UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

UVAJANJE ELEKTRONSKEGA PODPISA V IZBRANI BANKI

19494639
ANJA GORUP

Ljubljana, september 2016

IZJAVA O AVTORSTVU

Podpisana Anja Gorup, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Uvajanje elektronskega podpisa v izbrani banki, pripravljenega v sodelovanju s svetovalcem prof. dr. Mirom Gradišarjem.

IZJAVLJAM

1. da sem predloženo delo pripravila samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;

7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne 12.9.2016 Podpis študentke: Anja Gorup

KAZALO

KAZALO TABEL

KAZALO SLIK

UVOD

Opredelitev področja obravnave. Lastnoročni podpis je mehanizem, ki podpis enolično poveže s podpisnikom in pri tem izraža njegovo strinjanje s podpisano vsebino. Prve lastnoročne podpise so poznali že leta 1057, ko so dokumente podpisovali kralji (Brookfield, 1999). Kljub hitremu napredku v informacijski tehnologiji se fizične osebe v vsaki organizaciji ali podjetju dnevno srečujejo s klasičnim lastnoročnim podpisovanjem internih in eksternih dokumentov v papirni obliki.

V izbrani banki nastale dokumente podpisujemo na različnih nivojih odločanja. Lahko so predmet oddelka, sektorja, odbora (npr. odbora za odobravanje kreditov fizičnim ali pravnim osebam), posameznega področja ali uprave. Vsi dokumenti imajo vsaj dva podpisnika. Podpisnik lahko sedi za sosednjo mizo, je zaposlen na drugi lokaciji, odsoten, lahko pa je celo komitent banke.

Nekateri dokumenti gredo skozi več ciklov usklajevanja. Vsak cikel zahteva ponovno usklajevanje, podpisovanje in tiskanje. Dokument lahko ustvari analitik ali komercialist, ki ga natisne in fizično dostavi v podpis vodji ter direktorju področja. Če je vsebina potrjena z njune strani, na dokumentu popravimo podpisnike, ga ponovno natisnemo in dostavimo v podpis posameznemu odboru ter nazadnje še upravi banke.

Dokumenti so običajno začasne narave. V papirni obliki jih hranimo, digitaliziramo in uničimo skladno z Zakonom o varstvu osebnih podatkov (ZVOP-1). Po navadi je trajnost arhiviranja med letom dni in desetimi leti, odvisno od podatkov in vsebine dokumenta.

Uporaba papirne dokumentacije je povezana s stroški tiskanja, amortizacije tiskalnikov, papirja, rokovanja z dokumenti, ponovnega digitaliziranja, hrambe in uničenja.

Dandanes, tj. v času globalizacije, vse več poslovnih procesov informatiziramo. Iščemo hitro in enostavno informacijsko podporo. Informacijska tehnologija je za posamezno organizacijo ključnega pomena pri zagotavljanju konkurenčne prednosti na trgu. Ena izmed zadnjih ovir pri prehodu v popolnoma digitalno poslovanje je klasično podpisovanje dokumentov.

Lenz (2008, str. 9–11) pripisuje velik problem papirne dokumentacije predvsem v bančništvu in zavarovalništvu. Obema naj bi bil skupen en cilj, tj. doseči zanesljive procese, ki so varni in ugodni za dokazovanje resnične namere posameznika. Prav tako izpostavlja problem porabe časa in izvedbe morebitnih napak. Sklicuje se tudi na počasen potek dela in posledično doseganje nižje stopnje avtomatizacije.

Pomembno je krčenje stroškov z vidika podpisovanja, meni Lenz (2010, str. 7–8), ki pravi, da pričakovano izginjanje papirja iz internih delovnih procesov zmanjšuje stroške shranjevanja, posredovanja, digitaliziranja, indeksiranja in fizičnega arhiviranja. Večja

poraba papirja pomeni več onesnaženja, uničenih dreves in večjo porabo vode. Hkrati je mnenja, da ima z lastnoročnimi podpisi v okviru banke težave predvsem področje revizije, ki nima zagotovljene revizijske sledi pri pregledovanju posameznih transakcij (kdo, kdaj in kje je podpisal določen dokument). Opozarja tudi na neekonomičen, neavtomatiziran in neučinkovit delovni proces v primeru klasičnega podpisovanja. Prav tako Lenz izpostavlja problem združevanja podpisov več posameznikov, ki so ustvarjeni v različnem času in na različnem kraju. Informacij o izvedbi podpisov na papirju ni mogoče določiti. Omenja tudi morebitne napake pri digitalizaciji klasično podpisanih dokumentov.

Pri prepoznavanju podpisov posameznika prihaja tudi do zanikanja podpisa oz. prelaganja odgovornosti z ene osebe na drugo. V praksi je lastnoročni podpis težko primerjati z osebo, ki je njegova dejanska lastnica. Nemogoče je preveriti avtentičnost. Žužek in Dobnikar (2002) trdita, da se mora identificirati oseba, ki je zapis ustvarila in ga posredovala.

Nguyen (2009, str. 8) piše o nezaupanju pri izvedbi klasičnih podpisov in običajni izmenjavi transakcij med stranko ter posameznimi ustanovami preko spleta. Oseba s svojim podpisom ne jamči za ustrezno odgovornost. Podpis je lahko samo črtica, ki je ni mogoče povezati s posameznikom.

Gupta, Tung in Marsden (2003, str. 561–575) ugotavljajo, da lastnoročno podpisani dokumenti niso dostopni kadar koli in kjer koli. Ustvarjeni dokumenti morajo biti natisnjeni in podpisani, kopije teh dokumentov pa morajo biti shranjene v arhivih. Menijo, da samo posredovanje papirnatih dokumentov ni varno. Neznana oseba lahko dokument prestreže in podpis ponaredi.

Ganley (1998, str. 12–22) izpostavlja problem, ki nastane, če je nekdo lastnoročno podpisal dokument in bil vključen v določeno transakcijo. Ta oseba lahko kasneje zanika vključenost. V članku opisuje problematiko spreminjanja dokumentacije. Dokument lahko tretja oseba spremeni, ne da bi bil prvi podpisnik seznanjen s spremembo vsebine.

Entrust Securing Digital Identities & Information (2001-2003) navaja, da je v praksi izredno težko izslediti posameznika preko njegovega podpisa. Večina zaposlenih ne more potrditi podpisa kolega ali direktorja v podjetju. Podpis predstavlja dejansko formalnost, poznejše preverjanje pa je redkost. Ko je preverjanje podpisnikov potrebno za reševanje sporov, uporabimo posebne postopke, ki se sklicujejo na vsebino, spomin zaposlenih v kolektivu in vse druge razpoložljive dokaze, ki so pomembnejši kot sam fizični podpis.

Caldeira, Serrano, Quaresma, Pedron in Romao (2012, str. 196–202) ter Rigby (2014) trdijo, da neprestana uporaba papirja v takšnih in drugačnih sistemih ne pomeni nobenih finančnih koristi. Poudarjajo, da prinaša nezadovoljstvo strank in profesionalno nezadovoljstvo. Opažajo tudi slabšo kakovost informacij in več napak.

Solid (2010) opisuje problem vpogleda v dokumentacijo. Slednja je dostopna samo ožjemu krogu zaposlenih, za iskanje pa je potreben čas. V organizaciji dokument ni na razpolago nemudoma. Prav tako je potreben prostor za shranjevanje dokumentacije v izvirniku.

Abecker, Bernardi, Maus, Sintek in Wenzel (2000, str. 271–284) počasne delovne procese povezujejo s papirno dokumentacijo. Več kot je dokumentacije v fizični obliki, usklajevanj in prevzemanja odgovornosti, manj učinkoviti so procesi dela. Posledično je upočasnjena tudi realizacija zastavljenih ciljev.

Namen raziskave. Namen raziskave je v konkretni banki poenostaviti, pospešiti, modernizirati in povečati kakovost poslovanja z uporabo digitalnega podpisa. Izvedena bo analiza obstoječega stanja, predlagane pa bodo izboljšave poslovnih procesov.

Cilj raziskave. Cilja sta:

- analiza poslovnih procesov v banki in določitev tistih, kjer je uvedba digitalnega podpisa ekonomsko upravičena in
- predlog načina uvedbe digitalnega podpisa v izbrani banki.

Metode dela. Za izdelavo magistrskega dela bodo uporabljena znanja, pridobljena v času študija, pa tudi pridobljene izkušnje iz dela na banki. Področje digitalnega poslovanja bo raziskano s pomočjo pregleda domače in tuje literature.

V magistrskem delu sta zajeta dva pristopa raziskovanja, in sicer:

- deskriptivni pristop, ki zajema širok spekter literature na temo digitalnega podpisovanja in postavlja teoretična izhodišča za nadaljnjo analizo. Slednji bo uporabljen v prvem in drugem delu;
- analitični pristop, s katerim bo opravljena analiza poslovnih procesov v banki. Analizirani bodo obstoječe stanje v določeni banki in stroški uvedbe digitalnega podpisovanja, ugotovljeno pa bo tudi, kakšne so možnosti za izboljšave.

1 ELEKTRONSKI PODPIS

V vsaki organizaciji je treba neprestano sprejemati različne odločitve. Kamor koli se posameznik, zaposleni, stranka, direktor, član ali predsednik uprave obrne, dobi pred seboj list papirja in pisalo. Nalogo, novo ponudbo, izvedeno transakcijo, spremembo načina poslovanja ali pregled poročila je potrebno s podpisom ali parafo potrditi oziroma odobriti.

Lastnoročni podpisi imajo pomembno vlogo, vendar iz dneva v dan postajajo vedno večja ovira pri informatizaciji in digitalnem podpisovanju. Napredek na področju matematičnih

znanosti je prinesel razvoj kriptografskih metod, ki so osnova za digitalno podpisovanje. Hiter razvoj informacijske tehnologije je prispeval k priljubljenosti teh metod, ki so danes postale uveljavljena praksa. Nov sistem digitalnega podpisovanja prinaša manj napak, prelaganja odgovornosti in nižje stroške ter omogoča identificiranje posameznega podpisnika.

V tem poglavju je s teoretičnega vidika podrobneje opredeljeno področje digitalnega podpisovanja. V literaturi je s terminom digitalni podpis označenih več metod podpisovanja, ki se razlikujejo tako po varnosti kot po uporabnosti. Magistrsko delo se osredotoča na najnaprednejšo obliko podpisovanja, tj. elektronsko podpisovanje s kvalificiranim digitalnim potrdilom.

V magistrskem delu bo z besedno zvezo digitalni podpis enakovredno označen elektronski podpis s kvalificiranim digitalnim potrdilom.

1.1 Kaj je digitalni podpis

Podpis pomeni zapis imena in/ali priimka osebe pod določenim besedilom. Z njim oseba potrdi vsebino oziroma sprejme odgovornost zanjo.

Digitalno podpisovanje (ne digitalni certifikat) je matematična tehnika, uporabljena za potrditev avtentičnosti in celovitosti sporočila, programske opreme ali digitalnega dokumenta (Rouse, 2014).

Digitalni podpis je zaporedje bitov (vrednosti 0 ali 1), ki je odvisno od digitalne vsebine (npr. podpisanega dokumenta). Vsaka najmanjša sprememba že podpisanega dokumenta (dodajanje ali brisanje) vpliva na izračunani digitalni podpis in pomeni njegovo neveljavnost.

Na državnem portalu eUprava (2016) je opredeljeno, da digitalni podpis predstavlja sodobno alternativo klasičnemu podpisu in zagotavlja identiteto imetnika digitalnega potrdila, nezatajljivost lastništva poslanih e-podatkov ter celovitost (integriteto) sporočila. Slednje pomeni, da dela informacij ni mogoče spremeniti ali popraviti brez (vednosti) podpisnika.

Entrust Securing Digital Identities & Information (2001-2003) pojasnjuje, da je digitalni podpis termin, uporabljen za označevanje oziroma podpisovanje elektronskih dokumentov s postopkom, ki ga lahko dojemamo kot analogni podpis na papirju. Slednji omogoča uporabo posebne tehnologije, poznane pod imenom javni ključ šifriranja. Digitalni podpisi, ki jih poganja tehnologija javnih ključev, so širše znani kot najboljša praksa za zagotovitev digitalne odgovornosti pri elektronskih transakcijah. Hkrati predstavljajo najučinkovitejšo,

varno in najenostavnejšo metodo uporabe za zagotavljanje odgovornosti med vzpostavljanjem elektronskih transakcij.
Dewan (2005) predpostavlja, da digitalni podpis daje pomen avtentikaciji sporočila, ki preprečuje, da bi se sporočilo med prenosom spremenilo. Digitalni podpisi šifrirajo sporočilo z uporabnikovim privatnim ključem. Če bo podpis razrešen z uporabnikovim javnim ključem, bo ta vzpostavil identiteto lastnika in potrdil, da sporočilo ni bilo spremenjeno po opravljenem podpisu. Digitalni podpis je ustvarjen s šifriranjem posredovanega sporočila, kar pomeni, da ima vsak posredovani dokument različen digitalni podpis. Zaradi omenjenega razloga podpisa ni mogoče prestaviti z enega sporočila na drugo.

Za digitalno podpisovanje so priporočljive nekatere zahteve, ki jih izpostavlja Ganley (1998). Podpis mora biti odvisen od sporočila. Samo pošiljatelj elektronskega sporočila lahko ustvari pravilen digitalni podpis. Kdor koli sprejme sporočilo in digitalni podpis, lahko tega preveri in je posledično prepričan o originalu in integriteti sporočila.

Standard ISO 7498-2: 1989 določa: »Bistvena značilnost mehanizma podpisovanja je, da se lahko podpis izvede le z uporabo osebnih podatkov podpisnika. To pomeni, da je podpis overjen s kvalificiranim digitalnim potrdilom, ki ga je mogoče dokazati kateri koli tretji osebi (kot je sodnik ali arbiter) v vsakem trenutku« (ISO, 2000).

V primerjavi z ostalimi oblikami podpisov so digitalni podpisi daleč najenostavneje preverljivi in najbolj zanesljivi, kar se tiče zagotavljanja celovitosti vsebine dokumenta. Vsekakor pa ne moremo trditi, da digitalnih podpisov ni mogoče zlorabiti. Če gre za slabo izvajanje ali napačno podporo ustreznih procedur in procesov, niso nič zanesljivejši od lastnoročnih podpisov.

Digitalni podpisi so bistvenega pomena pri spodbujanju e-poslovanja, saj zagotavljajo, da so vse stranke vpisane v zavezujočem pogodbenem dogovoru (Chow, Conteras & Hamel, 2013). Herman (2002) trdi, da digitalno podpisovanje v bančništvu stranki omogoča predvsem svobodo za opravljanje storitev, kjer koli sama želi, kar je veliko bolje, kot da je omejena na opravljanje storitev v določeni poslovalnici. Prav tako digitalno podpisovanje predstavlja logičen in enostaven pomen spletne varnosti pri transakcijah ter zagotavljanju stranke in poslovanja kot zaupanja vredne (Nguyen, 2009).

Digitalni podpis lahko zlahka povežemo s posameznikom. Sledljivost je omogočena s kriptografijo javnega ključa.

Če se digitalno podpisovanje izvaja pravilno in če temelji na podpori javnega ključa, potem velja naslednje (Entrust Securing Digital Identitites & Information, 2001-2003):

- digitalni podpisi za elektronske dokumente predstavljajo to, kar lastnoročni podpisi predstavljajo na papirnih dokumentih;

- digitalni podpisi zagotavljajo zaupanja vreden dokaz o identiteti podpisnika, stranke;
- digitalni podpisi ne veljajo kot kopije podpisov na drugih dokumentih;
- digitalni podpisi zagotavljajo, da je posameznik podpisal dokument, ki pozneje ne more biti spremenjen v korist drugega posameznika (če je izvirni dokument spremenjen, postopek preverjanja to zazna) in
- digitalni podpisi imajo v večini držav pravne temelje enake lastnoročnim podpisom.

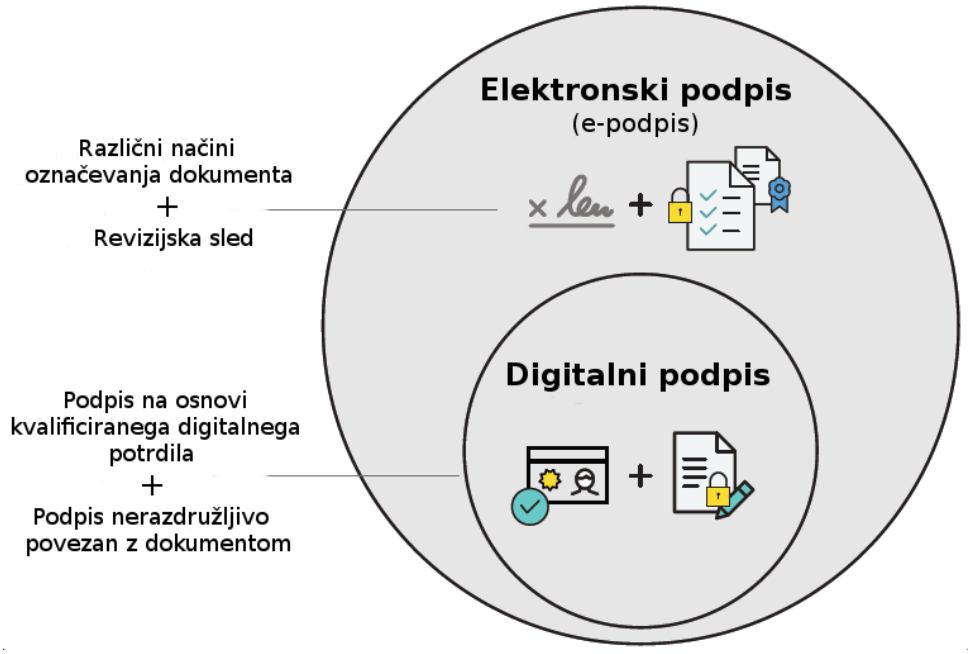
Poleg že omenjenega velja, da se lahko točen čas digitalnega podpisa zabeleži bolj zanesljivo kot pri lastnoročnem podpisu. To je zagotovljeno z uporabo zanesljivega časovnega žigosanja dokumenta.

Digitalno podpisovanje povezujemo s kriptografijo. Lah (2007) pojasnjuje: »Kriptologija je veda o tajnosti, šifriranju, zakrivanju sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza). Beseda prihaja iz grščine: kryptos logos pomeni skrita beseda. Uporabljata se še pojma enkripcija (šifriranje) in dekripcija (dešifriranje).«

Lesjak (2015) trdi, da je kriptografija znanstvena veda, ki uporablja zapletene matematične algoritme za izvedbo različnih varnostnih mehanizmov.

Prav tako nas Lah (2007) opozarja, da elektronski podpis pomeni kakršno koli oznako, narejeno z elektronskim medijem z namenom označitve dokumenta ali datoteke. Pojasnjuje, da je digitalni podpis elektronski podpis, narejen z uporabo kriptografije oziroma šifriranja.

Slika 1: Elektronski podpis v primerjavi z digitalnim podpisom



Vir: Adobe, Transform business processes with electronic and digital signature solutions from Adobe, 2015, str. 1.

Adobe (2015) s Sliko 1 pojasnjuje, da elektronski podpis (tudi e-podpis) predstavlja kakršen koli elektronski proces, ki nakazuje sprejemanje dogovora.

Elektronski podpis lahko uporablja različne metode za avtentikacijo identitete podpisnika, kot so elektronsko sporočilo, službena kartica ali telefonska potrditev. Dokazilo o podpisu se izkazuje z uporabo varnega procesa, ki zagotavlja revizijsko sled do končnega dokumenta.

Digitalni podpis je elektronski podpis, izveden s posebno metodo podpisovanja. Uporablja osebni certifikat za avtentikacijo identitete podpisnika. Dokazovanje podpisa se izvaja s primerjavo vsakega podpisa z dokumentom šifriranja. Veljavnost je zagotovljena s pomočjo zaupanja vredne certifikatne agencije.

1.2 Zakonodajni vidik elektronskega podpisa

V Sloveniji elektronski podpis urejata Zakon o elektronskem poslovanju in elektronskem podpisu (Ur. l. RS, št. 57/000, v nadaljevanju ZEPEP) ter Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje RS.

Elektronski podpis ureja ZEPEP v 1., 14., 15. in 28. členu. V 1. členu gre za obrazložitev pomena posameznih izrazov tega področja. Za področje, ki ga obravnavamo v magistrskem delu, so najpomembnejši izrazi zapisani s krepkim tiskom. 14. in 15. člen določata veljavnost in pomen elektronskega podpisovanja, 28. člen pa opredeljuje sestavine kvalificiranega digitalnega potrdila.

V omenjenem zakonu je zapisano:

1. člen
Posamezni izrazi, uporabljeni v zakonu, imajo naslednji pomen:

1. podatki v elektronski obliki so podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način;
2. elektronsko sporočilo je niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto;
3. **elektronski podpis** je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika;
4. **varen elektronski podpis** je elektronski podpis, ki izpolnjuje naslednje zahteve:

   — da je povezan izključno s podpisnikom;
   — da je iz njega mogoče zanesljivo ugotoviti podpisnika;

- da je ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom;
- da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi;

5. **časovni žig** je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času; varni časovni žig pa je elektronsko podpisano potrdilo overitelja, ki izpolnjuje pogoje iz prejšnje točke;
6. pošiljatelj elektronskega sporočila je oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila;
7. naslovnik elektronskega sporočila je oseba, ki ji je pošiljatelj namenil elektronsko sporočilo;
8. prejemnik elektronskega sporočila je oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila;
9. posrednik elektronskega sporočila je oseba, ki za drugo osebo pošlje, prejme, shrani elektronsko sporočilo ali nudi druge storitve v zvezi z elektronskim sporočilom;
10. podpisnik je oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis;
11. informacijski sistem je programska, strojna, komunikacijska in druga oprema, ki deluje samostojno ali v omrežju in je namenjena zbiranju, procesiranju, distribuciji, uporabi in drugi obdelavi podatkov v elektronski obliki;
12. podatki za elektronsko podpisovanje so edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa;
13. sredstvo za elektronsko podpisovanje je nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa;
14. sredstvo za varno elektronsko podpisovanje je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena tega zakona;
15. podatki za preverjanje elektronskega podpisa so edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa;
16. sredstvo za preverjanje elektronskega podpisa je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa;
17. oprema za elektronsko podpisovanje je strojna ali programska oprema ali njune specifične sestavine, ki jih overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov;
18. **potrdilo** je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto;
19. **kvalificirano potrdilo** je potrdilo iz prejšnje točke, ki izpolnjuje zahteve iz 28. člena tega zakona in ki ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena tega zakona;

20. overitelj je fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi;
21. storitev informacijske družbe je storitev, ki se običajno zagotavlja za plačilo na daljavo, z elektronskimi sredstvi in na posamezno zahtevo prejemnika storitev, pri čemer pomeni:

    — na daljavo, da se storitev zagotavlja, ne da bi bili strani sočasno prisotni;
    — z elektronskimi sredstvi, da se storitev na začetku pošlje in v namembnem kraju sprejme z elektronsko opremo za obdelavo (vključno z digitalnim stiskanjem) in shranjevanje podatkov in v celoti pošlje, prenese in sprejme po žici, radiu, optičnih sredstvih ali drugih elektromagnetnih sredstvih;
    — na posamezno zahtevo prejemnika storitev, da se storitev zagotavlja s prenosom podatkov na posamezno zahtevo.

    Storitve informacijske družbe vključujejo zlasti storitve prodaje blaga ali storitev, dostopa do podatkov ali oglaševanja na svetovnem spletu ter storitve dostopa do komunikacijskega omrežja, prenosa podatkov ali shranjevanja prejemnikovih podatkov v komunikacijskem omrežju. Storitve radijske in televizijske radiodifuzije niso storitve informacijske družbe po tem zakonu;
22. ponudnik storitev informacijske družbe je fizična ali pravna oseba, ki ponuja storitve iz prejšnje točke tega člena.

14. člen
Elektronskemu podpisu se ne sme odreči veljavnosti ali dokazne vrednosti samo zaradi elektronske oblike ali, ker ne temelji na kvalificiranem potrdilu akreditiranega overitelja, ali, ker ni oblikovan s sredstvom za varno podpisovanje.

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 sredstvo.

28. člen
1. Iz kvalificiranega potrdila mora biti ugotovljivo:

    — navedba, da gre za kvalificirano potrdilo;
    — ime ali firma in država stalnega prebivališča ali sedeža overitelja;
    — ime oziroma psevdonim imetnika potrdila z obvezno navedbo, da gre za psevdonim;
    — dodatni podatki o imetniku potrdila, ki so predpisani za namen, za katerega se bo potrdilo uporabljalo, ki pa ne smejo biti v nasprotju z namenom uporabe psevdonima;

- podatki za preverjanje elektronskega podpisa, ki ustrezajo podatkom za elektronsko podpisovanje pod nadzorom imetnika potrdila;
- začetek in konec veljavnosti potrdila;
- identifikacijska oznaka potrdila;
- varen elektronski podpis overitelja, ki je potrdilo izdal;
- morebitne omejitve v zvezi z uporabo potrdila;
- morebitne omejitve transakcijskih vrednosti, za katere se potrdilo lahko uporablja.

2. Če ni drugače dogovorjeno, potrdilo ne sme vsebovati podatkov, ki jih varuje poseben zakon.
3. Kvalificirana potrdila, izdana za potrebe osebnih dokumentov, vsebujejo poleg podatkov iz prvega odstavka tega člena tudi osebno identifikacijsko oznako, ki se lahko v ta namen sklicuje ali poveže s Centralnim registrom prebivalstva. Vlada Republike Slovenije podrobneje določi način določanja osebne identifikacijske oznake, vzpostavitev in vodenje registra osebnih identifikacijskih oznak ter pogoje in način sklicevanja ali povezovanja s Centralnim registrom prebivalstva v skladu s predpisi, ki urejajo varstvo osebnih podatkov.

Praktičen pomen 15. člena je v tem, da je to edina oblika digitalnega podpisa, ki je enakovreden lastnoročnemu digitalnemu podpisu s kvalificiranim digitalnim potrdilom. Ta podpis ima enako veljavnost in dokazno sredstvo. Primeren je za uporabo pri vseh poslih in drugih pravnih razmerjih, kjer je obvezna uporaba lastnoročnega podpisa (npr. sklenitev kreditne pogodbe, če imamo v mislih bančne posle, ali sklenitev nepremičninske pogodbe).

Pri pravnih razmerjih, kjer lastnoročni podpis ni potreben, je vseeno priporočljiva uporaba digitalnega podpisa.

V skladu z Evropsko unijo (v nadaljevanju EU) je do 1. julija 2016 veljalo, da je elektronski podpis v vseh državah članicah veljaven, če je na dokumentu jasno zapisano, da stranki sporazumno komunicirata elektronsko. S 1. julijem 2016 je v veljavo EU stopila uredba o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije, v nadaljevanju eIDAS (angl. *Electronic Identification and Authentication Services Regulation* (910/2014/EC)). Na slednjo je vezana Evropska digitalna agenda (angl. *Digital Agenda*), ki predstavlja enega izmed zastavljenih evropskih ciljev za leto 2020. eIDAS predstavlja skupek enotnih in standardiziranih pravil, ki zagotavljajo, da bodo sredstva elektronske identifikacije in elektronske avtentikacije, ki omogočajo dostop do javnih storitev na nacionalni ravni, vzajemno priznana in sprejeta po vsej EU, torej v vseh 28 državah članicah. Hkrati razširja pravni okvir za elektronski podpis in zajema tudi druge storitve zaupanja (Ministrstvo za javno upravo, 2015).

Po eIDAS ločimo med tremi elektronskimi podpisi, in sicer splošnim, naprednim in kvalificiranim. Splošno elektronsko podpisovanje predstavlja pravno sprejemljivost

elektronskega podpisa kot veljavno. Napredno elektronsko podpisovanje je predmet podpisovanja s pomočjo digitalnega certifikata preko interne ali lastne certifikatne agencije. Kvalificiran elektronski podpis temelji na kvalificiranem certifikatu, ki je izdan preko akreditirane certifikatne agencije, ta pa je predmet države članice EU in je skladna z zahtevami eIDAS. Taki certifikati naj bi bili shranjeni na ključku USB, pametni kartici ali na trdem varnostnem modulu (angl. *hardware security module – HSM*) v oblaku (Adobe, 2015a).

Smernice narekujejo tudi direktive Združenih narodov. Pomemben je modelni zakon Komisije OZN za mednarodno gospodarsko pravo (angl. *United Nations Commission on International Trade Law – UNCITRAL*) o elektronskem poslovanju (Uncitral, 2002).

1.3 Primerjava s klasičnim podpisom

Vsem najbolj poznan je lastnoročni podpis na papirju. Splošne opredelitve lastnoročnega podpisa zajemajo vse možne primere in oblike podpisovanja. Kako bi si posameznik najlažje predstavljal, kaj je podpis, pojasnjuje Toplišek, 2000: »Dejanje, s katerim se zapiše neko ime na konec listine zaradi potrditve njene veljavnosti. Podpis je lahko napisan ročno, natisnjen, vtisnjen, natipkan, vgraviran, fotografiran, izrezan iz ene listine in dodan drugi. Litografiran podpis, ki ga na listino odtisne stranka, zadostuje za namen podpisa. Prav tako je zadosten kateri koli znak, simbol ali sredstvo, ki si ga nekdo izbere zato, da ga le-ta predstavlja«.

Primarni karakteristiki klasičnega podpisa sta (Entrust Securing Digital Identities & Information, 2001-2003):

- namen povezave oz. sledljivosti do posameznika;
- splošno označevanje in/ali potrditev povezave posameznika z določenim dokumentom oziroma vsebino dokumenta.

Lastnosti lastnoročnega in digitalnega podpisa so predstavljene v Tabeli 1.

Glede na zgoraj predstavljene lastnosti digitalni podpis zagotavlja več funkcionalnosti, ki so zahtevane pri sodobnem digitalnem poslovanju.

Digitalni podpisi so veliko bolj varna osnova za področje pogodb in obveznosti kot lastnoročno podpisovanje. Ponujajo edino trajno rešitev za zagotavljanje zanesljivih dokazov o obveznostih v spletnem svetu.

Če je zagotovljena avtentičnost (podpisnik je res tisti, za kogar se proglaša), če podpisa ni mogoče ponarediti, ga kopirati, če se podpisanega dokumenta ne da spremeniti in podpisa

ni mogoče zanikati (podpisnik ne more prikriti, da ni podpisal dokumenta), potem lahko enačimo digitalni podpis z običajnim (Lah, 2007).

Tabela 1: Primerjava med lastnoročnim in digitalnim podpisom

Lastnost	*Lastnoročni podpis*	*Digitalni podpis*
Primernost za elektronske dokumente in transakcije	Ne	Da
Možno avtomatsko preverjanje podpisa	Ne	Da
Mogoča odkrivanja sprememb podpisanega dokumenta	Ne	Da
Uporaba pri zavezi k pogodbi ali dokumentu	Da	Da
Zakonodajno priznan	Da	Da

Vir: Entrust Securing Digital Identities & Information, Digital Signatures – Best Practice for e-Buisness Transactions, 2001-2003.

1.4 Prednosti in slabosti digitalnega podpisa

Poleg že omenjenih prednosti digitalnega podpisa obstajajo še dodatne.

Prednosti digitalnega podpisovanja v izbrani banki so:

- **hitrost:** Z digitalnim podpisovanjem nista potrebna vsakokratno tiskanje in fizično posredovanje papirjev posameznemu nivoju odločanja, v drugo poslovalnico ali v tujino. Prav tako ni potrebno skrbeti za vrstni red podpisnikov, saj to ureja dokumentni sistem. Celoten proces poteka avtomatsko, posamezniki pa so lahko o novem dokumentu obveščeni preko elektronske pošte ali mobilne aplikacije. Pospeši se tok dokumentov v organizaciji. S tem se poveča tudi učinkovitost. Če pride do slovničnih ali vsebinskih napak, te lahko hitro odpravimo in dokument ponovno posredujemo v podpisovanje.
- **mobilnost:** Če je posameznik odsoten, lahko dokument podpiše od doma ali na službeni poti. Možno je tudi digitalno podpisovanje elektronske pošte, ki dodatno poenostavi nekatere poslovne procese. Zaposleni lahko ne glede na lokacijo dela (npr. na lokaciji poslovnega partnerja ali stranke) dostopajo do vseh internih dokumentov elektronsko.
- **večja varnost:** Če nekdo spremeni že digitalno podpisan dokument, potem vsi podpisi na dokumentu postanejo neveljavni. Dokument mora biti ponovno podpisan s strani vseh podpisnikov. Tako je mogoče zavarovati dokument pred spremembami. Zaveden je tudi točen čas, ko je bil dokument podpisan.

- **nižji stroški:** Dokumentov za potrebe podpisovanja ni več potrebno tiskati v papirnati obliki. S tem se izničijo stroški porabe papirja, kuvert, poštnih storitev, nadstandardnih storitev hitre pošte, digitalizacije, arhiviranja in uničenja. Nekateri dokumenti tako lahko za vedno ostanejo v digitalni obliki.
- **povečanje produktivnosti zaposlenih:** Zaposleni bi čas, ki ga trenutno porabijo za administrativne zadeve, namenili delu, ki dejansko ustvarja dodano vrednost.
- **poslovanje brez papirja:** Zmanjšanje porabe papirja pozitivno vpliva na okolje in naravo.
- **večje zadovoljstvo strank:** Rokovanje z dokumenti in čakanje na podpis ustreznih oseb v organizaciji povzroča nezadovoljstvo strank in/ali poslovnih partnerjev (IDC, 2015).
- **povečanje prihodkov:** Prihodki se na dolgi rok izkažejo ravno na zaposlenih v organizaciji, saj manj zaposlenih naredi več (IDC, 2015).
- **zagotovitev revizijske sledi:** Pri vseh digitalno podpisanih (elektronskih) dokumentih je avtomatsko zagotovljena tudi revizijska sled (IDC, 2015).

Celostna izvedba digitalnega podpisovanja v organizaciji terja tudi vzpostavitev nekaterih dodatnih mehanizmov, ki podjetju predstavljajo finančni zalogaj. Mednje sodi tudi centralni dokumentni sistem, ki skrbi za digitalno podpisane dokumente. Tak sistem omogoča iskanje po dokumentih, sledljivost digitalnih podpisov ter posredovanje dokumentov v podpis. V takih sodobnih sistemih ima nadrejeni vpogled v to, katere dokumente so člani njegovega oddelka podpisali.

Za potrebe digitalnega podpisovanja je potrebno zagotoviti tudi storitve certifikatne agencije, ki zaposlenim izda digitalna potrdila. Certifikatna agencija je lahko organizirana interno ali preko zunanjega partnerja (npr. SIGEN-CA).

Ocenjevanje veljavnosti pogodb ali sporazumov, sklenjenih na spletu, je zapleteno zaradi brezpapirne narave posla, zato je nujno, da obstajajo standardi, ki so razviti za zagotovitev varnosti in zanesljivosti digitalnih podpisov (Chow, Conteras, & Hamel, 2013).

Standard ISO/IEC X.509 določa obliko in vsebino digitalnega potrdila ter opredeljuje vlogo certifikatne agencije. V kriptografiji predstavlja enega najpomembnejših standardov za področje infrastrukture javnega ključa, upravljanje digitalnih potrdil in šifriranje javnega ključa. Ključnega pomena je pri varnostnem protokolu (angl. *Transport Layer Security*), katerega naloga je varnost internetne in elektronske komunikacije. Standard opredeljuje format infrastrukture javnega ključa in seznam preklicanih potrdil, določa pa algoritem veljave potrdila (ISO, 2013).

Mehanizmi digitalnega podpisovanja so podrobneje opisani v standardih ISO/IEC 9796-2:2010, 14533:2012 ter 20008-2:2013.

Standard ISO/IEC 10118-3:2004 pokriva področje zgostitvenih funkcij.

1.5 Pregled uporabe digitalnih podpisov v storitvah javne uprave RS

V Republiki Sloveniji (v nadaljevanju RS) obstaja več organizacij, ki imajo za fizične in pravne osebe omogočen dostop do opravljanja določenih storitev z uporabo elektronskega podpisovanja s kvalificiranim digitalnim potrdilom. Gre za udoben in enostaven način opravljanja različnih storitev. V nadaljevanju bom podrobneje predstavila štiri primere portalov javne uprave RS, ki nudijo storitve, podprte s kvalificiranim digitalnim potrdilom.

Portal e-Vem je državni portal za samostojne podjetnike in podjetja. Na enem mestu lahko ustanovimo podjetje, tega vodimo in prenehamo z dejavnostjo (zapiranje). Preko portala e-Vem lahko tudi drugi poslovni subjekti (npr. javna uprava) vlagajo prijave, odjave in spremembe podatkov zaposlenih v obvezna socialna zavarovanja ter objavijo prosta delovna mesta. Na portalu e-Vem je možno urejati prijave v socialna zavarovanja za vse poslovne subjekte.

Na točki e-Vem lahko oddamo vloge za Agencijo RS za javnopravne evidence in storitve (AJPES), Davčni urad Republike Slovenije (DURS), Zavod za zdravstveno zavarovanje Slovenije (ZZZS) in Obrtno-poslovno zbornico Slovenije (OZS) (eVem, 2005).

Portal E-uprava zagotavlja storitve za državljane in podjetja. Za fizične osebe lahko opravimo storitve, povezane s pomembnimi življenjskimi dogodki, kot so npr. rojstvo otroka, selitev, zaposlitev in podobno. Za podjetja so na portalu koristne vsebine, povezane s pomembnimi dogodki za podjetja, zavode in društva (eUprava, 2016).

Portal eSodstvo zagotavlja vpogled v elektronsko zemljiško knjigo. Slednja je javna knjiga, namenjena vpisu in javni objavi podatkov o pravicah na nepremičninah in pravnih dejstvih v zvezi z nepremičninami. Za vodenje zemljiške knjige so pristojna okrajna sodišča. Vsi vpisi v zemljiški knjigi so javni. Javnost informatizirane glavne knjige je zagotovljena tudi preko spletnega zemljiško knjižnega portala (eSodstvo, 2016).

Portal eDavki predstavlja elektronsko davčno poslovanje za podjetja, fizične osebe in fizične osebe, ki so samostojni podjetniki. Gre za preprosto in varno izpolnjevanje ter oddajanje davčnih obrazcev z uporabnikovega računalnika. Preko eDavkov lahko fizične osebe poleg davčnih obrazcev oddajo napoved za odmero dohodnine, pravne osebe pa obrazce s področja davka na dodano vrednost ter vlogo za preverjanje identifikacijskih številk v EU. Na voljo sta tudi elektronski storitvi registracije davčnih zavezancev, e-poslovanje in izmenjava njihovih podatkov z davčnimi upravami ostalih članic EU, pa tudi preverjanje davčnih številk davčnih zavezancev iz držav članic EU. Uporabnik eDavkov lahko postane vsak davčni zavezanec, ki si priskrbi kvalificirano digitalno potrdilo (eDavki, 2016).

1.6 Trije primeri digitalnega podpisovanja v praksi

V poglavju bom predstavila tri primere digitalnega podpisovanja v praksi.

Podjetje Siemens Mexico se poslužuje enostavne rešitve, ki je omogočena posameznim podjetjem na trgu. Gre za aplikativno podporo Adobe Reader. Elektronsko podpisovanje poteka preko certifikata posameznega zaposlenega, ki vpiše svoje geslo. Elektronsko podpisani dokumenti tipa PDF so shranjeni na strežnikih. Iskanje poteka po vsebini ali po imenu. Vsaka skupina oddelkov, področje poslovanja, ima omogočen dostop samo do svojih dokumentov, ki so shranjeni na enem izmed strežnikov.

Podjetje Ricoh s sedežem v Angliji in s 3.100 zaposlenimi po celotni državi se je odločilo za uporabo celostne rešitve Adobe Document Cloud eSign. Slednja je po njihovem mnenju v veliko pomoč podjetju pri pridobivanju strank in zaposlenih.

Trenutno podjetje sklene 600 pogodb na mesec preko rešitve *Adobe DC eSign*. S spremembo so uspeli skrajšati čas za sklenitev posamezne pogodbe za pet dni. Ricoh je s prenovo poslovanja dosegel naslednje rezultate (Ricoh, 2015):

- odpravo fizičnih preprek – podjetje je pospešilo čas cikla prodajnih pogodb;
- brezpapirno poslovanje – z zmanjšano porabo papirja in goriva je podjetje izboljšalo svojo zavezo k trajnostnemu razvoju, ki predstavlja tudi glavni princip podjetja Ricoh;
- drastično izboljšanje poslovanja – podjetje je znižalo letne stroške poslovanja (papirja, tiskanja in pošte), hkrati pa povečalo produktivnost;
- odgovornost – varen elektronski sistem zagotavlja hitrejšo in natančnejšo podatkovno bazo ter omogoča racionalizacijo organizacijskega postopka za nove zaposlene.

S celotno programsko rešitvijo so odpravili tudi zamude podpisovanj in ob tem zagotovili novo zaposlenim, da izpolnijo vse potrebne obrazce ter sklenejo pogodbe o zaposlitvi v 15 minutah (Ricoh, 2015).

Celostno rešitev Adobe Document Cloud eSign lahko najdemo tudi v finančnem podjetju Diners Club, ki ima po svetu več milijonov strank. Mednarodna Diners Club franšiza v Angliji in na Irskem nudi tudi kartice za porabo ter potovalne in hišne računske rešitve za več tisoč fizičnih in pravnih strank letno.

Za izboljšanje produktivnosti in dostopa do storitev strank se je podjetje odločilo za elektronsko oddajo pristopnih dokumentov. Oddaja dokumentov zajema izpolnjevanje obrazcev, združenje in elektronski podpis s kvalificiranim digitalnim potrdilom. Pred spremembo je stranka potrebovala več dni, da je obrazce prebrala, jih izpolnila in oddala po pošti, včasih pa je na to pozabila. Danes prodajni predstavniki iz kontaktnega centra z nekaj kliki posredujejo vse dokumente stranki, z njo ostanejo na zvezi in ji po prejemu še

dodatno nudijo pomoč pri izpolnjevanju ter oddaji. Stranka tako med telefonskim pogovorom sklene pogodbo o sodelovanju.

Prednosti podjetja, ki izkorišča napredno rešitev, so (Diners Club, 2015):

- boljša produktivnost – pospešitev povprečnega časa za podpis in oddajo obrazcev z nekaj dni na 17 minut;
- pozitivne izkušnje strank – hiter in enostaven prijavni proces spodbuja hitrejšo kreditno porabo in zadrževanje strank;
- več strank – izboljšanje kazalcev, ki vliva zaupanje v prodajnega predstavnika kontaktnega centra;
- dosledna prijava – krajši čas, ki je bil namenjen pregledovanju in popravljanju.

2 MEHANIZEM DIGITALNEGA PODPISOVANJA

Število ljudi in podjetij na spletu iz dneva v dan narašča. Spletni dostop postaja vse hitrejši in cenejši. Ljudje uporabljamo internet za osebno komunikacijo, podjetništvo, nakupovanje in za opravljanje poslovnih transakcij. Internet je odprto komunikacijsko omrežje, ki prvotno ni bilo zasnovano za varno opravljanje storitev. Posamezniki so zelo zgodaj ugotovili, da lahko izkoristijo njegove pomanjkljivosti v svoj prid.

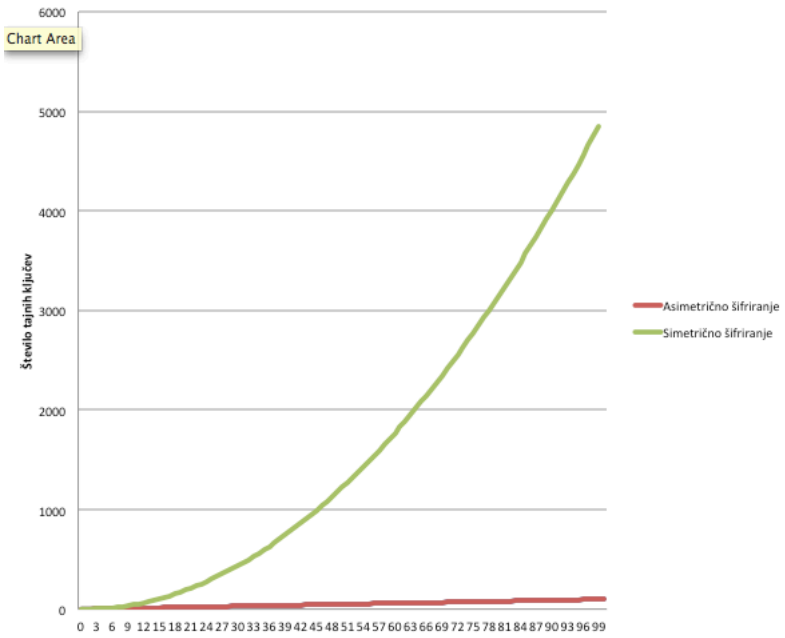
Če želimo, da internet postane tisto pravo poslovno in komunikacijsko orodje, moramo uporabnikom zagotoviti varno komunikacijo z uporabo mehanizmov šifriranja. Slednji so osnova za digitalno podpisovanje.

Obstaja več mehanizmov šifriranja. O simetričnem načinu šifriranja govorimo v primeru, ko uporabljamo isti tajni ključ za šifriranje in dešifriranje sporočila. Pošiljatelj in prejemnik uporabljata isti ključ, ki si ga morata vnaprej izmenjati na varen način (Jazbinšek, 2015).

Jerman Blažič (2006) trdi, da v primeru zaključene ali zaprte skupine takšen dogovor ne predstavlja posebnega problema. Tak način izmenjave ključa je neprimeren za digitalno poslovanje, saj vnaprej določen ključ pogojuje predhodno uskladitev. Eden izmed problemov pri simetrični kriptografiji je tudi potrebno število tajnih ključev in z njimi potrebnih uskladitev. Za tajno komunikacijo med dvema osebama je potreben zgolj en tajni simetrični ključ. Pri treh akterjih mora vsak posameznik poznati po dva ključa, da si lahko izmenja šifrirano sporočilo, kar skupaj pomeni obstoj treh različnih ključev. Pri varni komunikaciji petih uporabnikov bi moral vsak izmed njih poznati po štiri ključe. Tako bi bilo potrebnih deset tajnih ključev.

Z zelene krivulje na Sliki 2 je razvidno, da s številom uporabnikov število potrebnih ključev narašča eksponentno, kar je skrajno nepriročno za internetno komunikacijo, kjer obstaja na milijone uporabnikov.

Slika 2: Število uporabnikov v primerjavi s številom tajnih ključev



V zgodovini kot primer simetrične kriptografije najdemo nemški šifrirni stroj Enigma (Slika 3), ki so ga uporabljali med drugo svetovno vojno. Njegova naloga je bila zakrivati sporočila, namenjena koordinaciji vojaških enot.

Slika 3: Šifrirni stroj Enigma

Vir: Lautréamont, Enigma, 2015.

Danes simetričnega načina šifriranja skorajda ne uporabljamo več, saj ima asimetrični bistveno več prednosti.

Pri asimetričnem šifriranju ima vsak posameznik zasebni in javni ključ. Vsakdo, ki želi komunicirati tudi z osebo, ki je ne pozna, lahko s pomočjo njenega javnega ključa pošlje šifrirano sporočilo. Če imamo *n* število oseb, ki želijo med seboj komunicirati, potrebujemo *n* število parov ključev.

V nadaljevanju bom poglobljeno predstavila delovanje varnega digitalnega podpisovanja z uporabo asimetričnega šifriranja.

2.1 Definicija kvalificiranega digitalnega potrdila

Kvalificirano digitalno potrdilo KDP ali certifikat (angl. *Digital Certificate*) daje posamezniku možnost identifikacije, izvedbe podpisa na elektronskem dokumentu in varovanja zaupnih podatkov s šifriranjem.

Kvalificirano digitalno potrdilo je sodobna alternativa klasičnim osebnim identifikatorjem s specifičnim namenom, tj. zagotavljanje varnega in legitimnega e-poslovanja. Izdajajo jih za to pooblaščeni overitelji oz. certifikatne agencije (angl. *Certification Authorities*).

Digitalno potrdilo je računalniški zapis, ki vsebuje podatke o imetniku in organizaciji (ime, elektronski naslov, enolična številka, davčna številka organizacije ...), njegov javni ključ ter podatke o overitelju oz. izdajatelju digitalnega potrdila, obdobju veljavnosti digitalnega potrdila in uporabljenih algoritmih. Celotno digitalno potrdilo je podpisano s strani certifikatne agencije z zasebnim ključem. S tem je digitalno potrdilo zaščiteno pred ponaredbo.

Kvalificirana digitalna potrdila so sestavni del tehnoloških rešitev in nudijo dve osnovni funkcionalnosti (Uprava, 2015):

- vzpostavitev zaupanja do imetnika digitalnega potrdila;
- možnost šifriranja z uporabo asimetrične kriptografije.

Digitalno potrdilo je lahko izdano za osebo, organizacijo, podjetje, računalnik, spletno stran ali napravo (npr. strežnik). Na voljo je v različnih oblikah in formatih.

Digitalno potrdilo predstavlja enolično povezavo med imetnikom in javnim ključem. Je digitalni identifikacijski dokument. Primerjamo ga lahko z osebno izkaznico, le da je prirejeno za uporabo v digitalnem svetu. Uporabljamo ga za zagotavljanje varnega in legitimnega e-poslovanja. Kvalificirano digitalno potrdilo v Sloveniji lahko izda le izdajatelj, ki je vpisan v register overiteljev v Republiki Sloveniji (Bolha, 2015).

Digitalna potrdila so sredstva, s katerimi lahko potrošniki in podjetja izkoriščajo varnostne aplikacije z infrastrukturo javnih ključev (angl. *Public Key Infrastructure*), na kratko PKI. PKI vključuje tehnologijo, ki omogoča varno elektronsko poslovanje in internetno komunikacijo (Comodo, 2015).

Digitalna potrdila se uporabljajo tudi za zagotavljanje pristnosti javnih strežnikov. Brez uporabe digitalnih potrdil bi lahko vsakdo ustvaril svoj strežnik in se predstavljal kot pristni strežnik. Digitalna potrdila to težavo tako rešujejo, da identiteto strežnika oz. domene vežejo na njegov javni ključ. Digitalno potrdilo vsebuje podatke o imetniku (domena ali strežnik) in pripadajoči javni ključ. Ključno vlogo pri preverjanju pristnosti igrajo overitelji, ki jamčijo za pristnost imetnika (domene ali strežnika). Overitelji jamčijo za izdana potrdila (npr. za Googlovo elektronsko pošto) s svojim lastnim digitalnim potrdilom, ki ga v primeru overitelja imenujemo korensko digitalno potrdilo (angl. *Root certificate*). Brskalniki vsebujejo prednaložen seznam korenskih digitalnih potrdil, ki jim zaupajo. Overitelji digitalnih potrdil lahko določena izdana digitalna potrdila uvrstijo tudi na črni seznam, če se izkaže, da je prišlo do zlorabe (Holbl, 2011).

Trajanje digitalnih potrdil je časovno omejeno. V praksi so v uporabi pet let ali več, odvisno od namena uporabe in dolžine ključev. Po poteku sledita ponovna identifikacija in nova pridobitev para ključev. Časovna omejitev je posledica statističnega dejstva, da verjetnost izgube ali zlorabe zasebnega ključa s časom narašča. Prav tako so ranljivi tudi algoritmi (Jerman Blažič, 2006).

2.2 Certifikatne agencije

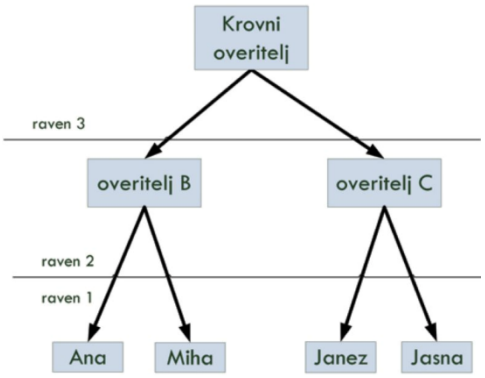
Pri elektronskem podpisovanju je nujno zagotoviti, da je oseba, ki je navedena na digitalnem potrdilu, dejanski lastnik digitalnega potrdila in posledično »pravi« podpisnik dokumenta. S tem namenom so se oblikovale certifikatne agencije (angl. *Certificate Authorities – CA)*, ki jim vsi zaupamo. V nasprotnem primeru bi moral vsak posameznik pred uporabo tujega javnega ključa preveriti istovetnost lastnika digitalnega potrdila. To bi bila zanj preobsežna naloga.

Certifikatna agencija je zaupanja vredno podjetje ali organizacija, ki izdaja elektronske dokumente, pri čemer predhodno preveri identiteto subjekta na internetu. Ti elektronski dokumenti se imenujejo digitalna potrdila in so najpomembnejši sestavni del varne komunikacije (Rouse, 2015).

Certifikatna agencija tako jamči, da je določena oseba res imetnik določenega para ključev. V praksi sprejema tudi vloge za digitalna potrdila in omogoča infrastrukturo za preverjanje veljavnosti potrdil (Holbl, 2015).

Zaupanje je običajno organizirano v hierarhijo, zato ga imenujemo hierarhično zaupanje. Kot prikazuje Slika 4, posameznik zaprosi overitelja za digitalno potrdilo. Za overitelja v redkih primerih jamči krovni overitelj. V teoriji imamo lahko več nivojev hierarhije, vendar v praksi uporabljamo le dva (overitelj in uporabnik).

Slika 4: Hierarhija zaupanja



Vir: Holbl, Infrastruktura javnih ključev, 2015.

Digitalna potrdila so podpisana s strani certifikatne agencije, ki jih je izdala. Slednja je zaupanja vredna tretja stranka, ki preverja usklajenost javnih ključev z identiteto, avtorjem elektronskega sporočila oziroma podpisnika dokumenta. Prednosti certifikatov in certifikatnih agencij so opazne v primeru, ko oba subjekta zaupata isti certifikatni agenciji. V tem primeru vsak posameznik spozna javna ključa z izmenjavo certifikatov, podpisanih s strani certifikatne agencije. Ko oba subjekta izmenjata javni ključ, ga lahko uporabljata za posredovanje šifriranih sporočil ali za preverjanje verodostojnosti podpisov na dokumentih. Certifikat dokazuje, da shranjen javni ključ v potrdilu pripada predmetu tega potrdila. Certifikatna agencija je odgovorna za preverjanje identitete subjekta pred izdajo potrdila. Nato podpiše potrdilo s pomočjo svojega zasebnega ključa, ki se uporablja za preverbo potrdila. Javni ključi certifikatne agencije so dandanes že vključeni v pakete programske opreme, kot so spletni brskalniki in operacijski sistemi. Lahko jih ročno doda tudi uporabnik sam (Microsoft, 2015).

Digitalna potrdila so lahko različna, in sicer glede na osebo ali organizacijo, ki jih je izdala. Obstajajo takšna, ki jih posameznik lahko izda sam (angl. *Self-signed certificate*), pa tudi takšna, ki jih izda posebej za to pooblaščena in verificirana ustanova.

Ustrezno digitalno potrdilo za varno elektronsko podpisovanje je v Sloveniji mogoče pridobiti pri overiteljih, ki so bili 1. 3. 2016 vpisani v Register overiteljev v Republiki Sloveniji.

Overitelji si med seboj zaupajo in javne ključe tudi izmenično podpisujejo. Med njimi so:

- SIGEN-CA (Ministrstvo za javno upravo);
- AC NLB (Nova Ljubljanska banka d.d., Ljubljana);
- POŠTA®CA Pošta Slovenije d.o.o.;
- HALCOM-CA (Ministrstvo za javno upravo);
- Ministrstvo za obrambo RS.

Prvi štirje overitelji izdajajo kvalificirana digitalna potrdila, kot to zahteva zakonodaja za fizične in pravne osebe ter fizične osebe, registrirane za opravljanje dejavnosti. Zadnji overitelj izdaja digitalna potrdila le za svojo interno rabo.

V Sloveniji je mogoče pridobiti digitalno potrdilo z obiskom ene izmed certifikatnih agencij in z dostavo zahtevka za kvalificirano digitalno potrdilo, tega pa lahko izpolnimo tudi preko varnih portalov. Po obdelavi zahtevka bodoči imetnik potrdila po pošti prejme avtorizacijsko kodo, po elektronski pošti pa referenčno številko. S prejemom obeh stvari lahko začne imetnik ustrezno uporabljati kvalificirano digitalno potrdilo (Ministrstvo za javno upravo, 2013). Certifikatna agencija posamezniku dodeli tako privatni kot javni ključ.

Ministrstvo za javno upravo loči med spletnimi kvalificiranimi digitalnimi potrdili in med posebnimi kvalificiranimi digitalnimi potrdili.

Spletna kvalificirana digitalna potrdila izdajatelja SIGEN-CA uporabljamo za (Ministrstvo za javno upravo, 2013a):

- varno spletno komuniciranje po protokolih SSL (angl. *Secure Sockets Layer*) in TLS (angl. *Transport Layer Security*);
- varno pošiljanje elektronske pošte po protokolu S/MIME (angl. *Secure Multipurpose Internet Mail Extensions*);
- šifriranje in dešifriranje podatkov v elektronski obliki;
- digitalno podpisovanje podatkov v elektronski obliki in izkazovanje istovetnosti imetnika;
- storitve oz. aplikacije, za katere se zahteva uporaba spletnih kvalificiranih digitalnih potrdil izdajatelja SIGEN-CA.

Posebna kvalificirana digitalna potrdila izdajatelja SIGEN-CA uporabljamo za (Ministrstvo za javno upravo, 2013a):

- šifriranje in dešifriranje podatkov v elektronski obliki;
- digitalno podpisovanje podatkov v elektronski obliki in izkazovanje istovetnosti imetnika;

- varno brisanje podatkov v elektronski obliki;
- storitve oz. aplikacije, za katere se zahteva uporaba posebnih kvalificiranih digitalnih potrdil izdajatelja SIGEN-CA.

Eden izmed overiteljev s posebnim statusom je tudi SIGOV-CA (angl. *Slovenian Governmental Certification Authority*). Sigov-ca je izdajatelj kvalificiranih digitalnih potrdil overitelja na ministrstvu za javno upravo (MJU). Digitalna potrdila izdaja za uslužbence v javni upravi (Ministrstvo za javno upravo, 2013b).

Certifikatne agencije igrajo enako vlogo tako doma kot tudi v tujini. V tujini veljajo za bolj priznane Comodo, Symantec, GoDaddy, GlobalSign, DigiCert in Entrust.

2.3 Algoritem RSA

RSA (angl. *Rivest - Shamir - Adlman*) je kriptografski algoritem za šifriranje z uporabo tehnologije javnega in privatnega ključa. Uporablja se v večini internetnih protokolov, ki vključujejo kriptografijo. Igra zelo pomembno vlogo v infrastrukturi javnega ključa in je temelj današnjih kriptografskih aplikacij (Chimielowiec, 2009).

Leta 1978 so Ron Rivest, Adi Shamir in Leonard Adelman na ameriškem inštitutu MIT objavili trenutno najbolj znan algoritem za zakrivanje podatkov z javnim ključem, na kratko algoritem RSA. Algoritem temelji na celoštevilski algebri in izkorišča lastnosti velikih praštevil. Bistvo algoritma se skriva v dejstvu, da je faktorizacija produkta dveh neznanih velikih praštevil računalniško zelo težek problem tudi za danes najhitrejši računalnik. Njegova šibka točka je počasnost v primerjavi s simetričnimi načini kriptiranja. Razlog je v izračunu šifriranja, saj gre za potenciranje dveh zelo velikih števil. Algoritem je tako primeren za skrivanje krajših sporočil. Za daljšo vsebino je značilnejše šifriranje povzetka sporočila, ki ga izračunamo s pomočjo zgoščevalne funkcije (Rivest, Shamir & Adleman, 1978).

Matematično delovanje algoritma RSA

Izberemo p in q, ki sta veliki praštevili.
Pri tem je n zmnožek teh dveh praštevil, kot prikazuje enačba (1).

$$n = p * q \tag{1}$$

S pomočjo dveh velikih praštevil in njunega zmnožka izračunamo koeficient, kot prikazuje enačba (2).

$$\Phi(n) = (p-1)\,(q-1) \tag{2}$$

Nato je potrebno izbrati tako celo število *e*, ki bo ustrezalo pogoju $1 < e < \Phi(n)$. Hkrati velja, da *n* in *e* nimata skupnih faktorjev.

$$(d*e) \bmod \Phi(n) = 1 \tag{3}$$

Iz formule (3) je mogoče sestaviti javni ključ, ki je sestavljen iz para števil *(e, n)*.
Prav tako je mogoče sestaviti zasebni ključ, ki predstavlja par števil *(d, n)*.

Naj bo *m* število (sporočilo), ki ga želimo šifrirati in za katerega velja pogoj $0 < m < n$, *c* pa šifrirano število (sporočilo) m. Šifrirano število c lahko dešifriramo s formulo X, število m pa lahko zašifriramo v sporočilo c s formulo Y. V primeru šifriranja daljšega niza znakov šifriramo znak za znakom.

FORMULI ZA KODIRANJE IN DEKODIRANJE

Enačba (4) prikazuje, kako sporočilo šifriramo.

$$c = m^e \bmod n \tag{4}$$

Kako sporočilo dešifriramo, izračunamo po enačbi (5).

$$m = c^d \bmod n \tag{5}$$

Praktični primer uporabe algoritma RSA

Za *p* in *q* v tem primeru uporabimo čim manjši praštevili, da lahko primer čim enostavneje izvedemo. Izbrali smo naslednji praštevili.

$p = 3$
$q = 11$

n dobimo tako, da pomnožimo *p* in *q*, kot prikazuje spodnja enačba (6).

$$n = 3 * 11 = 33 \tag{6}$$

$$(3 - 1)*(11 - 1) = 2 * 10 = 20 \tag{7}$$

Skladno s pogojem $1 < e < \Phi(n)$ izberemo število e.
V našem primeru je $e = 7$.

$d = 3$

$$((3 * 7) \bmod 20) = 1 \quad (8)$$

Javni ključ je predstavljen s parom $(e, n) = (7, 33)$.

Zasebni ključ je tako par $(d, n) = (3, 33)$.

Šifriranje, za katerega velja pogoj $0 < m < n$.
$m = 2$

$$c = 2^7 \bmod 33 = 29 \quad (9)$$

Dešifriranje:
$c = 29$

$$m = 29^3 \bmod 33 = 2 \quad (10)$$

2.4 Šifriranje

Digitalno podpisovanje deluje na osnovi tehnologije šifriranja. Jerman Blažič (2006) trdi, da je šifriranje temeljni postopek vseh varnostnih sistemov. Pravi, da je šifriranje uspešno, če naključni opazovalec ne more razvozlati izvirnega podatka zgolj na podlagi analize šifriranega niza. Še posebej pomembno vlogo ima šifriranje pri vprašanjih nacionalne varnosti, zato je pogosto predmet vojaških organizacij in varnostnih služb.

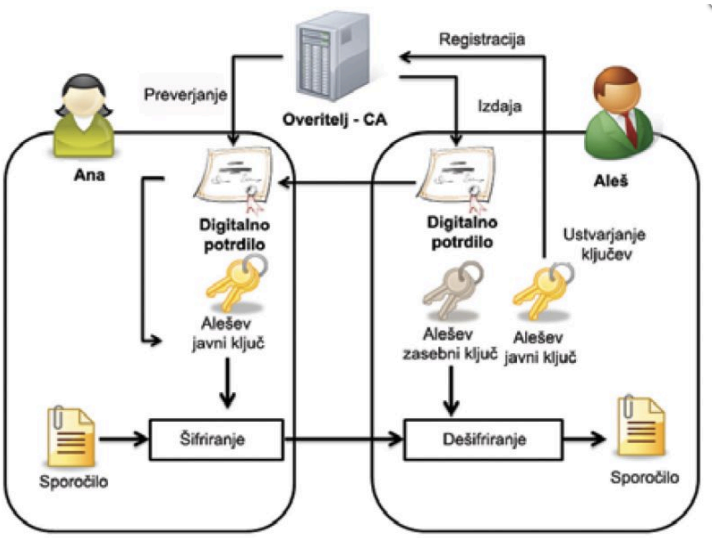
Namen digitalnega podpisovanja ni zaščita vsebine pred vpogledom, temveč zagotovitev povezave med podpisnikom in vsebino ter zaščito vsebine pred spreminjanjem.

V praksi za digitalno podpisovanje uporabljamo tehnologijo šifriranja na osnovi zasebnega in javnega ključa.

Slika 5 prikazuje Ano, ki si želi varno izmenjati sporočilo z Alešem. Pri tem za šifriranje sporočila uporabi Alešev javni ključ. Pri PKI ima pomembno vlogo tudi certifikatna agencija, ki jamči, da je javni ključ, ki ga je Ana uporabila, res del Aleševega digitalnega potrdila. Aleš lahko prejeto šifrirano sporočilo dešifrira s pomočjo svojega zasebnega ključa. Kljub uporabi šifriranja Aleš nima zagotovila o avtentičnosti sporočila. Prepričan je lahko le, da šifriranega sporočila med prenosom ni razvozlala tretja oseba (Holbl, 2015).

V praksi se javni in zasebni ključ vedno povezujeta in uporabljata v kombinaciji z digitalnimi potrdili. Ko z nekom delimo svoj javni ključ, dejansko delimo digitalno potrdilo, ki vsebuje naš javni ključ in ostale podatke (Holbl, 2015).

Slika 5: Prikaz šifriranja sporočila z uporabo asimetričnega algoritma



Vir: Holbl, Infrastruktura javnih ključev, 2015.

2.5 Digitalno podpisovanje s pomočjo infrastrukture PKI

Varno digitalno podpisovanje in druge varnostne metode v sodobnem e-poslovanju potekajo s pomočjo infrastrukture javnih ključev (angl. *Public Key Infrastructure* – v nadaljevanju PKI).

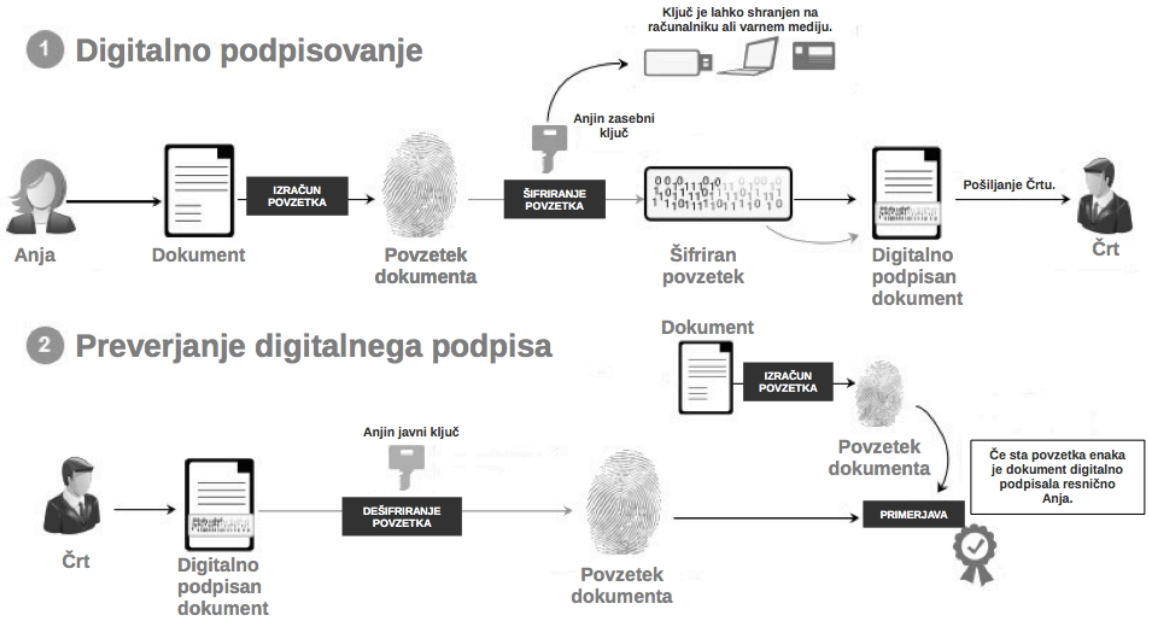
Infrastruktura javnih ključev je skupina procesov in standardov, uporabljenih za zagotovitev zelo varnega elektronskega prenosa informacij. Je standardiziran industrijski pristop, uporabljen v e-komerciali, internetnem bančništvu, zaupnih elektronskih sporočilih in drugih internetnih aktivnostih (Net-security, 2016).

Osnovo pri PKI predstavlja digitalno potrdilo, ki je izdano s strani certifikatne agencije. Digitalno potrdilo vsebuje osnovne podatke o lastniku, izdajatelju in javni ključ. Certifikatna agencija zagotavlja resničnost podatkov lastnika digitalnega potrdila. Za šifriranje in digitalno podpisovanje je potreben še zasebni ključ, ki je matematično povezan z javnim ključem. Vsi izdani javni ključi so objavljeni v spletni podatkovni bazi posamezne certifikatne agencije. Podatki, šifrirani z javnim ključem, so lahko dešifrirani z ustreznim in edinstvenim zasebnim ključem. Zasebni ključ predstavlja skrivnost posameznika in je shranjen na trdem disku računalnika posameznika ali na njegovi pametni kartici.

Slika 6 prikazuje digitalno podpisovanje dokumenta in preverjanje digitalnega podpisa s strani prejemnika. Anja želi dokument digitalno podpisati in ga poslati Črtu. Asimetrične metode šifriranja so počasnejše, zato se z zgoščevalno funkcijo najprej izračuna povzetek dokumenta. Slednjega Anja zašifrira s svojim zasebnim ključem. Šifriran povzetek dokumenta je digitalni podpis, ki skupaj z izvirno različico dokumenta sestavlja digitalno podpisan dokument.

Črt prejme digitalno podpisan dokument in ponovno, po enakem postopku, izračuna povzetek dokumenta. Z Anjinim javnim ključem je mogoče dešifrirati digitalni podpis dokumenta (Anjin povzetek). Če sta povzetka enaka, pomeni, da je dokument res podpisala Anja in da izvirni dokument po digitalnem podpisovanju ni bil spremenjen.

Slika 6: Digitalno podpisovanje z digitalnim potrdilom



Če želi nekdo zagotoviti avtentičnost lastnega sporočila, potem za šifriranje uporabi svoj zasebni ključ. Prejemnik lahko uspešno dešifrira sporočilo s prosto dostopnim javnim verifikacijskim ključem pošiljatelja. Na takšen način je zagotovljeno, da je sporočilo res prispelo od prave osebe (Dewan, 2005).

Postopek preverjanja podpisa je zelo občutljiv in zahteva brezkompromisno verodostojnost vseh elementov (digitalno potrdilo, verigo potrdil, avtoriziran čas preverjanja), sicer podpisu ne moremo zaupati (Jerman Blažič, 2006).

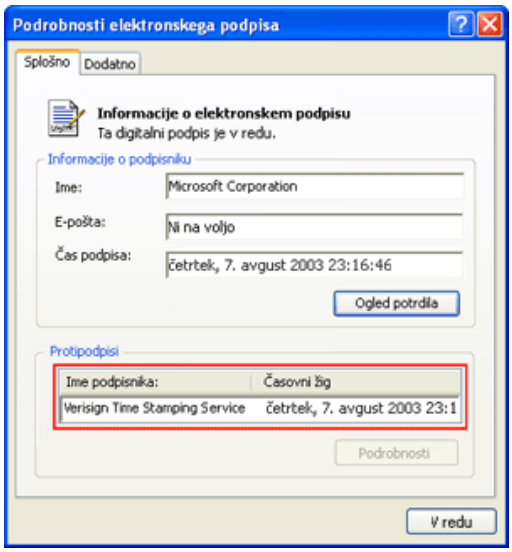
Digitalno podpisovanje lahko nadgradimo tudi s postopkom šifriranja in zagotovimo tajni prenos digitalno podpisanega dokumenta. V tem primeru bi Anja lahko že podpisan dokument zašifrirala s pomočjo Črtovega javnega ključa. Slednji bi pred ponovnim

izračunom povzetka sporočila najprej moral dešifrirati dokument s pomočjo svojega zasebnega ključa.

2.6 Časovni žig

Časovni žig (angl. *Time Stamp*) je posebna izpeljanka digitalnega zapisa, ki označuje, kdaj (časovno natančno) je bil določen dokument podpisan. Na enem mestu povezuje datum in čas podpisa z vsebino v elektronski obliki na kriptografsko varen način. Čas je potrebno črpati iz natančnega in verodostojnega časovnega vira (atomska ura). Primer časovnega žiga prikazuje Slika 7.

Slika 7: Primer časovnega žiga



Vir: Office, Primer časovnega žiga, 2015.

Časovni žig določenemu dokumentu se pripoji tako, da se povzetek vsebine posreduje strežniku TSA (angl. *Time Stamp Authority*). Strežnik posredovani vsebini doda čas in zadevo podpiše s svojim zasebnim ključem. S tem je zagotovljen dokaz, da je vsebina dokumenta obstajala. Poleg tega zadevo lahko še dodatno preverimo s ponovnim kreiranjem povzetka vsebine, ki naj bi se ujemala s primarno.

V okviru Ministrstva za javno upravo RS SI-TSA (angl. *Slovenian Time Stamping Authority*) izdaja varne časovne žige. Varni časovni žigi so namenjeni (Ministrstvo za javno upravo, 2009):

- zagotavljanju, da je bil dokument podpisan z veljavnim digitalnim potrdilom v določenem časovnem trenutku, in sicer na način, da povezuje datum in čas podpisa ter podatke v elektronski obliki na kriptografsko varen način;

- za potrebe, kjer je potrebno dokazati časovne lastnosti transakcij in drugih storitev.

Izdajatelj varnih časovnih žigov SI-TSA je del infrastrukture javnih ključev (PKI) overitelja na ministrstvu za javno upravo. SI-TSA izdaja varne časovne žige, namenjene aplikacijam, s katerimi upravljajo institucije javne uprave, od 10. septembra 2004 pa so na voljo tudi poslovnim subjektom in drugim končnim uporabnikom, ki s SI-TSA sklenejo dogovor.

2.7 Varnost

Posebno pozornost je zaradi odprtosti komunikacijskega medija potrebno nameniti zagotavljanju ustreznega nivoja varnosti (Lesjak, 2015).

Modernizacija za seboj prinaša tako pozitivne kot negativne učinke. Večina odraslih nima težav z uporabo sodobnih elementov v poslovnem in osebnem okolju, čeprav se le redko zavedajo varnostnih vidikov elektronskega poslovanja. Za varnost je potrebno poskrbeti na vseh področjih. Poleg varnega računalniškega okolja v organizaciji mora biti z geslom zavarovano tudi digitalno potrdilo.

Gesla so zelo pogosto uporabljena avtentikacijska metoda za prenos nezaupnih informacij med manjšim številom uporabnikov, pri prenosu zaupnih podatkov v distribuiranih okoljih pa so neprimerna. Danes je zahtevana bolj rigorozna oblika avtentikacije za potrditev identitete članov, vključenih v takšno vrsto komunikacije, in za avtentikacijo informacij, ki so bile posredovane (Net-security, 2015).

Varno elektronsko podpisovanje pomeni podpisovanje z ustreznim zaščitenim certifikatom.V sodobnem svetu varnost ne uspe vedno slediti napredku. Uporabniki pričakujemo absolutno varnost pred raznimi udori, ponaredki, zlorabami (prestrezanje informacij, kraja podatkov itd.) in manipulacijami (poneverba, lažna identiteta itd.) s podatki, piše Jerman Blažič (2006). Žal je absolutna varnost nemogoča. Nepridipravi s svojimi spretnostmi in poskušanjem najdejo pomanjkljivosti v varnostnih sistemih. Posledično prihaja tudi do možnih zlorab digitalnih potrdil.

Varnost je pri digitalnih podpisih odvisna tudi od tipa uporabljenih zgoščevalnih funkcij. Zgoščevalne funkcije (angl. *hash functions*) so algoritmi, ki poljudno dolg niz podatkov preslikajo v število fiksne dolžine, ki mu rečemo tudi kontrolna vsota. Eno sporočilo vedno preslikajo v isto kontrolno vsoto, lahko pa več različnih sporočil preslikajo v isto kontrolno vsoto. Zgostitveni algoritmi morajo biti enosmerni oz. nepovratni. To pomeni, da iz kontrolne vsote ni mogoče izračunati prvotnega sporočila. Če nastane najmanjša sprememba v sporočilu, se z njo bistveno spremeni tudi zgoščevalni rezultat. Zgoščevalne funkcije se tako uporabljajo za ohranitev integritete podatkov.

Primeri štirih zgostitvenih algoritmov in njihov rezultat za vhodni niz »Danes je lep dan«.

- MD5 (angl. *Message Digest*):
80f6daf3007c43dc48de425d7f7909a3

- SHA1 (angl. *Secure Hash Algorithm*):
ad1e565948dcc3699d212dc49e86f9824073a1d3

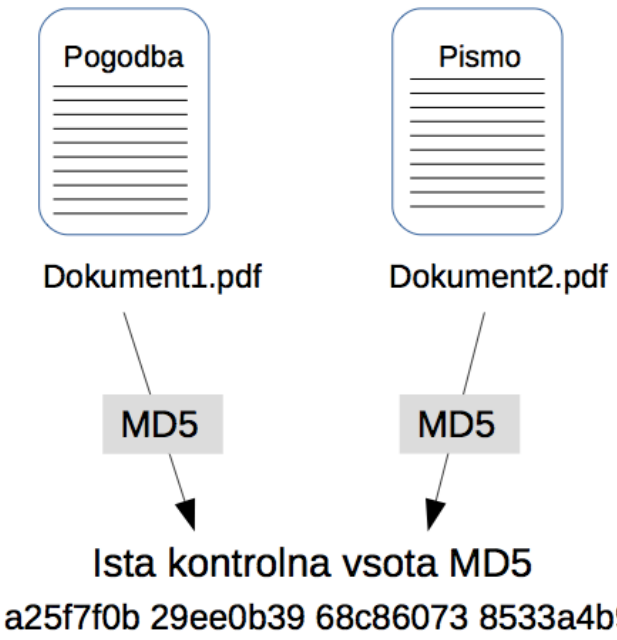
- SHA3-256:
c26495c767d9ad8449d0e7b213bee0a41d085a74f2f5f045125fd2f84e4cf6fb

- SHA3-512:
ec6d6ceb283f39efd1673931366cc25a7dc366c90ac880a1c8738a384abf9b357fe0048b6f6f69fae9e5b204e9579ba9064b62083f47e867bc83106963c26147

Zgostitveni algoritmi se med seboj razlikujejo po postopku izvedbe, hitrosti in dolžini rezultata. Vsak algoritem in njegove različice imajo različno definirano dolžino izhoda. Algoritem MD5 je najhitrejši algoritem, vendar je njegov izhod najkrajši.

Algoritem SHA 3 je bil izbran na mednarodnem tekmovanju. Mednarodni inštitut za standarde in tehnologijo (angl. *National Institute of Standards and Technology*) skrbi, da se pravočasno razvijejo novi in zmogljivejši zgostitveni algoritmi. Vzporedno z izboljševanjem računalniške tehnologije skrbi za varnost pred kolizijami in po potrebi razpiše tudi tekmovanje za boljši in močnejši algoritem (Stevens, 2012).

Slika 8: Primer dveh različnih sporočil in iste kontrolne številke



Problem z zgoščevalnimi algoritmi, ki ga srečamo v praksi, je kolizija. To pomeni, da obstajata dve različni smiselni sporočili, ki vrneta isto kontrolno vsoto. Primer prikazuje Slika 8. Slika je simbolična. Kolizija je odvisna tudi od števila bitov kontrolne vsote. Ena izmed lastnosti večine boljših zgostitvenih algoritmov je neobstoj formalne metode, ki bi za kontrolno vsoto lahko izračunala vhodni niz (kolizijo). Velja tudi, da imajo dobri zgostitveni algoritmi poseben učinek (angl. *avalanche efect*). Če vhodno sporočilo malenkostno spremenimo, se izhod drastično spremeni (Kovačič, Žagar & Štehalnik, 2010).

Če se na kratko dotaknemo zgostitvenega algoritma MD5, ki so ga razvili leta 1991 – algoritem se je uporabljal za overjanje digitalnih potrdil, danes pa se uporablja za zagotavljanje integritete podatkov v digitalni forenziki. Leta 2005 so Arjen Lenstra, Xiaoyun Wang in Benne de Weger prikazali izdelavo dveh X.509 certifikatov z različnimi javnimi ključi in isto MD5 zgoščeno vrednostjo. To pomeni, da sta dve popolnoma različni veljavni sporočili imeli isto kontrolno vsoto.

Leto dni kasneje je Vlastimil Klima objavil algoritem, ki je bil sposoben poiskati kolizijo na prenosnem računalniku v eni minuti. Običajno so znani napadi, ki omogočajo izračun kolizije na podlagi dveh poljudnih nizov vhodnih podatkov v samo nekaj urah. Danes v izogib kolizijam algoritma MD5 nihče več ne uporablja.

Vloga varnostne tehnologije omogoča preslikavo določenih formalnih postopkov v popolno elektronsko obliko. Kriptografski algoritmi so bili med drugim razviti za okoliščine, ko želimo doseči legitimnost določenih podatkov ali zapisov v elektronski obliki (dokument, faktura, pogodba in podobno), poudarja Jerman Blažič (2006).

Pred vdori v baze podatkov z občutljivo vsebino se morajo zavarovati tudi velike organizacije (predvsem finančne institucije). V mislih imamo predvsem spletno ribarjenje (angl. *phishing*). S slednjim je označeno pridobivanje gesel, uporabniških imen in podatkov o kreditnih karticah s pomočjo elektronske pošte, preko telefona ali spletnih strani znanih podjetij (predvsem bank, finančnih ustanov in spletnih prodajaln) z namenom kraje denarja (Skrt, 2004; Microsoft, 2016). Je ena od najbolj priljubljenih metod za krajo osebnih podatkov naivnih uporabnikov spleta. Goljufi in hekerji prek elektronske pošte uporabniku posredujejo povezavo do spletnega mesta, ki je na las podobno tistemu, ki ga ta pogosto obiskuje (Gmail, Paypal, Facebook). Skripta v ozadju podatke, ki jih je nič hudega sluteči uporabnik vnesel v prijavni polji, nato posreduje lastniku lažne spletne strani, posameznika pa praviloma preusmeri na pravo spletišče, kjer se mora prijaviti še enkrat. Spletni uporabniki v večini primerov ne posumijo, da se dogaja nekaj sumljivega, temveč proces, ki traja dlje kot običajno, dojemajo kot anomalijo. Ribarjenje je prvovrsten primer družbenega inženiringa. Kiberkriminalci, ki se ga lotijo, praviloma stavijo na izvabljanje osebnih podatkov z nagradnimi igrami ali pa, tako kot slovenske banke, zahtevajo preverjanje.

Članice Združenja bank Slovenije, banke in hranilnice od svojih komitentov nikoli ne zahtevajo posredovanja zaupnih osebnih podatkov preko elektronske pošte (Tomšič, 2015).

2.8 Načini uvedbe

Poznamo štiri načine prehodov na novo uporabo informacijskih sistemov oz. aplikativnih rešitev. Med štiri načine uvrščamo vzporedno uvedbo, neposredni pristop, pristopni oz. fazni pristop in pilotni način uvedbe. Za uvedbo digitalnega podpisovanja v izbrano banko se sklicujemo na dva preverjena pristopa za implementacijo novosti v velikih družbah. Prvi je spreminjanje poslovnih procesov »od spodaj navzgor« (angl. *Bottom-up*) in drugi »od zgoraj navzdol« (angl. *Top-down*). V nadaljevanju ju bomo podrobneje opisali.

- **Pristop od spodaj navzgor**

Pristop od spodaj navzgor je fazni oz. postopni pristop in pomeni sodelovanje s skupino pri izvedbi projekta. Člani skupine so vključeni pri vsakem koraku procesa upravljanja. Odločitve sprejemajo skupno, torej kot celotna skupina. Izbira metod in izvedba nalog je predmet celotne skupine. Proces načrtovanja je zagotovljen s pomočjo večjega števila ljudi. Časovnica projekta, finančna sredstva in rezultat so transparentni. Za pristop velja, da je prilagodljiv in agilen. Zagotovljeno je sodelovanje skupin, s strani skupine pa izpeljana preobrazba procesov. Prav tako v tem primeru govorimo o visoki motivaciji, saj ljudje sodelujejo pri razvoju projekta (Filev, 2008).

Makar (2015) je prepričan, da je za določitev nalog zadolžena projektna skupina, ki naloge definira in jih razdeli po specifičnih skupinah. Za pravilno implementacijo oz. izvedbo projekta bo projektna skupina s skupnimi močmi članov, ki jo sestavljajo, poiskala vse zahtevane naloge in proučila njihove možnosti.

Rezultat pristopa od spodaj navzgor je jasna in zelo podrobna časovna premica, ki je hkrati časovno zamudna. Urnik je osnovan s strani neposrednih strokovnjakov, ki imajo izkušnje s projekti. Načrtovanje poteka dlje, vendar so naloge in opravila ter čas točno določeni. Prav tako v to skupino uvrščamo določitev vseh s projektom povezanih stroškov. Tehnika prav tako zagotavlja načrtovanje po mesecih.

Pri takem pristopu govorimo o visoki pokritosti uvajanja v zgodnji fazi. Investicija se povrne že zgodaj. Velja, da hitreje opazimo organizacijske spremembe in imamo večji vpliv na organizacijo.

Kot pozitivne lastnosti pristopa lahko štejemo še uporabniško in poslovno poznavanje storitve oz. produkta. Prednosti realizacije so vidne že v zgodnji fazi. Veliko ročnih procesov lahko zamenjamo z avtomatičnim načinom (IBM, 2015).

Vpeljava novosti v podjetje poteka počasi in postopoma. Poslovne procese pustimo takšne, kot so. Najprej novost implementiramo samo v določene procese in nato naprej glede na odziv. Govorimo o ekonomično enostavnejši izvedljivosti oziroma rešitvi.

- **Pristop od zgoraj navzdol**

Pristop od zgoraj navzdol je implementacija, ki pomeni enkratno celostno spremembo poslovanja. V istem trenutku preuredimo vse poslovne procese. Za podjetje to pomeni hiter preobrat, ki lahko predstavlja težavnejše obdobje.

Filev (2008) pravi, da ta pristop ostaja zelo priljubljen pri sodobnem upravljanju projektov. Pristop od zgoraj navzdol pomeni, da vsa navodila, smernice in cilje narekuje najvišje vodstvo (angl. *Top management*). Vodstvo zagotavlja vse napotke, informacije, načrte in osnovne procese. Vsa pričakovanja so predstavljena vsakemu udeležencu projekta. Prav tako v svojem članku navaja, da je pristop neprilagodljiv, birokratičen in zahteva celotno kontrolo. Problem tega pristopa je manjša motiviranost zaposlenih, saj se ti zavedajo, da njihovo mnenje ne šteje.

Zgoraj omenjeni pristop vključuje pričetek s projektnim ciljem in drobljenje slednjega na manjše pakete. Ta pristop deluje odlično, če so v njegovem okviru jasno določene podrobnosti projekta. Hkrati je pomembno, da ima vodja projekta jasno zastavljeno celotno sliko vpeljave projekta v organizacijo (Makar, 2015). Avtor kot prednost pristopa navaja, da so glavne naloge hitro določene, podrobnosti pa najdene malce kasneje v projektni skupini. Prav tako sta hitro zagotovljena osnovno in kadrovsko načrtovanje. Na drugi strani kot slabost označi možnost napačno določenih podrobnosti brez podrobnega pregleda s strani projektne skupine. Pri uporabi tega pristopa časovno načrtovanje in stroški niso natančno znani.

Pristop je taktičen in z omejenim obsegom. Povračilo investicije se pokaže kasneje. Manjši je vpliv na celotno organizacijo, višji pa so stroški uvajanja (IBM, 2015).

Kovačič (2010) trdi, da je celovita programska rešitev v celoti povezan in na poslovnem modelu organizacije temelječ sistem. Slednji ob uporabi informacijske tehnologije poslovnim procesom organizacije in z njo povezanim poslovnim partnerjem zagotavlja optimalne možnosti načrtovanja, razporejanja virov in izvajanja poslovnih procesov ter ustvarjanja dodane vrednosti.

S celostno informacijsko rešitvijo mislimo na vpeljavo sistema digitalnega podpisovanja v bančno poslovanje, ki bo zajemalo vse funkcionalnosti od digitalnega podpisovanja do hranjenja in upravljanja dokumentacije. Za izbrano banko bi bila takšna rešitev dokumentni sistem Adobe (angl. *Adobe Reader DC Pro*).

3 UVEDBA DIGITALNEGA PODPISA V IZBRANO BANKO

V Sloveniji skozi vrata bank trenutno vstopa veliko število komitentov. Od tega jih večina želi opraviti tako storitev, ki bi jo lahko ob primerni informacijski podpori opravila tudi iz domačega naslonjača. Na področju digitalnega poslovanja s komitenti se uporablja kvalificirano digitalno potrdilo za opravljanje nekaterih storitev v elektronskih bankah.

Seznanjeni smo z dejstvom, da v času pisanja magistrskega dela nobena izmed slovenskih bank v internih poslovnih procesih še ni uporabljala digitalnega podpisovanja. Enako lahko trdimo tudi v primeru zunanjih relacij (komitent-banka). Danes se kvalificirana digitalna potrdila večinoma uporabljajo za vstopanje v elektronsko banko in opravljanje tam določenih elektronskih storitev. V elektronski banki lahko z digitalnim podpisom sklenemo depozit, ostalih, zahtevnejših storitev, kot je na primer kreditna pogodba, pa ne. Na osnovi zapisanega lahko trdimo, da tehnologija digitalnega podpisovanja v bankah ni optimalno izkoriščena.

Kot trdita Kovačič & Bosilj Vukšić (2005), bodo v prihodnjih letih poslovno uspešna le podjetja, ki bodo ustrezno preuredila svojo organiziranost, procese in tehnološko infrastrukturo. Danes so naprednost, prvobit in hitrost poslovanja še toliko bolj pomembne.

Ferk (2012) trdi, da posamezno podjetje izbira med različnimi metodami za povečanje učinkovitosti, če se odloči za celostne, vseobsegajoče ukrepe. Cilj vsakega podjetja je skrajšati pretočni čas materiala in aktivnosti ter povečati kakovost izdelkov in storitev, torej povečati učinkovitost podjetja. Bistvo ni samo v zmanjševanju stroškov, temveč tudi v povečanju dodane vrednosti.

Ne glede na posamezne analize in raziskovanja se procesno usmerjeno razmišljanje začne in konča v glavah zaposlenih v podjetju. Iz tega razloga jih je treba aktivno vključiti v analiziranje vseh operativnih poslovnih dogajanj, ki presegajo meje posameznih oddelkov.
V procesnem menedžmentu tako govorimo o treh najpomembnejših pojmih, med katerimi so zadovoljstvo kupcev (kakovost storitev in odpravljanje napak), čas (zmanjšanje potrebnega časa) in stroški (zmanjšanje stroškov).

Vsakodnevno se podjetja odločajo, ali naj potrebno orodje, rešitev ali storitev izdelajo sami ali jih kupijo na trgu. Ko/če se odločijo, da bodo potrebno storitev ali orodje izdelali, je naslednje logično vprašanje, ali imajo na razpolago vse potrebne prvine poslovnega procesa. Če tega nimajo, je vanje potrebno investirati. Odločitev narediti ali kupiti temelji na stroškovni privlačnosti obeh alternativ in jo je treba preverjati ter sprejemati za vsak konkreten primer posebej (Rebernik, 1999).

Poglavje v nadaljevanju nas bo seznanilo s pregledom obstoječega stanja v izbrani banki in spremembami stanja z uvedbo digitalnega podpisovanja. Hkrati se bomo osredotočili na potrebne investicije za njegovo izvedbo. Prav tako bomo spoznali trenutno dostopne

tehnične rešitve za digitalno podpisovanje na trgu. Ob zaključku bomo opravili metodo točkovanja in analizo stroškov ter koristi izbrane programske rešitve.

3.1 Pregled obstoječega stanja

V izbrani banki trenutno obstaja več nivojev potrjevanja. Govorimo o podpisovanju s strani posameznega zaposlenega, stranke, vodje, direktorja in skupine zaposlenih. S slednjim imamo v mislih predvsem specifične skupine (skupina za marketing, skupina za reševanje reklamacij strank) in odbore odločanja (kreditni odbor).

Danes vsaka organizacija izbira med več različnimi načini sodelovanja, podpisovanja ali potrjevanja. V izbrani banki uporabljamo naslednje tipe zunanjega in notranjega potrjevanja:

- **ustni dogovor** – redka oblika dogovora, ki pa je v posameznih primerih še vedno prisoten. Običajno zaposleni po njem posegajo na sestankih. Rezultat dogovora je kasneje v večini primerov prisoten v zapisniku;
- **parafiranje** – interna pravila banke zahtevajo uporabo parafiranja za zaposlene v banki in stranke. Več strani dolgi, pomembni dokumenti in pogodbe morajo biti parafirani. V primeru kreditne pogodbe mora biti vsaka stran posebej parafirana s strani stranke in komercialista v banki. S tem stranka potrjuje, da je s celotno vsebino seznanjena. Hkrati se v izogib morebitnim spremembam in zamenjevanju strani zagotovi predčasna varnost. Zaščitita se obe poslovni strani, torej tako banka kot stranka, pred možnostmi ponareditve dokumenta ali celo izgubo dokumenta. Pri internih zadevah zaposleni s parafo označi, da je dokument prebral, preveril in je z vsebino seznanjen. Parafiranje ni določeno in ni niti opredeljeno z nobenim pravnim aktom;
- **elektronska pošta** – elektronsko pošto v izbrani banki uporabljamo pri vsakdanji komunikaciji. Formalna raba poteka preko posameznega zaposlenega, ko se dogovarjamo o pomembnih vsebinah, vezanih na banko, kot so novi produkti, sodelovanje z zunanjimi podjetji, prijava na razpise, sestanki, potrditve zapisnikov, reševanje reklamacij in podobno. Neformalno dogovarjanje predstavlja neke vrste osebne zadeve posameznega zaposlenega, kot so dopust, prihod in odhod na delovno mesto, sprememba osebnih podatkov, krajša odsotnost, organizacija poslovne poti, izobraževanja ali seminarji;
- **lastnoročno podpisovanje** – gre za trenutno najpogostejši tip potrjevanja v izbrani banki, ki se uporablja za podpisovanje vseh formalnih dokumentov. Pri razmerju stranka-banka najdemo primer, kot so kreditna pogodba, depozitna dokumentacija, obrazci za naročilo novih kartic in podobno. Podpisan je vsak obrazec o opravljeni storitvi med stranko in banko. Samo na tak način ima banka dokazilo, kaj je naredila po naročilu stranke ali za kaj se je stranka obvezala. Lastnoročno se podpisuje tudi interne dokumente, ki jih zaposleni pripravljajo za višje nivoje odločanja. V tem primeru najdemo predloge za spremembo ponudbe v izbrani banki, spremembe delovanja

informacijskih sistemov, uvedbo nove funkcionalnosti v elektronskem bančništvu, izdajo garancij, zahtevke za spremembo obrestnih mer v aplikativni podpori, različna poročila in še mnogo drugih dokumentov. Prav tako se lastnoročno podpisujejo pogodbe o zaposlitvi in dodatki k pogodbam. Izbrana banka v svojem registru hrani in vzdržuje lastnoročne podpise zaposlenih. Zakona, ki bi definiral lastnoročno podpisovanje, nimamo. Pristnost podpisa ugotavlja sodišče s pomočjo grafologa;

- **žigosanje** – uporaba žiga v izbrani banki je pomembna predvsem v primeru posredovanja dokumentov s strani banke stranki. Prav tako je uporaba žiga obvezna za vse strogo formalne oblike posredovanja zadev, kjer so vključeni notar, višji nivoji odločanja, uprava banke, pravne službe in druge službe, ki poslujejo z zunanjimi partnerji. V izbrani banki se uporablja za prijavo na posebne razpise, oddajo dokumentacije poslovnim partnerjem, Združenju bank Slovenije, poročanje evropskim inštitucijam in poročanje Banki Slovenije. Žigosanje je na splošno opredeljeno s statutom. Če podjetje posluje z žigom, ga mora uporabljati, v nasprotnem primeru pa mora biti jasno navedeno, da podjetje posluje brez njega. Žig je uveljavljena praksa in zagotavlja verodostojnost dokumentov. Brez žiga je dokument neveljaven. Vsi žigi v izbrani banki so označeni z zaporednimi številkami in zavedeni v »registru žigov« z namenom dodatne kontrole, da je dokument res izdal podpisnikov oddelek, področje, sektor;
- **z notarjem** – dogovor skupaj z notarjem je zelo specifična oblika dogovora, ki ima najvišjo pravno veljavo. Uporablja se v primerih, kjer je potrebno zagotoviti istovetnost podpisnikov dokumenta. Najpogostejši primer so hipotekarne pogodbe, kjer se zahteva tudi notarski zapis, ki je nujen za vknjižbo v zemljiško knjigo. Dogovori pri notarju zahtevajo dodaten čas in dodatne stroške.

Hramba dokumentov v slovenskih bankah je določena z zakonom o varstvu dokumentarnega in arhivskega arhiva. Trajanje hranjenja dokumentov je določena z Zakonom o varstvu osebnih podatkov (ZVOP-1).

Hramba celotne dokumentacije v izbrani banki je odvisna od posamezne storitve oziroma vrednosti dokumenta. Za interno dokumentacijo obstajajo pravila, ki so določena z akti izbrane banke. Običajno se vsi pomembnejši dokumenti in sklepi hranijo v posebnem elektronskem arhivu, ki je v lasti banke. Za arhiviranje takih dokumentov skrbijo posebne službe v banki ter ostali za to zadolženi zaposleni. Dokumenti se običajno hranijo v fizični obliki v ognjevarnih omarah.

Hramba vseh dokumentov, ki so podpisani s strani stranke, poteka skladno z zakonodajo. Pravila so določena za vsako storitev posebej – za kreditno in depozitno pogodbo denimo velja, da ju je zaradi narave posla potrebno hraniti še pet let po preteku pogodbe. Vsi dokumenti, ki nosijo ime stranke, se digitalizirajo in pošljejo na elektronsko hrambo zunanjemu podjetju. Tam se hranijo v skladu z zakonsko predpisanim rokom. Uporaba slednjih je enostavna, saj jih je mogoče datumsko in vsebinsko poiskati. Poiščemo jih lahko po imenu, priimku in opravljeni storitvi. V primeru potrebe po dokumentu (npr.

sodnega spora) so dokumenti enostavno dosegljivi. Dokumentacija v izvirniku se po kontroli s strani zaledne službe uniči. Pri enostavnejših bančnih storitvah poteka neposredno elektronsko arhiviranje. Originalni dokument ostane v lasti stranke kot dokazilo o opravljeni bančni storitvi.

3.2 Poenostavitev poslovnih procesov z uporabo digitalnega podpisa

Poslovni proces (ang. *Business Process BP*) je skupek logično povezanih izvajalskih in nadzornih postopkov ter aktivnosti, katerih posledica oziroma izid je načrtovani izdelek ali storitev (Kovačič & Bosilj Vukšič, 2005). Je način, kako določena organizacija posluje, ustvarja vrednost in skrbi za svojo organizacijsko strukturo (Damij, 2009). Je tudi povezan nabor dejavnosti in nalog, ki imajo namen vhodnim elementom v proces za naročnika ali kupca dodati uporabno vrednost na izhodni strani procesa (Kovačič & Bosilj Vukšič, 2005).

Nadja Damij (2009) pojasnjuje, da je učinkovita in uspešna izvedba poslovnega procesa pogojena s sodelovanjem različnih poslovnih funkcij, torej s kvalitetno organiziranim delom različnih oddelkov in enot organizacije.

Čas oziroma hitrost je pomemben element v poslovnih procesih. Bistvenega pomena je predvsem v velikih organizacijah, ki z informacijsko tehnologijo zaostajajo za manjšimi sistemi.

Z modernizacijo in vse večjim elektronskim posredovanjem dokumentov je mogoče pospešiti tok dokumentov ter vzpostaviti vse večji nadzor nad posameznimi procesi. Tako je dokumentom omogočen hitrejši vstop v poslovne procese in zagotovljeno hitrejše ter nadzorovano potovanje skozi organizacijo. S tem se v organizaciji znižajo stroški poslovanja, povečata pa se kakovost poslovanja in zadovoljstvo strank (Microcop, 2015). To posledično pomeni tudi hitrejšo izvedbo poslov in več dobička.

Skladno z zgornjim si poglejmo, kako lahko digitalno podpisovanje v izbrani banki izboljša trenutno stanje.

V izogib morebitnim sporom z vidika nedokazljivosti je ustni dogovor smiselno zapisati in potrditi kot zapisnik ali elektronsko sporočilo.

Z digitalnim podpisom je najenostavneje nadomestiti lastnoročni podpis ali parafo na natisnjenih dokumentih. Takšni dokumenti nastanejo primarno v elektronski obliki in so kasneje natisnjeni. S tem mislimo na dokumente, nastale v Microsoft Wordu, formatu PDF ali v programu za elektronska sporočila. Vse tri omenjene dokumente je mogoče digitalno podpisati v obliki dokumenta z logotipom izbrane banke. Na tak način zagotovimo skladnost poslovanja z internimi pravili banke.

Dokumente, ki nastanejo pri poslovnih partnerjih ali strankah in jih je potrebno lastnoročno podpisati, lahko preslikamo v elektronsko obliko ter prav tako podpišemo s kvalificiranim digitalnim potrdilom.

Dokumente, ki jih žigosamo v izbrani banki, bi lahko določeni zaposleni podpisali z digitalnim certifikatom banke. S tovrstnim certifikatom ne bi smel operirati vsak zaposleni. Za njegovo uporabo bi bili pooblaščeni direktorji področja in vodje oddelkov. Uporaba bi bila lahko natančneje definirana z internimi akti banke.

Za posebne namene bi banka lahko uporabljala tudi certifikate posameznih oddelkov ali sektorjev – slednji bi bili v rokah vodilnih kadrov. Digitalno podpisane dokumente bi lahko dodatno opremili s sliko »žiga« visoke resolucije.

Pogodbe, garancije, notarske zapise, vpise v zemljiško knjigo in ostale dokumente, kjer morajo biti podpisi potrjeni s strani notarja, je mogoče zamenjati še s strani notarja pridobljenim dokumentom, ki je digitalno podpisan. Dokument bi lahko posameznik digitalno podpisal in ga kasneje posredoval notarju. Nato bi ga obiskal in tako omogočil preverbo istovetnosti. Po dejanski preverbi bi notar dokument podpisal s svojim kvalificiranim digitalnim potrdilom.

V ZDA že obstaja elektronsko notarstvo (angl. *eNotary*), ki pomeni elektronsko overjanje dokumentov. Digitalno podpisane elektronske dokumente notar potrdi z digitalnim certifikatom. Ena od metod, ki jih elektronsko notarstvo uporablja, sta digitalni podpis in notarski digitalni pečat za overjanje teh dokumentov, ki so potrjeni z digitalnim certifikatom. Elektronsko notarstvo je proces, kjer notar elektronski dokument potrdi z elektronskim podpisom in notarskim pečatom s svojega zasebnega ključa. Vsi podpisniki morajo biti sicer pri notarju prisotni tudi fizično, s čimer ta preveri njihovo identiteto, tudi če so podpisi že v digitalni obliki (Stoney, 2015).

V izbrani banki je smiselno vsem digitalno podpisanim dokumentom pripeti tudi časovni žig in s tem zagotoviti točen čas nastanka dokumenta ter podpisov. Tako zagotovimo revizijsko sled, ki je pomembna za vse zaposlene in revizorje.

Če poslovanje z dokumenti v fizični obliki popolnoma digitaliziramo, vsekakor pospešimo tok poslovanja, ki lahko pomeni tudi časovni in finančni prihranek.

3.3 Hramba digitalnih dokumentov

Za namene hrambe dokumentacije in z vidika ustrezne sledljivosti celotne dokumentacije v poslovnem sistemu je potrebno zagotoviti centralno arhiviranje.

Centralno arhiviranje predstavlja shranjevanje, obdelovanje in sledenje elektronskim dokumentom v organizaciji. Programska oprema zagotavlja kontrolo in organizacijo vseh dokumentov v podjetju na enem mestu. Takšni napredni sistemi zagotavljajo (AIIM, 2015):

- vstop in izstop dokumentov ter omejevanje dostopa posameznikom ali skupinam;
- zagotovljena je kontrola »verzij«, shranjene pa morajo biti vse spremenjene verzije;
- možnost prehoda na zadnjo ali predzadnjo verzijo, v kolikor se zadnja uniči ali spremeni;
- zagotovljena je revizijska sled posameznih dokumentov, pri čemer se ve, kdo je kdaj in kaj spremenil v posameznem dokumentu skozi njegov življenjski cikel;
- dokumenti so popisani, čakajo na podpis in so »časovno ožigosani«.

Sistem mora zagotavljati več različnih in kakovostnih funkcionalnosti. Omogočati mora ustvarjanje dokumentov, spreminjanje, posredovanje v podpisovanje, spremljanje trenutnega stanja, opozarjanje, da je dokument v podpisu, vmesno spreminjanje, podpisovanje, hranjenje dokumentov po področjih, procesih in upravljanje teh dokumentov, ko se nahajajo v arhivu. Zagotovljeno mora biti tudi iskanje po podpisnikih, času in vseh vsebinskih izrazih. Pomembno je, da do dokumentov dostopajo samo pooblaščene osebe.

Za izbrano banko so primerni dokumentni sistemi, ki imajo podporo za digitalno podpisovanje. Pomembno je uporabljati sistem, ki zagotavlja ustrezno hrambo dokumentov in upravljanje s slednjimi, da omogoča hitro in učinkovito iskanje dokumentov po vsebini, podpisnikih in ključnih besedah. V primeru iskanja po zgodovini ponudbe, bančnih primerov, stare prakse, različnih prednosti in slabosti preteklih dokumentov ter za izvedbo poročil je zelo pomemben čas iskanja. Prav tako je potrebno dokumente poiskati in jih urediti, v kolikor banko obišče revizija ali kakšna druga nadzorna služba. To lahko realiziramo le s pravilnim načinom in z zaporedjem hranjenja dokumentov, še najenostavneje pa neposredno elektronsko.

Hranjenje digitalnega dokumenta je v primerjavi z dokumentom v fizični obliki lažje, enostavneje in ceneje. V praksi se pravzaprav ne zavedamo, kdaj je dokument arhiviran in shranjen v ustrezno elektronsko mapo, saj postopek poteka popolnoma avtomatsko. Možnosti iskanja podpisanih dokumentov so široke. Dostop do dokumentacije je možen na več načinov in z različnih lokacij. Tudi takrat, ko je posameznik v tujini, lahko v trenutku poišče potrebne dokumente. Do želenega dokumenta lahko dostopa iz druge poslovalnice ali celo od doma.

Samo podpisovanje ne vključuje čakanja na podpisani dokument. Podpisnik po elektronski pošti ali pripadajoči mobilni aplikaciji prejme opozorilo, da ga čaka dokument za podpis. Prav tako je mogoče poskrbeti za ustrezno zaporedje podpisnikov in časovno identificirati

podpis. V kolikor pride med podpisovanjem do sprememb, pretekli podpisi postanejo neveljavni in podpisovanje se mora ponovno vzpostaviti.

3.4 (Kvalificirano) digitalno potrdilo za zaposlene v izbrani banki

V izbrani banki obstaja več različnih načinov posredovanja kvalificiranih digitalnih potrdil zaposlenim.
Izbrana banka bi lahko sama ustanovila certifikatno agencijo. V okviru slednje bi lahko ustvarila več kvalificiranih digitalnih potrdil in jih nato dodelila svojim zaposlenim. Poskrbeti bi morala za npr. petletno zamenjavo javnih in zasebnih ključev. Za interno rabo certifikatna agencija ne potrebuje vpisa v Register overiteljev v RS, saj gre za navadno digitalno potrdilo. V kolikor je slednje potrebno za podpis pogodb z dejansko pravno veljavo, je potrebno zagotoviti kvalificirano digitalno potrdilo. Če certifikatna agencija ni vpisana v Register overiteljev, to pomeni, da digitalni podpis ne izkazuje enake pravne veljavnosti kot lastnoročni podpis.

Izbrana banka bi lahko kupila kvalificirana digitalna potrdila za svoje zaposlene pri certifikatni agenciji. Ta možnost je z organizacijskega vidika enostavnejša, saj je vzpostavitev lastne certifikatne agencije zahteven postopek.

Izbrana banka bi lahko svoje zaposlene napotila v javno certifikatno agencijo, kjer bi pridobili lastno kvalificirano digitalno potrdilo. Ta način je za banko cenovno ugoden, enostaven in varen, saj je proces pridobivanja kvalificiranega digitalnega potrdila preložen na zaposlenega. Že danes več zaposlenih uporablja elektronsko banko in dostopa do ostalih javnih elektronskih storitev s kvalificiranim digitalnim potrdilom SIGEN-CA.

Za varnost digitalnih potrdil mora vsak zaposleni poskrbeti sam. Certifikat je potrebno hraniti na šifrirnem ključu USB, na pametni kartici ali na računalniku. Lesjak (2015) trdi, da zelo visok nivo varnosti za hranjenje zasebnega ključa zagotavlja pametna kartica, s katere je praktično nemogoče razkriti zasebni ključ. Zaposleni v izbrani banki bi lahko za namen hrambe uporabljali tudi svoje službene kartice za kontrolo dostopa. Kvalificirano digitalno potrdilo bi v izbrani banki lahko uporabili tudi za prijavo v lokalno računalniško omrežje z oddaljene lokacije.

Veljavnost digitalno podpisanih dokumentov ni povezana z veljavnostjo kvalificiranega digitalnega potrdila. Slednje običajno velja pet let, po tem obdobju pa ga je potrebno obnoviti. Obnovimo ga lahko že dva meseca pred potekom starega potrdila, kar pomeni, da lahko s kvalificiranim digitalnim potrdilom dokumente digitalno podpisujemo neprestano. Vsebina dokumenta, ko ga enkrat digitalno podpišemo, je podpisana in veljavna v skladu z dogovorom. Veljavnost potrdila lahko enačimo z osebno izkaznico, ki jo po preteku veljavnosti enostavno obnovimo (Ministrstvo za javno upravo, 2015a).

3.5 Pregled tehničnih rešitev na trgu

Tako domači kot tuji trg organizacijam ponuja rešitve, ki zagotavljajo elektronsko podpisovanje in centralno arhiviranje dokumentov. V magistrskem delu se osredotočamo na tri, po našem mnenju, globalno in kakovostno priznana podjetja, ki zagotavljajo različne rešitve. Opisali bomo celostno komercialno, odprtokodno in komercialno rešitev.

3.5.1 Celostna komercialna rešitev

Kot prvo možnost bomo proučili rešitev podjetja Adobe, ki so jo v angleščini poimenovali *Adobe Document Cloud eSign*.

Adobov dokumentni sistem predstavlja celostno rešitev za kakršno koli družbo, tudi finančno institucijo. Omogoča nam, da z nekaj kliki posredujemo dokument v podpis določeni osebi ob določenem času. Dokument najprej pripravimo, potem pa posredujemo v podpis eni ali več osebam. Avtomatični tokovi dela izvedejo ustrezno predlogo dokumenta in zagotovijo, da je vsak korak narejen v pravilnem zaporedju.

Rešitev Adobe ne zagotavlja izdelave dokumenta, ampak samo napredno upravljanje z dokumenti. Dokumente mora izbrana banka ustvariti z drugo aplikacijo (npr. Microsoft Office, Libre Office). S sistemom Adobe lahko sledimo dokumentom z različnih lokacij. V trenutku lahko preverimo, v katerem stanju se dokument nahaja, vključno z njegovo zgodovino (kdaj je odprt, podpisan in vrnjen). Omogoča nemoteno poslovanje ne glede na fizično lokacijo posameznika. Delo poteka enako, nova je le aplikativna podpora na računalnikih, na mobilnih telefonih ali tablicah.

Rešitev Adobe se lahko prilagodi lokalni zakonodaji in pravilom izbrane banke. Vsi dokumenti se nahajajo v oblaku ali na lokalnih strežnikih. Omogočeno je napredno iskanje po že podpisanih dokumentih. Prav tako se v okviru podpisovanja in iskanja dokumentov lahko definira skupine uporabnikov in zagotovi, da imajo do določenih dokumentov dostop omogočen samo pooblaščeni ljudje.

Izbrana banka je finančna institucija, ki svojih podatkov ne more zaupati drugim podjetjem (računalništvo v oblaku). Podatki so zaupne narave in zelo dragoceni. Kot ugledna ustanova si ne more privoščiti niti manjše možnosti zlorabe. Banka zato interne informacije hrani le na lastnih strežnikih. V okviru možnosti Adobe Document Cloud eSign se lahko vsi digitalno podpisani dokumenti in njihova celotna zgodovina hranijo na lokalnih strežnikih izbrane banke.

3.5.2 Odprtokodna rešitev

Z odprtokodno rešitvijo (angl. *open-source*) imamo v mislih aplikacijo Libre Office, izdano pod odprtokodno licenco. Libre Office je pisarniški paket z več programi, ki skupaj

sestavljajo najobsežnejšo prosto rešitev na trgu. Zajema program za pisanje, oblikovanje tabel in grafikonov, program za oblikovanje predstavitev in program za operiranje z bazami podatkov. Paket je zlahka mogoče nadgraditi in razširiti glede na potrebne funkcionalnosti ter predloge dokumentov, ki bi jih izbrana banka potrebovala. Kvaliteten oddelek IT se zlahka prilagodi potrebam izbrane banke. Program je enostaven za uporabo in prijazen do uporabnika.

Celotno upravljanje dokumentov in podatkov je možno na enem mestu brez stroškov licenc.

Paket lahko uporabljamo za izdelavo dokumentov, pa tudi za digitalno podpisovanje. Dokument, ki ga želimo digitalno podpisati, oblikujemo, shranimo in nazadnje elektronsko podpišemo s certifikatom. V postopku izvoza je omogočeno digitalno podpisovanje datotek PDF.

Ta rešitev omogoča, da dokumente digitalno podpišemo. Pošiljanje podpisanih dokumentov lahko poteka po elektronski pošti, vendar gre v tem primeru za ročno posredovanje dokumentov od ene osebe do druge. Sledljivost, shranjevanje sprememb in končnih zadev ter iskanje po dokumentaciji mora izbrana banka zagotoviti sama. Prav tako sta v njeni domeni oblikovanje skupin in omejevanje dostopa do določenih dokumentov.

V tem primeru izbrana banka hrani dokumente na svojih strežnikih. Varnost podatkov je tako zagotovljena.

3.5.3 Komercialna rešitev

Rešitev za digitalno podpisovanje, ki je najbližje trenutni uporabljeni tehnologiji, je Microsoft Word, ki ga najdemo v okviru paketa Microsoft Office 365 Business Premium.

Microsoft Word omogoča uporabniku elektronsko in digitalno podpisovanje dokumenta. Dokument glede na potrebe izbrane banke oblikujemo in ustrezno pripravimo na podpis. Ob zaključku lahko v Microsoft Wordu izberemo funkcijo »Zavaruj dokument« in v okviru slednje dodamo digitalni podpis.

Pri tej rešitvi si mora izbrana banka prav tako zagotoviti ali izdelati lasten dokumentni sistem z vsemi funkcionalnostmi, ki bodo zagotovile ustrezno delovanje digitalnega podpisovanja.

Proces posredovanja digitalno podpisanih dokumentov od zaposlenega do vodje in/ali do direktorja bi lahko potekal preko obstoječe aplikativne podpore, ki omogoča posredovanje elektronskih sporočil. Za vodje in direktorje bi bilo smiselno, da imajo urejen dostop do službenih elektronskih sporočil tudi preko mobilnega telefona.

Primerjava vseh treh rešitev

V Tabeli 2 je prikazana primerjava zgoraj opisanih rešitev.

Tabela 2: Primerjava rešitev

	Cena v EUR	*Dokumentni sistem*	*Digitalno podpisovanje*	*Izdelava dokumentov*	*Opomba*
Adobe DC eSign	18,29 EUR /mesec/osebo	DA	DA	NE	Potreben je urejevalnik za urejanje besedil.
Libre Office	0	NE	DA	DA	Potrebna sta interna ekipa za integracijo Libre Office in dokumentni sistem.
Microsoft Office (Word)	Skladno s pogodbo oz. 10,50 EUR /mesec/ uporabnika	NE	DA	DA	Potreben je dokumentni sistem.

3.6 Finančne analize

Prvi korak pri prenovi obstoječega sistema predstavlja analiza projekta in njegovih alternativ.

V nadaljevanju bodo izvedene tri analize. Ugotovljeno bo, na kakšen način je mogoče preoblikovati poslovni sistem v za vse prijaznejši in sodobnejši elektronski sistem z digitalnim podpisovanjem, pa tudi kolikšni so stroški uvedbe slednjega v izbrano banko.

Omejitve za oba primera so predstavljene v nadaljevanju.

- Študija bo izvedena na primeru 1.000 zaposlenih v izbrani banki.
- V obeh primerih imamo brezplačno pridobljena digitalna potrdila od obstoječe certifikatne agencije (npr. SIGEN-CA).
- Zaposleni imajo shranjeno kvalificirano digitalno potrdilo na svojem službenem računalniku, po potrebi pa tudi na mobilnem telefonu ali tablici.
- Upoštevamo, da ima leto 252 delovnih dni.

3.6.1 Analiza 1: Uvedba celovite sistemske rešitve *Adobe Reader DC Pro*

Za uporabo celovite sistemske rešitve Adobe bi morala izbrana banka rešitev kupiti pri podjetju Adobe. Samo nakup in neposredna implementacija nista mogoča. Potrebno je izvesti tudi določene modifikacije, in sicer celoten sistem prilagoditi bančnim službam. Potrebno bi bilo urediti skupine, pooblaščene osebe, odgovornosti, nivoje podpisovanja in podobne stvari, ki morajo biti nedvomno določene vnaprej.

Začetni strošek, ki ga mora plačati izbrana banka, je 18,29 EUR osebo/mesec z letno zavezo (Adobe, 2015b). To pomeni, da letni stroški znašajo 219.480 EUR/leto. Poleg tega je potrebno upoštevati vsaj minimalno pomoč oddelka IT. Gre za vsaj eno osebo, ki bi lahko poskrbela za izobraževanje in izvedbo prilagoditev.

3.6.2 Analiza 2: Uvedba prostega paketa Libre Office

Uporaba paketa je brezplačna. Vsi stroški so povezani z zaposlenimi v IT, ki celoten pisarniški paket prilagodijo bančnemu sistemu. Za ustrezno digitalno podpisovanje je v tem primeru potrebno razviti vse nivoje podpisovanja in zagotoviti ustrezno ter varno upravljanje z dokumenti.

Delo mestne uprave z 850 zaposlenimi so leta 2012 v mestu Aizu-Wakamatsu z Microsoft Officea preusmerili na Libre Office. Celotna podpora za 500 računalnikov je bila zagotovljena s strani dveh zaposlenih v oddelku IT. 15 % poslovanja še vedno poteka preko aplikacije Microsoft Office (Enoki, 2012). Iz tega lahko sklepamo, da bi za spremembo internega bančnega poslovanja v izbrani banki na en paket Libre Office potrebovali štiri predstavnike IT, ki bi poskrbeli za načrtovanje, uvedbo, izobraževanje in izvedbo prilagoditev.

V primeru, da bi popolnoma opustili rabo Microsoft Officea, bi prihranek znašal 84.000 EUR letno, kar pomeni približno sedem evrov mesečno na uporabnika.

3.6.3 Analiza 3: Uvedba paketa Microsoft Office

Izbrana banka trenutno pri svojem poslovanju že uporablja paket Microsoft Office. Na računalnikih zaposlenih je nameščena starejša verzija, ki ne omogoča digitalnega podpisovanja dokumentov. Za digitalno podpisovanje bi bilo na vse računalnike potrebno namestiti nov Microsoft Office 365 Business Premium. Slednji omogoča tudi digitalno podpisovanje dokumentov. Letni stroški za zaposlene bi znašali 126.000 EUR. Za celotno vzpostavitev oz. nadgradnjo delovanja in izobraževanje bi potrebovali še dva zaposlena v oddelku IT.

3.7 Izbira ustrezne programske rešitve

Na osnovi metode točkovanja bomo izbrali najustreznejšo programsko rešitev za izbrano banko. Za najboljšo rešitev bomo opravili tudi CBA.

3.7.1 Metoda točkovanja

Tabela 3: Metoda točkovanja

	Obrazložitev kriterija	**Uteži**	**MW**	**LO**	**A DC**
Tehnične zahteve	skupaj	**0,3**			
skladnost s trenutnimi rešitvami	1 slaba skladnost, 10 zelo dobra skladnost	0,04	10	4	9
čas vpeljave	1 dolg čas vpeljave, 10 najkrajši čas pričetka z uporabo	0,07	10	1	8
odvisnost od zunanjih podjetij	1 odvisnost je najslabša, 10 odlična odvisnost	0,07	8	3	10
izdelava internega dokumentnega sistema za hrambo dokumentov	1 potrebna je nadgradnja, 10 brez nadgradnje	0,07	1	1	7
potrebno interno izobraževanje	1 izobraževanje je neizogibno, 10 izobraževanje je nepotrebno	0,05	8	1	4
Funkcionalnosti	skupaj	**0,4**			
podpora za podpisovanje iz mobilnih naprav	1 podpora ni zagotovljena, 10 podpora je zagotovljena	0,05	1	1	10
digitalno podpisovanje	1 ni zagotovljeno, 10 je zagotovljeno	0,1	10	10	10
časovni žig	1 ni omogočeno, 10 je omogočeno	0,07	10	1	10
možnost pošiljanja dokumentov neposredno v podpis	1 ni omogočeno, 10 je zelo dobro omogočeno	0,08	5	3	10
primernost za eksterno rabo	1 neprimerno za zunanjo uporabo, 10 zelo primerno za uporabo	0,05	8	8	9
enostavnost uporabe	1 neuporabna funkcionalnost, 10 odična funkcionalnost	0,05	8	6	9
Stroški	skupaj	**0,3**			
strošek nakupa licenc za digitalno podpisovanje	1 zelo visok strošek nakupa, 10 zelo nizek strošek nakupa	0,1	4	10	3
strošek nakupa dodatnih licenc za urejevalnike besedil	1 zelo visoki dodtani stroški, 10 zelo nizki dodatni stroški	0,1	10	10	1
strošek zunanjega svetovanja	1 zelo visoki stroški zvetovanja, 10 zelo nizki stroški svetovanja	0,1	10	2	7
	SKUPAJ	**1**	**7,48**	**4,82**	**7,31**

Izbiro programske opreme za izbrano banko bomo izvedli z metodo točkovanja. Omenjena metoda je najbolj razširjena metoda vrednotenja in izbiranja, pravimo pa ji tudi analitična metoda.

Postopek izvedbe metode točkovanja je predstavljen v nadaljevanju.

- Najprej določimo temeljna merila (kriterije) in jih po potrebi razčlenimo na podkriterije (podmerila).
- Za presojanje konkretnega kriterija je potrebno podrobneje poznati pomen vsakega posameznega kriterija v odnosu do ostalih kriterijev. V našem primeru je razpon kriterijev določen od 1 do 10.
- Vsem kriterijem v nadaljevanju določimo utež. Ta kaže, kakšen vpliv ima posamezen kriterij na izbiro oz. kakšna je njegova moč v primerjavi z drugimi kriteriji.
- Sledi dodeljevanje točk posameznemu kriteriju, čemur pravimo tudi problem dodeljevanja.
- Nazadnje sledita množenje točk z utežmi in skupen seštevek.

Za izvedbo metode točkovanja smo določili tri skupine kriterijev. Slednje smo izbrali skladno z zahtevami, ki bi jih izpostavila izbrana banka. Ločili smo jih na tehnične zahteve, funkcionalnosti in stroške. Iz Tabele 3 lahko vidimo, da ima glede na izbrane in opisane kriterije največ točk programska rešitev Microsoft Office. Takoj za njo je programska rešitev Acrobat Cloud DC eSign.

3.7.2 Analiza stroškov in koristi izbrane rešitve

Za izbrano banko je najugodnejša izbira programska rešitev Microsoft Office. Programsko izbiro smo izvedli z metodo točkovanja, v kateri je že upoštevana groba analiza stroškov in koristi, ki zadostuje za primerjavo. Za izbrano rešitev smo v nadaljevanju opravili podrobnejšo CBA (angl. *Cost – Benefit Analysis*), ki naj bi bila ekonomsko zanimivejša. CBA je pogoj za uspešno izvedbo projekta. Opredelimo jo lahko kot poslovno disciplino, ki združuje nabor opravil, tehnik in znanj, potrebnih za odkrivanje poslovnih potreb, poslovnih priložnosti, poslovnih izzivov in iskanje ustreznih rešitev zanje. Pri tem sledimo smernicam poznavanja poslovne analize (Business Analysis Body of Knowledge – BABOK), ki jih postavlja svetovno združenje poslovnih analitikov (angl. International Institute of Business Analysis).

Enačba 9 prikazuje vse denarne tokove D_k prihodnjih n let z diskontno stopnjo i, ki so zmanjšani za začetno investicijo I_0. Neto sedanja vrednost je ena od najpogosteje uporabljenih meril za presojanje smiselnosti investicijskega projekta. Upošteva vse denarne tokove podjetja in časovne vrednosti denarja (Berk, Lončarski & Zajc, 2002, str. 97). Za izračun neto sedanje vrednosti smo uporabili letno diskontno stopnjo, ki na letni ravni znaša 9 %.

$$NSV = \frac{D_1}{1+i} + \frac{D_2}{(1+i)^2} + \ldots + \frac{D_n}{(1+i)^n} - I_0 = \left(\sum_{k=1}^{n} \frac{D_k}{(1+i)^k} \right) - I_0 \qquad (9)$$

Tabela 4 prikazuje neto sedanjo vrednost (v nadaljevanju NSV) za Microsoft Office v izbrani banki.

Tabela 4: Analiza stroškov in koristi za programsko rešitev Microsoft Office

Leto	**1**	**2**	**3**	**4**	**5**	**Skupaj**
Stroški dokumentarnega sistema	-1.000.000					
Stroški vzdrževanja	-80.000	-80.000	-80.000	-80.000	-80.000	
Stroški letnega najema	-126.000	-126.000	-126.000	-126.000	-126.000	
Skupaj stroški	**-1.206.000**	**-206.000**	**-206.000**	**-206.000**	**-206.000**	
Prihranki ukinitev interne pošte in arhiviranja	100.000	100.000	100.000	100.000	100.000	
Prihranki brezpapirnate	900.000	850.000	800.000	750.000	700.000	
Skupaj prihodki	**1.000.000**	**950.000**	**900.000**	**850.000**	**800.000**	
Dobiček/Izguba	**-206.000**	**744.000**	**694.000**	**644.000**	**594.000**	
Kumulativa	-206.000	538.000	1.232.000	1.876.000	2.470.000	
Diskontirani stroški	-1.106.422	-173.386	-159.069	-145.935	-133.885	-1.718.699
Diskontirani prihodki	917.431	799.595	694.965	602.161	519.945	3.534.098
NPV	-188.990	626.209	535.895	456.225	386.059	1.815.399
ROI						182%
PP						4,85
i	0,09					

V izračunu so upoštevani dejavniki, predstavljeni v nadaljevanju.

- **Začetna investicija**: zajema stroške dokumentarnega sistema, kar pomeni načrtovanje, izvedbo in vzpostavitev celotnega dokumentnega sistema v izbrani banki.
- **Stroški letnega najema**: predstavljajo vsakoletni nakup licenc za Microsoft Office za 1.000 ljudi oz. računalnikov. Ena licenca stane 10,50 EUR na uporabnika na mesec, če

je sklenjen letni najem (Microsoft, 2016a). Poleg slednjega smo upoštevali še delo IT oddelka, ki mora vzpostaviti programsko rešitev, da se ta uspešno uporablja.

- **Skupaj stroški**: predstavljen je skupen seštevek vseh letnih stroškov, povezanih z uvedbo digitalnega podpisovanja.
- **Prihranki**: predstavljajo ukinitev fizičnega arhiviranja, interne pošte in prihranek papirja ter tiskalnikov.
- **Skupaj prihodki**: predstavljajo skupen seštevek vseh letnih prihodkov.

Pri izračunu smo upoštevali trajanje investicije v obdobju petih let. Programsko rešitev bi bilo smiselno izvesti, če je njegova NSV večja ali enaka nič. Če ima podjetje na izbiro več alternativ programske rešitve, bo izbralo tisto, ki ima največjo pozitivno NSV. V našem primeru NSV predstavlja 1.815.399 EUR, kar pomeni, da je projekt smiselno izpeljati.

Pri analizi smo upoštevali tudi donosnost investicije (angl. Rate On Investment – ROI). Donosnost investicije je kazalnik, s katerim primerjamo donose z investicijo v projekt. Pri našem izračunu je dobičkonosnost naložbe 182-%.

Prav tako smo pri analizi upoštevali kazalec dobe vračila vloženih sredstev (angl. Payback Period – PP). Izračun nam je pokazal, da se investicija povrne v petih letih.

4 PREDLOG REŠITVE ZA IZBRAN POSLOVNI PROCES

Ko uspemo elektronsko povezati večino svojih partnerjev, pa tudi zaposlenih, elektronsko poslovanje doseže največji poslovni učinek. Velja namreč, da le na tak način ukinemo ali vsaj minimiziramo količino tradicionalnih papirnih dokumentov (Lesjak, 2015).

V tem poglavju bomo opisali obstoječ poslovni proces v izbrani banki in prenovo slednjega z digitalnim načinom podpisovanja ter poslovanja.

Študija je neodvisna od izbrane infrastrukture v banki in predpostavlja, da je sistem digitalnega podpisovanja že vzpostavljen.

Izbrane poslovne procese bomo primerjali s klasično obliko podpisovanja na podlagi izbranih sodil. Slovar slovenskega knjižnega jezika z besedo sodilo označuje merilo, kriterij.

Za vsakršno analizo je zelo pomembna izbira ustreznega sodila, od tega pa tudi rezultat in ocenjevanje. Sodilo je mera, s pomočjo katere bomo lahko upravičili našo investicijo oz. posodobitev sistema poslovanja.

Za analiziranje obstoječega poslovnega procesa (angl. *AS-IS*) v izbrani banki smo določili ustrezna sodila. Izbrana sodila so veljavna v primeru uporabe klasičnega podpisovanja. V primeru digitalnega podpisovanja je vrednost izbranih sodil nič.

- Sodila, ki jih je mogoče finančno ovrednotiti, so:

  - strošek na stran dokumenta – kot strošek so upoštevane aktivnosti, med katerimi so tiskanje, papir, amortizacija, arhiviranje, uničenje dokumenta;
  - strošek na dokument – strošek zajema poštnino;
  - porabljen režijski čas na stran dokumenta – v ta čas štejemo tiskanje, digitaliziranje, kopiranje;
  - porabljen čas na dokument – sem so vključeni podpisovanje, rokovanje z dokumentom, priprave za pošiljanje, digitaliziranje v primeru dislocirane enote ter čas, ko v banki ni stranke.

- Sodili, ki izkazujeta nemerljive koristi, sta:

  - prihranek časa stranke (ni potreben obisk) in
  - prihranek na gorivu.

Obstajajo tudi indirektne koristi, ki jih je težje finančno ovrednotiti, in sicer:

- ne potrebujemo več arhiva v fizični obliki;
- ne potrebujemo zaposlenih v arhivu;
- ne potrebujemo razreza dokumentacije;
- prihranimo čas pri iskanju starih dokumentov.

V nadaljevanju je predstavljeno obstoječe stanje poslovnega procesa dokumentarnega poslovanja. Osredotočamo se na dokument bančne garancije.

4.1 Področje dokumentarnega poslovanja v izbrani banki

Opis problema

Bančna garancija je instrument zavarovanja, s katerim je mogoče zavarovati pogodbene obveznosti v domačem in mednarodnem poslovanju. Z bančnimi garancijami se zmanjšujejo nevarnosti med poslovnimi partnerji v primeru neplačila oziroma neizpolnjevanja drugih pogodbenih obveznosti v dogovorjenih rokih.

Garancija predstavlja prednosti tako za nalogodajalca kot za upravičenca. Za nalogodajalca je koristna, saj s pridobitvijo bančne garancije pogodbenemu partnerju dokazuje poslovno resnost in finančno stabilnost.

Prednost za upravičenca je v tem, da se s pridobljeno bančno garancijo izogne tveganju plačilne nesposobnosti pogodbenega partnerja in dobi nepreklicno obvezo banke za plačilo garancijskega zneska ob predložitvi pisne zahteve za plačilo ter izjave, da nalogodajalec garancije ni izpolnil pogodbenih obveznosti.

Načelo, ki ga mednarodna praksa dosledno spoštuje na področju garancij, plačljivih »na prvi poziv«, je »najprej plačaj, šele nato izpodbijaj zahtevek za plačilo«, čemur v angleščini pravimo »Pay first – argue later«.

Bančne garancije, plačljive »na prvi poziv«, po enotnem mnenju judikature in pravne znanosti predstavljajo samostojno abstraktno obvezo banke za plačilo garantiranega zneska pod pogoji, navedenimi v garanciji.

Glavne karakteristike bančne garancije so:

- popolna ločenost garancije od osnovnega posla (neakcesornost);
- samostojnost in abstraktnost obveze banke;
- obveza plačila garantnega zneska pod pogojem, da upravičenec izpolni pogoje, navedene v garanciji.

Z garancijami (tako z domačimi kot s tujimi) se je mogoče zavarovati pred različnimi tveganji, npr. za pravočasnost plačila, plačilo carinskih dajatev, vračilo posojila, vračilo danega depozita, varščine ali avansa, dobro izvedbo posla, resnost ponudbe pri sodelovanju na razpisih, odpravo napak v garancijski dobi itd.

Udeleženci pri garancijskem poslovanju so predstavljeni v nadaljevanju.

- Nalogodajalec je v garanciji naveden kot stranka, ki je svoje obveznosti iz osnovnega posla zavarovala z garancijo. Nalogodajalec je lahko, a ne nujno, tudi stranka, ki da natančna navodila za izdajo garancije.
- Garant izda garancijo, neodvisno od osnovnega posla med nalogodajalcem in upravičencem. Pred morebitno zahtevo po izplačilu garantiranega zneska, ki ga mora plačati na prvi poziv, se zavaruje s pogodbo o izdaji garancije.
- Upravičenec z garancijo zavaruje svoje interese po osnovnem poslu, ki ga je sklenil z nalogodajalcem.

Garancije delimo na dve večji skupini glede na položaj banke v poslu. Ločimo izdane oz. nostro in prejete oz. loro garancije. Podpisovanje je predmet vsakega garancijskega pisma in dokumenta, imenovanega Notifikacija prejete garancije.

Za izdajo garancije je potrebno navesti:

- identiteto nalogodajalca;
- identiteto upravičenca;
- identiteto garanta, ki izdaja garancijo;
- številko garancije;
- osnovni posel, ki zahteva izdajo garancije.

Osnova za izdajo garancije je osnovna pogodba s poslovnim partnerjem, ki je lahko različnih oblik, npr. pogodba, predračun, račun, potrditev naročila, razpisna dokumentacija ipd. Iz osnovne pogodbe izhajajo obveznosti nalogodajalca garancije, ki jih banka z izdajo garancije prevzema nase. Izjemno pomembno je, da pred izdajo garancije natančno preberemo osnovno pogodbo in se z njo seznanimo.

Ko je garancija izdana, je garant ne more več preklicati. Le upravičenec jo lahko vrne oz. garanta sprosti vseh obvez po garanciji.

V nadaljevanju bomo natančneje opredelili postopek za izdajo garancije. Celoten poslovni proces je prikazan v Prilogi 3. Potrebo po garanciji izkaže podjetje. To posreduje podpisan in z žigom opremljen nalog za izdajo garancije skupaj z dokumentacijo, ki izkazuje predmet posla. S tem natančneje mislimo na sklenjeno pogodbo med nalogodajalcem in upravičencem garancije, izdan račun, razpisno dokumentacijo in podobno. Celotno dokumentacijo skrbnik podjetja pregleda in posreduje v oddelek garancij. Po potrebi prosi podjetje za dodatne dokumente ali dopolnitve. Za izdajo garancije v izbrani banki mora skrbnik podjetja pripraviti in nato pridobiti podpisan predlog za izdajo garancije, sklep ter pogodbo o izdaji garancije. Podpisi za predlog in sklep so interni ter običajno zajemajo podpis skrbnika podjetja (pripravljavca) in njegovega vodje ali direktorja. Pogodba o izdaji garancije pa je pogodba med banko (podpis skrbnika podjetja in direktorja sektorja) in stranko (podpis in žig podjetja).

Zaposleni v oddelku garancij pripravi osnutek garancije in jo posreduje podjetju v pregled. Po potrditvi osnutka s strani podjetja in prejemu vse potrebne dokumentacije s strani skrbnika podjetja (podpisani predlog, sklep in pogodba o izdaji garancije) zaposleni pripravi garancijo, jo podpiše in posreduje nadrejenim v podpis.

Garancije lahko upravičencu posredujemo na tri različne načine, in sicer v obliki pisma, kot notifikacijo na drugo banko in kot kontragarancijo na drugo banko. Slednji dve pomenita, da garancijo posredujemo preko sistema medbančnega pošiljanja šifriranih sporočil (angl. *Society for Worldwide Interbank Financial Telecommunication – SWIFT*). Zaposleni v oddelku garancij pripravi osnutek in ga natisnjenega posreduje v podpis vodji in direktorju. Osnutek garancije pospravi v mapo z ostalo dokumentacijo. Včasih je poleg garancije potrebno izdati tudi pismo o nameri za izdajo garancije. Slednje vsebuje enake podpisnike kot garancija.

Izdaja garancije v obliki pisma pomeni izdajo na predtiskanem papirju banke (papir s predtiskanim logotipom banke). Teh oblik garancij je največ, še posebej v primeru domačega poslovanja. Bančno garancijo v obliki pisma pripravi in oblikuje zaposleni. Zaposleni natisne štiri kopije garancije. Ena velja kot original, ostali dve pa kot kopija. Garancijo in kopije podpiše, odtisne žig, položi vse v podpisno mapo in nese v podpis vodji. Ko slednji podpiše, gre podpisna mapa v podpis direktorici sektorja. V podpisni mapi je lahko samo ena garancija s kopijami. Podpisovanje poteka z zadržkom glede na trenutne naloge, obveznosti in odsotnost nadrejenih.

Kopije garancij in vseh potrebnih dokumentov (npr. računov, razpisne dokumentacije, sklepov) se hranijo v izbrani banki, fizično, in sicer v posebnih mapah v ognjevarni omari. Hramba v pisarni traja tekom veljavnosti garancije. Po preteku veljavnosti mapo zaposleni prestavijo v arhiv banke. Tam počaka še nadaljnjih deset let, v izjemnih primerih pa tudi več. Na koncu sledi razrez celotne dokumentacije. Trenutno je poleg arhiviranja dokumentov v fizični obliki zagotovljeno tudi elektronsko arhiviranje. Celotna dokumentacija se digitalizira in shrani v e-arhiv.

Pri notifikaciji loro garancij izbrana banka ne prevzema lastne obveze po tej garanciji, temveč upravičencu slednjo le prenese. Kljub temu, da ne prevzema lastne obveze, pa preveri podpisnike na garanciji oziroma preveri pravilnost šifre sporočila, s katero je tuja banka poslala garancijo. Po preveritvi svojemu komitentu, upravičencu garancije, potrdi verodostojnost dokumenta in ga opozori na morebitne nevarnosti, ki bi zanj izhajale iz samega teksta brez poznavanja osnovnega posla. Izbrana banka upravičencu garancije posreduje dokument, ki ga podpišeta pripravljavec in vodja.

Iz Slike 9 lahko razberemo pregled naslednjih aktivnosti:

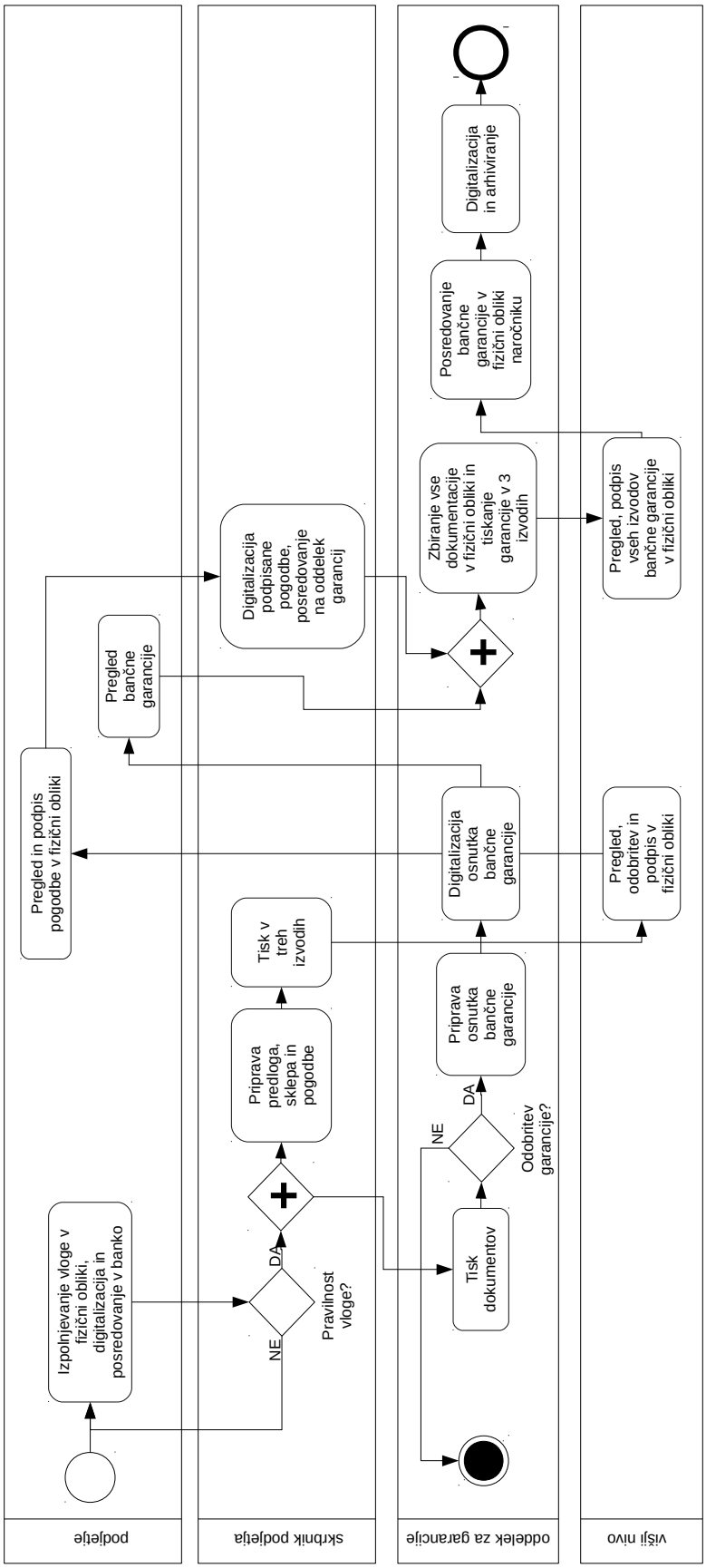
- število natisnjenih dokumentov (original in kopije): 12;
- število lastnoročnih podpisov: 30;
- število prenosov dokumentov: 9.

Predlog rešitve

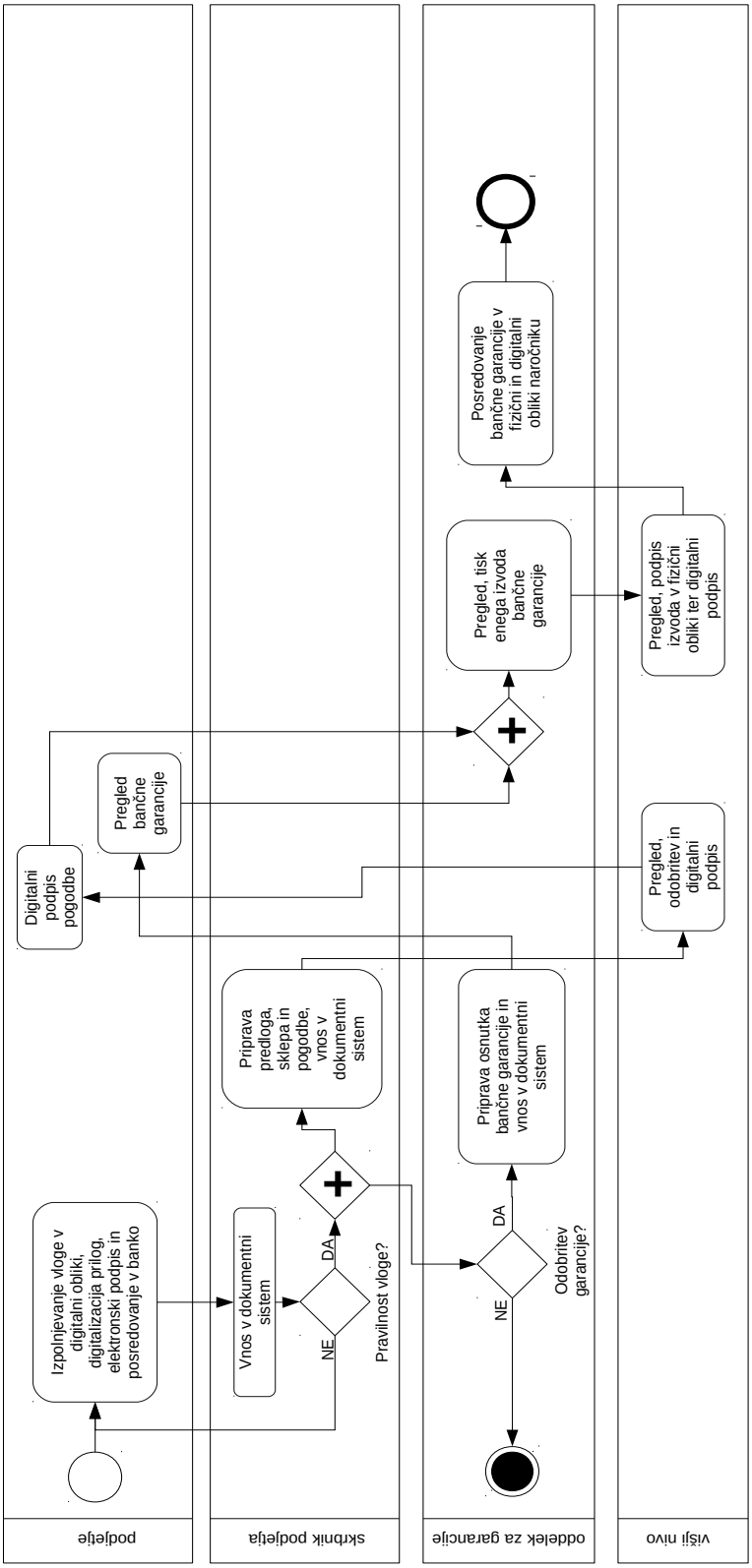
Predlagamo, da se v oddelek, ki je specializiran za izdajo garancij, uvede podpisovanje s kvalificiranim digitalnim potrdilom. Poslovni proces z uvedbo digitalnega podpisovanja je prikazan na Sliki 10.

Stranki bi lahko že na začetku poslovanja, ob oddaji naloga za izdajo garancije, omogočili, da nalog odda z digitalnim podpisom podjetja. Prav tako ima na nalogu možnost, da označi, ali bo vse dokumente podpisovala digitalno in ali ji zadostuje prejem garancije v elektronski obliki z digitalnim podpisom. Pri tem bi ji omogočili hitrejšo izdajo dokumenta.

Slika 9: Poslovni proces oddelka garancij po uvedbi digitalnega podpisovanja v formatu BPMN



Slika 10: Poslovni proces oddelka garancij po uvedbi digitalnega podpisovanja v formatu BPMN



Predlog, sklep, pogodbo in garancijo bi lahko vodje, direktorji in zaposleni podpisovali ter potrjevali elektronsko s kvalificiranim digitalnim potrdilom. To pomeni, da bi zaposleni z ustreznim programom pripravil dokument in ga digitalno podpisal ter posredoval vodji v potrditev. Vodja bi po elektronski aplikaciji dobil dokument v podpis, kjer koli bi se nahajal. Dokument bi elektronsko podpisal in ga posredoval naprej. Zaposleni bi lahko že od oddaje spremljal stanje dokumenta in komentarje ter po potrebi izvedel možne popravke.

V izjemnih primerih bi garancijo izdali tudi v papirni obliki. To bi za izbrano banko pomenilo en dokument, ki ne bi predstavljal večjih stroškov.

Iz Slike 10 lahko razberemo pregled naslednjih aktivnosti:

- število natisnjenih dokumentov (po potrebi): 1;
- število lastnoročnih podpisov (po potrebi): 3;
- število digitalnih podpisov: 13;
- število prenosov dokumentov: 6.

Omejitve pri študiji prihrankov

Pri študiji moramo upoštevati določene predpostavke, predstavljene v nadaljevanju.

- Pri opisu poslovnega procesa predpostavljamo, da imamo v izbrani banki že vse izpolnjene pogoje za digitalno podpisovanje. Zagotovljeni so certifikati in njihova hramba za vsakega zaposlenega.
- Predpostavljamo, da bi večino garancij lahko izdali v elektronski obliki.
- Pri poslovnem procesu se osredotočamo na samo izdajo bančnih garancij, brez upoštevanja sprememb garancij in pisem o nameri za izdajo garancije.
- Analiza ne vključuje dejstva, da zaposleni včasih pomotoma natisne dokument ali natisne garancijo z napakami.
- Predpostavljamo, da izbrana banka na letnem nivoju izda 2.500 garancij.
- Predpostavljamo, da izbrana banka v povprečju za izdajo ene garancije natisne 40 strani.
- Predpostavljamo, da je strošek na stran dokumenta 0,1 EUR.
- Predpostavljamo, da je čas na stran 20 sekund.
- Predstavljamo, da čas na dokument znaša deset minut, če poleg slednjega še ni obiska stranke pa 25 minut.
- Predpostavljamo, da strošek dela, ovrednoten s ČD (človek dan), predstavlja 200 EUR.

Študija prihrankov

Trenutno stanje predstavljamo v nadaljevanju.

- Sodila, ki jih je mogoče finančno ovrednotiti, so:

  - strošek na stran dokumenta je 10.000 EUR/leto;
  - porabljen režijski čas na stran dokumenta je 69 ČD, kar preračunano pomeni 13.888 EUR/leto;
  - porabljen čas na dokument je 67 ČD, kar preračunano pomeni 13.541 EUR/leto.

- Sodila, ki izkazujejo nemerljive koristi, so:

  - prihranek časa stranke (ni potreben osebni obisk banke).

Obstajajo tudi indirektne koristi, ki jih je težje finančno ovrednotiti:

- ne potrebujemo več arhiva v fizični obliki;
- ne potrebujemo zaposlenih v arhivu;
- ne potrebujemo razreza dokumentacije;
- prihranimo pri iskanju po starih garancijah;
- stranka ne porabi časa in stroškov za prevzem garancije.

S študijo torej ugotavljamo, da je letni prihranek oddelka garancij v izbrani banki pri uporabi digitalnega podpisovanja **37.430 EUR/leto**.

4.2 Dokumentacija, sklenjena med zaposlenim in izbrano banko

Opis problema

Zelo majhen in enostaven primer za uvedbo digitalnega podpisovanja predstavlja prav povezava predaje dokumentov med zaposlenim in izbrano banko. Natančen opis postopka je prikazan na Sliki 11.

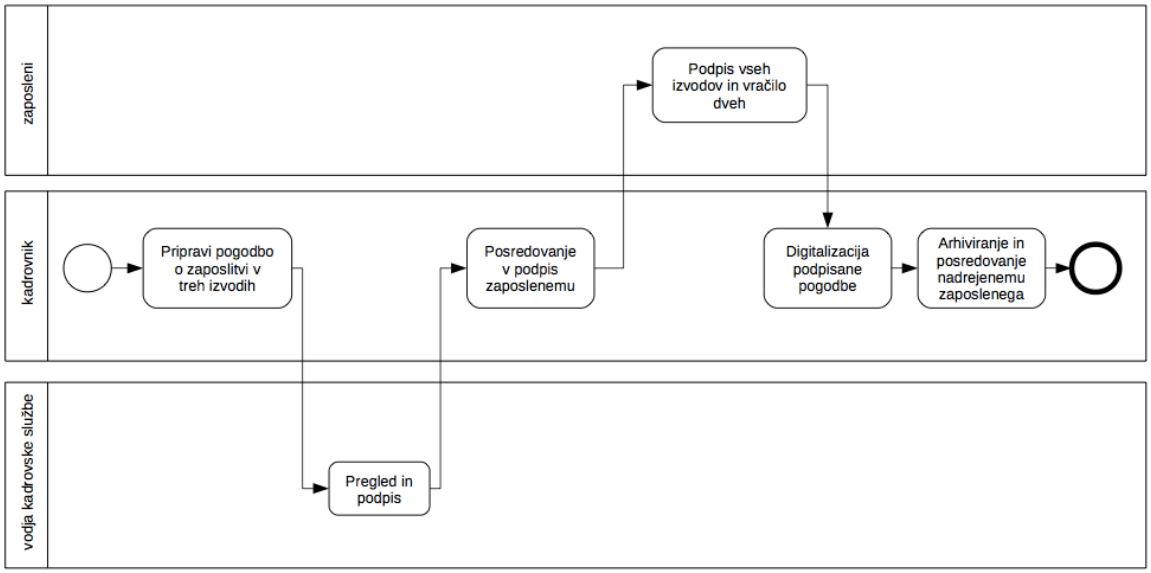
Izbrana banka ima odprtih več podružnic. V njih in na drugih lokacijah opravljajo svoje delo zaposleni izbrane banke. Z različnimi reorganizacijami, s spremembami nazivov, spremembo plače in podobnih kadrovskih zadev mora vsak zaposleni podpisati novo pogodbo o zaposlitvi, včasih pa samo dodatek k pogodbi o zaposlitvi. Običajno dokumentacijo pripravi kadrovska služba. Kadrovnica večstransko pogodbo v vsaj treh izvodih natisne, podpiše in posreduje v podpis direktorju. Nazadnje jo s spremnim pismom v podpis posreduje po pošti še zaposlenemu. Zaposleni pogodbo podpiše, zadrži en izvod, drugega pa vrne v kadrovsko službo. Tretji je shranjen pri direktorju zaposlenega.

S Slike 11 lahko razberemo pregled naslednjih aktivnosti:

- število natisnjenih dokumentov (original in kopije): 3;

- število lastnoročnih podpisov: 9;
- število prenosov dokumentov: 6.

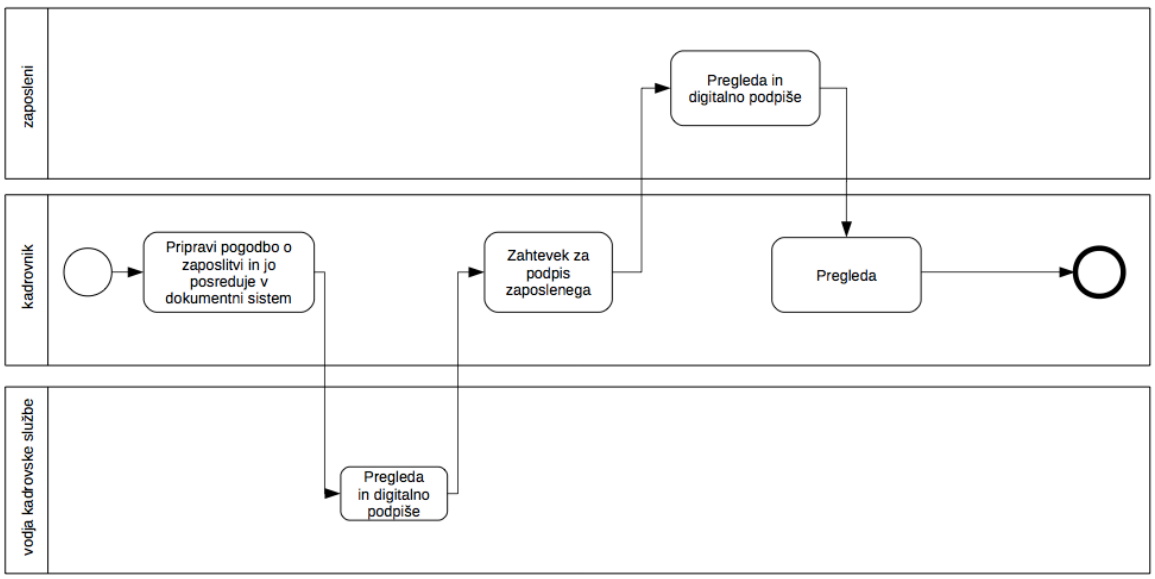
Slika 11: Obstoječi poslovni proces oddelka za kadrovanje v formatu BPMN



Predlog rešitve

Med izbrano banko in zaposlenimi bi lahko dokumentacija potekala v elektronski obliki in z vključitvijo digitalnega podpisovanja. Dokumenti bi bili shranjeni elektronsko. Prav tako bi bilo iskanje po preteklih dokumentih enostavno izvedljivo, brez poštnih in drugih dodatnih stroškov. Prenovljen poslovni proces prikazuje Slika 12.

Slika 12: Poslovni proces Oddelka za kadrovanje po uvedbi digitalnega podpisovanja v formatu BPMN



S Slike 12 lahko razberemo pregled naslednjih aktivnosti:

- število natisnjenih dokumentov (original in kopije): 0;
- število digitalnih podpisov: 3;
- število prenosov dokumentov: 3.

Omejitve pri študiji prihrankov

Za analizo smo upoštevali izhodišča, predstavljena v nadaljevanju.

- Vsaka pogodba je sestavljena iz šestih strani.
- Vsako pogodbo natisne izbrana banka v treh izvodih.
- Na letnem nivoju se za 1.000 zaposlenih povprečno natisneta vsaj dva dokumenta. V to številko uvrščamo tudi tiste, ki se na novo zaposlijo ali zapustijo banko.
- 600 zaposlenim se pogodbe in anekse posreduje po interni pošti, 400 zaposlenim po zunanji pošti.
- Predpostavljamo, da strošek na stran dokumenta znaša 0,1 EUR.
- Predpostavljamo, da čas na stran znaša 20 sekund.
- Predstavljamo, da čas na dokument znaša deset minut.
- Predpostavljamo, da strošek dela, ovrednoten s ČD (človek dan), predstavlja 200 EUR.

Študija prihrankov

Obstoječe stanje predstavljamo v nadaljevanju.

- Sodila, ki jih je mogoče finančno ovrednotiti, so:
  - strošek na stran dokumenta je 1.200 EUR/leto;
  - strošek na dokument je 400 EUR/leto;
  - porabljen režijski čas na stran dokumenta je preračunan na 1.666 EUR/leto;
  - porabljen čas na dokument je 4.166 EUR/leto.

- Sodila, ki izkazujejo nemerljive koristi, so:
  - prihranek na času (ni potreben osebni obisk zaposlenega ali kadrovnice);
  - prihranek na gorivu do dislocirane enote.

Obstajajo tudi indirektne koristi, ki jih je težje finančno ovrednotiti:

- ne potrebujemo več arhiva v fizični obliki;
- ni stroškov dela z arhivom;

- ne potrebujemo razreza dokumentacije;
- prihranek pri iskanju starih pogodb;
- ni več dvomov, ali je bila pogodba podpisana ali je bila po pošti izgubljena.

S študijo torej ugotavljamo, da je letni prihranek oddelka za kadrovanje v izbrani banki pri uporabi digitalnega podpisovanja **7.433 EUR/leto**.

SKLEP

Z magistrskim delom smo posegli v aktualno področje, za katerega lahko upravičeno predvidevamo, da bo prihodnost varnega digitalnega poslovanja. Proučevali smo področje digitalnega podpisovanja v izbrani banki. Sami mehanizmi podpisovanja so razviti že 40 let, vendar se v praksi uporabljajo šele zadnjih 15 let. Kljub temu po naših informacijah v letu 2016 ni nobene slovenske banke, ki bi v večji meri uporabljala digitalno podpisovanje pri svojih internih poslovnih procesih.

Na to področje so nas usmerila sledeča spoznanja:

- v Sloveniji postaja to področje vedno bolj uporabno, saj je klasično podpisovanje ovira pri informatizaciji in brezpapirnem poslovanju. V tujini je to področje veliko bolj razvito in široko uporabljeno;
- pri večjih podjetjih se digitalno podpisovanje trenutno šele uveljavlja.

Glede na zgornja spoznanja smo želeli raziskati in proučiti rešitev problema podpisovanja v izbrani banki oziroma podati konkretne iztočnice za izboljšanje obstoječega sistema podpisovanja v izbrani banki.

Pokazali smo, da na trgu obstajajo različne tehnične rešitve za implementacijo digitalnega podpisovanja. Razlikujejo se v funkcionalnostih in ceni. Njihova izbira je predvsem odvisna od zmožnosti lastnega vložka in sposobnosti oddelka IT. Taka obsežna sprememba, kot je način podpisovanja v poslovnem procesu, običajno zahteva tudi modernizacijo poslovnega procesa in storitve integracije zunanjih svetovalcev IT.

Na nivoju EU imamo od julija 2016 na osnovi uredbe o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije, na kratko eIDAS (angl. *Electronic Identification and Authentication Services Regulation* (910/2014/EC)), standardizirano zakonodajo, ki ureja digitalno podpisovanje. Še najmanjše razlike v zakonodaji članic EU, ki so bile prisotne, so sedaj odstranjene, pravnih ovir za uporabo digitalnega podpisovanja pa znotraj EU ni več.

Študija je pokazala, da je digitalno podpisovanje možno uvesti z različnimi tehničnimi rešitvami, ki vse enakovredno opravljajo svojo funkcijo (digitalno podpisovanje

dokumentov). Analizi uvedbe digitalnega podpisovanja v poslovna procesa sta pokazali, da je skupni prihranek dveh poslovnih procesov višji od 44.863 EUR. Če bi upoštevali vse poslovne procese v izbrani banki, bi bil prihranek še večji, in sicer zaradi še večjega števila digitaliziranih poslovnih procesov ter popolne opustitve papirnega poslovanja.

Priporočamo, da v izbrani banki banka izbere celostno rešitev. To pomeni, da izkoristi prednosti podpisovanja, posredovanja, sledenja in upravljanja ter hranjenja celotne dokumentacije z eno aplikacijo. V tem primeru z digitalnem podpisovanjem pridobimo kar največ indirektnih koristi (npr. ukinitev arhiva dokumentov, zmanjšanje odhodne pošte, ukinitev interne pošte).

Z gotovostjo lahko trdimo, da se bo v izbrani banki način podpisovanja in potrjevanja moral spremeniti ter postati enostavnejši in hitrejši.

Digitalno podpisovanje je prihodnost in se mu v zelo kratkem času ne bo mogoče izogniti.

LITERATURA IN VIRI

1. Abecker, A., Bernardi, A., Maus, H., Sintek, M. & Wenzel, C. (2000) Information supply for business processes: coupling workflow with document analysis and information retrieval. Knowledge-Based Systems, 13 (5), 271–284.
2. Adobe. (2015). Transform business processes with electronic and digital signature solutions from Adobe. Najdeno 18. aprila 2016 na spletnem naslovu https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-transform-business-processes-with-electronic-and-digital-signature-solutions.pdf
3. Adobe. (2015a). Global Guide to Electronic Signature Law. Najdeno 18. aprila 2016 na spletnem naslovu https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-guide-to-electronic-signature-law.pdf
4. Adobe. (2015b). Price. Najdeno 20. aprila 2016 na spletnem naslovu https://acrobat.adobe.com/si/en/pricing/pricing.html
5. AIIM. (2015). What is Document Management (DMS)? Najdeno 16. Septembra 2015 na spletnem naslovu http://www.aiim.org/What-is-Document-Management
6. Berk, A., Lončarski, I., in Zajc, P. (2002). Poslovne finance. Ljubljana. Ekonomska fakulteta. 292 str.
7. Brookfield, K. (1999). *Pisave.* Murska Sobota: Pomurska založba
8. Bolha. (2015). Preverjeni uporabnik. Najdeno 10. maja 2016 na spletnem naslovu http://www.bolha.com/koristno/pomoc-in-varnost/preverjeni-uporabnik
9. Caldeira, M., Serrano, A., Quaresma, R., Pedron, C. & Romao. M. (2012) Information and communication technology adoption for business benefits: A case analysis of an integrated paperless system. International Journal of Information Management, 32 (2), 196–202
10. Chimielowiec, A. (2009). Fixed points of the RSA encryption algorithm. Theoretical Computer Science, 5B, (02) 106
11. Chow, S., Contreras, J. & Hamel, L. (2013) Transactions. Najdeno 25 julija 2015 na spletnem naslovu http://cyber.law.harvard.edu/olds/ecommerce/transactions.html
12. Comodo. (2015). Introduction to digital certificates. Najdeno 15. julija 2015 na spletnem naslovu https://www.comodo.com/resources/small-business/digital-certificates-intro.php
13. Damij, N. (2009). Management poslovnih procesov: modeliranje, simuliranje, inovacija in izboljšanje. Ljubljana. Vega. 182 str.
14. Dewan, M. (2005). An Idiots Guide to Public Key Infrastructure. Najdeno 14. Aprila 2016 na spletnem naslovu https://www.giac.org/paper/gsec/2171/idiots-guide-public-key-infrastructure/103692
15. Diners Club. (2015). Najdeno 20. aprila 2016 na spletnem naslovu http://www.adobe.com/content/dam/Adobe/en/customer-success/pdfs/diners-club-uk-ireland-case-study.pdf
16. eDavki. (2016). Elektronsko davčno poslovanje. Najdeno 15. marca 2016 na spletnem naslovu https://edavki.durs.si/OpenPortal/Pages/StartPage/StartPage.aspx

17. Enoki. (2012). Najdeno 20. marca 2016 na spletnem naslovu http://conference.libreoffice.org/talks/2013/content/sessions/034/files/LibOConf2013_Case_Studies_of_migration_to_LibreOffice_in_Japan.pdf
18. Entrust Securing Digital Identities & Information. (2001-2003). *Digital Signatures – Best Practice for e-Business Transactions*. Najdeno 22. julija 2015 na spletnem naslovu https://www.entrust.com/wp-content/uploads/2013/05/digsig_transactions.pdf
19. eSodstvo. (2016). Najdeno 25. marca 2016 na spletnem naslovu https://evlozisce.sodisce.si/esodstvo/index.html
20. eUprava. (2016). Ministrstvo za javno upravo. Najdeno 10. aprila 2016 na spletnem naslovu https://e-uprava.gov.si
21. eVem. (2005). Portal za podjetja in podjetnike. Najdeno 11. aprila 2016 na spletnem naslovu http://evem.gov.si/evem/drzavljani/zacetna.evem
22. Ferk, Hans. (2012). Pot do konkurenčnosti. Prenova poslovnih procesov. Ljubljana. GV Založba.
23. Filev. (2008). Top-down and Bottom-up Project Management: Leveraging the Advantages of the Two Approaches. Najdeno 18. Aprila 2016 na spletnem naslovu https://www.wrike.com/blog/top-down-and-bottom-up-project-management-leveraging-the-advantages-of-the-two-approaches/
24. Ganley, M. (1998). Digital Signatures (str. 12–22) Information Security Technical Report
25. Gupta, A., Tung, Y. A. & Marsden, J. R. (2003). Digital signature: use and modification to achieve success in next generation e-business processes. Information and management, 41 (2004), 561–575.
26. Herman, A. (2002). Major bank signs up for digital signature verification technology. Elsevier Science.
27. Holbl, M. (2011). SSL in afera Diginotar. Najdeno 15. aprila 2016 na spletnem naslovu http://www.monitor.si/clanek/ssl-in-afera-diginotar/124865/
28. Holbl, M. (2015). Infrastruktura javnih ključev. Najdeno 18. oktobra 2015 na spletnem naslovu http://www.monitorpro.si/168174/praksa/infrastruktura-javnih-kljucev/
29. IBM. (2015). Advantages and Disadvantages of the top-down and bottom-up implementation approaches. Najdeno 15. marca 2016 na spletnem naslovu https://publib.boulder.ibm.com/tividd/td/ITIM/SC32-1708-00/en_US/HTML/im460_plan76.htm
30. IDC. (2015). Addressing the Document Disconnet. Najdeno 18. marca 2016 na spletnem naslovu https://wwwimages2.adobe.com/content/dam/Adobe/en/news-room/pdfs/201503/IDCInfoBrief.pdf
31. ISO. (2013). Standard ISO/IEC. Najdeno 18. aprila 2016 na spletnem naslovu http://www.iso.org/iso/home/standards.htm
32. Jazbinšek, U. (2015). Kaj je šifriranje? Najdeno 25. marca 2016 na spletnem naslovu http://www.e-uspeh.com/kaj-je-sifriranje.html
33. Jerman Blažič, A. (2006). Informacijska varnost. Monitor. Najdeno maja 2004 na spletnem naslovu http://www.monitor.si/clanek/informacijska-varnost/122021/?xURL=301

34. Kovačič, A. in Bosilj Vukšić, V. (2005). Management poslovnih procesov Prenova in informatizacija poslovanja s praktičnimi primeri. Ljubljana. GV Založba.
35. Kovačič, A., Žagar, M. in Štehalnik. S. (2010). MD5 na zatožni klopi. Najdeno 28. aprila 2016 na spletnem naslovu http://matej.owca.info/predavanja/MD5_na_zatozni_klopi.pdf
36. Kovačič, A. (2010). Prenova in informatizacija poslovanja, učna skripta. Ljubljana: Ekonomska fakulteta.
37. Lah, P. (2007). Uporaba kriptografije v internetu. Najdeno 25 julija 2015 na spletnem naslovu http://www.si-ca.si/kripto/index.htm
38. Lautreamont, A. (2015). Enigma. Najdeno 5. marca 2016 na spletni strani: http://www.lelephant-larevue.fr/un-cafe-avec-alan-turing/
39. Lenz, J. (2008). *Biometric Signature Verification – a sign of the times?*. Biometric Technology today, 16 (4), 9–11
40. Lenz, J. (2010). Taking signatures seriously – making signature biometrics meet digital signatures. Science Direct, 7–8
41. Lesjak, I. (2015). Varen elektronski podpis kot temelj elektronskega poslovanja. Najdeno 5. marca 2016 na spletnem naslovu http://www.ltfe.org/objave/varen-elektronski-podpis-kot-temelj-elektronskega-poslovanja/
42. Makar, A. (2015). Top-Down vs. Bottom-Up Project Management Strategies. Najdeno 22. aprila 2016 na spletnem naslovu https://www.liquidplanner.com/blog/how-long-is-that-going-to-take-top-down-vs-bottom-up-strategies/
43. Microcop. (2015). Upravljanje dokumentov in poslovnih procesov. Najdeno 11. septembra 2015 na spletnem naslovu http://www.mikrocop.si/sl/resitve/upravljanje-dokumentov-in-poslovnih-procesov/?gclid=Cj0KEQjw98mvBRD-_ciSovKhq7gBEiQAEvsBZ1KgXl8NcgLpNnBa4S1-MMuZ9D9lehX2pa1xTRAysOYaAnaB8P8HAQ
44. Microsoft. (2015). Description of digital certificates. Najdeno 18. aprila 2016 na spletnem naslovu https://support.microsoft.com/en-us/kb/195724
45. Microsoft. (2016). Phishing symptoms. Najdeno 20. aprila 2016 na spletnem naslovu https://www.microsoft.com/en-us/security/online-privacy/phishing-symptoms.aspx
46. Microsoft. (2016a). Paketi in cene. Najdeno 16. aprila 2016 na spletnem naslovu https://products.office.com/sl-si/business/compare-office-365-for-business-plans
47. Ministrstvo za javno upravo RS. (2009). Osnove varnih časovnih žigov. Najdeno 15. avgusta 2015 na spletnem naslovu http://www.si-tsa.gov.si/osnove.php
48. Ministrstvo za javno upravo. (2009a) Arhiviranje zaščitenih dokumentov. Najdeno 15. avgusta 2015 na spletnem naslovu http://www.sigen-ca.si/arhiviranje.php
49. Ministrstvo za javno upravo. (2013). Kako pridobiti spletno digitalno potrdilo Sigenca. Najdeno 16. avgusta 2015 na spletnem naslovu http://www.sigen-ca.si/pridobitev_fizicni.php
50. Ministrstvo za javno upravo. (2013a). Predstavitev izdajatelja SIgenca. Najdeno 15. avgusta 2015 na spletnem naslovu http://www.sigen-ca.si/predstavitev-SIGEN-CA.php

51. Ministrstvo za javno upravo. (2013b). Predstavitev izdajatelja SIgovca. Najdeno 16. avgusta 2015 na spletnem naslovu http://www.sigov-ca.gov.si/predstavitev-SIGOV-CA.php
52. Ministrstvo za javno upravo. (2015). Kako do ustreznega digitalnega potrdila. Najdeno 21. julija 2015 na spletnem naslovu http://e-uprava.gov.si/storitve/cms/page/kje_dobiti_cert
53. Ministrstvo za javno upravo. (2015a). Ogled digitalnega potrdila. Najdeno 14. Aprila 2016 na spletnem naslovu http://www.sigen-ca.si/osebni/ogledEE.php
54. Net-security. (2016). What is a Public Key Infrastructure? Najdeno 23. aprila 2016 na spletnem naslovu http://www.net-security-training.co.uk/what-is-a-public-key-infrastructure/
55. Nguyen, M. (2009). If everybody's signature became digital…. Science direct, 8
56. Office. (2015). Primer časovnega žiga. Najdeno 18. aprila 2016 na spletnem naslovu https://support.office.com/sl-si/article/Kako-ugotoviti-ali-je-elektronski-podpis-vreden-zaupanja-0464f8ab-fefa-4bc7-af0d-e07a12f7097e
57. Rebernik, M. (1999). Ekonomika poslovanja. Maribor. Ekonomsko-poslovna fakulteta
58. Rivest, R., Shamir, A. & Adleman, L. (1978). A method of obtaining digital signatures and public key cryptosystems. Comm. ACM 21, pp. 120–126
59. Rigby, D. (2014). Digital-Physical Mashups. Harvard business review (September 2014) Najdeno 15. aprila 2016 na spletnem naslovu https://hbr.org/2014/09/digital-physical-mashups
60. Ricoh. (2015). Najdeno 15. oktobra 2015 na spletnem naslovu https://www.adobe.com/content/dam/Adobe/en/customer-success/pdfs/ricoh-uk-case-study.pdf
61. Rouse, M. (2014) Digital signature. Najdeno 27 julija 2015 na spletnem naslovu http://searchsecurity.techtarget.com/definition/digital-signature
62. Rouse, M. (2015). Certificate Authority CA. Najdeno 27. julija 2015 na spletnem naslovu http://searchsecurity.techtarget.com/definition/certificate-authority
63. Solid. (2010) Paperless case study. Najdeno 27. julija 2015 na spletnem naslovu http://www.soliditsolutions.com/wp-content/uploads/2010/08/Paperless-Office-Case-Study.pdf
64. Skrt. (2004). Phising. Najdeno 15. aprila 2016 na spletnem naslovu: http://www.nasvet.com/phishing/
65. ISO. (2000). Standard ISO 7498-2: 1989. Najdeno 15. marca 2016 na spletnem naslovu http://www.iso.org/iso/catalogue_detail.htm?csnumber=14256
66. Stevens, M. (2012). "Cryptanalysis of MD5 & SHA-1". Najdeno 15. marca 2016 na spletnem naslovu http://2012.sharcs.org/slides/stevens.pdf
67. Stoney. (2015). Official documents. Najdeno 18. marca 2016 na spletnem naslovu https://commonwealth.virginia.gov/official-documents/notary-commissions/
68. Tomšič. (2015). Kako se izogniti trikom spletnega ribarjenja. Najdeno 15. aprila 2016 na spletnem naslovu http://www.siol.net/novice/tehnologija/racunalnistvo/2015/01/kako_se_izogniti_trnkom_spletnega_ribarjenja_phishing.aspx

69. Toplišek, J. (2000). Lastnoročni podpis in njegov vpliv na elektronsko sporočanje. Najdeno 22. marca 2016 na spletnem naslovu http://www2.arnes.si/~rzjtopl/slo/lastnor.htm
70. Uncitral. (2002). Model Law on Electronic Signatures with Guide to Enactment 2001. Najdeno 5. marca 2016 na spletnem naslovu https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf
71. Uprava. (2015). Kvalificirana digitalna potrdila. Najdeno 18. marca 2016 na spletnem naslovu http://e-uprava.gov.si/e-uprava/dogodkiPoslovni.euprava?zdid=1341&sid=1253
72. Zakon o elektronskem poslovanju in elektronskem podpisu (2000). Uradni list RS. (št. 57/2000, 23. junij 2000)
73. Zakon o varstvu osebnih podatkov. (2004). *Ur. l. RS.* (št. 86/04, 5. avgust 2004)
74. Žužek, A. & Dobnikar, A. (2002). Arhiviranje digitalno podpisanih elektronskih dokumentov. Najdeno 23. julija 2015 na spletnem naslovu http://mail.pokarhmb.si/fileadmin/www.pokarhmb.si/pdf_datoteke/Radenci2002/ZUZEK-DOBNIKAR_02.pdf