Varne komunikacije

Vsebina

Elektronski dokumenti

Živimo v času, ko je postal osebni računalnik standardni del pisarniške opreme, podobno kot je bil še nedavno tega pisalni stroj. Večino dokumentov, ki jih potrebuje podjetje pri svojem poslovanju, nastaja danes s pomočjo računalnika. Šele ko tak dokument izpišemo s pomočjo tiskalnika, dobimo dokument v klasični obliki, to je na papirju. Običajno pred izpisom dokument shranimo tudi na disku računalnika. Ker je shranjen v elektronski obliki, imenujemo tak dokument tudi elektronski dokument.

Elektronski dokument shranjen na disku lahko ponovno pregledamo, lahko ga izpišemo na tiskalniku, lahko pa ga po potrebi tudi popravimo. V poslovnem pismu lahko, na primer, spremenimo naslovnika, popravimo datum, spremenimo še kakšno malenkost in že imamo pripravljeno pismo za novega partnerja. V tem je velika prednost elektronskih dokumentov, obenem pa je ravno v tem tudi težava. Elektronske dokumente je preveč lahko spreminjati, da bi nam brez posebnih varnostnih mehanizmov lahko služili kot zanesljiv arhiv. Če želimo kdaj kasneje z zanesljivostjo vedeti, kakšno je bilo pismo v originalu, moramo še vedno arhivirati njegovo kopijo na papirju. Samo arhiv v elektronski obliki ne zadošča. To velja toliko bolj za dokumente, ki so pravno veljavni, kot so to na primer pogodbe.

Izmenjava elektronskih dokumentov

Velik del v poslovanju podjetja predstavlja izmenjava različnih dokumentov kot so pogodbe, računi, naročila, poslovne informacije in podobno. Taka izmenjava lahko poteka v okviru samega podjetja ali pa med podjetjem in njegovimi partnerji. Klasične dokumente, ki so namenjeni partnerju na drugi lokaciji, lahko tja odnese kurir ali pa jih pošljemo po pošti. Taka izmenjava je lahko zelo zamudna, še posebej kadar gre za partnerje v tujini. Široka uveljavitev telefaksa je močno skrajšala ta postopek. Dokument stiskamo na tiskalniku, ga vstavimo v svoj telefaks in že čez nekaj trenutkov ima partner na mizi svojo kopijo dokumenta. Če imamo v svojem računalniku vgrajeno kartico s telefaksom, lahko ta postopek še skrajšamo. Dokumenta sploh ni potrebno tiskati na svojem tiskalniku, temveč ga lahko tiskamo neposredno na telefaksu svojega partnerja.

Pogosto imamo opravka z dokumenti, ki jih želi imeti partner v elektronski obliki, ker jih želi v taki obliki shraniti ali pa jih mora še nadalje obdelati. Taka so na primer razna poročila, prispevki novinarjev, ki prispejo v uredništvo časopisa, dopisi, ki jih damo v prevod ali lekturo, ali pa podatki, ki jih je potrebno vnesti v bazo podatkov. Če tak dokument nastane na računalniku, ga najprej izpišemo na papir, nato ga pošljemo svojemu partnerju, ki ga mora ponovno vnesti v računalnik. Tak postopek je zamuden poleg tega pa lahko pride do napak pri ponovnem vnašanju. Izpisu in ponovnemu vnašanju se lahko izognemo, če dokument pošljemo kar v elektronski obliki. Dokument shranimo na disketo in disketo pošljemo po pošti.

Izmenjava elektronskih dokumentov se močno poenostavi, če smo s svojim računalnikom vključeni v globalno omrežje Internet in je vanj vključen tudi naš partner. V tem primeru lahko dokument s pomočjo elektronske pošte pošljemo neposredno s svojega računalnika na računalnik svojega partnerja. Tudi njegov odgovor lahko sprejmemo neposredno na svojem računalniku. Tak način izmenjave elektronskih dokumentov je izredno učinkovit, predvsem hiter in poceni. Hitrost in cena pri tem nista odvisna od oddaljenosti našega partnerja.

Zaupni dokumenti in zasebnost

Dokumenti, ki jih izmenjujemo s svojimi partnerji so pogosto zaupne narave in zato želimo, da bi imel vanje vpogled samo tisti, ki so mu namenjeni, vsem ostalim pa želimo vpogled onemogočiti. To imenujemo zasebnost. Pri izmenjavi klasičnih dokumentov zagotovimo zasebnost tako, da dokumenta ne pošiljamo na dopisnici, temveč ga pošiljamo v zaprti ovojnici. Podobno lahko storimo tudi z dokumentom na disketi. Zasebnost v tem primeru sloni na upanju, da bo odprla ovojnico natančno tista oseba, ki ji je dokument namenjen, vsi ostali pa bodo pustili ovojnico nedotaknjeno.

Največkrat se že sami zavedamo, da na ta način nismo zagotovili ne vem kako velike zasebnosti. Vsakdo, ki dobi dokument v roke, lahko ovojnico odpre, prebere dokument in ga shrani nazaj, ne da bi naslovnik za to izvedel. Poleg tega je dokaj pogosto, da pošto, ki je namenjena direktorju, najprej prebere njegova tajnica, ki ne more vnaprej vedeti, da je dokument zaupne narave. Bolj pomembne dokumente bi bilo zato potrebno že na ovojnici označiti kot zaupne in jih po možnosti zapečatiti, tako da jih ni mogoče odpreti, ne da bi to opazili. Žal taki dokumenti pritegnejo nase večjo pozornost in so še bolj zanimivi za tiste, ki jim niso namenjeni. Četudi kasneje ugotovimo, da je bil dokument odprt, je zasebnost izgubljena, pomembni podatki pa so prišli v napačne roke. Zelo zaupnih dokumentov zato verjetno ne bomo zaupali pošti, ampak jih bo raje odnesel kurir, ali pa jih bomo predali osebno.

In kako je z zasebnostjo dokumentov, ki jih pošljemo po elektronski pošti preko Interneta? Stopnja zasebnosti pri tem približno ustreza zasebnosti, ki jo dosežemo, če dokument pošljemo po pošti. Ravno tako kot ni prav pogosto, da bi pisma na pošti odpirali poštni uradniki ali poštar, tako tudi pošte na Internetu običajno nihče ne prebira. Vendar to ni nemogoče! Podobno kot imajo najlažji dostop do navadne pošte poštni uradniki, imajo najlažji dostop do pošte na Internetu tisti, ki s tem omrežjem upravljajo, čeprav ni običajno, da bi jo prebirali.

O tem, kako je mogoče doseči večjo stopnjo zasebnosti pošte na Internetu, tako, ki močno presega zasebnost običajne pošte, pa bomo govorili v nadaljevanju.

Verodostojnost dokumentov

Velika večina dokumentov, s katerimi imamo opravka, običajno ni zelo zaupnih, pomembna pa je njihova verodostojnost. Takšne so predvsem različne pogodbe in uradne izjave. Verodostojnost izjave zagotavljamo s svojim lastnoročnim podpisom, na pogodbah pa morajo biti lastnoročni podpisi vseh strank. Čeprav se tega običajno ne zavedamo, ima lastnoročni podpis na dokumentu dva različna pomena. Podpis pomeni, da je dokument istoveten, to je tak kot je bil takrat, ko smo ga podpisali, pomeni pa tudi, da se strinjamo z njegovo vsebino. Kadar sta izpoljnjeni obe funkciji govorimo o verodostojnosti dokumenta. Verodostojnost dokumenta, ki temelji na lastnoročnem podpisu, sloni na dveh predpostavkah:

- da podpisa ni mogoče ponarediti in
- da se dokumenta, potem ko je bil enkrat podpisan, ne da več spreminjati.

Obe predpostavki sta le deloma točni. Še posebej je vprašljiva druga predpostavka, da dokumenta ni mogoče naknadno spreminjati, če se zavedamo, da je danes večina pogodb stiskanih na tiskalniku, spetih z navadnimi sponkami in podpisanih zgolj na zadnji strani. Zelo enostavno je tako pogodbo razpeti, zamenjati liste v sredini, ali pa dodati nekaj besed na prazne prostore, ki so spuščeni med posameznimi členi ali na koncu odstavkov. Trdimo lahko, da v vsakdanjem življenju poslujemo večinoma z dokumenti, ki imajo zagotovljeno dokaj nizko verodostojnost in velik del poslovanja temelji predvsem na zaupanju.

In kako je z verodostojnostjo elektronskih dokumentov? Elektronskega dokumenta ni mogoče lastnoročno podpisati, poleg tega pa je zelo enostavno popraviti njegovo vsebino. O tem, kako je mogoče zagotoviti bistveno večjo verodostojnost elektronskega dokumenta, kot jo zagotavlja lastnoročni podpis, bo govora v nadaljevanju.

Šifriranje dokumentov

Če želimo zagotoviti zasebnost nekega dokumenta ga moramo šifrirati tako, da ga zna dešifrirati tisti, ki mu je dokument namenjen, vsem ostalim pa je vsebina dokumenta nedostopna. Šifrirati je mogoče tako klasične kot elektronske dokumente. Pri tem imajo prednost elektronski dokumenti, ker tu postopek šifriranja in dešifriranja opravi računalnik. Šifriran dokument lahko pošljemo po elektronski pošti,

ne da bi tvegali, da ga bo prebral nekdo, ki mu ta dokument ni namenjen, pa četudi bi ga uspel nekako prestreči. Stopnja zasebnosti, ki jo dosežemo s šifriranjem je odvisna predvsem od učinkovitosti šifrirnega postopka in tajnosti dešifrirnega postopka. Dešifrirni postopek mora namreč poznati samo tisti, ki mu je dokument namenjen. Le tako je namreč mogoče zagotoviti, da nihče drug ne bo mogel dešifrirati dokumenta.

Šifriranje je uporabljal že Julij Cezar pred več kot 2000 leti, ko je pošiljal pošto Ciceru. Uporabljal je zelo enostaven postopek šifriranja.
Vse črke v besedilu je zamenjal s črkami, ki so bile za tri mesta naprej v latinski abecedi. Beseda CESARUS je bila na ta način šifrirana v FHVDUAV. Cezar je uporabljal isti postopek tudi, ko si je dopisoval z drugimi prijatelji. Ker so morali vsi poznati postopek, da so lahko prebrali svojo pošto, jim je to omogočalo, da so prebrali tudi pošto namenjeno Ciceru. Postopek je bil tudi izredno enostaven. Nekdo, ki se danes ukvarja s šifriranjem, bi tak postopek z lahkoto razvozlal že na osnovi dveh do treh šifriranih stavkov. Kljub tej enostavnosti pa je v tem postopku skrita osnovna ideja šifriranja. Dober šifrirni postopek mora danes izpolnjevati naslednje pogoje:

Zasebnost ne sloni na tajnosti samega šifrirnega postopka temveč na tajnosti posebnega ključa za dešifriranje. Z drugimi besedami
to pomeni, da ima lahko vsakdo na voljo računalniški program za dešifriranje, vendar mu to nič ne pomaga, če ne pozna tajnega ključa.
Postopek šifriranja mora biti enostaven, to je, s pomočjo računalnika izvedljiv v čim krajšem času.
Postopek dešifriranja mora biti enostaven za tistega, ki pozna tajni ključ in praktično neizvedljiv za tistega, ki tega ključa ne pozna,
četudi pozna sam postopek dešifriranja in ima na razpolago zmogljiv računalnik.

Poglejmo si to na primeru šifriranja, ki ga je uporabljal Cezar. Že pri tem postopku lahko ločimo ključ od samega postopka. Postopek bi lahko tu opisali na naslednji način:

Vasko črko besedila nadomesti z črko, ki nastopa v abecedi K znakov kasneje. Ko prideš do konca abecede, nadalj štetje zopet na začetku.

Pri tem postopku predstavlja število K tajni ključ. Ker je Cezar uporabljal izključno ključ K = 3, zasebnost njegovega postopka očitno ni

temeljila na tajnosti ključa temveč na tajnosti samega postopka. Kasneje je cesar Avgust uporabljal isti postopek s ključem K=25.

Varnost tega postopka ne more sloneti samo na tajnosti ključa, ker je mogočih le 24 različnih ključev. Pri K = 25 je namreč šfrirano
sporočilo enako originalu. S preizkušanjem vseh 24 možnih ključev bi že v tistih časih zlahka dešifrirali sporočilo.

Simetrično šifriranje

Simetrično šifriranje štejemo za klasičen postopek šifriranja. Da je simetrično pravimo zato, ker je za šifriranje uporabljen isti ključ kot
za dešifriranje. To je bil do pred nedavnim tudi edini možni način šifriranja.

Med simetričnimi šifrirnimi postopki se je najbolj uveljavil DES (data encription standard), ki je kot šifrirni postopek za poslovno
uporabo (poslovanje bank, poslovanje borze, ...) standariziran v ZDA. Pri tem postopku se za šifriranje in dešifriranje uporablja isti
ključ. V odvisnosti od izbranega ključa DES najprej po zapletenih pravilih premeče črke po tekstu, jih zamenja z drugimi in nato
ponovno premeče. Po večkratni ponovitvi tega postopka iz šifriranega dokumenta ni več mogoče razbrati originalnega , če ne poznamo
tajnega ključa, ki bi omogočil, da bi postopek izvedli v obratni smeri. Za enkrat DES velja za varen postopek šifriranja, saj ga v vsem
času njegovega obstoja še nikomur ni uspelo razbiti, čeprav so se s tem ukvarjali vrhunski strokovnjaki s področja šifriranja.

Edini znani postopek, s katerim bi bilo mogoče razbiti DES, je preizkušanje vseh možnih ključev. Pri DES postopku je tajni ključ dolg 56
bitov (56 znakov dolgo zaporedje enk in ničel), tako da je na voljo velikansko število različnih kombinacij. Če bi imeli na razpolago
računalnik, ki za preizkušanje 1000 ključev porabi le eno sekundo, bi za to, da bi preizkusili vse kombinacije, potrebovali več kot dva
miliona let. Ker pa so računalniki vedno bolj zmogljivi, se strokovnjaki bojijo, da bi se ta čas preveč skrajšal in že razmišljajo o tem, da
bi bilo potrebno dolžino ključa pri DES postopku povečati.

Pri postopku šifriranja s simetričnim ključem lahko nastopi težava pri izmenjavi ključev. Da bi lahko naš partner, ki smo mu poslali
šifriran dokument po elektronski pošti, ta dokument prebral, mora namreč poznati tajni ključ, s katerim smo ta dokument šifrirali. Tega

mu ne moremo poslati kar po elektronski pošti, kajti tisti, ki bi utegnil prestreči dokument, lahko ravno tako prestreže tudi tajni ključ.
Najbolje je, da se o tajnem ključu, ki ga bomo uporabljali, z njim prej osebno dogovorimo. Težava nastopi pri partnerjih, ki so oddaljeni in se z njimi še nismo dogovorili za tajni ključ, ali pa se sploh še nismo srečali. Z njimi se za ključ lahko dogovorimo po telefonu, ki pa, kot vemo, ne zagotavlja prav velike stopnje zasebnosti.

Asimetrično šifriranje

Pri tem načinu šifriranja je celoten ključ sestavljen iz dveh delov, ključa za šifriranje in ključa za dešifriranje. Dokument šifriramo s prvim ključem na tak način, da ga ni mogoče dešifrirati, četudi ta ključ poznamo. Tako šifriranje imenujemo enosmerno šifriranje, ker je postopek izvedljiv le v eni smeri. Enosmerno šifriranje ne bi imelo smisla, če ne bi obenem obstajal tudi drugi ključ, to je ključ za dešifriranje, s katerim je sporočilo dokaj enostavno dešifrirati. Oba ključa predstavljata par ključev.

Vsakemu ključu za šifriranje pripada natanko en ključ za dešifriranje, vendar je, če poznamo samo prvega, nemogoče uganiti drugega.
Če bi bilo to mogoče, bi lahko vsakdo, ki pozna ključ za šifriranje, uganil tudi ključ za dešifriranje in z njegovo pomočjo dešifriral dokument. Postopek šifriranja ne bi bil več enosmeren.

Na prvi pogled se morda zdi, da s tem nismo nič pridobili, le postopek je bolj zapleten, ker potrebujemo sedaj namesto enega kar dva ključa. Vendar temu ni tako. Ker s pomočjo ključa za šifriranje ni mogoče dešifrirati dokumenta, lahko ta ključ vsi poznajo. Ključ za šifriranje lahko javno objavimo, lahko ga pošiljamo po elektronski pošti ali pa sporočimo po telefonu. Vsakdo, ki ta ključ pozna nam lahko z njim šifrira sporočilo, ne more pa ga dešifrirati. Ta del ključa imenujemo tudi javni ključ.

Ključ za dešifriranje mora ostati zaseben, ker lahko z njegovo pomočjo dokument dešifriramo. Ta del ključa imenujemo tudi zasebni ključ. Našega zasebnega ključa ni potrebno poznati nikomur drugemu, ker za šifriranje dokumenta ni potreben. In ker zasebnega ključa ni potrebno z nikomer izmenjati, je tudi nevarnost, da bi ga kdo odkril, manjša.

Povzamimo na kratko. Pri asimetričnem postopku šifriranja uporabljamo za šifriranje javni ključ. Z njim lahko vsak šifrira nam namenjene zaupne dokumente, ne da bi poznal naš zasebni ključ. Svoj zasebni ključ poznamo le sami, zato lahko edini dešifriramo dokumente, ki so bili šifriran z našim javnim ključem. Celo tisti, ki je dokument šifriral, ga ne more več dešifrirati, če je slučajno izgubil original. Ker je ključ za šifriranje pri asimetričnem šifriranju javen imenujemo tak postopek tudi šifriranje z javnim ključem.

Zaenkrat je edini znani postopek asimetričnega šifriranja tako imenovani RSA postopek, ki je dobil ime po začetnicah priimkov svojih avtorjev. V ZDA je RSA postopek patentiran, zato mora vsak, ki ga želi legalno uporabljati, plačati avtorske pravice. Ta patent nima veljave zunaj meja ZDA. RSA postopek šifriranja je priznan kot izjemno varen postopek in zadovoljuje tudi najstrožje vojaške zahteve, ki jih tudi DES s 56 bitov dolgim ključem ne izpoljnjuje več.

Edina težava pri RSA postopku je v tem, da je računsko zelo zahteven in potrebujemo za šifriranje in dešifriranje daljšega sporočila na počasnem računalniku preveč časa. V praksi je zato zelo uporaben mešani postopek. Pri tem postopku šifriramo dokumente po nekem klasičnem simetričnem postopku, kot je to na primer DES. Za šifriranje vsakega dokumenta uporabimo nov naključno izbran simetrični ključ. Ker je postopek simetričen, mora ta ključ poznati tudi tisti, ki mu je dokument namenjen, to je njegov prejemnik.

Naključno izbrani simetrični ključ asimetrično šifriramo z javnim ključem prejemnika in mu ga pošljemo skupaj s šifriranim dokumentom. Prejemnik najprej s svojim zasebnim ključem dešifrira simetrični ključ in šele s pomočjo tega ključa nato dešifrira tudi sam dokument. Na ta način smo ohranili vse prednosti asimetričnega postopka, pridobili pa smo na hitrosti, ki je sedaj praktično enaka kot pri simetričnih postopkih.

Digitalni podpis

Govorili smo že o tem kako lahko z lastnoročnim podpisom zagotavljamo verodostojnost klasičnih dokumentov, vendar pa to ne velja za elektronske dokumente, ki jih ne moremo lastnoročno podpisati. Iznajdba RSA asimetričnega postopka šifriranja je hkrati omogočila tudi

uvedbo digitalnega podpisa, s katerim lahko lahko v enaki ali celo mnogo večji meri zagotavljamo verodostojnost elektronskih
dokumentov.

Digitalni podpis imenujemo podpis le zato, ker opravlja enako funkcijo kot lastnoročni podpis in ne zato, ker bi mu bil kakorkoli
podoben. Ideja digitalnega podpisa je v osnovi zelo preprosta, omogočila pa jo je izmenljivost ključev RSA postopka. Običajno
dokument šifriramo z javnim ključem prejemnika, ki nato ta dokument dešifrira s svojim zasebnim ključem. RSA pa omogoča tudi
obrnjen postopek: dokument, ki smo ga šifrirali s svojim zasebnim ključem, lahko prejemnik dešifrira z našim javnim ključem. S tem
nismo zagotovili zasebnosti dokumenta, ker ga lahko dešifrira vsak, ki pozna naš javni ključ, teh pa je lahko zelo veliko. Tak način
šifriranja pa lahko služi kot digitalni podpis. Ker smo mi edini, ki poznamo naš zasebni ključ, smo tudi edini, ki smo lahko z njim šifrirali
dokument. Nihče, ki ne pozna našega zasebnega ključa ne more šifrirati dokumenta na tak način, da bi ga bilo mogoče dešifrirati z našim
javnim ključem. Če v dokumentu, ki je šifriran z našim zasebnim ključem, nekdo spremeni en sam znak, s tem onemogoči dešifriranje
dokumenta z našim javnim ključem. Šifriranje dokumenta z zasebnim ključem zato zagotavlja verodostojnost dokumenta in ga zato
lahko obravnavamo kot digitalni podpis. Da lahko nekdo tak dokument prebere, ga mora najprej dešifrirati z našim javnim ključem,
obenem s tem pa dobi tudi potrdilo o njegovi verodostojnosti, oziroma z drugimi besedami, preveri naš digitalni podpis.

Težava pri opisanem načinu digitalnega podpisa je v tem, da je podpisani dokument v šifrirani obliki, zato ga moramo pred vsakim
branjem dešifrirati, kar pa ni najbolj praktično. Bolj praktičen bi bil podpis, ki ga , podobno kot lastnoročni podpis, dodamo na koncu
dokumenta, ne da bi bilo za to potrebno šifrirati sam dokument. Pojavi se vprašanje, ali je mogoče na tak način zagotoviti verodostojnost
dokumenta. Ali lahko na ta način preprečimo, da bi nekdo prekopiral naš podpis pod svoj dokument, ali pa, da bi spremenil vsebino
dokumenta, ki smo ga že podpisali?

Odgovor na zgoraj postavljena vprašanja je pritrdilen. Da bi bilo to mogoče, moramo najprej tvoriti prstni odtis dokumenta. Prstni odtis
dokumenta je neko zaporedje znakov (število), ki ga dobimo (izračunamo) iz dokumenta na tak način, da se vsaka, še tako majhna
sprememba dokumenta odraža tudi v njegovem prstnem odtisu. Postopek je lahko zelo enostaven, vendar mora biti tak, da nihče ne zna

sestaviti smiselnega dokumenta z vnaprej predpisanim prstnim odtisom. Takega postopka ni težko najti, znanih je veliko ustreznih postopkov.

Če poznamo prstni odtis originalnega dokumenta, lahko preverimo istovetnost tako, da izračunamo prstni odtis dokumenta, ki ga preverjamo, in ga primerjamo s prstnim odtisom originala. Če sta prstna odtisa enaka, je tudi dokument, ki ga preverjamo, enak originalu.

Elektronski dokument lahko podpišemo tako, da najprej izračunamo njegov prstni odtis in nato ta prstni odtis šifriramo s svojim privatnim ključem. Tako šifriran prstni odtis priključimo dokumentu kot svoj digitalni podpis. Tak dokument lahko vsakdo prebere, ne da bi ga moral za to dešifrirati. Ko želi preveriti podpis, z našim javnim ključem dešifrira prstni odtis dokumenta v podpisu in ga primerja s prstnim odtisom, ki ga izračuna iz samega dokumenta. Če se ujemata, potem ve, da smo dokument podpisali mi, ki edini poznamo zasebni ključ in tudi, da dokumenta po tem, ko je bil podpisan, nihče več ni spreminjal.

Pomen ključev

Videli smo, da zasebnost pri asimetričnim šifrirnem postopku kakor tudi verodostojnost digitalno podpisanega dokumenta v celoti sloni na tajnosti zasebnega ključa. Če ta ključ nekdo odkrije, lahko po eni strani dešifrira vse zaupne dokumente, ki so šifrirani z našim javnim ključem, po drugi strani pa lahko v našem imenu digitalno podpisuje dokumente, ki jih mi sami sicer ne bi podpisali. Za tajnost svojega zasebnega ključa moramo zato sami v celoti prevzeti odgovornost. Ne smemo podlečti privlačni možnosti, da bi, na primer, svoji tajnici zaupali svoj zasebni ključ zato, da bi lahko v našem imenu podpisovala manj pomembne dokumente. Z njim bo lahko namreč podpisovala tudi zelo pomembne dokumente, brala našo zaupno pošto ali pa ga bo celo zaupala nekomu drugemu. Kasneje ne bo več mogoče ločiti dokumentov, ki smo jih podpisali sami in dokumentov, ki jih je v našem imenu podpisala tajnica. Tajnica sme zato podpisovati le s svojim zasebnim ključem, za katerega sama prevzema odgovornost. Mi jo lahko le pooblastimo, da s svojim ključem v našem imenu podpisuje določene dokumente. V tem je bistvena razlika med lastnoročnim in digitalnim podpisom. Lastnoročnega podpisa

ne moremo, pa četudi bi to hoteli, zaupati svoji tajnici ali svojemu prijatelju, pri digitalnem podpisu pa tega samo ne smemo storiti. To je naša odgovornost.

In kako je z javnim ključem? Javni ključ mora biti res javen, bolj ko je javen, bolje je. Poglejmo zakaj je to potrebno. Vzemimo, da želimo svojemu novemu partnerju poslati zaupen dokument, v katerem je opisan tehnični postopek za izdelavo našega novega proizvoda. Dokument šifriramo z njegovim javnim ključem in prepričani smo, da tega dokumenta ne bo mogel prebrati nihče drug kot naš partner, ki edini pozna svoj zasebni ključ.

To drži samo, če je ključ s katerim dokument šifriramo res javni ključ našega partnerja. In kaj če ni? Kaj se lahko zgodi, če nam je nek vsiljivec uspel podtakniti lažen ključ. V veri, da je to javni ključ našega partnerja, z njim šifriramo zaupni dokument. Vsiljivec, ki nam je ključ podtaknil, lahko sedaj ta dokument dešifrira. Res je, da takega dokumenta naš partner ne more več dešifrirati s svojim zasebnim ključem (ker je bil šifriran z lažnim ključem) in hitro ugotovi, da je nekaj narobe. Vendar je tedaj že prepozno.

Vsiljivec, ki mu je uspelo podtakniti javni ključ, lahko šifriran dokument tudi v celoti prestreže, tako da sploh ne dospe do našega partnerja. Prestreženi dokument dešifrira, ga prebere, ponovno šifrira s pravim javnim ključem in ga pošlje našemu partnerju. Partner niti ne opazi, da se je nekdo vmešal. Na videz je vse v najlepšem redu. Ta problem imenujemo problem lažne identitete.

Problemu lažne identitete se lahko izognemo, če je javni ključ res javen, tako, da ga vsi poznajo in je objavljen na javno dostopnih krajih. Vsiljivcu je potem izredno težko podtakniti nek lažen ključ. Še bolje pa je, če nam svoj javni ključ sporoči naš partner osebno, vendar s tem izgubimo večino prednosti, ki jo ima asimetrični postopek šifriranja.

In kako je z javnim ključem pri digitalnem podpisu? Tu nam služi javni ključ zato, da z njim preverimo podpis na dokumentu. Pri mnogih dokumentih, naprimer pri pogodbah, s podpisom dokumenta ne potrjujemo samo njegove vsebine, temveč sprejemamo nase tudi obveznost. Ravno podpis je tisti, ki nas zavezuje, da svojo obveznost tudi opravimo. Tu ne zadošča več, da nam partner osebno sporoči svoj javni ključ. Kasneje, ko ne uspe opraviti obveznosti, h kateri ga zavezuje pogodba, lahko namreč zanika, da je ključ njegov in s tem

tudi, da je on podpisal pogodbo. Ta problem imenujemo problem zanikanja identitete.

Tudi problemu zanikanja identitete se lahko bolj ali manj izognemo, če poskrbimo, da je javni ključ res javen, kajti ključ, ki je objavljen javno, je zelo težko kasneje zanikati. Še bolje pa je, če nam partner predhodno potrdi verodostojnost svojega javnega ključa s svojim lastnoročnim podpisom.

Upravljanje z javnimi ključi

V prejšnjem poglavju smo videli, da v zvezi z izmenjavo javnih ključev nastopata predvsem dva problema: problem lažne identitete in problem zanikanja identitete. Reševanje teh dveh problemov, na način kot je opisan v prejšnjem poglavju, prinese kopico organizacijskih težav. Da bi se izognili lažni identiteti moramo z vsakim svojim partnerjem najprej osebno izmenjati javna ključa, da pa bi se izognili zanikanju identitete, moramo obenem izmenjati tudi potrdili o verodostojnosti teh ključev. S tem smo izgubili skoraj vso prednost, ki jo ima asimetrično šifriranje pred simetričnim.

Večini opisanih težav se lahko izognemo, če imamo na voljo službo, ki skrbi za upravljanje z javnimi ključi. In kaj nam lahko taka služba nudi?

Taka služba je nekakšen posrednik med partnerji pri izmenjavi javnih ključev. Če želimo komunicirati z uporabo javnega ključa, lahko pri taki službi registriramo svoj javni ključ. Ob registraciji overovimo svoj ključ s svojim lastnoročnim podpisom, obenem pa tudi ta služba overovi svoj ključ (to je ključe odgovorne osebe). Če te službe ne bi imeli na voljo, bi morali podoben postopek izpeljati z vsakim svojim partnerjem posebej.

Ob registraciji ključa služba digitalno podpiše naš javni ključ in s tem potrdi njegovo verodostojnost. Tako podpisan ključ objavi na svojem strežniku javnih ključev, na katerem ga lahko najde vsak, ki ima dostop do Interneta. Podobno lahko na tem strežniku tudi sami najdemo ključe svojih partnerjev . Ker nam digitalni podpis službe zagotavlja verodostojnost tega ključa nam ni treba več razmišljati o lažni identiteti oziroma o zanikanju identitete. Da našemu partnerju ni potrebno preverjati našega javnega ključa na strežniku javnih

ključev, mu lahko svoj javni ključ pošljemo tudi po elektronski pošti. Digitalni podpis službe tudi v tem primeru zagotavlja njegovo verodostojnost. Ker je ključ take službe običajno objavljen tudi v javnih občilih, lahko verodostojnost podpisa preverijo tudi tisti, ki svojega ključa niso registrirali pri tej službi in zato tudi niso osebno prejeli njenega javnega ključa.

Na prvi pogled se zdi, da moramo sedaj, namesto da bi zaupali svojemu partnerju, zaupati neki službi za upravljanje z javnimi ključi.
Vendar temu ni tako. Ker je naš javni ključ objavljen na strežniku javnih ključev, lahko njegovo verodostojnost vedno preverimo. To je občasno tudi priporočljivo, ker s tem vršimo nadzor nad službo. Podobno lahko naredi vsak drug, ki je pri tej službi registriral svoj ključ.
Če bi služba podpisala nek lažen ključ, bi to na ta način kaj hitro odkrili, eno samo tako odkritje pa bi pomenilo tudi propad te službe.
Služba je namreč pogodbeno vezana s svojimi strankami.

Poleg tega, da naš ključ registrira in ga javno objavi, pa nam lahko taka služba nudi tudi druge usluge. Vzemimo, da je iz kakršnega koli razloga nekdo odkril naš zasebni ključ. Javni ključ, ki ustreza temu zasebnemu ključu moramo nujno takoj razveljaviti, da ne bi moglo priti do nadaljnih zlorab. Služba v takem primeru poskrbi za to, da ključ takoj briše iz strežnika ključev, na strežniku pa objavi preklic ključa s točnim časom preklica. Vsak, ki bo preveril veljavnost našega ključa na strežniku, bo takoj ugotovil, da ta ključ ni več veljaven, obenem pa bo lahko našel na njem naš novi ključ. Vsem naročnikom pa služba tudi po elektronski pošti sporoči vse ključe, ki so bili razveljavljeni. Na ta način lahko močno zmanjšamo škodo, ki jo utegne povzročiti razkritje zasebnega ključa.