

**UNIVERZA V LJUBLJANI  
FAKULTETA ZA UPRAVO**

**Diplomsko delo**

**UVEDBA SISTEMA ZA UPRAVLJANJE  
Z DOKUMENTI V ORGAN DRŽAVNE UPRAVE**

**Irena Zalar**

**Ljubljana, februar 2013**

**UNIVERZA V LJUBLJANI  
FAKULTETA ZA UPRAVO**

DIPLOMSKO DELO

**UVEDBA SISTEMA ZA UPRAVLJANJE  
Z DOKUMENTI V ORGAN DRŽAVNE UPRAVE**

Kandidatka: Irena Zalar  
Vpisna številka: 04039642  
Študijski program: Univerzitetni študijski program Uprava 1. stopnja  
Mentor: izr. prof. dr. Ljupčo Todorovski

Ljubljana, februar 2013

## **IZJAVA O AVTORSTVU DIPLOMSKEGA DELA**

Podpisana Irena Zalar, študentka univerzitetnega študijskega programa Uprava 1. stopnja, z vpisno številko 04039642, sem avtorica diplomskega dela z naslovom Uvedba sistema za upravljanje z dokumenti v organ državne uprave.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega lastnega raziskovalnega dela,
- sem poskrbela, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili,
- sem poskrbela, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili,
- sem pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisala v predloženem delu,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del bodisi v obliki citata bodisi v obliki skoraj dobeseidnega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorstvu in sorodnih pravicah, Uradni list RS, št. 21/95), kršitev pa se sankcionira tudi z ukrepi po pravilih Univerze v Ljubljani in Fakultete za upravo,
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za upravo,
- je elektronska oblika identična tiskani obliki diplomskega dela ter soglašam z objavo dela v zbirki »Dela FU«.

Diplomsko delo je lektorirala: Mira Koren mag. upr. ved

Ljubljana, 1. 2. 2013

Podpis avtorice:



## POVZETEK

Z rastjo elektronskega poslovanja je količina podatkov in njihovega pretoka vedno večja. Ob ugotavljanju, da proizvajalci informacijskih rešitev z uporabo novih tehnologij iščejo in najdejo nove načine za reševanje uporabniških zahtev, je uvedba sistemov za upravljanje z dokumenti tudi oziroma predvsem v državni upravi, neizogibna. Sistem za upravljanje z dokumenti pa ne prinaša zgolj posodobljenega načina upravljanja informacij, temveč tudi večjo integracijo z ostalimi sistemi.

V diplomski nalogi je prikazana uvedba sistema za upravljanje z dokumenti v obravnavani organ državne uprave, podrobneje pa sta primerjani dve kategoriji dokumentov. Dokumenti s stopnjo zaupnosti terjajo natančno sledenje zakonskim podlagam in z vidika varnosti predstavljajo tehnični izziv, uvedba sistema za upravljanje z dokumenti na področje finančno računovodskih dokumentov pa s seboj prinaša tudi organizacijske spremembe, integracijo z zalednimi sistemi ter spremembe poslovnih procesov.

Rezultati predstavljeni v diplomski nalogi kažejo na to, da je uvedba sistema za upravljanje z dokumenti za različne kategorije dokumentov odvisna od številnih dejavnikov. Večje spremembe v načinu dela in njegovi organizaciji terjajo veliko pripravljenost uporabnikov na spremembe, prenova obsežnih poslovnih procesov pa uvedbo posamezne kategorije dokumentov lahko precej upočasnijo. Ključna naloga organizacije, kot dela javne uprave, je v razumevanju problematike in aktivnem vključevanju v spremembe, tako v smislu aktivnega sodelovanja pri posodabljanju pravnih podlag, kot organizacije dela.

**Ključne besede:** sistem za upravljanje z dokumenti, dokument, arhiviranje, tajni podatek, račun.

## **SUMMARY**

### **IMPLEMENTATION OF A DOCUMENT MANAGEMENT SYSTEM IN PUBLIC ADMINISTRATION**

The development of e-business contributes to the continuous growth in the quantity of data and amount of data transfer. Developers of information systems are continuously finding new solutions to the data growth problem, and therefore, the implementation of document management systems in the public administration becomes inevitable. The implementation of these systems not only modernizes the management of information in public administration, but also results in greater integration with other systems.

The thesis describes the process of implementation of a document management system in a selected public administration organization with an emphasis on two document categories. Namely, the documents with a designated level of confidentiality require strict adherence to the legal framework and consequently represent a technical challenge in the field of information system security. On the other hand, the implementation of a document management system in the field of financial and accounting documents requires certain organizational changes, integration of existing information systems, as well as changes of existing business processes.

The results presented in the thesis point to the different factors that influence the implementation of a document management system in public administration. Extensive changes of the work process and organization demand the cooperation of the users and acceptance of implemented changes, while the renovation of large business processes can result in slower implementation for a particular document category. The crucial task of the organization, as a part of public administration, is to understand the relevant issues and actively cooperate in the implementation of changes, which include the renovation of the legal framework as well as the organization of the work process.

**Keywords:** document management systems, document, archiving, confidential data, invoice.

# KAZALO

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA .....	III
POVZETEK.....	V
SUMMARY .....	VI
KAZALO.....	VII
KAZALO PONAZORITEV .....	IX
KAZALO GRAFIKONOV .....	IX
KAZALO SLIK.....	IX
KAZALO TABEL.....	IX
SEZNAM UPORABLJENIH KRATIC IN OKRAJŠAV.....	X
1    UVOD .....	1
2    OSNOVNI KONCEPTI ELEKTRONSKEGA POSLOVANJA Z DOKUMENTI.....	3
2.1    DOKUMENT .....	3
2.2    KATEGORIJE DOKUMENTOV .....	3
2.3    DOKUMENTI V PAPIRNI IN ELEKTRONSKI OBLIKI .....	5
2.4    ELEKTRONSKA HRAMBA DOKUMENTOV .....	6
3    PРАВNA UREDITEV ELEKTRONSKE HRAMBE.....	10
3.1    ZAKON O ELEKTRONSKEM POSLOVANJU IN ELEKTRONSKEM PODPISU.....	10
3.2    UREDBA O POGOJIH ZA ELEKTRONSKO POSLOVANJE IN ELEKTRONSKO PODPISOVANJE .....	10
3.3    ZAKON O VARSTVU DOKUMENTARNEGA IN ARHIVSKEGA GRADIVA .....	11
3.4    UREDBA O VARSTVU DOKUMENTARNEGA IN ARHIVSKEGA GRADIVA.....	11
3.5    ENOTNE TEHNOLOŠKE ZAHTEVE IN NOTRANJA PRAVILA .....	11
3.6    UREDBA O VAROVANJU TAJNIH PODATKOV.....	13
4    SISTEMI ZA UPRAVLJANJE Z ELEKTRONSKIMI DOKUMENTI.....	14
4.1    TEHNOLOGIJA EDMS.....	14
4.1.1    ŽIVLJENJSKI CIKEL DOKUMENTA .....	15
4.2    ELEKTRONSKO PODPISOVANJE.....	17
4.3    INFORMACIJSKA VARNOST .....	17
4.4    AKREDITACIJA HRAMBE GRADIVA V ELEKTRONSKI OBLIKI.....	19

5	UVEDBA SISTEMA ZA UPRAVLJANJE Z DOKUMENTI V IZBRANEM ORGANU DRŽAVNE UPRAVE .....	20
5.1	ELEKTRONSKO OBVLADOVANJE DOKUMENTARNEGA GRADIVA .....	20
5.1.1	OD ZAJEMA DO ARHIVA .....	21
5.1.1.1	Zajem prejetih dokumentov .....	22
5.1.1.2	Evidentiranje prejetih dokumentov.....	22
5.1.1.3	Izdelovanje in evidentiranje lastnih dokumentov .....	22
5.1.1.4	Elektronsko podpisovanje in overjanje dokumentov.....	23
5.1.2	OSEBNI PODATKI.....	23
5.1.3	ZBIRKE DOKUMENTARNEGA GRADIVA.....	23
5.1.4	POZITIVNI UČINKI UVEDBE INTRENUTNE POMANJKLJIVOSTI.....	24
5.2	BREZPAPIRNO POSLOVANJE NA FINANČNO RAČUNOVODSKEM PODROČJU, E-RAČUN .....	25
5.2.1	UVAJANJE ELEKTRONSKEGA POSLOVANJA S PODROČJA RAČUNOV NA NIVOJU DRŽAVNE UPRAVE .....	26
5.2.2	UVAJANJE ELEKTRONSKEGA POSLOVANJA S PODROČJA RAČUNOV V OBRAVNAVANEM ORGANU DRŽAVNE UPRAVE.....	28
5.2.3	UVAJANJE INTEGRACIJE SISTEMOV MFERAC IN EDS .....	29
5.2.4	ANALIZA UVEDBE IN CILJI PRENOVE POSLOVANJA NA FINANČNO RAČUNOVODSKEM PODROČJU .....	30
5.2.5	UGOTOVITVE.....	32
5.3	DOKUMENTI S STOPNJO ZAUPNOSTI .....	33
5.3.1	STOPNJA VAROVANJA INFORMACIJSKEGA SISTEMA V OBRAVNAVANEM ORGANU DRŽAVNE UPRAVE.....	34
5.3.2	SLABOSTI PRED UVEDBO ZAJEMA V EDS.....	35
5.3.3	UVEDBA EDS NA PODROČJE DOKUMENTOV S STOPNJO ZAUPNOSTI ....	35
6	POVZETEK OBDELANIH PODROČIJ.....	39
7	ZAKLJUČEK .....	43
	LITERATURA IN VIRI.....	45



## **KAZALO PONAŽORITEV**

### **KAZALO GRAFIKONOV**

Grafikon 1: Uspešnost uvedbe glede na elemente EDMS.....	41
--	----

### **KAZALO SLIK**

Slika 1: Poraba delovnega časa pri delu z dokumenti.....	6
Slika 2: Prikaz življenjskega cikla dokumenta .....	14
Slika 3: Shematski prikaz sistema za elektronsko upravljanje dokumentov.....	15
Slika 4: Pošiljanje metapodatkov računa.....	27
Slika 5: Dokumentni sistem ustvarja pet elementov.....	39

### **KAZALO TABEL**

Tabela 1: Komponente štirih tipov dokumenta s stopnjo zaupnosti .....	36
Tabela 2: Analiza uspešnosti uvedbe posameznih področij .....	40

## SEZNAM UPORABLJENIH KRATIC IN OKRAJŠAV

EDMS	angl. Electronic Document Management Systems
EDS	Elektronski dokumentni sistem
AIIM	angl. The Association for Information and Image Management
ESUD	Elektronski sistem za upravljanje z dokumenti
ETZ	Enotne tehnološke zahteve
UUP	Uredba o upravnem poslovanju
UVTP	Urad za varovanje tajnih podatkov
ZEPEP, ZEPEP-UPB1	Zakon o elektronskem poslovanju in elektronskem podpisu
ZVDAGA	Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih
UVDAGA	Uredba o varstvu dokumentarnega in arhivskega gradiva
MoReq	Model zahtev za upravljanje elektronskih dokumentov
MFERAC	Enotni računovodski sistem Ministrstva za finance
DPS	Državni proračun Slovenije
GKS	Glavna knjiga s saldakonti
OS	Osnovna sredstva
GKS	Domača in tuja blagajna
STK	Stanovanjski krediti

# 1 UVOD

Rast količine informacij v svetu je vedno večja, k temu je pripomogel predvsem razvoj informacijskih tehnologij in elektronskega poslovanja. Velike količine dokumentov upravljanih na klasičen način, so postale vedno večja ovira za nemoteno delo in hitro sprejemanje poslovnih odločitev. Potrebe po učinkovitejšem krmiljenju dokumentov so sprožile hiter razvoj elektronskih sistemov za upravljanje z dokumenti. Osnovni namen uvedbe takih sistemov je izboljšati poslovne procese, katerih temeljni elementi so predvsem dokumenti kot nosilci informacij. Celovito upravljanje dokumentov v elektronski obliki je zahtevno in 'multidisciplinarno' področje. Rešitve informacijske tehnologije pa ne prinašajo vseh pozitivnih učinkov brez organizacijskih sprememb, optimizacije poslovnih procesov in zagotavljanja varnosti podatkov. Z rastjo elektronskega poslovanja je količina podatkov in njihovega pretoka vedno večja. Ob ugotavljanju, da proizvajalci informacijskih rešitev z uporabo novih tehnologij iščejo in najdejo nove načine za reševanje uporabniških zahtev, je uvedba sistemov za upravljanje z dokumenti predvsem v državno upravo neizogibna.

V obravnavani organizaciji je bila pred uvedbo sistema za upravljanje z dokumenti v uporabi aplikacija, ki je omogočala decentralizirano evidenco vnosa in sledenje dokumentom. Njena bistvena pomanjkljivost je bila v tem, da ni omogočala popolnega nadzora nad dokumenti, prav tako se je v aplikaciji vodila le evidenca o dokumentih. Le ti so bili posredovani po navadni pošti in shranjeni na klasičen način v papirni obliki. Dokumente je bilo potrebno fotokopirati in dostavljati različnim osebam na različne lokacije. Obstajal je klasičen arhiv, kar je pomenilo dolgotrajnejše iskanje obstoječih dokumentov. Uporabniki so s svojimi dokumenti lahko delali le na lokaciji, kjer so bili dokumenti shranjeni.

Nov informacijski sistem je zajel celotni življenjski cikel dokumentov, od prejema oziroma izdelave dokumenta do njegove hrambe v stalni zbirki. Bistvo uvedbe sistema za upravljanje z dokumenti pa ni zgolj v posodobljenem načinu upravljanja dokumentov, temveč v večji integraciji z ostalimi že obstoječimi sistemi. Omogočiti mora funkcionalno in tehnološko povezljivost z ostalimi procesi organizacije.

Namen naloge je raziskati razloge in učinke uvedbe sistema za upravljanje z dokumenti v obravnavani organ državne uprave. Podrobneje bom primerjala uvedbo dveh kategorij dokumentov, ki sta značilni za obravnavano organizacijo. Dokumenti s stopnjo zaupnosti predstavljajo predvsem tehnični izziv, uvedba sistema za upravljanje z dokumenti na področje finančno računovodskih dokumentov pa s seboj prinaša tudi organizacijske spremembe.

Cilj naloge je ugotoviti, ali je elektronski sistem za upravljanje dokumentarnega gradiva v obravnavani organizaciji resnično zajel celotni življenjski cikel dokumenta in kako je uvedba aplikacije vplivala na ostale poslovne procese v organizaciji.

V okviru tega cilja bom skušala ugotoviti, kako se organizacija spoprijema z implementacijo v nov sistem specifičnih kategorij dokumentov.

V diplomski nalogi bom preverila pravilnosti naslednjih dveh hipotez:

- Sistem za upravljanje z dokumenti omogoča upravljanje z dokumentarnim gradivom v elektronski obliki tako, da zajema celotni življenjski cikel dokumentov od prejema oziroma izdelave do hrambe v stalni zbirki.
- Ob uvedbi sistema za upravljanje z dokumenti je potrebno upoštevati kategorizacijo dokumentov, ki s seboj prinese specifično problematiko.

Pri pripravi diplomske naloge sem uporabila primerjalno analizo, saj primerjam stanje pred in po implementaciji nove informacijske rešitve. Z uporabo deskriptivne metode sem obdelala področje uvajanja elektronskega poslovanja v finančno računovodskem procesu. Veliko predhodnih raziskav obravnava področje elektronskih dokumentnih sistemov, kot na primer raziskava o elektronskem sistemu za upravljanje z dokumenti. (Zebec, 2012) Prav tako so narejene raziskave o vidikih hrambe elektronskega dokumentarnega gradiva (Antolinc, 2009), nekaj raziskav obravnava varovanje in zaščito podatkov v sistemih za upravljanje z dokumenti (Žitko, 2011), nekaj raziskav omenja tudi uvedbo dokumentnega sistema kot orodja za izboljšanje kakovosti poslovnih procesov na praktičnih primerih iz gospodarskega sektorja. (Kožuh, 2008) in (Prijanovič, 2011) Le nekaj pa jih omenja upravljanje z digitaliziranimi dokumenti v javni upravi. (Koren, 2010)

V diplomskem delu želim predstaviti uvedbo sistema za upravljanje z dokumenti v organ državne uprave. Predstavila bom pet večjih poglavij, v prvem delu bom preučila osnovne koncepte elektronskega poslovanja z dokumenti, preverila bom različne kategorije dokumentov ter razlike med klasičnim in elektronskim dokumentom. V drugem delu bom pregledala zakonske podlage, ki so postavile temelje elektronskemu poslovanju, v tretjem delu bom predstavila tehnologijo elektronskega dokumentnega sistema ter področje varnosti in zaščite podatkov. V zadnjem delu bom analizirala različne možnosti uvedbe elektronskih dokumentov s finančno računovodskega področja in preučila problematiko evidentiranja dokumentov s stopnjo zaupnosti ter navedla prednosti in slabosti, ki so jih prinesle tehnične rešitve njihovega evidentiranja.

## **2 OSNOVNI KONCEPTI ELEKTRONSKEGA POSLOVANJA Z DOKUMENTI**

Upravljanje z vedno večjo količino dokumentov je brez ustreznega sistema in orodij postalo težko in zamudno opravilo. Obvladovanje dokumentov v elektronski obliki je široko področje, obsega tako informacijsko tehnologijo kot tudi organizacijske izzive. Vključuje spremembe poslovnih procesov in njihovo optimizacijo ter se hkrati ukvarja z zagotavljanjem varnosti. Elektronski sistemi še niso dovolj pogosti, pri uvajanju manjkajo praktične izkušnje kako se lotiti problemov, ki jih pred tem nismo poznali, niti pričakovali.

Bistvena naloga sistemov elektronskega upravljanja z dokumenti je omogočiti dostop do informacij vsem v organizaciji na varen in organiziran način. Običajno so dokumenti napisani na papirju, zaradi vedno večje informatizacije pa vse več dokumentov nastaja predvsem v elektronski obliki. Prednost le teh je v hitrejšem in lažjem ustvarjanju, hitrejši obdelavi, njihovem organiziranju in hranjenju. Hitrejše in lažje ustvarjanje dokumentov pa je tudi razlog za nastajanje vedno večjih količin dokumentov. Ročno obdelovanje velike mase dokumentov je vse manj obvladljivo, terja ogromno časa, povečuje stroške poslovanja, s količino pa se večja tudi odstotek izgubljenih dokumentov. Oteženo je zagotavljanje varnosti, kontrole in sledljivosti dokumentov.

Za razumevanje sistema za upravljanje z dokumenti je treba poznati nekatere ključne koncepte.

### **2.1 DOKUMENT**

Dokument je zapisana informacija, ki je oblikovana ali prejeta. Sam po sebi dokument ni omejen na papirni medij, ampak je lahko tudi v elektronski obliki.

“Dokument je vsak zapis, ki nastane pri poslovanju pravne ali fizične osebe ter ima praviloma določeno obliko in vsebino. Lahko je izviren ali reproduciran, pisan, risan, tiskan, fotografiran, fotokopiran, fonografski, v elektronski obliki ali kako drugače zapisan zapis, ki je pomemben za poslovanje družbe. Dokument je lahko zapisan na različne nosilce (glinasta ploščica, papir, filmski trak, magnetni trak, optični disk in drugi) z različnimi načini zapisa (rokopis s pisalom, pisalni stroj, informacijska strojna in programska oprema ter drugo). Dokumente pri poslovanju združujemo v spise, zadeve, dosjeje ali po vrstah dokumentov. Skupek dokumentov, spisov, zadev, dosjejev, drugih zapisov in gradiv, ki nastajajo pri poslovanju, pa imenujemo dokumentarno gradivo ali dokumentacija.” (Žumer, 2008, str. 22)

### **2.2 KATEGORIJE DOKUMENTOV**

Dokument je vedno povezan z določeno aktivnostjo, ki jo proži organizacija oziroma posameznik. Dokumente glede na njihov izvor, zvrst, vsebino, roke hranjenja, stopnjo zaupnosti ipd., razvrščamo v različne kategorije.

Glede na izvor, so dokumenti lahko prejeti, torej tisti, ki jih organizacija prejme od strank oziroma poslovnih partnerjev. Lastni dokumenti so tisti, ki nastajajo pri delu organizacije in so namenjeni uporabi v organizaciji. Sem sodijo razni organizacijski predpisi, sklepi, informacije in drugo. Odposlani dokumenti pa so tisti dokumenti, ki jih naslovimo na poslovne partnerje ali stranke, sami pa obdržimo kopijo odposlanega.

Glede na zvrst ločimo poslovne in uradne dokumente. Poslovne dokumente si organizacije med seboj izmenjujejo v poslovnih procesih. Uradne dokumente pa prejemajo, odpošiljajo in obravnavajo predvsem organi javne uprave.

Vsebina dokumenta nam sporoča neko informacijo, ki jo dokument vsebuje. Odvisno od pomena vsebine dokumenta in glede na njegove pravne posledice, dokumente razvrščamo v različne kategorije. Pri tem nam je v pomoč klasifikacijski načrt, ki je osnovni in najpomembnejši šifrant za razporejanje dokumentarnega gradiva. V njem so zapisane vsebine dela, ki so razvrščene na osnovi decimalne klasifikacije.

Roki hranjenja dokumentarnega ali arhivskega gradiva se določajo glede na vsebino. Osnove za določanje rokov hranjenja dokumentarnega gradiva organov javne uprave določa Navodilo za določanje rokov hranjenja dokumentarnega gradiva organov javne uprave (Uradni list RS, št. 81/2005). Dokumentarnemu gradivu, ki ni arhivsko ali trajno dokumentarno gradivo, pa so roki hranjenja določeni s strani predstojnika organa oziroma z veljavnimi področnimi predpisi (računovodski standardi, varstvo osebnih podatkov, tajni podatki ipd.).

Z zaupnimi dokumenti se najpogosteje srečujejo zaposleni v državni upravi ter podjetja oziroma posamezniki, kadar za državni organ nabavljajo blago ali izvajajo storitve, ki so tajne narave. Zakon o tajnih podatkih (ZTP-UPB2, Uradni list RS, št. 50/2006) določa naslednje stopnje zaupnosti: interno, zaupno, tajno in strogo tajno. Zakon opredeljuje tajni podatek kot dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v tem zakonu zavarovati pred nepoklicanimi osebami in ki je v skladu s tem zakonom določeno in označeno za tajno. Obravnavanje tajnih podatkov je v Zakonu o tajnih podatkih opredeljeno kot: določanje, označevanje, dostop do podatka, uporaba, evidentiranje, razmnoževanje, posredovanje, prenos, uničevanje nosilcev tajnih podatkov, hramba, arhiviranje ter drugi ukrepi in postopki, s katerimi se zagotavlja njihova varnost. Tajnemu podatku se stopnja tajnosti določi ob njegovem nastanku oziroma ob začetku izvajanja naloge organa, katere rezultat bo tajni podatek. Pri tem mora pooblaščen oseba pisno oceniti možne škodljive posledice za varnost države ali za njene politične ali gospodarske koristi, če bi bil podatek odkrit nepoklicani osebi. Vsak tajni podatek oziroma vsak dokument, ki vsebuje tajne podatke, mora biti označen s stopnjo tajnosti in s podatki o organu. Definicije stopenj zaupnosti so v Zakonu o tajnih podatkih določene v trinajstem členu. Stopnja zaupnosti se določi glede na možne škodljive posledice za varnost države, ali za njene politične oziroma gospodarske koristi, ki lahko nastanejo ob razkritju podatkov. Določi jih lahko predstojnik organa, funkcionarji, ki

so za to pooblaščen z zakonom, ali pa jih je pooblastil predstojnik organa in osebe, ki so v organu zaposlene in imajo pisno pooblastilo predstojnika organa.

Stopnje zaupnosti:

- "STROGO TAJNO" se določi za tajne podatke, katerih razkritje nepoklicani osebi bi ogrozilo vitalne interese Republike Slovenije ali jim nepopravljivo škodovalo;
- "TAJNO" se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko hudo škodovalo varnosti ali interesom Republike Slovenije;
- "ZAUPNO" se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo varnosti ali interesom Republike Slovenije;
- "INTERNO" se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo delovanju ali izvajanju nalog organa.

Pooblaščen oseba mora tajnost podatka preklicati, ko ni več pogojev, ki so za takšen status podatka določeni v Zakonu o tajnih podatkih. Tako tajnost lahko preneha na določen datum, z nastopom določenega dogodka, s potekom določenega časa in s preklicem tajnosti. (MNZ, 2012)

### **2.3 DOKUMENTI V PAPIRNI IN ELEKTRONSKI OBLIKI**

Papir kot nosilec informacij ima v življenju ljudi pomembno vlogo in jo bo vsaj deloma ohranil tudi v prihodnosti.

Pred iznajdbo papirja pred dvema tisočletjema, so ljudje pisali in risali na naravne materiale, na primer na kamen, kosti, glino, drevesno skorjo in drugo. Papir je bil tudi glavni nosilec in posrednik učenja, znanja, kulture in politike. Šele v zadnjem stoletju pa svoje misli zapisujemo tudi na sodobna komunikacijska sredstva in medije.

Dokumenti, ki jih danes uporabljajo organizacije, so zato v različnih oblikah, tako fizičnih kot elektronskih. Različne oblike pa imajo različno stopnjo zaupanja v verodostojnost dokumentov. Višja je stopnja zaupanja v verodostojnost dokumenta, manjša je njegova uporabnost in težji je dostop do informacij, ki so shranjene na njem. Tako je papir kot nosilec informacij najenostavnejša oblika na kateri lahko dokazujemo verodostojnost, vendar pa je kot nosilec informacij tudi najmanj primeren za uporabo.

Dokumenti v papirni obliki imajo naslednje slabosti:

Iskanje informacij ali podatkov na papirju je zelo zamudno opravilo, pogosto se zgodi da dokumenta, ki ga potrebujemo, sploh ne najdemo. Zato ostane veliko znanja in uporabnih informacij, ki so shranjene v dokumentih, neuporabnih. Papirno dokumentacijo je tudi zelo težko obvladovati in nadzorovati pred nepooblaščenimi vpogledi. V primeru, da je papirni dokument uničen, je ponovna vzpostavitev prejšnjega stanja praktično nemogoča. Prav tako je shranjevanje vedno večje količine dokumentov izredno drago.

Najnižjo stopnjo zaupanja imajo dokumenti v elektronski obliki. Brez tehnologije, kot so digitalna potrdila, časovno žigovanje in elektronski podpis je stopnja zaupanja v njihovo

verodostojnost zelo nizka. So pa elektronski dokumenti zaradi enostavne dostopnosti najprimernejši za uporabo.

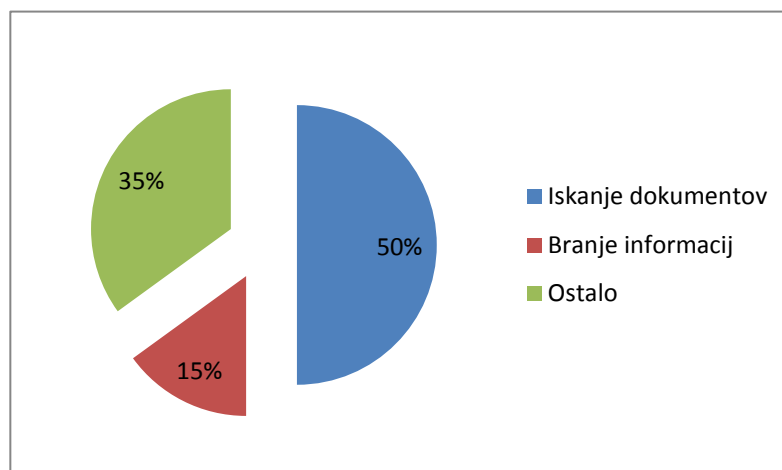
Elektronski dokumenti so tako imenovani elektronski zapisi. To so podatki, informacije, sporočila in druge vsebine, ki nastajajo oziroma so zapisane pri elektronskem oziroma tako imenovanem računalniškem poslovanju s pomočjo informacijske in komunikacijske tehnologije na magnetnih in optičnih nosilcih oziroma na strojno berljivih nosilcih zapisov. (Žumer, 2001, str. 44)

Dokumenti v elektronski obliki omogočajo hitro računalniško pregledovanje, obdelujemo jih lahko v različnih bazah podatkov, prostor za njihovo shranjevanje pa je bistveno manjši od papirnega arhiva, vendar pa se pri dokumentih v elektronski obliki srečujemo z drugačnimi težavami. Ali imamo zadnjo verzijo dokumenta? Kako so dokumenti zavarovani? Ali dokumente lahko pravočasno dostavimo vsem, ki jih potrebujejo? V kakšnem zaporedju naj zaposleni obravnavajo dokumente?

## 2.4 ELEKTRONSKA HRAMBA DOKUMENTOV

Elektronsko hranjeno gradivo je lažje dostopno, njegova hramba pa zahteva tudi bistveno manj prostora kot papirni arhiv. Med elektronskimi podatki veliko lažje iščemo. Iskanje nekega dokumenta v zbirki, ki obsega več polic, je lahko zamudno opravilo, računalnik pa ga opravi v kratkem času. Slika 1 prikazuje porabo delovnega časa pri delu z dokumenti. Kar 50 % časa zaposleni porabimo za iskanje dokumenta, 35 % za ostala opravila in do 15 % za branje informacij.

**Slika 1: Poraba delovnega časa pri delu z dokumenti**



Vir: Zebec (2010, str. 25)

Ena izmed najpomembnejših lastnosti elektronskih podatkov se nanaša na možnost njihovega hitrega in sledljivega posredovanja ključnim sodelavcem. Pomembna prednost elektronske hrambe dokumentov je varovanje zaupnih dokumentov. Elektronska hramba



omogoča varovanje z natančno definicijo pravic dostopov posameznika ali skupine uporabnikov in z natančnim časovnim beleženjem dostopov.

Poleg naštetih prednosti se je potrebno zavedati tudi nekaterih pomanjkljivosti, ki jih elektronski podatki prinašajo ter se jim pravi čas in na pravilen način izogniti. Hramba v elektronski obliki se namreč bistveno razlikuje od klasične hrambe.

»Črnilo in papir že s svojimi fizičnimi lastnostmi v veliki meri zagotavljata celovitost in avtentičnost vsebine, ki jo tvorita, medtem ko podatki v elektronski obliki nimajo materialne oblike. Posledica tega je, da poseganje v vsebino elektronsko zapisanih podatkov (takšno poseganje je lahko posledica zavestnega dejanja, pomote, nesreče ali drugih razlogov) ne pušča sledov na način, kot jih pušča npr. manjkajoči označen list papirja ali izbrisan tekst na njem.« (Perklik, 2012)

»Podatki niso namenjeni le podpori pri odločitvah ali pravni varnosti ustvarjalca, temveč lahko zagotavljajo trajno in zgodovinsko vrednost naslednjim generacijam, zato je odgovornost organizacij obravnavati podatke na tak način, da se ohranjata njihova vrednost in dostopnost do dokumentov tudi prihodnjim generacijam.« (Horjak, M., 2011, str. 42)

Bistveni razlogi za shranjevanje dokumentov na sodobnih nosilcih so:

- zaščita pred poškodbami ali izgubo dokumentov,
- izvornih dokumentov ne vrnemo na svoje mesto (v regulator v arhivu),
- nadzor nad uporabo dokumentov,
- vpogled, sprememba ali izpis dokumenta ni popolnoma nadzorovan,
- dostopnost in razpoložljivost dokumentov je večja,
- ob uporabi klasičnega arhiva časovna in krajevna neodvisnost ni mogoča, kopiranje in razpošiljanje kopij na oddaljene lokacije pa predstavlja izgubo časa in denarja,
- stroški arhivskih prostorov so nižji.

### **Temeljna načela za izvajanje e- hrambe**

Da bi zagotovili temeljne zahteve za izvajanje e-hrambe, je treba zagotoviti, da so dokumenti:

- avtentični, kar pomeni, da je dokument to, kar v svoji vsebini trdi da naj bi bil (Dečman, 2007);
- celoviti, kar zagotavlja, da vsebina dokumenta ni bila spremenjena na kakršenkoli način. Sama oblika dokumenta ne zagotavlja tudi zaščite pred spreminjanjem vsebine, kot to velja pri papirni obliki dokumenta. Vsebina je pri papirni obliki vezana na nosilec, v digitalni obliki pa ne;
- dostopni in razumljivi, zagotovljena morata biti varovanje pred izgubo in hkrati dostop v vsem času trajanja hrambe. Zagotovljena morata biti tudi reproduciranje in primernost reprodukcij za uporabo;
- primerni za obdelavo in potencialno ponovno uporabni.

»S hitrimi spremembami informacijske tehnologije elektronske oblike zapisa in nosilci zapisa za hrambo podatkov zastarijo vsakih nekaj let, tako pa tudi tehnologija, potrebna za hrambo in uporabo elektronsko arhiviranega gradiva. To zahteva prenos podatkov iz enega sistema hrambe podatkov v novejši sistem in obliko.« (Žumer, 2008, str. 329) Dokument v digitalni obliki lahko ohranimo le, če se nosilec in zapis prilagajata vedno novim tehnologijam.

»Čeprav je mogoče elektronsko hrambo opredeliti kot zadnjo fazo življenjskega cikla dokumenta (če ne gre v poznejše varno uničenje), lahko brez zadržkov zavrđimo, da gre za pomembnejši del celotnega življenjskega cikla dokumenta.« (Dečman, 2007)

### **Primer dolgoročne hrambe na papirju in v elektronski obliki na računu**

**Dolgoročna hramba na papirju** - Prejete račune z vsemi potrebnimi prilogami (naročilnica, dobavnica, prevzemnica in likvidacijski list) po zaključenem procesu likvidacije običajno spnemo skupaj za vsako naročilo posebej, preluknjamo in vstavimo v registrator. Na ta način so računi shranjeni v primernih arhivskih prostorih, do katerih imajo dostop samo pooblašćene osebe (DOSTOPNOST).

Račun, ki je natisnjen s postopkom termične obdelave (in ni obstojen), običajno pred hrambo fotokopiramo z laserskim tiskalnikom in s tem zmanjšamo možnost izbrisa podatkov (UPORABNOST).

Težje pa je zagotoviti, da med obdobjem hrambe ni nihće odstranil (ali dodal) kakšnega papirja in s tem spremenil izvirnik dokumenta (CELOVITOST). V papirnem svetu to rešujemo v praksi tako, da ugotavljamo celovitost na način, ali ima en račun ob sebi vse obvezne priloge. Vsebino paketa standardiziramo in pooblastimo osebo, ki pred arhiviranjem preveri, ali so vsi paketi celoviti. Pooblašćene osebe zaradi strahu, da ne bi bilo kaj narobe oziroma pomanjkljivo opravljeno, iste dokumente večkrat prilagajo drugim osnovnim dokumentom. Tako postanejo računi priloge pogodbam ali carinski dokumentaciji, čeprav so že v osnovi shranjeni v registratorju med prejetimi računi. Eden od razlogov, da kopiramo v nedogled in odlagamo kopije po arhivih, je torej strah. Drugi razlog je, da smo zaradi procesa ustvarili takšno mapo, ki je vključevala tudi kopije. Pred arhiviranjem je treba iz takšnih map izločiti te priloge oziroma dokumente, ki so že v arhivu.

Če ne moremo zagotoviti celovitosti, je posledično tudi težje dokazati, da je vsebina računa enaka kot pred arhiviranjem (AVTENTIČNOST). Pri tem so nam na voljo forenziki in grafologi, ki ugotavljajo pristnost lastnoročnih podpisov. V praksi se bolj redko lotevamo takšnega dokazovanja pristnosti. Pristnost dokumentov skoraj vedno dokazujemo skozi vsebine povezanih dokumentov, ki dokazujejo verjetnost poslovnega dogodka, ki naj bi ga »sporni« dokument dokumentiral (veriga od zahtevka za nabavo oziroma ponudbe do plačilnega naloga).

**Elektronska dolgoročna hramba elektronskih kopij papirnih izvirnikov oziroma skenogramov** - Papirni račun z vsemi prilogami skeniramo, označimo z iskalnimi atributi, klasificiramo in shranimo v sistem za dolgoročno elektronsko hrambo. Tako shranjen račun lahko preprosto poiščemo in je uporabnikom dostopen le v nekaj korakih. Za

omejitev dostopa do dokumentov skrbijo v sistem vnešene uporabniške pravice (DOSTOPNOST).

Račun je v sistemu za dolgoročno elektronsko hrambo shranjen skladno s standardom Enotne tehnološke zahteve (ETZ). ETZ opredeljuje, v kakšnem formatu naj bodo dokumenti v elektronski obliki zapisani, da jih bomo lahko prebrali tudi po preteku večletnega obdobja (UPORABNOST).

Za preverjanje in dokazovanje, da smo pri zajemu v sistem za dolgoročno elektronsko hrambo skenirali vse pripadajoče liste enega računa, skrbijo različne kontrole, s katerimi nadzorujemo proces pretvorbe (CELOVITOST). To je celovitost zajema oziroma pretvorbe. Za celovitost dokumenta pri hrambi pa moramo znati dokazati, da se ni spreminjal (dodajal/odvzemal).

Za zagotavljanje nespremenljivosti elektronskih zapisov v celotnem obdobju elektronske hrambe (AVTENTIČNOST) poskrbimo z različnimi tehnološkimi sredstvi, kot so varni časovni žig, varni elektronski podpis, »prstni odtis« dokumenta, ciklično preverjanje dokumentov in podobno. Po navadi rešujemo zagotavljanje celovitosti in avtentičnosti z enakimi tehnološkimi in organizacijskimi prijemi. (Pauletič, I., 2011)

### **3 PRAVNA UREDITEV ELEKTRONSKE HRAMBE**

Tako pri klasični, kot pri elektronski hrambi moramo upoštevati predpise, ki zagotavljajo verodostojnost, trajnost, celovitost in dostopnost.

Le elektronska hramba, ki upošteva predpisane zakonske pogoje, standarde in priporočila, zagotavlja podatkom v elektronski obliki pravno veljavnost in verodostojnost ter hkrati njihovo varno ter zanesljivo arhiviranje.

#### **3.1 ZAKON O ELEKTRONSKEM POSLOVANJU IN ELEKTRONSKEM PODPISU**

V Sloveniji je temelje hrambi elektronskega gradiva postavil leta 2000 sprejeti Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1, Uradni list RS, št. 98/04). Bistveni pomen zakona je, da pod posebnimi pogoji elektronskemu podpisu priznava enako pravno veljavo in dokazno vrednost, kot jo ima v papirnatem svetu lastnoročni podpis.

Dokumenti, zapisi ali podatki se lahko hranijo tudi v elektronski obliki (Žumer, 2008, str. 330):

- če so podatki, vključeni v elektronskem dokumentu ali zapisu, dosegljivi in primerni za kasnejšo uporabo,
- če so podatki shranjeni v obliki, v kateri so bili oblikovani, poslani ali prejeti ali v kaki drugi obliki, ki verodostojno predstavlja oblikovane, poslane ali prejete podatke,
- če je iz shranjenega elektronskega sporočila mogoče ugotoviti, od kod izvira, komu je bilo poslano ter čas in kraj njegovega pošiljanja ali prejema,
- če uporabljena tehnologija in postopki zadostno onemogočajo spremembo ali izbris podatkov, ki ju ne bi bilo mogoče enostavno ugotoviti, ali če obstaja zanesljivo jamstvo glede nespremenljivosti sporočila.

#### **3.2 UREDBA O POGOJIH ZA ELEKTRONSKO POSLOVANJE IN ELEKTRONSKO PODPISOVANJE**

Podrobnejše pravne in tehnične detajle je uredila Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000, 2/2001, 86/2006). Uredba določa merila, ki se uporabljajo za presojanje izpolnjevanja zahtev za delovanje overiteljev, ki izdajajo kvalificirana potrdila. Opredeľuje tudi vsebino notranjih pravil overiteljev, ki izdajajo kvalificirana potrdila. Prav tako definira tehnične pogoje za elektronsko podpisovanje in preverjanje varnih elektronskih podpisov in časovno veljavnost kvalificiranih potrdil in pogojev uporabe varnih časovnih žigov.

### **3.3 ZAKON O VARSTVU DOKUMENTARNEGA IN ARHIVSKEGA GRADIVA**

Zakon o varstvu dokumentarnega in arhivskega gradiva (ZVDAGA, Uradni list RS, št. 30/2006), vsebuje in poudarja načelo »ohranjanja dokumentarnega gradiva oziroma uporabnosti njegove vsebine«, saj ureja način, organizacijo, infrastrukturo in izvedbo zajema ter hrambe dokumentarnega gradiva v fizični in elektronski obliki, veljavnost oziroma dokazno vrednost takega gradiva, varstvo arhivskega gradiva in pogoje za njegovo uporabo. Določa tudi naloge arhivov in javne arhivske službe ter s tem povezane storitve in nadzor nad izvajanjem. Zakon izenačuje verodostojnost digitalno in analogno reproduciranih kopij z izvirniki na papirju, če tako digitalizacija kot hranjenje in dostop potekajo v skladu s predpisi.

Arhivski zakon je pravno uveljavil elektronske podatke in dokumente v digitalni obliki, tj. izvirne elektronske dokumente, pa tudi reprodukcije različnih oblik dokumentov, če so bili zajeti, pretvorjeni ali reproducirani v digitalno obliko ter zapisani na nosilce pod pogoji, ki temeljijo na zakonskih načelih (Žumer, 2008, str. 331):

- ohranjanja dokumentarnega gradiva in uporabnosti njegove vsebine,
- trajnosti gradiva in trajnosti reprodukcije njegove vsebine,
- celovitosti, nespremenljivosti, integralnosti, urejenosti in dokazljivosti vsebine in reprodukcije vsebine,
- dostopnosti in varstva kulturnega spomenika.

### **3.4 UREDBA O VARSTVU DOKUMENTARNEGA IN ARHIVSKEGA GRADIVA**

Uredba o varstvu dokumentarnega in arhivskega gradiva (UVDAGA, Uradni list RS, št. 86/2006), kot podzakonski akt, podrobneje ureja delovanje in notranja pravila organizacij, ki hranijo dokumentarno in arhivsko gradivo. Ureja pripravo na zajem in hrambo gradiva v fizični in digitalni obliki, notranja pravila o hrambi dokumentarnega gradiva, splošne pogoje ter registracijo in akreditacijo opreme in storitev za digitalno hrambo.

### **3.5 ENOTNE TEHNOLOŠKE ZAHTEVE IN NOTRANJA PRAVILA**

Enotne tehnološke zahteve za elektronsko hrambo gradiva v digitalni obliki (ETZ), ki jih je na podlagi ZVDAGA sprejel in objavil Arhiv Republike Slovenije na spletni strani konec leta 2006, v skladu s predpisi, mednarodnimi standardi in priporočilom MoReq (Model zahtev za upravljanje elektronskih dokumentov) ter zahtevami informacijske in arhivske stroke, določajo postopke elektronske hrambe in druga opravila, povezana s hranjenjem elektronskega gradiva v digitalni obliki ter hrambo gradiva v drugih oblikah.

Arhiv Republike Slovenije je aprila 2011 sprejel drugo različico ETZ 2.0., kjer so poglavja vsebinsko zaokrožena in zahteve usmerjene k posameznim skupinam uporabnikov (javnopravne osebe in zasebnopravne osebe kot ponudniki storitev). ETZ je tako oblikovan v tri sklope:

- uvodna poglavja,

- enotne tehnološke zahteve za zajem in hrambo gradiva v digitalni obliki in
- dodatne enotne tehnološke zahteve za ponudnike, strojno in programsko opremo ter storitve (postopki akreditacije opreme...).

### Notranja pravila

Z nekaterimi pomanjkljivostmi se lahko spopademo s tehničnimi sredstvi, ki preprečujejo poseganje v avtentičnost in celovitost elektronsko hranjenih dokumentov, za druge pa le tehnična sredstva niso dovolj in so zato potrebni tudi organizacijski ukrepi. Načeloma je pri zagotavljanju varovanja informacij vedno potrebno ravnovesje med obema vrstama ukrepov - več organizacijskih ukrepov zagotovimo, manj bomo potrebovali tehničnih in obratno, vedno pa je najboljša in najbolj zanesljiva rešitev sestavljena iz prave mere obeh, ta pa je odvisna od različnih dejavnikov. Notranja pravila ureja Zakon o varstvu dokumentarnega in arhivskega gradiva (ZVDAGA, Uradni list RS, št. 30/2006, 18. člen), ki pravno veljavnost in dokazno vrednost elektronsko hranjenih dokumentov pogojuje z obstojem in izvajanjem posebnih notranjih pravil o hrambi dokumentarnega gradiva. Enota dokumentarnega gradiva v elektronski obliki je zato na podlagi zakona enaka izvorni enoti le, če je bila pretvorba in hramba tega gradiva opravljena v skladu z notranjimi pravili, ki jih je predhodno potrdil Arhiv Republike Slovenije.

Podrobneje način priprave sprejetja in zahtev za potrditev notranjih pravil določa Uredba o varstvu dokumentarnega in arhivskega gradiva. Vse javnopravne osebe ali podjetja, ki izvajajo zajem in hrambo gradiva v digitalni obliki ter spremljevalne storitve in želijo to storitev akreditirati, potrebujejo notranja pravila. Pravila izdelajo v obliki internega pravnega akta, ki mora biti potrjen s strani Arhiva Republike Slovenije. Ta pravila definirajo notranjo organizacijo, vloge in odgovornosti ter kompetence in usposobljenost zaposlenih. Opisujejo glavne dele posameznih procesov, kot so na primer zajem gradiva, pretvorbo, preverjanje in drugo. Določajo tudi odgovorne osebe za izvedbo posameznega procesa ter opredeljujejo dokumentacijo, ki pri zajemu in hrambi nastaja. To so različne evidence, na primer evidence o zajemu in evidence napak.

Nadzor izvajanja notranjih pravil vrši Arhiv Republike Slovenije preko preizkušenih revizorjev informacijskih sistemov.

### **3.6 UREDBA O VAROVANJU TAJNIH PODATKOV**

Uredba o varovanju tajnih podatkov (UVTP, Uradni list RS, št. 74/05) določa načine in oblike označevanja tajnih podatkov, fizične, organizacijske in tehnične ukrepe ter obvezne sestavine postopkov za varovanje tajnih podatkov. Uredba v 28. členu v skladu z uporabo predpisov o poslovanju z dokumentarnim gradivom določa pogoje za evidentiranje dokumentov, ki vsebujejo tajne podatke, kadar se uporablja informacijska tehnologija. Pogoj ločene hrambe je izpolnjen, če se uporablja rešitev, ki je fizično ločena od drugih informacijskih rešitev, ali pa temelji na tehnologiji navideznega zasebnega omrežja in uporablja kripto zaščitne postopke in ukrepe, ustrezne stopnji tajnosti obdelovanih tajnih podatkov ter izpolnjuje druge pogoje, določene v predpisu iz 39. člena te uredbe.

## 4 SISTEMI ZA UPRAVLJANJE Z ELEKTRONSKIMI DOKUMENTI

Sistemi za upravljanje elektronskih dokumentov omogočajo obvladovanje velike količine podatkov, kjer število zapisov lahko dosega milijone dokumentov, uporablja pa jih tisoče uporabnikov ne glede na lokacijo uporabe. Soočene z naraščajočo kompleksnostjo in zahtevnostjo informacijskih tehnologij, organizacije vse pogosteje posegajo po tehnologijah, ki prinašajo nove funkcionalnosti in lažji dostop do znanja, hkrati pa bistveno ne posegajo v delovanje obstoječih sistemov. Sistemi za upravljanje dokumentov lajšajo delo uporabnikov, hkrati pa skrbnikom poslovnih procesov omogočajo boljši nadzor. (Golob, 2005)

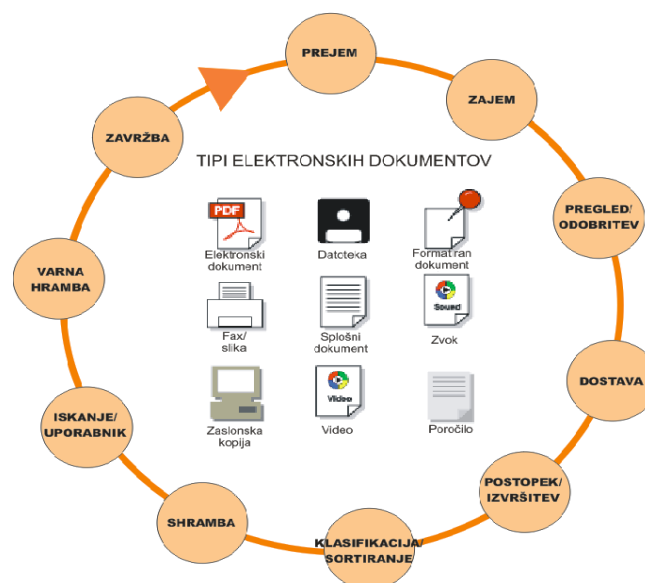
Sprague (1995, str. 31) elektronske sisteme za obvladovanje dokumentov definira kot sisteme, ki:

- uporabljajo moderno informacijsko tehnologijo,
- vsebujejo dokumente v obliki, ki je razumljiva in strukturirana ter
- omogočajo kreiranje, shranjevanje, prenos, obdelovanje in priklic dokumentov za organizacijske potrebe.

### 4.1 TEHNOLOGIJA EDMS

Elektronski sistem za obvladovanje dokumentov (angl. EDMS – Electronic Document Management ) je informacijski sistem, ki obvladuje dokumente v elektronski obliki ter jih nadzira skozi njihov življenjski cikel od nastanka do arhiviranja. (Dular, 2005, str. 610)

Slika 2: Prikaz življenjskega cikla dokumenta



Vir: I-ON Communications (2012)



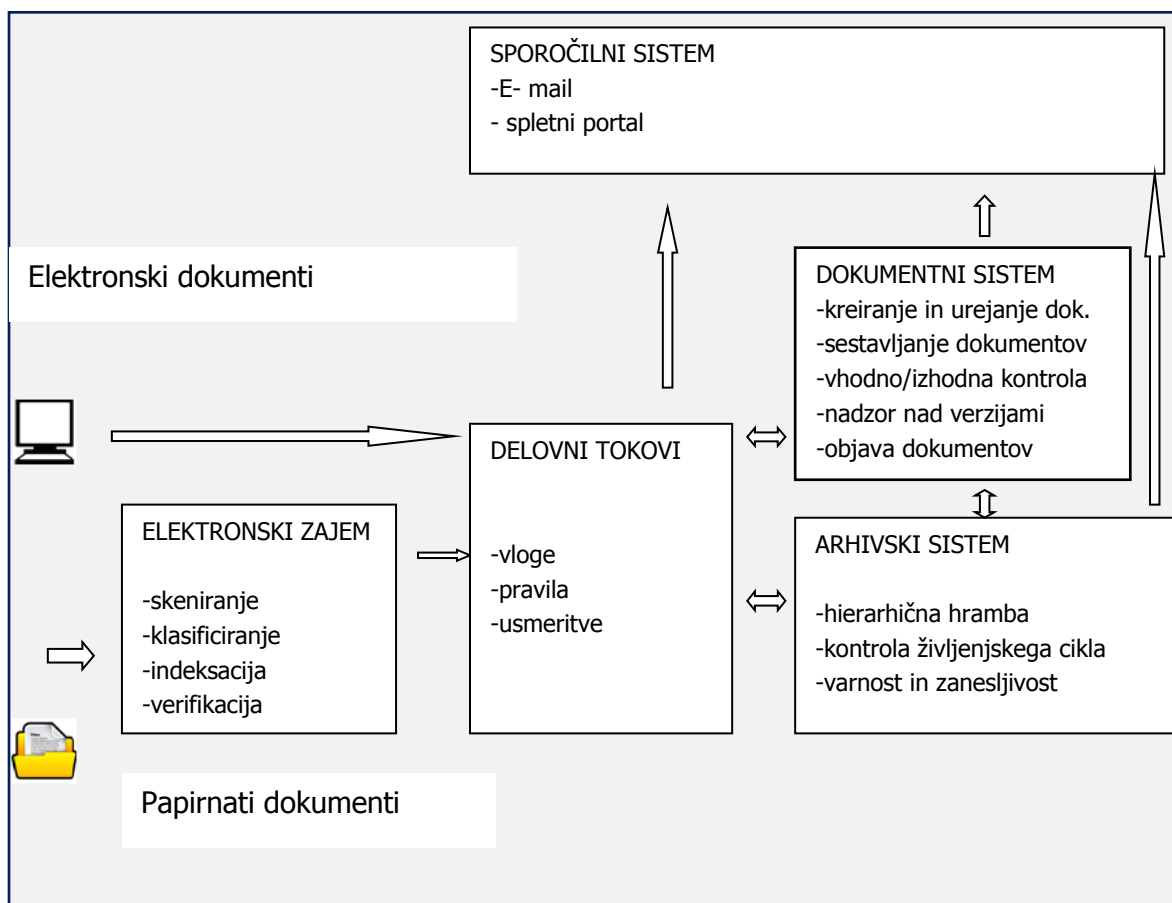
#### 4.1.1 ŽIVLJENJSKI CIKEL DOKUMENTA

Vsak dokument gre skozi faze življenjskega cikla, kot jih prikazuje Slika 2:

- nastanek: dokument lahko nastane v ali izven organizacije, lahko je popolnoma nov, ali pa je samo verzija predhodnika,
- pregledovanje: zelo redki dokumenti nastanejo samo na enem mestu, večinoma so rezultat skupinskega dela,
- potrjevanje: dokument mora biti potrjen pred objavo in veljavnostjo,
- varen dostop: dokument omogoča izmenjavo informacij in idej ter pogosto poraja nastanek novih dokumentov,
- izločanje iz arhiva: izločanje ali zavrnitev lahko pomeni uničenje, izročitev v javne arhive ali pa kakšno drugo aktivnost prenosa dokumenta iz arhiva.

Elektronski arhiv mora zagotavljati nadzor in upravljanje z vsemi fazami življenjskega cikla dokumentov (nastanek, pregledovanje, varen dostop in izločanje iz arhiva). V vsaki fazi mora ponuditi tudi ustrezna orodja za delo z dokumenti, predvsem je to pomembno v fazi nastanka dokumenta, kjer je potrebna podpora za skupinsko delo.

**Slika 3: Shematski prikaz sistema za elektronsko upravljanje dokumentov**



Vir: Golob (2004, str. 3)

Slika 3 prikazuje arhitekturo sistema za upravljanje elektronskih dokumentov z vsemi navedenimi tehnologijami in sporočilnim sistemom, ki povezuje module.

**Elektronski zajem** dokumentov je sestavljen iz digitalizacije dokumentov, klasificiranja, indeksacije in verifikacije. Omogoča zajem dokumentov iz različnih virov, vključuje pa tudi opremo za digitalizacijo, tehnologijo obdelovanja obrazcev in inteligentno prepoznavanje znakov. EDMS omogoča tudi vnos metapodatkov dokumentom ročno ali samodejno. Elektronski zajem se zaključi z verifikacijo dokumentov.

**Dokumentni sistem** je jedro sistema za upravljanje elektronskih dokumentov. Dokumentni sistem skrbi za:

- kreiranje in urejanje dokumentov,
- zagotavljanje podpore za sodelovanje uporabnikov pri oblikovanju vsebine dokumenta, pri njegovem potrjevanju, objavi in seznanjanju,
- vhodno in izhodno kontrolo,
- nadzor nad verzijami dokumentov,
- objavo dokumentov,
- obveščanje o novih dokumentih,
- povratne informacije o tem, kdo je bil seznanjen s spremembami dokumenta,
- zagotavljanje revizijske sledi,
- replikacijo dokumentov, ki jo omogoča klasifikacijski sistem med strežniki, za kopiranje in skupno rabo informacij o dokumentu. Replikacija omogoča izboljšanje storitev iskanja in skupne rabe dokumentov v primeru večjega števila strežnikov.

Dokumentni sistem nam delo z dokumenti olajša, poskrbeti pa mora tudi za varno obvladovanje pravic dostopa do dokumenta in do operacij, ki jih uporabnik nad dokumentom lahko vrši. Vključevati mora elektronski podpis in preverjanje istovetnosti (avtentikacijo) uporabnikov.

### **Arhiviranje dokumentov**

Pri arhivu gre za hierarhično urejeno hrambo razvrščenih dokumentov. Vsak dokument (objekt) v arhivu ima pripadajočo indeksno kartico (arhivska kartica), na kateri so navedeni podatki o tem objektu (metapodatki). Postopki obvladovanja arhiva zagotavljajo varnost, ki določa kdo ima pravico dostopa do posameznega objekta ter nadzorujejo hrambo objektov, ki določa koliko časa se posamezen objekt hrani in na kakšen način ga izločimo iz arhiva. Elektronsko arhiviranje lahko opredelimo kot zadnjo fazo, vendar najpomembnejšo fazo sistema za celovito upravljanje z dokumenti. Vsi objekti v elektronskem arhivu se sistematično upravljajo, vsi postopki pa so nadzorovani. Elektronski arhiv primarno omogoča funkcije zajema, hierarhične shrambe, varnega dostopa in nadzora življenjskega cikla dokumentov. Vsi objekti v elektronskem arhivu morajo biti tudi ustrezno zaščiteni. Elektronski arhiv mora tako zagotavljati elemente avtentikacije ter avtorizacije uporabnikov na različnih ravneh – od celotnega arhiva do posameznega hranjenega objekta. Znotraj elektronskega arhiva je potrebno tudi popolno sledenje vsem dogodkom, administrativnim in uporabniškim. Tako lahko zagotovimo verodostojnost zapisov v elektronskem arhivu. Podatke o uporabniški aktivnosti lahko uporabimo tudi za analizo dostopov, ki nam pokaže prednostne zahteve (želje) uporabnikov ali pa nam omogoči personalizacijo elektronskega arhiva. (Golob, 2004)

## 4.2 ELEKTRONSKO PODPISOVANJE

V želji po zagotovitvi celovitosti in avtentičnosti podatkov so bile v preteklosti razvite različne tehnike, ki so se z napredkom tehnologije izboljševale. Danes sta najučinkovitejše sredstvo za zagotavljanje celovitosti in avtentičnosti podatkov digitalni podpis in časovni žig. Njuno pravno enakost z lastnoročnim podpisom pri uporabi pod določenimi pogoji, zagotavlja Zakon o elektronskem poslovanju in elektronskem podpisu.

Varen elektronski podpis mora biti povezan izključno s podpisnikom in je tako iz njega mogoče zanesljivo ugotoviti podpisnika. Hkrati mora biti podpis tehnološko zasnovan tako, da je povezan s podatki, na katere se nanaša, in bi bila opazna vsaka sprememba teh podatkov ali povezava z njimi, ki bi se zgodila po podpisu. Podpisnik mora podpis oblikovati s pomočjo sredstev za varno elektronsko podpisovanje pod svojim izključnim nadzorom.

Varen elektronski podpis mora biti overjen še s kvalificiranim digitalnim potrdilom, ki ga lahko izda le akreditirani overitelj, njegova vloga pa je v dokazovanju istovetnosti identitete lastnika javnega ključa. Nadalje varen časovni žig zagotavlja podpis dokumenta z veljavnim digitalnim potrdilom v določenem trenutku. Časovni žig povezuje datum in čas podpisa, identiteto podpisnika in podatke v elektronski obliki na kriptografsko varen način.

## 4.3 INFORMACIJSKA VARNOST

Informacijska varnost je poleg človeškega faktorja, prostorov, informacijske tehnologije in postopkov povezanih z upravljanjem elektronskega gradiva ena od temeljnih gradnikov sistema e-hrambe. Principi informacijske varnosti temeljijo na celovitosti, razpoložljivosti in dostopnosti ter zaupnosti in tajnosti podatkov.

Pojem **celovitosti** predstavlja varovanje podatkov pred neavtoriziranimi spremembami ter točnosti in popolnosti podatkov. **Razpoložljivost in dostopnost** razumemo v smislu varovanja podatkov in servisov pred prekinitvami v delovanju ter zagotavljanju podatkov pooblaščenim uporabnikom v času in na način, kot jih potrebujejo. **Zaupnost in tajnost** pa predstavlja varovanje poslovnih in osebnih podatkov pred razkritji. Tako informacijska varnost obsega določanje in uporabo ukrepov za zaščito tajnih podatkov, ki se obdelujejo, shranjujejo in prenašajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov pred naključno ali namerno izgubo tajnosti, celovitosti ali razpoložljivosti ter ukrepov za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov. Z vidika sistema upravljanja varovanja informacij (SUVI) je potrebno na osnovi zakonodaje, predpisov, direktiv, uredb, standardov in dobre prakse sprejeti organizacijske in tehnološke ukrepe.

**Organizacijski ukrepi** zajemajo redno posodabljanje ocene tveganja, sprejetje ustreznih poslovnikov in politike o varovanju informacij, nujno potrebno je razmejiti odgovornosti in dolžnosti pri izvajanju načel varovanja informacij ter skrbeti za ustrezno raven varnostne kulture zaposlenih.

**Tehnološki ukrepi** zajemajo implementacijo varnostnih tehnologij, kot so požarni zidovi, protivirusna zaščita, sistemi za nadzor dostopa do sistemov in mrež, digitalna potrdila in omogočanje uporabe le teh v aplikacijah ter mnoge druge.

Informacijska varnost je vedno odvisna od človeških virov. Zato mora organizacija poskrbeti, da svoje zaposlene redno izobražuje in usposablja, nove zaposlene pa ustrezno preveri.

Informacijski sistemi, kjer se smejo obravnavati tudi tajni podatki morajo zadostiti ustreznim varnostnim zahtevam Urada za varovanje tajnih podatkov. Le ta določa splošne varnostne zahteve šifrirnih rešitev. Šifrirne rešitve so šifrirna strojna in programska oprema in sistemi, ki se uporabljajo za varovanje podatkov v komunikacijsko informacijskih sistemih v katerih se obravnavajo tajni podatki. Potrdilo o varnostni ustreznosti izda Urad Vlade RS za varovanje tajnih podatkov za vsako šifrirno rešitev posebej. Potrdilo se izda na podlagi ovrednotenja predložene šifrirne rešitve, ki ga opravi Komisija za informacijsko varnost v primeru, da se bodo uporabile v sistemih, ki obravnavajo tajne podatke. Urad za varovanje tajnih podatkov vodi evidence šifrirnih rešitev, za katere je izdano potrdilo o varnostni ustreznosti.

Splošne varnostne zahteve šifrirnih rešitev so naslednje (UVTP, 2012):

- izvedeni morajo biti takšni šifrirni primitivi, ki omogočajo zaščito tajnih podatkov,
- zaščiten mora biti pred nepooblaščenim ravnanjem in uporabo,
- onemogočiti mora nepooblaščen odkritje vsebine in varnostno pomembnih parametrov,
- onemogočiti mora nepooblaščen in neugotovljivo spreminjanje šifrirnih modulov in algoritmov, vključno z nepooblaščenim spreminjanjem, nadomeščanjem, vrinjenjem ali izbrisom šifrirnih ključev in drugih varnostno pomembnih parametrov,
- med delovanjem mora biti vidno stanje v katerem je,
- zagotovljeno mora biti pravilno delovanje varnostnih mehanizmov,
- zagotovljeno mora biti odkrivanje napak med delovanjem in vzpostavljen mehanizem, ki preprečuje kompromitiranje varnostno pomembnih parametrov

#### **4.4 AKREDITACIJA HRAMBE GRADIVA V ELEKTRONSKI OBLIKI**

S ciljem regulacije trga ponudnikov opreme in storitev ZVDAGA (Uradni list RS, št. 30/2006, 83. člen in 85. člen) hrambo arhivskega in dokumentarnega gradiva ureja s postopkom registracije ponudnikov in akreditacije pri Arhivu Republike Slovenije. Akreditacija opreme storitev elektronske hrambe pomeni, da je način izvajanja storitve v celoti preverjen, zato predstavlja najvišji možni nivo zakonske skladnosti. Akreditacija je postopek, s katerim Arhiv Republike Slovenije prizna skladnost ponujene opreme ali storitev elektronske hrambe z Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih (Uradni list RS, št. 30/2006), Uredbo o varstvu dokumentarnega in arhivskega gradiva (Uradni list RS, št. 86/2006), Enotnimi tehnološkimi zahtevami in pravili stroke.

Akreditacija tako hranjenemu elektronskemu gradivu zagotavlja:

- Avtentičnost: dokazljivost povezanosti reproducirane vsebine z vsebino izvirnega gradiva oz. izvorom tega gradiva (ZVDAGA, Uradni list RS, št. 30/2006, 27. člen) in
- verodostojnost: »ohranjanje izvirnih lastnosti dokumenta v daljšem časovnem obdobju glede na kontekst, strukturo in vsebino« - dokument je tisto, kar naj bi bil. (Hajtnik, 2011)

## **5 UVEDBA SISTEMA ZA UPRAVLJANJE Z DOKUMENTI V IZBRANEM ORGANU DRŽAVNE UPRAVE**

V izbranem organu državne uprave je bil v letu 2011 uveden sistem za upravljanje z dokumenti. Zahteve izbranega organa državne uprave glede informacijske rešitve so bile precej specifične. Informacijski sistem uporablja preko 4000 uporabnikov, ki delajo na različnih lokacijah v Sloveniji in tujini. Spletno aplikacijo za elektronsko upravljanje z dokumenti je bilo treba povezati še z drugimi sistemi, kot na primer z informacijskim sistemom za oddajo javnih naročil in sklepanje ter spremljanje realizacije pogodb, s sistemom za digitalno podpisovanje, z internim poštnim strežnikom in pisarniškim paketom MS Office.

Poleg zahtev po povezavah z omenjenimi informacijskimi sistemi je pri vpeljavi elektronskega upravljanja z dokumentarnim gradivom poseben izziv predstavljalo tudi upoštevanje strogih varnostnih ukrepov. Interno omrežje izbranega organa namreč nima fizične povezave z internetom in je povsem ločeno omrežje.

Nova informacijska rešitev naj bi zajela celotni življenjski cikel dokumentov, od prejema oziroma izdelave dokumenta do njegove hrambe v stalni zbirki. Hkrati pa je bilo potrebno razviti tak informacijski sistem, ki bo znotraj organizacije funkcionalno in tehnološko omogočal povezljivost s poslovnimi procesi, ki so že bili informacijsko podprti.

Osnovni namen implementacije novega sistema je bil poleg celovitega upravljanja z dokumentarnim gradivom, poenotenje poslovanja in povečanje kakovosti ter učinkovitosti poslovnih procesov.

Spletna aplikacija danes evidentira celotno življenjsko pot dokumentarnega gradiva, hkrati pa uporabnikom omogoča, da elektronsko pošto izmenjujejo tudi z 'zunanji' naslovniki. Za to se uporablja fizičen prenos sporočil prek pomnilniških ključkov, ki je avtomatiziran in ga celovito opravljajo v glavnih pisarnah.

### **5.1 ELEKTRONSKO OBVLADOVANJE DOKUMENTARNEGA GRADIVA**

Dokumentni sistem se povezuje z zalednimi sistemi, aplikacijami in drugimi zbirkami podatkov ter raznimi evidencami, kar je bil eden izmed pomembnih pogojev pri odločanju organizacije za ta informacijski sistem.

Da bi se izognili prepogostemu spreminjanju in specifičnemu prilagajanju aplikacije posameznim uporabnikom, ima dokumentni sistem definiran in uveden splošni vmesnik za povezavo, s katerim komunicira z ostalim 'svetom'. Integracija omogoča združevanje šifrantov znotraj organizacije ter dnevno osvežitev ali prenašanje iz drugih sistemov (dobavitelji, stroškovna mesta, druge baze podatkov). Aplikacija omogoča tudi tako vrsto integracije, ki omogoča prenos določene akcije, izvedene v sistemu, na neki zaledni

sistem. Na primer: ko se v EDS digitalno podpiše dokument, je to informacijo mogoče sporočiti zalednemu sistemu.

EDS je povezan z informacijskim sistemom za vodenje kadrovske evidence, kjer se nahajajo informacije o tem, kateri organizacijski enoti zaposleni pripada, kakšno stopnjo zaupnosti dokumenta lahko posamezni zaposleni obravnava, vzpostavljena je tudi povezava s signirnimi znaki in klasifikacijskim načrtom, ki je osnova za razvrščanje zadev in dokumentov obravnavanega organa državne uprave.

Vzpostavljena je povezava s šifrantom poslovnih partnerjev v obliki izvedene zbirke osebnih podatkov, kjer je bilo potrebno s preišljenimi in učinkovitimi postopki zagotoviti ustrezno varstvo osebnih podatkov, obenem pa ne žrtvovati učinkovitosti doseganja zasledovanih ciljev z vidika učinkovitosti, praktičnosti in varnosti. Tako so v evidence vpisani le podatki, ki jih posreduje pošiljatelj in ki so potrebni, da se mu odgovori (ime, priimek, naslov, kraj, država). Podatki o zaposlenih niso del te evidence, razen če z organizacijo komunicirajo preko vhodno/izhodne pošte. V tem primeru se podatki zabeležijo na podlagi njihove pošte in ne iz kadrovske evidence. Vsi vpogledi se zabeležijo v dnevnik dostopov. Iskanje po šifrantu se, kadar je najden poleg imena in priimka tudi naslov fizične osebe, zabeleži v dnevnik dostopov. Hkrati se zabeleži tudi namen vpogleda (npr. vpis pošiljatelja vhodne pošte). V dnevnik dostopov se beleži tudi iskanje subjektov s strani administratorja sistema, ko le ta uporabi možnost izvoza subjektov, pa mora zato navesti razlog izvoza.

EDS je uporabniško naravnani sistem. Uporabnika vodi skozi njegove zadožitve in delovne procese preko uporabnikovih aktivnosti, saj se možne akcije, ki jih mora uporabnik v nekem trenutku izvesti, avtomatično prilagajajo trenutni aktivnosti, uporabnikovi vlogi in njegovim pravicam. Zaradi povezave s pisarniško zbirko MS Office in poštnim programom Outlook aplikacija omogoča izvajanje dela z dokumenti kar v urejevalniku besedil Word, obveščanje o novi nalogi pa poteka preko programa Outlook.

Po uvedbi nove informacijske rešitve je bila ustanovljena delovna skupina za upravljanje s spremembami, ki skrbi za nadaljnji razvoj in povezovanje obstoječih informacijskih sistemov z EDS, zaznava in analizira potrebe po spremembah ter pripravlja možne rešitve EDS. Delovna skupina sodeluje z udeleženci posameznih procesov z namenom analiziranja možnosti in izdelave rešitev za optimizacijo posameznih procesov ter postavlja prioritete in roke realizacije sprememb, ki jih usklajuje s predstavniki posameznih procesov.

### **5.1.1 OD ZAJEMA DO ARHIVA**

Vhodna pošta se zaradi razpršenosti organizacijskih enot po Sloveniji in v tujini zajema na več mestih. Uporabniki na posameznih vstopnih točkah lahko prejemajo le dokumente, ki so naslovljeni na njihovo organizacijsko enoto, hkrati pa morajo biti za to opravilo pooblaščen.

### **5.1.1.1 Zajem prejetih dokumentov**

Na prejeti dokument je potrebno najprej odtisniti prejemno štampljko z datumom prejema. Dokument se nato opremi s črtno kodo, in skenira. V primeru, da je na ovojnici navedena oznaka 'Osebno' ali 'Odpira naslovnik', se pošta v zaprti ovojnici posreduje naslovljencu. Če ta kasneje presodi, da je vsebina pošte pomembna za delo organa, posreduje pošto vstopni točki, ki izvede zajem in evidentiranje gradiva.

### **5.1.1.2 Evidentiranje prejetih dokumentov**

Uslužbenec najprej preveri kvaliteto zajema in samodejno prenesene podatke (črna koda), potem pa vnese še osnovne podatke o prejetem dokumentu. Nekateri podatki se ustvarijo avtomatično, na primer številka dokumenta, po uvrstitvi v zadevo tudi zbirka gradiva, samodejno se izbere aktivna zbirka – zbirka nerešenih zadev, podatek o vstopni točki, datum zajema, datum evidentiranja in črna koda. Podatke, kot so pošiljatelj, vrsta pošiljke ali vrsta dokumenta, uslužbenec izbira iz seznamov, le manjši nabor podatkov, kot so število prilog, kratka vsebina dokumenta, pa zahteva ročni vnos.

O dokumentu se vodijo tudi podatki, ki se nanašajo na način hrambe (ali gre za elektronski in/ali fizični dokument), pregled dela na dokumentu, kjer sistem samodejno ustvarja pregled vseh izvedenih akcij na dokumentu - sledenje. Nadalje se vodi podatek o pravici do izvedb akcij na dokumentu, kjer se vodijo podatki o stopnji zaupnosti dokumenta in podatki o nosilcih pravic za dostop do dokumenta, omogočen pa je tudi v pogled v vsebinsko povezane dokumente.

Ko je preverjanje o tem ali so vneseni vsi metapodatki zaključeno, se dokument posreduje v potrjevanje pristojnemu naslovniku. Prejeti dokumenti se shranjujejo v depojih vstopnih točk. Ločeno se shranjujejo dokumenti z omejenim rokom hrambe in dokumenti, ki imajo status arhivskega gradiva. Na koncu postopka zajema in evidentiranja se dokument posreduje v reševanje pristojni organizacijski enoti.

### **5.1.1.3 Izdelovanje in evidentiranje lastnih dokumentov**

Uporabnik lastne dokumente v sistemu vidi v posebnem razdelku 'Lastni dokumenti'. Nov dokument je potrebno uvrstiti v zadevo in ga posredovati v reševanje sodelujočim, potrjevalcem in nazadnje podpisnikom dokumenta. Med urejanjem dokumenta sodelujoči vidnosti še nimajo. Potrjevalci in podpisniki lahko po shranitvi vnašajo spremembe neposredno na dokument.

Če se dokument pošilja zunanjim naslovnikom, se mu pripne podatek, da gre za izhodni dokument. Pošiljatelj navede zunanje prejemnike in način posredovanja (elektronska, fizična oblika) in pošto preusmeri v Glavno pisarno. Glavna pisarna s pomočjo pomnilniškega ključka pošto prenese v drugo omrežje in ga posreduje zunanjim naslovnikom.



#### **5.1.1.4 Elektronsko podpisovanje in overjanje dokumentov**

V skladu s 102. členom Zakona o obrambi ima obravnavani organ državne uprave organiziran enoten in avtonomen informacijski ter telekomunikacijski sistem. Upravlja z infrastrukturo javnih ključev za potrebe obrambe države SIMoD-PKI (angl. Slovenian Ministry of Defence Public Key Infrastructure).

V okviru SIMoD-PKI deluje korenski overitelj, podrejeni overitelji digitalnih potrdil in izdajatelji varnih časovnih žigov.

Digitalna potrdila overiteljev SIMoD-PKI so danes namenjena izključno službeni uporabi v obravnavanem organu.

Osnovni nameni uporabe digitalnih potrdil overiteljev SIMoD-PKI so:

- preverjanje digitalnega podpisa ali
- šifriranje ali
- preverjanje digitalnega podpisa in šifriranje.

Overitelji izdajajo in upravljajo digitalna potrdila za:

- zagotavljanje varnostnih storitev pri hranjenju in prenosu podatkov z ali brez stopnje tajnosti,
- digitalno podpisovanje datotek, sporočil in elektronskih obrazcev,
- preverjanje istovetnosti oseb in gradnikov komunikacijsko informacijskega sistema kot so strežniki, usmerjevalniki, požarne pregrade in imeniki. (MO RS, 2012)

#### **5.1.2 OSEBNI PODATKI**

Posebna pozornost je v sistemu elektronskega poslovanja z dokumenti namenjena tudi specifični obravnavi osebnih podatkov. Vsem dokumentom, ki vsebujejo osebne podatke in so bili zajeti ali izdelani v EDS, je potrebno dodatno omejiti vidnost. Takšni dokumenti so na primer odločbe o sprejemu v delovno razmerje, o premestitvi, sklepi o prenehanju delovnega razmerja, o upokojitvi, o disciplinski odgovornosti, dovoljenje za dostop do tajnih podatkov, zdravniško spričevalo in mnogo drugih. Uslužbenec, ki je pristojen za reševanje zadeve z dokumenti, ki vsebujejo osebne podatke, mora za vidnost dokumenta obvezno vpisati razlog vpogleda v dokument.

#### **5.1.3 ZBIRKE DOKUMENTARNEGA GRADIVA**

Zbirke dokumentarnega gradiva, roke in načine hrambe določa Uredba o upravnem poslovanju. Dokumentarno gradivo se tako hrani v zbirki nerešenih zadev, tekoči zbirki in stalni zbirki. Organi vodijo tudi evidence izločenega gradiva, kjer so zbrani le identifikacijski podatki o dokumentih od preteka roka hrambe dalje.

V zbirki nerešenih zadev so dokumenti vidni vsem uslužbencem, ki so zadolženi za posamezne dokumente oziroma morajo biti z njimi seznanjeni. Dokumenti v fizični obliki, ki niso bili zajeti v EDS se hranijo pri uslužbencih, ki so zadolženi za njihovo rešitev. Preden se zadeva reši, morajo biti zaključeni vsi dokumenti. Potem nosilec zadeve zadevo zaključi, skrbniki dokumentov v fizični obliki pa morajo skrbniku tekoče zbirke predati tudi

dokumente v fizični obliki, ta pa nato v sistem zavede spremembo mikrolokacije dokumentov.

Prenos dokumentarnega gradiva iz tekoče v stalno zbirko ureja 185. člen Uredbe o upravnem poslovanju (UUP, Uradni list RS, št. 20/05, št. 101/10). Po tej določbi se dokumentarno gradivo iz tekoče zbirke prenese v stalno zbirko po poteku dveh let, najkasneje do konca marca naslednjega leta.

Pred prenosom pa se iz tekoče zbirke odbere dokumentarno gradivo, katerega rok hrambe je dve leti ter se izloči in uniči. Prenos zadev iz tekoče v stalno zbirko se ne izvaja avtomatično, ampak ročno, saj se hkrati izloča nepotrebno dokumentarno gradivo. Arhivar na seznamu označi dokumente, ki ustrezajo pogojem za prenos, to je, da je rok hrambe daljši od dveh let in da so se v tekoči zbirki že hranili polni dve koledarski leti. Pri tem lahko v stalno zbirko prevzame posamezne dokumente, za ostale iz iste zadeve pa sproži postopek uničenja. Najprej izvede poizvedbo o dokumentarnem gradivu, ki je predmet predaje v stalno zbirko, potem pa tudi poizvedbo, katerim zadevam oziroma dokumentom je skladno z načrtom klasifikacijskih znakov organizacije rok hrambe dve leti potekel. Na seznamu tako dobi dokumente, ki se lahko uničijo. Po potrditvi dokumentov za izločitev, se za posamezno organizacijsko enoto pripravi Zapisnik o uničenju dokumentov in seznam dokumentov, ki je bil predan v stalno zbirko. Organizacijska enota fizične dokumente uniči ter podpiše Zapisnik o uničenju dokumentov. Po podpisnem zapisniku o uničenju, se številka zapisnika prenese med podatke o uničenju k posameznim uničenim dokumentom, dokumentom v elektronski obliki pa EDS samodejno izbriše sliko.

Obravnavani organ državne uprave posluje z akreditiranim sistemom za elektronsko upravljanje z dokumentarnim gradivom. V tem trenutku pa žal še nima potrjenih notranjih pravil, saj je to glede na specifičnost delovanja in obsežnost organa precej obsežen postopek. Pričakovati je, da bo do zaključka postopka potrditve notranjih pravil prišlo zelo kmalu. To bo pomembno vplivalo na poslovanje z dokumentarnim gradivom, saj bo po ZVDAGA (Uradni list RS, št. 30/2006, 31. člen) vsaka enota varno hranjenega gradiva v digitalni obliki štela za enako posamezni enoti izvirnega gradiva. V skladu s 13. členom istega zakona pa bo zadoščeno pogojem, da se izvirno gradivo po opravljeni pretvorbi iz papirnega v digitalno obliko lahko uniči. Shranjevanje izvirnih dokumentov z omejenim rokom hrambe v depojih vstopnih točk bo tako optimizirano.

#### **5.1.4 POZITIVNI UČINKI UVEDBE INTRENUTNE POMANJKLJIVOSTI**

»Kljub velikemu številu prednosti, ki jih prinaša implementacija elektronskega dokumentnega sistema je po ocenah AIIM 50% implementacij neuspešnih.« (Zebec, 2010, str. 27) Razlogi za to so v nepopolni implementaciji, neupoštevanju vseh ključnih elementov EDMS, predvsem uporabnikov, ki zavračajo spremembe, nepravilni klasifikaciji dokumentov in mnogih drugih.

Z uvedbo EDS je bil v obravnavanem organu državne uprave dosežen želeni cilj, doseči celovito digitalizacijo internega poslovanja in vhodno izhodnih tokov dokumentarnega gradiva ter hitrejši pretok informacij v organu.

Med razloge, da je bila uvedba EDS v obravnavanem organu državne uprave uspešna, pa lahko naštejemo naslednje:

1. prehod na nov sistem je bil istočasen za vse uporabnike obravnavanega organa,
2. projekt je imel močno podporo vodstva,
3. pripravljenost uporabnikov na prehod je bila dobra, mnogi so sodelovali v prototipni izvedbi, prav vsi pa so bili vključeni v izobraževanje,
4. e-pismenost uporabnikov je bila na zadovoljivi ravni,
5. uspešno je bila presežena vsebinska in organizacijska heterogenost organizacije,
6. močna tehnična in vsebinska podpora na številno najmočnejših lokacijah v obliki podpore uporabnikom.

Vsaka novost prinese uvedne težave in nujno terja čas, da se zaposleni navadijo nanjo. Končni cilj uvedbe EDS je poslovati povsem brezpapirno. Na ta način se bo skrajšal čas obravnave posameznega dokumenta in povečala sledljivost obravnave dokumenta. Nov sistem pa omogoča tudi večjo preglednost poslovanja. Navsezadnje se z uvedbo ponuja tudi priložnost za spremembo organizacije, saj omogoča podporo delu na skupinskih projektih iz oddaljenih lokacij brez fizične prisotnosti.

Med pozitivne učinke uvedbe dokumentnega sistema lahko štejemo:

- prihranek časa zaradi hitrejšje izmenjave podatkov - dokumenti, oziroma njihove zadnje različice so na voljo vsem, ki v procesu sodelujejo že med nastajanjem dokumenta, zagotovljen je dostop do zadnje različice dokumenta, dokument lahko uporabniki pregledujejo in vnašajo pripombe neposredno vanj. Polovica dokumentov je pregledanih in podpisanih v manj kot enem dnevu,
- prihranek pisarniškega in potrošnega materiala, potreba po tiskanju dokumentov se je bistveno zmanjšala,
- prihranek pri prostoru za papirni arhiv je vedno večji,
- povečala se je varnost in nadzor nad dokumenti,
- povečala se je hitrost pošiljanja in iskanja dokumentov,
- večja je tudi kakovost pri poslovanju s strankami,
- delo z dokumentarnim gradivom je sledljivo, dokumenti se ne izgubljajo, zato delo poteka neprimerno hitreje in enostavneje.

Trenutne pomanjkljivosti, ki se kažejo po uvedbi elektronskega dokumentnega sistema so predvsem obsežni poslovni procesi, ki jih v celoti še ni mogoče združevati z elektronskim dokumentnim sistemom. Razlogi za to so bodisi v sledenju področnih predpisov, ki še niso ustrezno posodobljeni, ali pa v potrebni spremembi organizacije dela. Delna uvedba pa vzbuja dvome v to, da bodo doseženi pravi rezultati.

## **5.2 BREZPAPIRNO POSLOVANJE NA FINANČNO RAČUNOVODSKEM PODROČJU, E-RAČUN**

V vsaki organizaciji nastaja obsežna dokumentacija na vseh področjih delovanja. Dokumentacija s področja financ in računovodstva pa ima za posledico spremembe v

poslovnih dogodkih, ki spreminjajo stanje sredstev, obveznosti do virov sredstev ter prihodke in odhodke. Elektronsko poslovanje s to kategorijo dokumentov mora torej poleg že omenjenih pravnih podlag omogočati tudi področna zakonodaja.

Gre torej za precej obsežno področje, v katerem nastopa množica, tako prejetih, kot tudi lastnih in odposlanih dokumentov. V nadaljevanju bom opisala poslovanje na finančno računovodskem področju v izbranem organu in na nivoju države, ker sta oba segmenta med seboj močno povezana.

### **5.2.1 UVAJANJE ELEKTRONSKEGA POSLOVANJA S PODROČJA RAČUNOV NA NIVOJU DRŽAVNE UPRAVE**

Informacijski sistem (IS) MFERAC (enotni računovodski sistem Ministrstva za finance) neposrednim proračunskim uporabnikom in Ministrstvu za finance omogoča nadzor izvrševanja proračuna in vodenja enotnega računovodstva. Projekt MFERAC je voden na državni ravni s strani Ministrstva za finance, vanj pa so vključena vsa ministrstva in organi v sestavi, v zadnjem obdobju pa tudi lokalna samouprava. Vse rešitve, ki so implementirane so takoj na razpolago vsem državnim organom, samo uvajanje pa je običajno daljši proces, saj zahteva tudi organizacijske in druge spremembe v posameznih ministrstvih, organih v sestavi in občinah.

»Tako je v okviru državne uprave informacijski sistem MFERAC edini že implementirani sistem, ki sledi hitro se spreminjajoči zakonodaji na obravnavanih področjih. Informacijski sistem MFERAC sestavljajo medsebojno povezane aplikacije, ki pokrivajo področja priprave, nadzora in izvajanja državnega proračuna, glavne knjige in saldakontov, kadrovske evidence in stroškov dela, vodenja osnovnih sredstev, stanovanjskih kreditov in najemnin ter domače in devizne blagajne.« (Sladoje, Dimc, 2010)

Projekt uvajanja e-računov v poslovanje državne uprave je ena od pomembnih nalog, ki si jih je zadalo vodstvo projekta MFERAC. Cilj projekta je v zagotovitvi zajema elektronskih in fizičnih računov v dokumentni sistem, obravnava teh računov, izmenjava podatkov z IS MFERAC in dostop do računov v elektronski obliki iz IS MFERAC. Cilj uvedbe je tudi, da zajame različne dokumentarne sisteme, ki jih uporabljajo različni organi državne uprave.

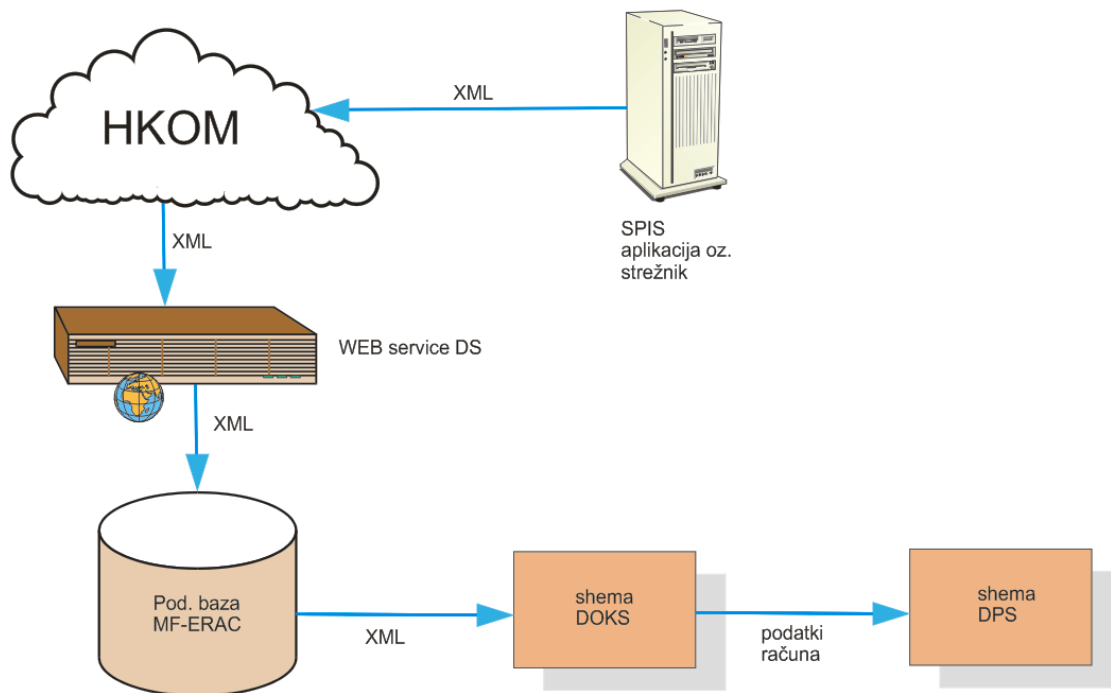
Izgradnja sistema je bila razdeljena v več faz. (Mrzel, Muljavec, 2011)

Prva faza izgradnje sistema je vsebovala evidentiranje vhodnih računov v dokumentni sistem in prikaz slike računa v IS MFERAC:

- evidentiranje in skeniranje računa v dokumentnem sistemu,
- enkratni vnos podatkov in prenos evidenčnih podatkov ter slike računa v MFERAC,
- sledljivost fazam obdelave posameznega računa.

Prva faza obdelave računa je potekala pri evidentiranju osnovnih metapodatkov in skeniranju računa.

**Slika 4: Pošiljanje metapodatkov računa**



Vir: Kralj (2010)

Slika 4 prikazuje povezavo dokumentnega sistema SPIS (dokumentni sistem za podporo pisarniškemu poslovanju) s sistemom MFERAC. Prikazana je izmenjava metapodatkov računa med sistemoma preko Hkom omrežja.

Druga faza povezave je omogočila potrjevanje računa s strani odgovornih oseb preko dokumentnega sistema in povratno informacijo o potrditvi v IS MFERAC (sprememba statusa računa). Omogočen je bil tudi elektronski podpis odredbe za izplačilo iz proračuna, ki je izdelana v MFERAC ter evidentiranje povratne informacije o podpisu v MFERAC. Tako je bilo dodanih pet novih pomembnih funkcionalnosti:

- izmenjava statusov potrjevanja računov,
- združevanje elektronskih odredb,
- pošiljanje e-odredb v EDS,
- e-podpisovanje odredb v EDS,
- samodejno evidentiranje povratne informacije iz EDS v MFERAC.

Tretja faza je omogočila še prikaz slike računa v aplikaciji Glavna knjiga s saldakonti.

## **5.2.2 UVAJANJE ELEKTRONSKEGA POSLOVANJA S PODROČJA RAČUNOV V OBRAVNAVANEM ORGANU DRŽAVNE UPRAVE**

V obravnavanem organu se računi vodijo v Knjigi prejetih računov v aplikaciji IS MFERAC-DPS.

Račun pride v Glavno pisarno, kjer ga opremijo z žigom – datumom prejema. Kurir račune dvakrat dnevno fizično nese iz Glavne pisarne v Službo za finance. Nekatere račune pa organizacijske enote dobijo direktno. Vnosnih mest, kjer račune evidentirajo tudi sami, ima obravnavana organizacija zaradi velike dislociranosti več deset. Glavna pisarna in Služba za finance tako evidentirata približno 30% vseh prejetih računov. Služba za finance, kot tudi dislocirane organizacijske enote, ki račun prejmejo direktno, le tega evidentirajo v aplikaciji MFERAC-DPS (Državni proračun Slovenije). V primeru da to izvede Služba za finance, račun fizično odpošlje organizacijski enoti, ki je plačnik računa. Finančni delavec račun pregleda, če ta ni pravilen, ga zavrne dobavitelju in o tem z dopisom obvesti Službo za finance. Če je račun pravilen, ga finančnik fizično odpošlje v pregled strokovni službi. Po potrditvi strokovne službe finančni delavec v MFERAC-DPS izdelava odredbo za izplačilo iz proračuna. Račun in pripadajočo odredbo opremi še z vso zakonsko zahtevano dokumentacijo ter jo preda v podpis odredbodajalcu. Podpisano odredbo s pripadajočo dokumentacijo pošlje v kontrolo v Službo za finance, kjer ugotovijo ustreznost dokumentacije in finančno pravilnost izdelane odredbe. Odredbo elektronsko pošljejo v Službo za računovodstvo (DPS-GKS), istočasno pa v Službo za računovodstvo fizično posredujejo tudi zbrano dokumentacijo. Nekatere odredbe in račune v Službo za računovodstvo pošlje kar finančni delavec organizacijske enote, brez predhodne kontrole finančne službe. V Službi za računovodstvo dokumentacijo pregledajo še iz računovodskega stališča in po predpisanih postopkih izvedejo plačilo.

V letu 2011 je bilo na opisan način obdelanih skoraj 80.000 računov s strani 4000 poslovnih partnerjev. Zanimivo je dejstvo, da je slaba tretjina računov izstavljena s strani desetih različnih dobaviteljev, kar je dobra osnova za nadaljnje uvajanje e-računov in posledični prihranek tako finančnih, kot tudi kadrovskih virov.

V obstoječem stanju izvajanja procesa evidentiranja, kontrole in izvedbe plačila so ugotovljene naslednje slabosti:

- računi se založijo oziroma izgubijo,
- pomanjkljiva je sledljivost obravnave računa – ni točne informacije, kje se račun trenutno nahaja, predvsem je to problem pri vsebinski likvidaciji s strani strokovnih delavcev,
- časovni zamiki zaradi lokacijske razpršenosti in kontrolnih točk (kontrola finančnega poslovanja v Službi za finance in računovodska obdelava v Službi za računovodstvo),
- poraba papirja zaradi tiskanja zakonsko zahtevanih dokumentov in arhiviranja na več mestih,
- nekonsistentno izvajanje procesa,

- prevelika razdrobljenost, ki je pogosto posledica zajema podatkov na mestu nastanka.

Navedene slabosti tako predstavljajo naslednja tveganja:

- zamude pri plačilih,
- netransparentno poslovanje,
- oteženo ugotavljanje časovnih zakasnitev pri posameznih strokovnih službah.

### **5.2.3 UVAJANJE INTEGRACIJE SISTEMOV MFERAC IN EDS**

V obravnavanem organu državne uprave je bilo vzpostavljeno testno okolje tako, da sta se povezala oba ključna sistema, MFERAC in EDS. V tem času je bila že omogočena druga faza evidentiranja vhodnih računov, kar je pokazalo na določene prednosti in slabosti:

#### **Prednosti:**

- Račun je evidentiran v dokumentnem sistemu in se ne vodi več kot 'nevidentirano gradivo' (le to je opremljeno le z žigom in datumom prejema). MFERAC DPS vsebuje modul za evidentiranje računov, vendar pa bi na ta način pridobili tudi evidenco računov enako kot za ostale dokumente.
- Bistveno se je povečala sledljivost, transparentnost in pretočnost finančnih dokumentov.
- Omogočeno je bilo digitalno podpisovanje odredb za izplačilo iz proračuna.

#### **Slabosti:**

- Bistveno povečan obseg dela v glavni pisarni in ostalih vstopnih točkah, saj bi na ta način morali skenirati in opremiti z obveznimi metapodatki še približno 80.000 vhodnih dokumentov, kamor pa niso vštete vse obvezne priloge kot so naročilnica, dobavnica, materialni list, prevzemni zapisnik in druge.
- Originalni dokument - račun ni hranjen v depozitu glavne pisarne, pač pa je v fizični obliki potoval skozi vse organizacijske enote do Službe za računovodstvo. Pravilnik o postopkih za izvrševanje proračuna (Uradni list RS, št. 50/2007), ki med drugim ureja tudi postopke, obrazce in druge dokumente za prevzemanje obveznosti v breme proračuna ter evidentiranje prevzetih obveznosti trenutno še ne predvideva elektronskega poslovanja na finančno računovodskem področju za organe javne uprave.
- V tem času se je kot velika pomanjkljivost izkazalo tudi omogočeno spreminjanje podatkov v MFERAC brez vednosti podpisnika v EDS. V EDS se je prenesla PDF datoteka odredbe, kakršna je bila v trenutku prenosa v EDS, na strani MFERAC-DPS, pa ni bilo onemogočenega spreminjanja tega dokumenta. Pri samodejnem evidentiranju povratne informacije iz EDS v MFERAC se je spremenil le status odredbe, ni pa prišlo do vnovičnega preverjanja podpisane vsebine.

#### **5.2.4 ANALIZA UVEDBE IN CILJI PRENOVE POSLOVANJA NA FINANČNO RAČUNOVODSKEM PODROČJU**

V informacijskem sistemu MFERAC se izdelata veliko finančno računovodskih dokumentov. Dokumenti se praviloma izpišejo na tiskalnikih, posredujejo se v podpis eni ali več pooblaščenim osebam, krožijo med organizacijskimi enotami in se na koncu življenjskega cikla shranijo v arhiv. Uradne dokumente je potrebno v skladu z Uredbo o poslovanju z dokumentarnim gradivom registrirati in shraniti. Ravnanje s finančno računovodskimi dokumenti pa ureja tudi Zakon o financah in na njegovi podlagi Pravilnik o postopkih za izvrševanje proračuna.

Glede na težave, s katerimi se organizacija spopada v procesu obvladovanja finančno računovodske dokumentacije so cilji prenove sistema naslednji:

- zagotoviti, da bodo računi pri odgovorni osebi še isti dan, ko so prispeli ter s tem pospešiti likvidacijo računov,
- v elektronsko obliko zajeti vse vhodne račune,
- odpraviti ročno prenašanje računov od ene k drugi odgovorni službi v organizaciji,
- optimizirati finančno računovodski proces,
- uvesti večji nadzor nad dokumenti v smislu nadzorovanega dostopa do dokumentov v obeh sistemih v skladu s poslovnimi pravili,
- uvesti elektronsko hranjenje računov in se s tem izogniti potrebi po dodatnem prostoru za fizični arhiv.

Glede na cilje prenove IS MFERAC, ki ga uporabljajo državni organi, obravnavani organ trenutno lahko izbira med tremi fazami uvedbe e-računa. V nadaljevanju bom opisala prednosti in slabosti uvedbe posamezne faze.

##### **Prva faza**

Uvedba prve faze vsebuje evidentiranje in skeniranje računa v dokumentnem sistemu, enkratni vnos podatkov, prenos evidenčnih podatkov in slike računa v MFERAC ter sledljivost fazam obdelave posameznega računa.

Z uvedbo obravnavanega procesa se v prvi fazi večinoma spremeni le način dela uporabnikov. Proces obdelave vhodnih računov sestavljajo naslednji podprocesi:

**Glavna pisarna:** vsi računi, ki se zdaj le datirajo, se po novem skenirajo, hkrati se na tem mestu vnese še obvezne metapodatke, kot so datum prejema, datum zavedbe, poslovni partner in tip dokumenta.

**Služba za finance:** knjiga prispelih računov - strokovni delavec metapodatkom v dokumentnem sistemu doda še ostale podatke iz originalnega dokumenta. Ti so: originalna številka računa, datum izdaje računa, datum zapadlosti, datum opravljene storitve, transakcijski račun, vsebinski nosilec računa in njegova šifra organizacijske enote.

S tem so zadoščeni vsi pogoji, da se račun avtomatično prenese v sistem MFERAC. Finančni delavec v organizacijski enoti po elektronski pošti dobi sporočilo, da je prejel nov račun. Ko ga pregleda in odobri, ga posreduje v strokovno obdelavo k pooblaščenim osebam.



Pooblaščenca oseba je o novo prispelem računu obveščena po elektronski pošti. Ko bo račun potrdila, bo sistem o tem obvestil finančnega delavca, hkrati pa se bo spremenil tudi status računa v MFERAC-DPS. Finančni delavec sedaj obdeluje račun v sistemu MFERAC, ki mu zagotavlja tudi kompleksne finančne kontrole.

**Prednosti:** Račun je zajet v trenutku prejema v glavno pisarno, večja je sledljivost evidentiranih računov, sistem omogoča enostaven pregled nad računi v obdelavi, s tem se zmanjšuje možnost izgube ali neobdelanost računov zaradi odsotnosti pooblaščenih oseb.

**Priložnosti:** Zaradi spremenjenega vhoda računa, je tehtno analizirati podproces Knjige prispelih računov, saj trenutno opravlja tudi funkcijo glavne pisarne. Z uvedbo EDS pa se delo razdeli na dva podprocesa.

**Pomanjkljivosti:** Dodatno delo za glavno pisarno, ki je račune do zdaj le datirala, izvirniki dokumentov v fizični obliki bodo kljub evidentiranju v EDS potovali k finančnemu delavcu v organizacijski enoti, saj tako določa Pravilnik o postopkih za izvrševanje proračuna (Uradni list RS, št. 50/2007).

## **Druga faza**

Uvedba druge faze omogoča združevanje elektronske odredbe za izplačilo iz proračuna (v nadaljevanju odredbe), samodejno posredovanje le te v EDS, digitalno podpisovanje odredbe ter povratno informacijo o odločitvi podpisnika odredbodajalca (odobri/ne odobri) v MFERAC.

Finančni delavec v organizacijski enoti delo v aplikaciji MFERAC-DPS, ko račun podpiše pooblaščenca oseba, nadaljuje tako, da izdela odredbo ter poskrbi, da se vsa obvezna dokumentacija tudi v elektronski obliki veže na vhodni račun. Ti dokumenti so lahko v papirni ali elektronski obliki, saj nastajajo v zunanjih sistemih (dobavnica, gradbena situacija...) ali v zalednih sistemih organizacije (naročilnica, naročilni list za naročanje po sklenjeni pogodbi, prevzemni zapisnik, materialni list in drugi). V primeru, da je na odredbi označeno, da mora biti posredovana v pregled v Službo za finance v Oddelek za kontrolo finančnega poslovanja (v nadaljevanju OKFP), bo odredbo v elektronskem dokumentnem sistemu najprej prejel delavec v OKFP. Sicer bo v trenutku pošiljanja v podpis posredovana k odredbodajalcu, ta pa bo o tem obveščen po elektronski pošti. Povratna informacija o odločitvi podpisnika bo spremenila status odredbe v odobreno, finančni delavec pa bo nato odredbo lahko posredoval v Službo za računovodstvo.

**Prednosti:** Poenostavljen je postopek za podpisnika, saj odredbo podpiše elektronsko in se ne sooča več z goro papirne dokumentacije, omogočen je dostop do digitaliziranih dokumentov tudi podpisnikom, ki sicer niso uporabniki IS MFERAC, čas podpisovanja dokumentov se bistveno skrajša, skenirani in na račun vezani so tudi vsi obvezni pripadajoči dokumenti, ki se pojavijo v procesu (naročilnica, dobavnica, materialni list, zapisnik o kakovostnem prevzemu in drugi).

**Slabosti:** Uvedba druge faze bi obremenila vstopne točke oziroma glavno pisarno, saj je računov veliko, še več pa je spremnih dokumentov. Pregledovanje elektronskih oblik računov in ostalih spremnih dokumentov je na zaslonu precej težavno opravilo, zato obstaja bojazen, da bodo dokumenti manj kakovostno pregledani in se bo povečalo število napak, ali pa bodo uporabniki dokumente vseeno tiskali na papir.

**Priložnosti:** Odgovornost za pravilnost posameznega podatka se lahko znova presodi, saj ni več potrebno pregledovati pravilnosti vnosa posameznega podatka na vseh stopnjah kontrole.

### **Tretja faza**

Popolnoma brezpapirno poslovanje bi omogočila šele tretja faza uvedbe, ki predvideva ogled slike računa tudi v računovodski aplikaciji GKS (Glavna knjiga s saldakonti). Trenutno to ni mogoče zaradi zakonskih omejitev, poleg tega pa je ogled večjega števila dokumentov precej zamuden in uporabniku neprijazen.

### **5.2.5 UGOTOVITVE**

Čeprav gre z vidika uvajanja elektronskega dokumentnega sistema in dela z dokumenti za enega pomembnejših procesov, ta žal v obravnavani organizaciji še ni zaživel. Razlogi za to so v njegovi kompleksnosti, saj v procesu nastopa veliko število različnih vsebinskih nosilcev. Ključne vloge v procesu imajo Glavna pisarna in dislocirane vstopne točke, Služba za finance s Knjigo prispelih računov, organizacijske enote s svojimi finančnimi službami in strokovnimi potrjevalci, ki račune vsebinsko likvidirajo, odredbodajalci, ki s podpisom odgovarjajo za zakonitost, gospodarnost, upravičenost in namembnost porabe proračunskih sredstev, Služba za finance v vlogi kontrole finančnega poslovanja ter Služba za računovodstvo, ki izvede plačilo in poskrbi za ustrezne knjižbe v poslovne knjige.

Vzrok, zakaj uvedba predstavlja velik in težek korak je kompleksnost področja, saj ta vključuje tako organizacijske, vodstvene kot tudi sociološke probleme, na drugi strani pa tehnološke in zakonske omejitve.

Trenutno je na voljo več možnih scenarijev uvedbe, od možnosti uvedbe zgolj prve faze, ki terja najmanj organizacijskih sprememb in prilagoditev in ne predstavlja prenove poslovanja, temveč obstoječe aktivnosti pokriva z elektronskimi dokumenti do zadnje faze, ki terja spremenjen način dela, vendar pa zato bistveno povečuje učinkovitost poslovanja. Koristi uvedbe bi se pokazale na več področjih. Razbremenjena bi bila kurirska služba, prav tako pa tudi služba računovodstva, ki ima tudi nalogo arhiviranja finančno računovodskih dokumentov. Bistveno bi se zmanjšali tudi materialni stroški, saj bi z uvedbo odpravili kopiranje računov za lastne arhive v posameznih organizacijskih enotah.

Ne glede na vse prednosti, digitalizirani računi, ki jih prejmemo v fizični obliki le delno rešujejo problem premalo učinkovitega poslovanja z računi. Z vzpostavitvijo elektronskega poslovanja bi računi prispeli v elektronski obliki, skeniranje in evidentiranje papirnih dokumentov pa bi postalo prej izjema kot pravilo. V prihodnosti si lahko obetamo tak

način izmenjave podatkov, vendar je v tem trenutku integracija obstoječih sistemov optimalna rešitev. Na podlagi izkušenj pri vpeljavi, bo prehod na elektronsko poslovanje zagotovo predstavljal manjšo in lažje obvladljivo spremembo dela.

Na sprejem odločitve o načinu uvedbe bodo vplivali različni dejavniki: vsebinska in organizacijska heterogenost, podpora vodstva, sodelovanje med različnimi organizacijskimi enotami, strah pred spremembami, nepripravljenost uporabnikov na uvedbo novosti ter izobraževanje.

### **5.3 DOKUMENTI S STOPNJO ZAUPNOSTI**

Zaupne informacije in zaupne podatke je potrebno varovati na poseben način zato, da se z njihovim razkritjem ali zlorabo ne bi povzročale škodljive posledice organizaciji, njenim zaposlenim ali celo širše, državnemu interesu. Bistvo varovanja zaupnosti se kaže v tem, da se smejo s takimi informacijami in podatki, ki so označeni kot zaupni, seznaniti samo upravičeni in pooblaščen posamezniki.

Z zaupnostjo lahko razumemo omejevanje pravice dostopa do pridobivanja take vrste podatkov in informacij ter zmožnost sprejemanja in ohranjanja pridobljenih zaupanih informacij in podatkov, ki so namenjeni le določenim posameznikom.

»Tajni podatki se določajo, obravnavajo in shranjujejo v skladu z Zakonom o tajnih podatkih (ZTP-UPB2, Uradni list RS, št. 50/2006). Kot je zapisano že v 1. členu tega zakona, so se po njem dolžni ravnati državni organi, organi lokalnih skupnosti, nosilci javnih pooblastil ter drugi organi, gospodarske družbe in organizacije, ki pri izvajanju zakonsko določenih nalog pridobijo ali razpolagajo s tajnimi podatki. Za tajnega se določi podatek, ki je tako pomemben, da bi z njegovim razkritjem nepoklicani osebi nastale škodljive posledice za varnost države ali za njene politične ali gospodarske koristi, in se nanaša na: javno varnost, obrambo, zunanje zadeve, obveščevalno in varnostno dejavnost državnih organov Republike Slovenije. V ta okvir sodijo tudi sistemi, naprave, projekti in načrti ter znanstvene, raziskovalne, tehnološke, gospodarske in finančne zadeve. Vendar le, kadar so pomembni za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije.« (Žitko, 2011)

Osebe, ki so za to pooblaščen, morajo glede na možne škodljive posledice razkritja zaupnih podatkov le tem določiti eno od spodaj navedenih tajnosti (ZTP-UPB2, Uradni list RS, št. 50/2006)

- STROGO TAJNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi ogrozilo vitalne interese Republike Slovenije ali jim nepopravljivo škodovalo;
- TAJNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko hudo škodovalo varnosti ali interesom Republike Slovenije;
- ZAUPNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo varnosti ali interesom Republike Slovenije;

- INTERNO, ki se določi za tajne podatke, katerih razkritje nepoklicani osebi bi lahko škodovalo delovanju ali izvajanju nalog organa.

Varovanje in obravnavanje zaupnih podatkov podrobneje določajo naslednje pravne podlage (UVTP, 2012):

- Zakon o tajnih podatkih (ZTP-UPB2, Uradni list RS, št. 50/06, št. 9/10 in št. 60/11),
- Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Uradni list RS, št. 48/07),
- Uredba o varovanju tajnih podatkov (Uradni list RS, št. 74/05, 7/11 in 24/11-popr.),
- Sklep o določitvi pogojev za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja (Uradni list RS, št. 94/06).

Zaupno gradivo se mora poleg samega obravnavanja v postopku nastajanja, tudi po predaji pristojnemu arhivu obravnavati ločeno in varovano po prepisanih postopkih. Tako Uredba o upravnem poslovanju v 191. členu, kot Uredba o varstvu dokumentarnega in arhivskega gradiva v 42. členu določata, da se dokumentarno gradivo, ki vsebuje tajne podatke po Zakonu o tajnih podatkih hrani ločeno.

Ločena hramba gradiva pa prinaša tako koristi kot slabosti.

Med **prednosti** ločene hrambe štejemo hitrejšo najdbo dokumentacije v zbirki, celovito varovanje občutljivih podatkov in razvrščanje po stopnjah tajnosti.

Med **slabosti** ločene hrambe lahko štejemo finančni vložek potreben za zagotavljanje tehničnih pogojev varovanja, kontroliran dostop do dokumentov, administriranje dostopov in vpogledov v dokumentacijo in drugo. (Lavrič, 2008, str. 47)

### **5.3.1 STOPNJA VAROVANJA INFORMACIJSKEGA SISTEMA V OBRAVNAVANEM ORGANU DRŽAVNE UPRAVE**

Obravnavani organ ima zaradi specifik poslovanja ter zahtev po varnosti in razpoložljivosti sistema, organiziran enoten in avtonomen informacijski ter telekomunikacijski sistem, ki z zunanjimi omrežji (Hkom, Internet, ipd.) fizično ni povezan. Prav tako tudi upravlja z infrastrukturo javnih ključev za potrebe obrambe države SIMoD-PKI. Organizacija je pridobila tudi potrdilo o varnostni ustreznosti šifrirne rešitve, ki ga je izdal Urad za varovanje tajnih podatkov, kar pomeni, da so v sistemu lahko hranjeni podatki s stopnjo tajnosti INTERNO.

Prenos podatkov med omrežji se sme izvajati le preko izmenljivih nosilcev podatkov, s katerimi je potrebno ravnati v skladu z varnostno politiko organizacije in v skladu z notranjimi pravilniki. Pri prenosu v zunanja omrežja je treba upoštevati tudi normative akte zakonov o tajnih podatkih in varovanju osebnih podatkov, ki urejajo varovanje v zvezi z vrsto podatkov in v skladu z njimi poskrbeti za zagotovitev zaupnosti in celovitosti podatkov. Za zagotavljanje večje varnosti, ekonomičnosti in praktičnosti se lahko tajni podatki vključno do stopnje tajnosti TAJNO shranjujejo na mikrofilme, magnetne, optične

ali druge vrste nosilcev tajnih podatkov. Shranjevanje mora potekati skladno z zahtevami in navodili organizacije tako, da je zadoščeno zahtevam predpisov, ki urejajo dokumentarno in arhivsko gradivo. Zagotovljena mora biti enaka stopnja varnosti in celovitosti, razpoložljivost in verodostojnost teh podatkov.

Obravnnavani organ državne uprave se z dokumenti stopnje zaupnosti INTERNO in višje srečuje dokaj pogosto.

Po Dravec (2009) je ena največjih pomanjkljivosti varovanja podatkov poleg varnostne kulture posameznikov predvsem sledljivost dokumentov. Z uvedbo elektronskega dokumentnega sistema pa je organizacija dobila mehanizem, ki poleg nadzora nad dokumenti omogoča tudi njihovo sledljivost. Zato se je kmalu po uvedbi EDS pojavila tudi potreba po uvedbi zajema in evidentiranja dokumentov s stopnjo zaupnosti.

Ker ima komunikacijsko informacijski sistem obravnavanega organa varnostno dovoljenje za delovanje sistema do stopnje tajnosti INTERNO (akreditacijo), lahko v elektronskem dokumentnem sistemu obdeluje in hrani tudi dokumente, ki vsebujejo tajne podatke do stopnje tajnosti INTERNO. Dokumente z višjo stopnjo tajnosti pa v EDS lahko le evidentira.

### **5.3.2 SLABOSTI PRED UVEDBO ZAJEMA V EDS**

Slovenska zakonodaja zelo temeljito ureja načine varovanja tajnih podatkov. Odgovornost posameznika in njegova varnostna kultura pa sta tista dejavnika, ki sta v praksi odločilna za dejansko izvajanje zaščite zaupnih dokumentov. Skladno s predpisi mora imetnik hraniti dokumente v varovanih prostorih in železnih omarah s predpisanimi oznakami, glede na stopnjo tajnosti podatkov, ki jih vsebujejo. Zaradi pomanjkljive odgovornosti pa je v preteklosti prihajalo do nepooblaščenega dostopa do dokumentov. Posledično so se ti dokumenti lahko tudi nepooblaščno kopirali. Evidenca o tem, kje so zaupni dokumenti hranjeni je bila zato nezanesljiva. Sledljivost dokumentov po evidentiranju je bila slabša od zelene.

Problem izdelave rešitve je bil precej kompleksen. V prvi vrsti je bilo potrebno zagotoviti podatek o nivoju tajnosti, do katere posamezen udeleženec lahko dostopa. Evidenca dovoljenj za dostop do tajnih podatkov je zdaj zagotovljena preko integracije z informacijskim sistemom MFERAC, v modulu Kadrovske evidence. Ažurno posodabljanje teh podatkov pa je postalo zelo pomemben dejavnik zagotavljanja varnosti.

EDS je moral poleg nadzora nad elektronskimi dokumenti, zagotoviti tudi nadzor nad fizičnimi izvodi zaupnih dokumentov.

### **5.3.3 UVEDBA EDS NA PODROČJE DOKUMENTOV S STOPNJO ZAUPNOSTI**

Tabela 1 prikazuje komponente različnih tipov dokumenta glede na njihov izvor in stopnjo zaupnosti. Posamezna stopnja zaupnosti določa lokacijo hrambe in podatke, ki se v dokumentnem sistemu vodijo o dokumentu.

**Tabela 1: Komponente štirih tipov dokumenta s stopnjo zaupnosti**

Dokument	Komponente		
Vhodni dokument INTERNO brez prepovedi kopiranja	Elektronski dokument s sliko-vsebino	Elektronska evidenca za sledenje fizičnega dokumenta	Fizični dokument (hrani se v glavni pisarni)
Vhodni dokument INTERNO s prepovedjo kopiranja in višje stopnje tajnosti od INTERNO	Elektronski dokument brez slike	Elektronska evidenca za sledenje fizičnega dokumenta	Fizični dokument (pri odgovorni osebi)
Lastni dokument INTERNO	Elektronski dokument s sliko-vsebino in z oceno tveganja	Elektronska evidenca za sledenje fizičnega dokumenta- za vsak posamezen izvod	Fizični dokument za vsak izvod pri odgovornih osebah
Lastni dokument višje stopnje tajnosti od INTERNO	Elektronski dokument brez slike	Elektronska evidenca za sledenje fizičnega dokumenta- za vsak posamezen izvod	Fizični dokument za vsak izvod pri odgovornih osebah

Vir: Lasten

**Lastni dokument s stopnjo zaupnosti interno brez prepovedi kopiranja**

Strokovni delavec mora dokument pripraviti iz ustrezne predloge, ki je izdelana z ustreznimi oznakami tajnosti in ima že tudi prilogo z oceno škodljivih posledic, ki je po zakonu o tajnih podatkih obvezna. Strokovni sodelavec pripravi vsebino dokumenta in hkrati označi razloge za prenehanje tajnosti (dogodek ali datum). Določi še potrjevalce in podpisnike dokumenta. Sistem mu omogoča izbiro le tistih podpisnikov, ki so pooblaščen za navedeno stopnjo tajnosti. Podpisnik hkrati podpiše tako oceno škodljivih posledic, kot sam dokument.

Vsebino dokumenta INTERNO vidijo nosilec dokumenta, potrjevalci in podpisniki dokumenta. Oseba, ki ima sicer vpogled v zadevo, v kateri se dokument nahaja, vidi le metapodatke tega dokumenta, ne vidi pa vsebine.

Podpisnik lahko takoj, ko dokument podpiše, zahteva tudi tiskanje papirnega izvoda. Gre za tiskanje z identifikacijo, hkrati pa je potrebno označiti, komu je tiskan izvod predan. Tako se vrši tudi pravilen nadzor nad papirnimi izvodi.

Podpisan dokument strokovni sodelavec lahko distribuira znotraj internega omrežja, če je to navedeno na samem dokumentu, za kasnejšo distribucijo pa mora zaprositi odgovorno osebo.

### **Lastni dokument višjih stopenj zaupnosti in interno s prepovedjo kopiranja**

Strokovni delavec v sistemu EDS odpre nov dokument in sicer evidenčno. Za to izbere naprej pripravljeno predlogo. Le te so pripravljene glede na stopnjo tajnosti, saj morajo dokumenti s stopnjo tajnosti in glede nanjo, imeti še dodatne oznake. Odgovorna oseba digitalno podpiše le oceno možnih škodljivih posledic, samega dokumenta pa v EDS ne vidi. Vsebino dokumenta podpiše na papirju. Evidenca števila papirnih izvodov in podatek, kje je dokument hranjen se vodi v EDS.

### **Vhodni dokument s stopnjo zaupnosti interno**

V Glavni pisarni s tovrstnimi dokumenti lahko rokujejo samo pooblaščenec in usposobljene osebe. Če gre za dokument, ki je označen z 'Osebno – v roke', velja, da se ga obravnava kot dokument s prepovedjo kopiranja in se ga v Glavni pisarni ne skenira.

Če te oznake nima, je dokument dovoljeno skenirati, potrebno pa je označiti, da gre za dokument s stopnjo zaupnosti INTERNO. Ko so dokumentu dodani tudi vsi metapodatki, se ga lahko posreduje naslovniku, papirni izvod pa hrani glavna pisarna ločeno od dokumentov brez stopnje zaupnosti. Če strokovni delavec ugotovi, da je potrebna izdelava fizičnega izvoda dokumenta, v EDS izdela zahtevek zanj in izbere osebo, ki je s strani predstojnika pooblaščenec za izdelavo pisarniške odredbe za kopiranje dokumenta. Odgovorna oseba za tiskanje potem, ko je pisarniška odredba podpisana, dobi obvestilo o dovoljenju za tiskanje dokumenta.

### **Vhodni dokument višjih stopenj zaupnosti in interno s prepovedjo kopiranja**

Prejeti dokumenti višjih stopenj tajnosti in dokumenti s prepovedjo kopiranja se v Glavni pisarni le evidentirajo. Naslovnik dobi evidentiran dokument brez slike in evidenco papirnega izvoda, ki je zaveden v EDS. Papirni izvodi se v tem primeru ne hranijo v Glavni pisarni, pač pa se v zaprti kuverti posredujejo naslovniku. V EDS se vidi mesto hrambe izvornika dokumenta.

### **Prednosti po dopolnitvah EDS**

Delo z dokumenti stopnje tajnosti INTERNO (brez prepovedi kopiranja) je izenačeno z delom z dokumenti brez stopnje tajnosti. Dokumenti se skenirajo, pri lastnih dokumentih pa se ureja in podpisuje Wordov dokument in se distribuira v elektronski obliki.

EDS je omogočil popolno sledljivost dokumentov s stopnjo zaupnosti, nadzor nad tiskanjem dokumentov in nadzor nad tem, kje se tiskani dokumenti hranijo.

Če katerakoli oseba, ki ima dostop do dokumenta stopnje tajnosti INTERNO, potrebuje papirni izvod (recimo za udeležbo na sestanku), lahko zahteva izdelavo papirnega izvoda. Nosilec papirnega izvoda pa od tu nosi odgovornost, da je izvod pravilno varovan in da evidenca papirnih izvodov pravilno odraža njihovo številčno stanje. Če je tiskan izvod predviden za izhodno pošto, se ne predaja drugi osebi, ampak se pošlje v izhodno pošto. Vsi fizični izvodi so tako evidentirani, v sistemu EDS pa se vidi, komu so bili predani. Prav tako sta onemogočena shranjevanje vsebine dokumenta na lokalni disk in uporaba funkcije zaslonske kopije (print screen).

Fizični izvodi so vodeni v elektronski obliki in so povezani z elektronskim dokumentom. Posamičen elektronski dokument ima lahko več fizičnih izvodov, vsak od njih pa se obravnava kot svoja (samostojna) entiteta.

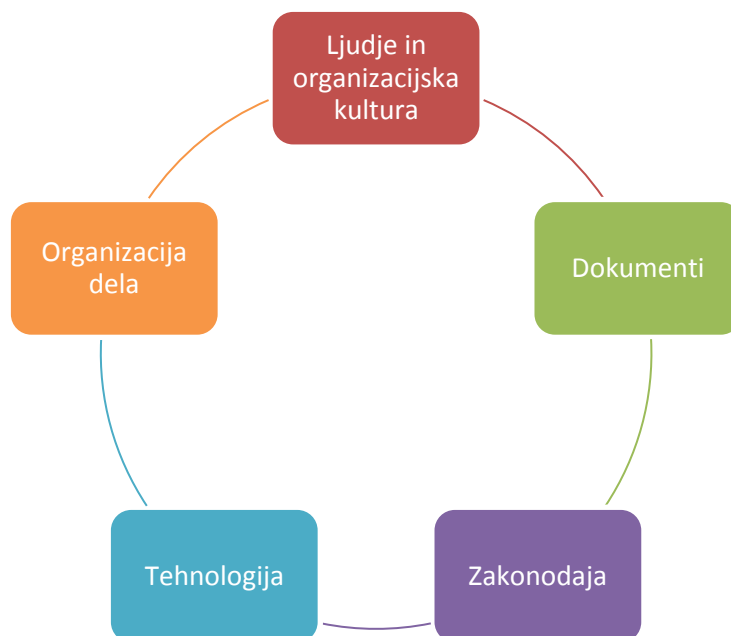
Dokumenti višjih stopenj tajnosti od INTERNO so v dokumentni sistem zavedeni evidenčno, dosegljiva pa je tudi informacija o lokaciji fizičnih izvodov.



## 6 POVZETEK OBDELANIH PODROČIJ

Dokumentni sistem sestavlja pet elementov prikazanih na Sliki 5. To so tehnologija, zakonodaja, ljudje in organizacijska kultura, organizacija dela in dokumenti.

**Slika 5: Dokumentni sistem ustvarja pet elementov**



Vir: PIA IS (2012)

Sistem za upravljanje z dokumenti poleg novih tehnologij, ki omogočajo posodobljen način upravljanja dokumentov in informacij prinaša oziroma zahteva večjo integracijo z ostalimi sistemi. Uvedba zahteva tudi organizacijske spremembe in spremembe poslovnih procesov. K sodelovanju pri načrtovanju in vzpostavljanju sistema je potrebno pritegnili bodoče uporabnike, saj tako sistem postane bolj prilagojen potrebam organizacije in zaposleni raje sodelujejo, ker v uvedbi sistema vidijo določene prednosti. Že od samega začetka projekta, pa je potrebna tudi močna podpora vodstva. Ne nazadnje pa je pri vseh postopkih izgradnje sistema potrebno upoštevati obstoječe zakonske predpise.

V nalogi sem obdelala uvedbo sistema za upravljanje z dokumenti v obravnavani organ državne uprave, podrobneje pa sem raziskala uvedbo oziroma analizo uvedbe dveh različnih kategorij dokumentov. Tako račun kot finančni dokument, kot dokument s stopnjo tajnosti, sta kategoriji dokumentov, s katerimi se ravna drugače kot z ostalim dokumentarnim gradivom. Zato je bilo za uvedbo sistema za upravljanje z dokumenti na ti dve področji potrebno spremeniti funkcionalnosti aplikacije, potrebna pa je tudi prenova poslovnih procesov in organizacije dela. Nadvse pomembna pa je tudi pripravljenost ključnih uporabnikov na spremembe.

## Analiza uspešnosti uvedbe posameznih področij

Uspešnost izvedbe sem analizirala na podlagi petih elementov, ki tvorijo sistem za upravljanje z dokumenti. Stopnje uspešnosti sem uvrstila v pet kategorij: uspešno, delno uspešno, manj uspešno, neuspešno in v fazi odločanja.

**Tabela 2: Analiza uspešnosti uvedbe posameznih področij**

Element dokumentnega sistema	Celovita digitalizacija dokumentarnega gradiva	Dokument s stopnjo zaupnosti	Račun
<b>Zakonodaja</b>	Nepotrjena notranja pravila	Popolnoma ustreza	Področni predpisi na nivoju države še niso popolnoma usklajeni.
<b>Tehnologija</b>	Popolnoma ustreza	Popolnoma ustreza	Digitalizacija je omogočena, predstavlja pa precej dodatnega dela za udeležence v procesu.
<b>Ljudje in organizacijska kultura</b>	Vodstvo, upravljalci sistema in uporabniki so nov sistem sprejeli	Popolnoma ustreza	Področje zahteva prenovu poslovnega procesa, v katerega je vključenih več vsebinskih nosilcev. Ključne odločitve so v fazi sprejemanja.
<b>Dokumenti vseh oblikah</b>	Zajet je celoten življenjski cikel dokumentarnega gradiva, specifične kategorije dokumentov še niso v celoti implementirane	Popolnoma ustreza	Specifična kategorija, ki zajema veliko število prilog. Ogled dokumenta zgolj na ekranu predstavlja za uporabnike oteženo delo.
<b>Organizacija dela in obvladovanje procesov</b>	Organizacija dela na področju dokumentarnega gradiva popolnoma ustreza	Popolnoma ustreza	Optimizacija finančno računovodskega procesa se še proučuje.

Vir: Lasten

V Tabeli 2 so predstavljeni elementi, ki tvorijo sistem za upravljanje z dokumenti. Analizirala sem različna področja uvedbe, pri čemer ugotavljam uspešnost uvedbe glede na posamezne elemente.

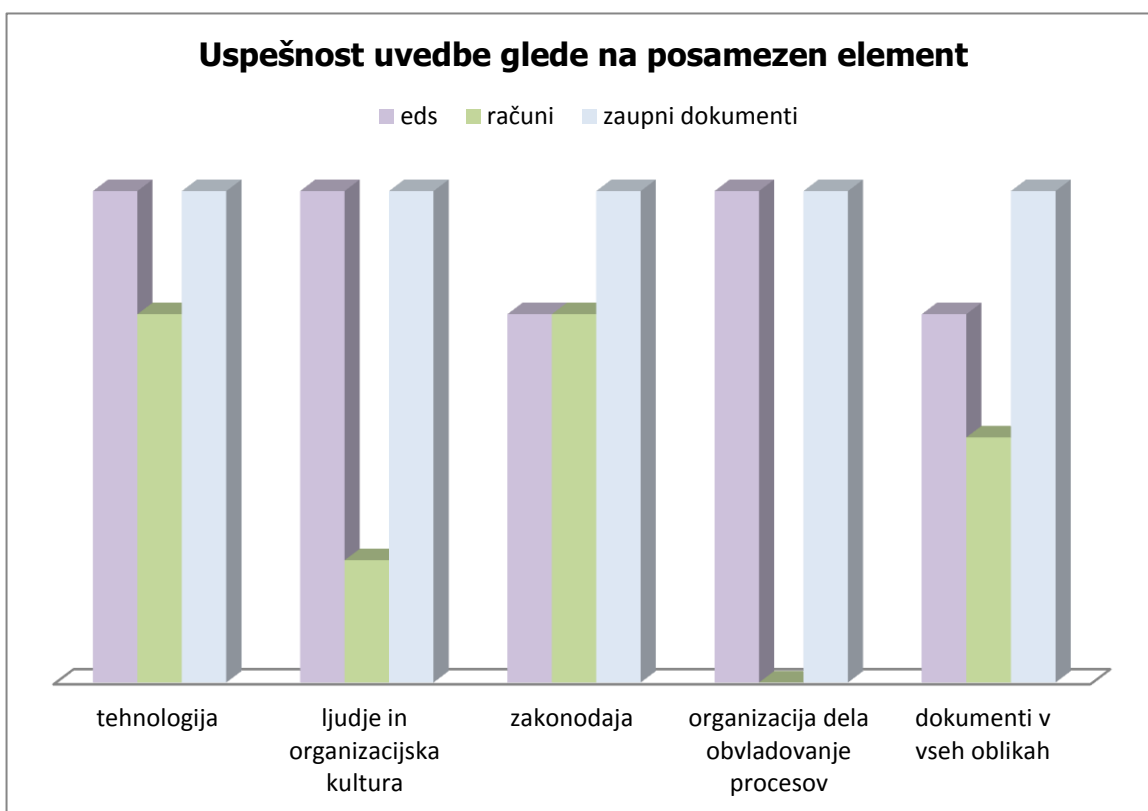
Prav v vseh elementih se je za uspešno izkazala uvedba EDS na področju dokumentov s stopnjo zaupnosti. Razloge za to vidim predvsem v sodobnih pravnih aktih in prilagodljivi informacijski tehnologiji. Dejstvo pa je, da pri prenovi procesa niso bile potrebne večje organizacijske spremembe. Uporabniki so tudi zato novost dobro sprejeli.

Na področju celovite digitalizacije dokumentarnega gradiva obravnavani organ državne uprave še ni povsem uspešen. Uvedba sistema za upravljanje z dokumenti na tem področju je bila v obravnavanem državnem organu dobro sprejeta. Na uspeh je vplivalo več dejavnikov; predvsem močna podpora vodstva, dobro sodelovanje uporabnikov v pilotni izvedbi, izobraževanje in dobra vsebinska ter tehnična podpora. Uvedba EDS je

zajela celoten življenjski cikel dokumentarnega gradiva. Trenutno pa implementacija EDS še ni dosegla vseh procesov, pri čemer ugotavljam, da so izvzeti dokumenti specifičnih kategorij. Ena od prednostnih nalog organa ostaja tudi priprava notranjih pravil, ki so še zadnji pogoj za uvedbo izvajanja dolgoročne hrambe dokumentarnega gradiva, kot ga predpisuje ZVDAGA.

Na področju računov oziroma procesa finančnega poslovanja trenutno ostaja največ nerešenih problemov. Brezpapirno poslovanje na tem področju bo lahko steklo šele z uveljavitvijo posodobljenega Pravilnika o postopkih za izvrševanje proračuna RS. Trenutno veljavni pravilnik namreč še ne predvideva elektronskega podpisovanja finančnih dokumentov. Po izkušnjah ostalih organov državne uprave bi nova tehnologija na uspešnost izvedbe lahko vplivala uspešno, ne moremo pa spregledati dejstva, da digitalizacija papirnih dokumentov predstavlja tudi precej dodatnega dela, predvsem v Glavni pisarni in ostalih vstopnih točkah, kamor so dokumenti v papirni obliki naslovljeni in se zdaj ne skenirajo. Tovrstni dokumenti so se pred uvedbo EDS vodili kot evidenčno gradivo. Uvedba EDS na finančno področje pomeni, da bosta procesa postala neločljivo povezana, kar pa nujno spreminja tudi organizacijo dela. Kot razlog za to, da področje finančnega poslovanja še ni implementirano v EDS naj navedem še kompleksnost področja, saj ta vključuje tako organizacijske, vodstvene kot tudi sociološke probleme, na drugi strani pa tehnološke in zakonske omejitve.

**Grafikon 1: Uspešnost uvedbe glede na elemente EDMS**



Vir: Lasten

Grafikon 1 prikazuje področja, kjer trenutno obstaja največ oziroma najmanj problemov pri uvedbi.

Z vsemi navedenimi ugotovitvami lahko le delno potrdim postavljeno hipotezo, da sistem za upravljanje z dokumenti omogoča upravljanje z dokumentarnim gradivom v elektronski obliki tako, da zajema celotni življenjski cikel dokumentov od prejema oziroma izdelave do hrambe v stalni zbirki. Izpolnjeni morajo biti prav vsi robni pogoji, pri čemer bi izpostavila predvsem usklajenost pravnih aktov in obvladovanje sprememb v samem procesu obvladovanja dokumentarnega gradiva in ostalih podprocesih.

Z gotovostjo pa lahko potrdim hipotezo, da je ob uvedbi sistema za upravljanje z dokumenti potrebno upoštevati kategorizacijo dokumentov. V različnih poslovnih procesih nastopajo številčno in vsebinsko heterogene skupine uporabnikov in nosilcev procesov. Tako je na primer v popolnosti uspela uvedba kategorije dokumentov s stopnjo zaupnosti, kar je predstavljalo precejšen tehnični izziv. Področje se ponaša z vzorno urejenimi in sodobnimi pravnimi akti, prenova samega procesa pa ni terjala večjih organizacijskih sprememb. Za kategorijo finančno računovodskih dokumentov je značilno, da je del obsežnega poslovnega procesa, ki ima lastno evidenco dokumentov in ni del dokumentarnega sistema. Uvedba EDS na to področje terja večje organizacijske spremembe, prav tako pa tudi spremembe področne zakonodaje. Uvedba EDS bo povzročila tudi precej spremenjen način dela, med drugim so za to kategorijo dokumentov značilne številne priloge, ki pa jih je v digitalni obliki težje obvladovati.

## 7 ZAKLJUČEK

Sistemi za upravljanje z dokumenti so v kompleksnih organizacijah postali nujni in nepogrešljivi, saj omogočajo učinkovito spremljanje poslovanja organizacije. Omogočajo sledljivost dokumentov, hiter dostop, enostavno iskanje in varno hrambo. V obravnavanem organu poslovanje z dokumentarnim gradivom v veliki meri že poteka v elektronski obliki. Vzpostavljen je bil tudi sistem, ki v skladu z informacijskimi varnostnimi standardi dovoljuje obravnavo posameznih vrst občutljivih podatkov.

Če lahko trdimo, da je delo z dokumenti v novem sistemu lažje in enostavnejše, pa tega ne moremo trditi za samo uvedbo takšnega sistema. Uvedba upravljanja z elektronskimi dokumenti zahteva spremembe v organizacijski strukturi organizacije in spremembe poslovnih procesov, zato je bila že od samega začetka projekta potrebna močna podpora vodstva. K sodelovanju pri načrtovanju in vzpostavljanju sistema je bilo koristno pritegnili tudi bodoče uporabnike, saj je na ta način sistem postal bolj prilagojen potrebam organizacije, zaposleni pa so sistem hitreje in bolje sprejeli. V novem načinu dela so videli določene prednosti pred klasičnim sistemom za upravljanje z dokumentarnim gradivom.

Namen naloge je bil raziskati razloge in učinke uvedbe sistema za upravljanje z dokumenti v obravnavani organ državne uprave in ugotoviti, ali uvedeni sistem omogoča upravljanje z dokumentarnim gradivom v elektronski obliki tako, da zajame celoten življenjski cikel dokumentov.

Bistvena ugotovitev je bila, da je ob upoštevanju vseh elementov, ki tvorijo EDMS, vpeljava takega sistema lahko uspešna tudi v tako velikem in heterogenem sistemu, kot je obravnavani organ. Cilj uvedbe EDS je bil v zagotovitvi pravočasnega, pravilnega in popolnega evidentiranja dokumentarnega gradiva, kar je organizaciji v celoti uspelo. V tem trenutku pa žal še nima potrjenih notranjih pravil, saj je to glede na specifičnost njenega delovanja in obsežnost, precej dolgotrajen postopek. Sprejem notranjih pravil bo pomembno vplival na poslovanje z dokumentarnim gradivom, saj bo optimizirana tudi fizična hramba gradiva po digitalizaciji.

Nov sistem omogoča tudi povezljivost z ostalimi poslovnimi procesi. Ti se med seboj razlikujejo, saj obravnavajo različne kategorije dokumentov in jih je potrebno vsakega posebej opredeliti. Nekateri procesi so v novem sistemu dokumentiranja uspešno zaživel, spet drugim pa to še ni uspelo.

Podrobneje sem primerjala uvedbo dveh kategorij dokumentov: račun kot finančno računovodsko kategorijo dokumenta in dokument s stopnjo zaupnosti. Njuna skupna lastnost je, da predstavljata specifični kategoriji dokumentov, s katerimi se organizacija ukvarja.

Na podlagi opisanih dejstev ugotavljam, da organizacija še ni izkoristila vseh priložnosti, ki jih novi sistem ponuja.

Na področju brezpapirnega poslovanja s finančno računovodskimi dokumenti sem predstavila možne stopnje implementacije. Za izbiro prave možnosti morajo vsebinski nosilci, ki so del procesa, preučiti vse možne različice, saj slednja od njih prinaša tako določene prednosti kot tudi slabosti. Na tem področju trenutno obstajajo tudi zakonske omejitve, saj vsi področni predpisi še niso usklajeni. Tu mislim predvsem na Pravilnik o postopkih za izvrševanje proračuna RS, ki predpisuje podpisovanje finančnih dokumentov v fizični obliki. Trenutno se že pripravlja njegova posodobitev.

Glede na pozitivne učinke uvedbe EDS pri obravnavi zaupnih dokumentov ugotavljam, da tudi implementacija brezpapirnega poslovanja s finančnega področja lahko prinese več pozitivnih kot negativnih posledic ne ozirajoč se na to, katera različica bi se vpeljala. Ne glede na vse prednosti, ki bi jih prinesla uvedba digitaliziranih finančnih dokumentov, pa je to šele začetek, saj bo vzpostavitev elektronskega poslovanja v prihodnosti odpravila zajem in digitalizacijo, kar trenutno predstavlja večjo obremenjenost. V prihodnost pa moramo stopati pripravljeni, zato je prenova finančno računovodskega poslovanja naloga za danes, implementacijo v obstoječi sistem pa moramo v tem smislu videti kot odlično priložnost.

Uvedba sistema zajema celotno organizacijo in nujno prinaša tudi organizacijske spremembe in spremembe poslovnih procesov. Ključna naloga organizacije, kot dela javne uprave, je v razumevanju problematike in aktivnem vključevanju v spremembe, tako v smislu aktivnega sodelovanja pri posodabljanju pravnih podlag, kot tudi organizacije in optimizacije dela.

## LITERATURA IN VIRI

### – SAMOSTOJNE PUBLIKACIJE

- ANTOLINC, Vanja (2009). Informacijski vidik hrambe elektronskega dokumentarnega gradiva. Fakulteta za upravo, Ljubljana.
- DRAVEC, Anita (2009). Varovanje tajnih podatkov v Republiki Sloveniji: formalni vidik vs. Praksa. Fakulteta za družbene vede, Ljubljana.
- KOREN, Melita (2010). Upravljanje z digitaliziranimi dokumenti v javni upravi. Fakulteta za upravo, Ljubljana.
- KOŽUH, Gregor (2008). Uvedba dokumentnega sistema kot orodja za izboljšanje kakovosti poslovnega procesa. Ekonomska fakulteta, Ljubljana.
- PRELESNIK, Vita (2009). Elektronsko arhiviranje v upravi. Fakulteta za upravo, Ljubljana
- PRIJANOVIČ, Jernej (2011). Umestitev EDMS v poslovni informacijski sistem. Fakulteta za računalništvo in informatiko, Ljubljana.
- ZEBEC, Aleš (2010). *Elektronski sistem za upravljanje z dokumenti*. Ekonomska fakulteta, Ljubljana.
- ŽITKO, Katja (2011). Varovanje in zaščita podatkov v informacijskih sistemih za upravljanje z dokumenti. Fakulteta za upravo, Ljubljana.
- ŽUMER, Vladimir (2008). Poslovanje z zapisi: Upravljanje in hramba dokumentarnega gradiva, klasifikacijski načrti za razvrščanje gradiva z roki hrambe in elektronska hramba gradiva v digitalni obliki, Planet GV, Ljubljana.
- ŽUMER, Vladimir (2001). Priročnik za ravnanje z dokumentarnim in arhivskim gradivom. Planet GV, Ljubljana.

### – ČLANKI V REVIJAH

- DEČMAN, Mitja (2007). Začetek dolgoročne elektronske hrambe v slovenski upravi: trenutno stanje in scenariji prihodnosti. V: SETNIKAR CANKAR, Stanka (ur.) XIV. Dnevi slovenske uprave 2007, Portorož, str. 103-122.
- DIMC, Maja, SLADOJE, Andreja (2010). Integracija IS MFERAC z drugimi informacijskimi sistemi proračunskega uporabnika. V: TURK ŠKRABA, Mira (U.) Uporabna informatika 2010 št. 4, letnik XVIII.
- DULAR, Tomaž (2005). Kako obvladovati dokumentacijski tok v poslovnem informacijskem sistemu. V: NOVAKOVIČ, Sašo (ur.) Zbornik posvetovanja. 2005, Portorož, str. 609-613.
- HORJAK, Marjeta (2011). Razvoj modela kriterijev za odločanje o uvedbi elektronske hrambe dokumentov. *Economic and business review*. 2011, Letnik 13, str 42.

## – **PREDPISI**

- (2006). Navodilo za določanje rokov hranjenja dokumentarnega gradiva organov javne uprave (Uradni list RS, št. 81/2005).
- (2001). Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje. Uradni list RS, št. 77/2000, št. 2/2001.
- (2005). Uredba o varovanju tajnih podatkov. Uradni list RS, št. 74/05.
- (2006). Uredba o varstvu dokumentarnega in arhivskega gradiva (UVDAGA). Uradni list RS, št. 86/2006.
- (2004). Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1). Uradni list RS, št. 98/04.
- (2006). Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). Uradni list RS, št. 30/06.
- (2006). Zakon o tajnih podatkih (ZTP-UPB2). Uradni list RS, št. 50/2006.

## – **VIRI Z INTERNETA**

- ARHIV RS (2012). Temeljna načela za izvajanje e-hrambe. Privzeto 20. 9. 2012 iz: [http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/izobrazevanje/2012/BDomanjko\\_jun\\_2012.pdf](http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/izobrazevanje/2012/BDomanjko_jun_2012.pdf).
- GOLOB, Sašo (2005). Upravljanje z dokumenti kot sistem za kvalitetnejše upravljanje z znanjem. Privzeto 10. 9. 2012 iz: [www.stat.si/radenci/referat/golob.doc](http://www.stat.si/radenci/referat/golob.doc).
- DOMANJKO, Boris (2012). Strokovno usposabljanje za uslužbence javno pravnih oseb. Privzeto 10. 9. 2012 iz: [http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/izobrazevanje/2012/BDomanjko\\_jun\\_2012.pdf](http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/izobrazevanje/2012/BDomanjko_jun_2012.pdf).
- HAJTNIK, Marjeta (2011). Usposabljanje za delavce ponudnikov storitev. Privzeto 15. 9. 2012 iz: [http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/izobrazevanje/2011/Usposabljanje\\_ponudniki\\_29.11.2011\\_THajtnik.pdf](http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/izobrazevanje/2011/Usposabljanje_ponudniki_29.11.2011_THajtnik.pdf).
- ION COMMUNICATIONS(2012). Enterprise Document Management System. Privzeto 10. 9. 2012 iz: <http://www.i-on.net/eng/solution/edms/edm/keyfeatures/index.html>.
- LAVRIČ, Tomaž (2008). Zaupni podatki v dokumentarnem in arhivskem gradivu. Privzeto 15. 10. 2012 iz: [http://www.pokarh-mb.si/fileadmin/www.pokarh-mb.si/pdf\\_datoteke/Radenci2008/Lavri\\_\\_2008.pdf](http://www.pokarh-mb.si/fileadmin/www.pokarh-mb.si/pdf_datoteke/Radenci2008/Lavri__2008.pdf).
- MINISTRSTVO ZA NOTRANJE ZADEVE (2012). Dostop do tajnih podatkov. Privzeto 15. 10. 2012 iz: [http://www.mnz.gov.si/si/mnz\\_za\\_vas/osebni\\_in\\_tajni\\_podatki/dostop\\_do\\_tajnih\\_podatkov/](http://www.mnz.gov.si/si/mnz_za_vas/osebni_in_tajni_podatki/dostop_do_tajnih_podatkov/).
- MINISTRSTVO ZA OBRAMBO (2012). Infrastruktura javnih ključev SIMoD-PKI. Privzeto 15. 10. 2012 iz: <http://www.simod-pki.mors.si/>.



- MINISTRSTVO ZA PRAVOSODJE IN JAVNO UPRAVO (2012). Pravna pojasnila glede ureditve elektronskega podpisa. Privzeto 10. 9. 2012 iz: <http://www.si-ca.si/pravnapojasnila.php>.
- MRZEL, Matija, MULJAVEC, Suzana (2011). Elektronske odredbe v javni upravi. Privzeto 10. 10. 2012 iz: [http://www.iju2011.si/images/stories/predstavitve/Stanje%20informatizacije/IJ%20U%202011\\_Muljavec,Mrzel%20-%20Elektronske%20odredbe%20v%20javni%20upravi.pdf](http://www.iju2011.si/images/stories/predstavitve/Stanje%20informatizacije/IJ%20U%202011_Muljavec,Mrzel%20-%20Elektronske%20odredbe%20v%20javni%20upravi.pdf).
- PAULETIČ, I. (2011). Česa ne smete spregledati pred uvedbo dolgoročne elektronske hrambe. Privzeto 25. 10. 2012 iz: <http://www.frodx.com/pdf/FrodX-prirocnik-deh.pdf>.
- PERKLIK (2012). Prednosti elektronske pred klasično hrambo. Privzeto 15. 10. 2012 iz: <http://www.perklik.si/?q=node/28>.
- PIA IS (2012). Dokumentni sistem - prihranek časa in denarja. Privzeto 15. 9. 2012 iz: <http://www.odos.si/Docs/pv.pdf>.
- SPRAGUE, Ralph (1995). Electronic document management. Privzeto 15. 10. 2012 iz: <http://www.etchouse.com/mcma503/readings/sprague-1995.pdf>.
- URAD RS ZA VAROVANJE TAJNIH PODATKOV (2012). Navodilo za odobritev šifrirnih rešitev. Privzeto 15. 9. 2012 iz: [http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Navodilo\\_odobritev\\_sifrirnih\\_resitev.pdf](http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Navodilo_odobritev_sifrirnih_resitev.pdf).
- URAD VLADE RS ZA VAROVANJE TAJNIH PODATKOV (2012). Informacijska varnost. Privzeto 15. 9. 2012 iz: [http://www.uvtp.gov.si/si/delovna\\_podrocja/dokumentacijska\\_varnost/](http://www.uvtp.gov.si/si/delovna_podrocja/dokumentacijska_varnost/).
- URAD ZA URADNE PUBLIKACIJE EVROPSIH SKUPNOSTI EUROPEAN COMMUNITIES (2001). Moreq: Model requirements for the management of electronic records – MoReq Specification – Model zahtev za upravljanje elektronskih dokumentov, specifikacija MoReq., Arhiv Republike Slovenije. Privzeto 15. 10. 2012 iz: <http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/zakonodaja/specifikacija.pdf>.