UVOD

Seminarsko nalogo s tem naslovom sem si izbral, zato ker tudi sam uporabljam digitalni podpis in poslujem preko interneta oziroma ga uporabljam za spletno bančništvo. Digitalni podpis je zelo dobra zadeva, saj lahko na hitro potrdiš kakšne dokumente ali plačaš svoje račune preko interneta se pravi preko spletnega bančništva, saj je ta varianta tudi cenejša in hitrejša od klasične plačilne poti. Provizija je tudi v takšnem primeru tudi nižja.

Sam že kar dobro poznam zadevo, zato bom to tudi vpisal v nalogo. Kaj pravzaprav je digitalni podpis, kako si ga pridobimo in zakaj ga lahko uporabljamo.

KAJ JE DIGITALNI PODPIS

Digitalni podpis je računalniški zapis, ki vsebuje podatke o imetniku. Njegovo ime, elektronski naslov, enolična identifikacijska številka itd. ter njegov javni ključ, poleg tega pa še podatke o izdajatelju digitalnega podpisa in veljavnost digitalnega potrdila.

Digitalni podpis je tudi nadomestek oziroma ima enako težo, kot lastnoročni podpis. Uporabljamo ga v elektronskem poslovanju ter je namenjen preverjanju pristnosti podatkov bodisi identifikaciji podpisnika. Danes se ogromno dokumentov ne prenaša več v tiskani obliki, temveč že prevladuje elektronsko poslovanje, saj je hitrejše.

Digitalni podpis je narejen z uporabo kriptografije tako, da tisti, ki podpiše se pravi podpisnik dokument ali datoteko zašifrira s svojim zasebnim ključem. Od šifrira jo lahko vsak, ki pozna njegov javni ključ, to pa se šteje kot preverjanje podpisa.

Digitalni podpis se lahko sporočilu samo doda ali se ga vgradi v samo sporočilo. Sam podpis mora zagotavljati avtentičnost pri katerem verjamemo da je podpisani res tisti za katerega se izdaja, da se podpis ne mora ponarediti oz. kopirati, da se podpisanega dokumenta ne da spremeniti.

Digitalno podpisovanje mora omogočati tudi spletna stran, ki digitalni podpis zahteva npr. e-uprava ali elektronsko bančništvo, katerega tudi sam uporabljam. Zato je potrebno na podpisnikov osebni računalnik namestiti komponent za digitalni podpis, ki od njegovega spletnega brskalnika zahteva, da izbrani dokument digitalno podpiše.

Varen elektronski podpis izpolnjuje zahteve, ki so izključno povezani s podpisnikom, da je iz njega mogoče zanesljivo ugotoviti podpisnika. Ustvarjen mora biti s sredstvi za varno elektronsko poslovanje, ki so pod podpisnikovim nadzorom. Tudi povezan je s podatki, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi, na katere se nanaša.

UPORABA DIGITALNEGA PODPISA

Postopek kako pridobiti digitalni podpis sem našel na e-upravi katerega bom tudi uporabil in ga opisal.

Prosilec za digitalno potrdilo prinese izpolnjen zahtevek skupaj z veljavnim uradnim dokumentom s sliko. Lahko je osebna izkaznica, potni list, vozniško dovoljenje ali drug uradno veljaven osebni dokument in davčno številko na katerokoli upravno enoto. Obrazec za zahtevek dobi na spletni strani http://www.sigen-ca.si/obrazci-fo.php.

Seznam upravnih enot s podatki o uradnih urah je na spletni strani posamezne upravne enote oziroma je vidno tudi na spletni strani http://www.sigen-ca.si/RA-fizicne.php.

Zaposleni na upravni enoti zanesljivo ugotovijo istovetnost prosilca, preverijo verodostojnost podatkov iz zahtevka in na zanesljiv način posredujejo podatke Ministrstvu za javno upravo oz. izdajatelju SIGEN-CA. SIGEN-CA na podlagi odobrenega zahtevka pripravi referenčno številko in avtorizacijsko kodo, ki sta unikatni za vsakega prosilca posebej. Referenčno številko pošlje prosilcu po elektronski pošti, avtorizacijsko kodo pa s poštno pošiljko. V povprečju traja postopek pridobitve teh podatkov pet delovnih dni oziroma mora izdajatelj SIGEN-CA najkasneje v 10 dneh od oddaje pravilno izpolnjenega elektronskega zahtevka poslati podatke za prevzem digitalnega potrdila.

Prosilec se z brskalnikom priključi na ustrezno spletno stran SIGEN-CA, vtipka referenčno številko in avtorizacijsko kodo ter nato prevzame svoje digitalno potrdilo. Postopek prevzema in zaščite digitalnega potrdila je opisan na spletnih straneh SIGEN-CA:

http://www.sigen-ca.si/fizicne\_osebe.php.

Postopek pridobitve oz. vloge za pridobitev digitalnega podpisa je brezplačno. Tako, da ni taks in drugih stroškov, ki bi nastali v zgornjem primeru, katerega sem opisal.

Veljavnost digitalnih potrdil je 5 let. Po preteku veljavnosti mora imetnik, če želi še nadaljnje uporabljati elektronske storitve z digitalnim potrdilom SIGEN-CA, pridobiti novo potrdilo. Zadnja dva meseca pred potekom veljavnosti digitalnega potrdila lahko imetnik z veljavnim digitalnim potrdilom SIGEN-CA za fizične osebe odda zahtevek za novo potrdilo preko spletnega obrazca.

E-STORITVE MOŽNE Z UPORABO DIGITALNIH POTRDIL

Na spletni strani (http://www.gzs.si/slo/6679) je priročnik, ki govori o razvoj e-poslovanja oz. e-komuniciranja, ki temelji v veliki meri na zaupanju in varnosti, ki ju čutijo uporabniki do elektronskih komunikacij in izdajateljev digitalnih potrdil. Številne aplikacije obstajajo, ki so povezane z digitalnimi podpisi oziroma potrebujejo le-te za delovanje. Na tak način poteka elektronska izmenjava podatkov, varen in avtenticiran dostop do podatkovnih baz, sklepanje pogodb, plačila, dostop do različnih storitev podjetij ali uprave, nabava, e-arhivi in podobno. Prehod na elektronski način opravljanja storitev po eni strani prinaša veliko prednosti, npr. enostavnost, dostopnost, ipd., po drugi strani pa ima lahko velik vpliv na delovanje in organizacijo znotraj same institucije.

Tudi seje Vlade RS potekajo na elektronski način in gradiva se izmenjujejo v e-obliki, omogočena je varna elektronska izmenjava e-podatkov med različnimi institucijami državne in javne uprave ter gospodarstva, možne so finančne transakcije in naročanje blaga oz. storitev po internetu. Na DURS-u je postavljen sistem za e-davčno poslovanje, s čimer je omogočena tudi oddaja DDV in dohodnine preko interneta, itd.

Možno je tudi preko interneta naročiti izpiske iz matičnih knjig, prav tako pa je možno z digitalizacijo dostopati do najbolj pogostih formularjev npr. potrdilo o državljanstvu, spremembe stalnega in začasnega prebivališča, evidenca gospodinjstev, sprememba imena, preklici in naročila osebnih listin, ipd. Šole in univerze pripravljajo preko interneta vpis na fakulteto, prijavo diplomskih nalog ali izpitov, itd. Za pravne in fizične osebe so storitve internetnega dostopa do uradnega lista, sodnega registra, plačevanje preko interneta, e-avkcije, e-kompenzacije, itd.

DIGITALNO PODPISOVANJE

Ključa v kriptografiji javnega ključa sta dualna. To pomeni, da lahko opravimo postopek šifriranja tudi obratno. Z zasebnim ključem sporočilo zašifriramo z javnim pa ga od šifriramo. Če pošljemo skupaj s sporočilom tudi isto sporočilo zašifrirano z našim zasebnim ključem, se bo prejemnik lahko prepričal, da smo sporočilo zagotovo poslali samo mi, saj bo z našim javnim ključem lahko od šifriral sporočilo ki smo ga prej zašifrirali z našim zasebnim ključem.

Na primer, da želi Thomas poslati Špeli neko sporočilo. Pri tem imata oba vsak svoj zasebni ključ in javni ključ od drug drugega. Thomas uporabi svoj zasebni ključ, da zašifrira sporočilo. Sporočilu pripne svoje ne zašifrirano sporočilo in vse skupaj zašifrira z Špelinim javnim ključem ter to pošlje Špeli. Špela oboje skupaj od šifrira s svojim zasebnim ključem. Poleg Thomasovega sporočila ima tudi zašifrirano sporočilo, ki se imenuje digitalni podpis in ko ga odklene z Thomasovim javnim ključem, se prepriča, da je sporočilo zares prišlo od Thomasa. Ne pozabimo, da je podpis potreben za to, ker bi sicer lahko vsak, ki ima Špelin javni ključ, pošiljal zašifrirana sporočila.

Vedeti je potrebno, da overovitelj s svojim certifikatom podpiše certifikat uporabnika in tako zagotavlja da lastnik zasebnega dela certifikata, ki ga je overovitelj digitalno podpisal, zares last tistega, ki je v njem označen. Uporabnik javnega certifikata pa mora tako pridobiti samo certifikat od overitelja. Certifikati overiteljev pristojnih za overjanje internetnih strani so vključeni v večino internetnih brskalnikov. Certifikat poleg ključev in podpisa vsebuje tudi ime in priimek lastnika in morebiten elektronski naslov, drugih osebnih podatkov, pa certifikat običajno ne vsebuje.

PRAVNI VIDIK DIGITALNEGA PODPISA

ZAKON o elektronskem poslovanju in elektronskem podpisu. Uradni list RS, št. 57/2000 (23. 6. 2000), 2000: v Sloveniji ureja področje elektronskega poslovanja in elektronskega podpisa Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1). ZEPEP prepoveduje diskriminacijo elektronske oblike podatkov (dokumentov), omogoča enačenje veljavnosti elektronske in papirne oblike dokumentacije, in opredeljuje pogoje, pod katerimi je varen elektronski podpis enakovreden lastnoročnemu.

14. člen: »Elektronskemu podpisu se ne sme odreči veljavnosti ali dokazne vrednosti samo zaradi elektronske oblike, ali ker ne temelji na kvalificiranem potrdilu ali potrdilu akreditiranega overitelja, ali ker ni oblikovan s sredstvom za varno elektronsko podpisovanje.« (http://www.uradni-list.si/1/objava.jsp?urlid=200498&stevilka=4284)

15. člen: »Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost.« (http://www.uradni-list.si/1/objava.jsp?urlid=200498&stevilka=4284)

Varen elektronski podpis, overjen s kvalificiranim digitalnim potrdilom ima torej enako dokazno vrednost kot lastnoročni podpis. Kvalificirano digitalno potrdilo je potrdilo, ki izpolnjuje določene v zakonu opredeljene zahteve glede vsebine in overiteljske agencije, ki digitalno potrdilo izda.

IZDAJATELJI DIGITALNIH PODPISOV

V Sloveniji si lahko digitalni podpis pridobimo preko Sigen-CA. Na spletu imajo postopke pridobitve za fizične osebe na njihovi spletni strani in sicer na http://www.sigen-ca.si/fizicne\_osebe.php , kjer se odpre spletna stran Sigen-CA, na kateri je opisan postopek in navodila, kako pridemo do podpisa. Prav tako so nam v pomoč na tej spletni strani pogosta vprašanja, ki se nahajajo na levi strani te povezave. Prav tako nam POŠTARCA omogoča pridobitev digitalnega podpisa. Vsa navodila so na tej povezavi http://postarca.posta.si/ . Pridobitev digitalnega potrdila pa nam omogoča tudi HALCOM na njihovi spletni strani http://www.halcom.si/.

V Register overiteljev v Republiki Sloveniji na področju digitalnih potrdil izdajateljev so vpisani:

• Pošta Slovenije, d. o. o.

• Nova Ljubljanska banka, d. d.

• Halcom Informatika, d. o. o.

HRAMBA IN RAVNANJE Z DIGITALNIM POTRDILOM

Poskrbeti moramo, da nezaželena oseba nima dostopa do našega zasebnega ključa. Naš zasebni ključ je zaščiten z geslom. Skrbno moramo varovati tako svoj zasebni ključ, kot tudi geslo. Overitelj priporoča, da digitalno potrdilo in zasebni ključ hranimo na pametni kartici. Uporaba pametnih kartic v primerjavi z uporabo drugih medijev, diska (baze brskalnika), zmanjšuje možnosti zlorabe.

V brskalniku Mozilla digitalno potrdilo in zasebni ključ zaščitimo z geslom, ki ga nastavimo prek menija Edit -> Preferences -> Privacy&Security -> Master Passwords, v brskalniku Firefox pa Tools -> Options -> Privacy -> Saved Passwords -> Change Master Password.

Hranjenje digitalnega potrdila in zasebnega ključa na disku je manj zanesljivo, omogoča pa izdelavo varnostnih kopij našega digitalnega potrdila. Zato je priporočljiva izdelava varnostne kopije na zgoščenko, če nam delovno okolje to omogoča. Z zgoščenko moramo ravnati v skladu z navodili proizvajalca zgoščenk. Varnostno kopijo svojih ključev, na zgoščenki ali USB ključu, je potrebno shraniti na varnem mestu, da preprečimo njihovo zlorabo ter, da je to dostopno samo nam.

Naše geslo za zaščito profila in zasebnih ključev mora biti dolgo vsaj 8 znakov. Programska oprema nam pri prevzemu posebnega digitalnega potrdila narekuje izbiro gesel, ki omogočajo pomembne mehanizme zaščite za preprečitev napada na osnovi slovarja (iskanje gesel s pomočjo slovarja besed), lahko pa se geslo še bolj zaščiti na naslednji način:

• mešana uporaba velikih in malih črk, števil in posebnih znakov,

• geslo dolžine vsaj 8 znakov,

• izogibamo se besedam, ki so zapisane v slovarjih.

V primeru spremembe, vezane na digitalno potrdilo, zlorabe ali možnosti zlorabe je potrebno o tem nemudoma obvestiti, v mojem primeru je to SIGEN-CA. V primeru zlorabe ali možnosti zlorabe je potrebno takoj oz. čim hitreje oddati vlogo za preklic potrdila, osebno ali preko e-pošte, ali na dežurno telefonsko številko za preklic.

ZAKLJUČEK

Samo vsebina kaj je digitalni podpis in kako ga pridobimo mi ni bila tuja, saj ga tudi sam uporabljam za plačevanje računov. Uporaba digitalnega podpisa je zelo uporabna, saj nam veliko stvari lahko poenostavi.

V nalogi sem napisal oziroma opisal kaj je digitalni podpis, kje ga lahko pridobimo itn. Opisal sem tudi zakaj ga na primer sploh uporabljamo in kako poteka pošiljanje sporočila z digitalnim podpisom. Menim, da je uporaba digitalnega podpisa vsekakor zelo uporabna in dobrodošla, saj je cenejše (npr. nižje provizije položnic z uporabo spletnega bančništva), hitrejše ter nekako razbremenijo posameznika. S tem pa tudi razbremenimo zaposlene in same vrste pri institucijah, kot npr. samo na Upravni enoti (če oddajamo vloge preko spleta…) oziroma se izognemo morebitni prenatrpanosti.

V sami predstavitvi pa bom tudi pokazal uporabo digitalnega podpisa in sicer kako ga uvozimo v spletni brskalnik. Nato bom pokazal tudi, kje ga lahko uporabljamo npr. na spletnem bančništvu, e-upravi…

POVZETEK

Digitalni podpis je računalniški zapis, ki vsebuje podatke o imetniku. Digitalni podpis je tudi nadomestek oziroma ima enako težo, kot lastnoročni podpis. Pridobimo ga lahko na kateri koli upravni enoti. Uporabljamo pa ga tudi za poslovanje. Dan danes večina poslovnežev uporablja digitalni podpis, saj tako poslovanje teče hitreje.

Tudi fizične osebe se ga poslužujejo, saj ga imajo oziroma uporabljajo za plačevanje računov ali poslovanje, če govorimo o samostojnih podjetnikih. Uporablja se ga tudi za podpis dokumentov. Tako ljudem ni potrebno pošiljati dokumentov v tiskani obliki, s takšnim načinom in ravnanjem pa tudi prispevamo k ohranjanju narave oziroma do družbene odgovornosti.

VIRI IN LITERATURA

1. http://www.egradiva.net/moduli/upravljanje\_ik/17\_digitalni\_podpis/01\_datoteka.html

2. http://e-uprava.gov.si/e-uprava/dogodkiPrebivalci.euprava?zdid=780&sid=244

3. http://www.gzs.si

4. http://www.halcom-ca.si/?section=16

5. http://www.ltfe.org/category/objave/varnost/

6. http://postarca.posta.si/

7. http://www.sigen-ca.si/pridobitev\_fizicni.php

8. http://www.uradni-list.si/

9. POTOČAR, Z. in RAZGORŠEK, J.: Informatika. Novo mesto, 2009