vrednosti kot identifikacijo I druge osebe. Nato pošlje H_n vsem k osebam.
3. Vsaka od k oseb doda datum in čas na zgostitev dokumenta, podpiše celo stvar in je pošlje nazaj Cicibeli.
4. Cicibela zbere vse časovne žige in jih shrani kot enega.

Kriptografski varen pseudo-naključni generator števil prepreči Cicibelo da namenoma izbere nepoštenih k oseb kot overitelje. Zgostitvena fukncija daje identitete overiteljev in zato je težko goljufati v koraku (1). Če bi Cicibela želela goljufati, potem bi morala prepričati vseh k oseb da sodelujejo. Ker so osebe izbrane naključno, verjetnost da ji uspe je zelo majhna. Ko obstaja možnost da nekaj oseb ne pošlje časovnega žiga takoj po zahtevi, vzame se neka podmnožica od k, ki je potrebna da bi žig veljal.

Izboljšave protokolov za časovno žigosanje vključujejo uporabo dvojiških dreves da bi se povečalo število časovnih žigov, ki so odvisi od določenega žiga. Priporoča se objava zgostitve dnevnih časovnih žigov na javnemu mestu, kot so časopisi. Taka zgostitev je objavljena v vsaki nedeljni izdaji New York Times-a od leta 1992.

6. Zaključek

V okviru tega projekta sam predstavil osnovne koncepte digitalnih dokumentov: arbitražo, digitalno podpisovanje in časovno žigosanje. Opisal sam veliko protokolov, od bolj enostavnih, ki se tudi danas uporabljajo v nedigtalnemu svetu, vse do takih, katerih podlaga je globoko v kriptografiji. Omenjeni protokoli in zaključki, vezani uz posamezne, se lahko implementirajo na veliki večini digitalnih dokumentov: bančne transakcije, digitalni arhivi patentov, digitalne pogodbe itn. Odvnisno od tega za kaj potrebujemo protokol, koliko varna mora biti rešitev, in koliko denarja smemo uporabiti, izberemo posamezno rešitev za vsak problem.

Elektronsko poslovanje končno dobiva svoj prostor tudi v Sloveniji. Vse več slovenskih podjetij omogoča nakupovanje v spletnih trgovinah, banke ponujajo strankam nove storitve elektronskega bančništva, državna uprava počasi le oznanja, da bomo državljani morda lahko določene opravke, na primer sodelovanje na javnih razpisih, oddajo napovedi dohodnine ali pridobivanje izpiskov iz matične in zemljiške knjige, kmalu opravili tudi po internetu. Čez čas bodo verjetno v elektronski obliki tudi osebne izkaznice in potni listi, večji obseg elektronskega poslovanja pa smemo v kratkem pričakovati tudi med podjetji (business-to business).

Upam da bo predstavljeno znanje pomagalo bralcu, da se boljše seznani z delovanjem protokolov, ki se uporabljajo za obdelav digitalnih dokumentov.

Literatura

[1] Bruce Schneier: "Applied cryptography", 1996
[2] Mitja Dečman: "Časovno žigosanje v elektronskem poslovanju in njegova implementacija v slovenski državni upravi", 2001
[3] "Elektronski podpisi", Monitor, slovenska računalniška revija, oktober 2000