

UNIVERZA V LJUBLJANI  
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Simon Šafhalter

ELEKTRONSKI ARHIV

DIPLOMSKO DELO NA  
VISOKOŠOLSKEM STROKOVNEM ŠTUDIJU

Mentor: pred. mag. Igor Škraba

Ljubljana, 2010



Št. naloge: 00479/2009

Datum: 15.10.2009

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **SIMON ŠAFHALTER**

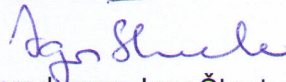
Naslov: **ELEKTRONSKI ARHIV**  
**ELECTRONIC ARCHIVE**

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija

Tematika naloge:

V nalogi preglejte zakonske zahteve za elektronsko arhiviranje ter tehnologije in orodja za realizacijo elektronskega arhiva. Opišite primer realizacije zakonsko skladnega elektronskega arhiva.

Mentor: \_\_\_\_\_

  
pred. mag. Igor Škraba



Dekan: \_\_\_\_\_

  
prof. dr. Franc Solina

Univerza  
v Ljubljani  
Fakulteta za računalništvo  
in informatiko

Tižaška 25  
1000 Ljubljana, Slovenija  
telefon: 01 476 84 11  
faks 01 426 46 47  
www.fri.uni-lj.si  
e-mail: dekanat@fri.uni-lj.si



Št naloge: 00479/2009

Datum: 15 10 2009

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **SIMON ŠAFHALTER**

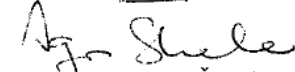
Naslov: **ELEKTRONSKI ARHIV  
ELECTRONIC ARCHIVE**

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija

Tematika naloge:

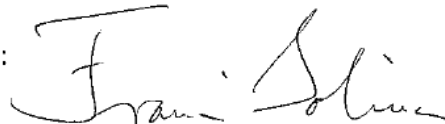
V nalogi preglejte zakonske zahteve za elektronsko arhiviranje ter tehnologije in orodja za realizacijo elektronskega arhiva. Opišite primer realizacije zakonsko skladnega elektronskega arhiva.

Mentor: \_\_\_\_\_

  
pred. mag. Igor Škraba



Dekan: \_\_\_\_\_

  
prof. dr. Franc Solina

**IZJAVA O AVTORSTVU**  
**diplomskega dela**

Spodaj podpisani/-a SIMON ŠAFHALTER,

z vpisno številko 63050355,

sem avtor/-ica diplomskega dela z naslovom:

ELEKTRONSKI ARHIV

---

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal/-a samostojno pod mentorstvom (naziv, ime in priimek)

pred. mag. Igor Škraba

in somentorstvom (naziv, ime in priimek)

- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

V Ljubljani, dne \_\_\_\_\_ Podpis avtorja/-ice: \_\_\_\_\_

II

## **Zahvala**

Zahvalil bi se rad svoji družini za omogočanje študija in večno podporo ter vsem prijateljem, ki mi stojijo ob strani.

Posebna zahvala gre mojemu mentorju mag. Igorju Škrabi za nasvete in pomoč med pisanjem diplomskega dela.

Zahvaljujem se tudi sodelavcem v podjetju ZZI d.o.o., ki so mi pomagali pri izdelavi diplomskega dela.

# Kazalo

Povzetek .....	1
Abstract.....	3
1. Uvod .....	5
2. Elektronsko arhiviranje.....	6
2.1. Zakaj elektronski arhiv, zakaj digitalni dokument in zakaj digitaliziranje?.....	6
2.2. Prednosti in slabosti elektronskega arhiva.....	8
2.3. Pot do popolnega elektronskega poslovanja.....	8
3. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih.....	9
3.1. Vsebinska področja ZVDAGA.....	10
3.1.1. Temeljna načela zakona.....	10
3.1.2. Dokumentarno gradivo .....	11
3.1.3. Arhivsko gradivo .....	12
3.1.4. Arhivska javna služba.....	12
3.1.5. Zagotavljanje infrastrukture in storitev .....	12
3.1.6. Nadzor .....	12
3.1.7. Novosti .....	12
3.2. Notranja pravila ZVDAGA .....	12
3.3. Usklajenost z drugimi zakoni, predpisi in standardi.....	13
3.4. Strojna in programska oprema.....	14
3.4.1. Strojna oprema.....	14
3.4.2. Programska oprema .....	14
3.5. Nosilci in oblike zapisa za dolgoročno hrambo dokumentarnega gradiva.....	15
3.5.1. Oblika zapisa .....	15
3.5.2. Nosilec zapisa .....	15
3.6. Varovanje in zaščita informacij.....	16
3.7. Informacijska infrastruktura - varnost .....	16
3.7.1. Organizacijski vidik.....	17
3.7.2. Tehnološki vidik .....	17
3.8. Razvoj in vzdrževanje (aplikacijskih) informacijskih sistemov.....	17
3.9. Zagotavljanje neprekinjenega delovanja .....	18
3.10. Elektronski podpis .....	18
3.11. eHramba.si kot primer dolgoročne elektronske hrambe.....	19
4. Tehnologije sistema eHramba.si .....	20
4.1. Storitveno orientirana arhitektura .....	20
4.1.1. Tehnološki vidik SOA .....	20
4.2. Porazdeljeni sistemi .....	21
4.2.1. Cilji pri načrtovanju porazdeljenega sistema.....	22
4.2.2. Zasnova strojne opreme porazdeljenih sistemov.....	23
4.2.3. Zasnova programske opreme porazdeljenih sistemov .....	24
4.3. Sistem sporočilnih vrst .....	25
4.4. IBM WebSphere .....	26
4.5. IBM WebSphere MQ.....	27
5.5.1. Arhitektura sistema IBM WebSphere MQ .....	27
4.6. IBM WebSphere Message Broker.....	28

## IV

4.7. Časovno žigosanje.....	29
4.7.1. Sistem eKeeper .....	30
4.8. Sistem IBM Content Manager .....	30
4.9. Simple Object Access Protocol.....	31
4.9.1. Struktura SOAP sporočila.....	32
4.9.2. Primer zahteve in odgovora SOAP .....	33
5. Storitve eHramba.si.....	34
5.1. Skladnost z zakonodajo.....	35
5.2. Varnost hranjenega gradiva .....	36
5.3. Arhitektura sistema eHramba.si.....	36
5.4. Podsystem za hranjenje podatkov .....	37
5.4.1. Podsystem za hranjenje opisnih podatkov .....	37
5.4.2. Podsystem za hranjenje vsebine dokumentov.....	38
5.4.3. Podsystem za hranjenje revizijskih sledi .....	38
5.5. Podsystem za funkcije nad dokumenti.....	39
5.5.1. Vnos dokumenta .....	39
5.5.2. Brisanje dokumenta.....	39
5.6. Asinhrona obdelava.....	40
5.7. Funkcije SOAP .....	41
5.8. Ostali sistemi.....	42
5.8.1. Sistem pooblastil .....	42
5.8.2. Sistem za razvrščanje dokumentov .....	42
5.9. Uporabniški vmesnik .....	42
5.9.1. Portal .....	42
5.9.2. Odjemalec .....	43
5.9.3. Ostali uporabniški vmesniki.....	44
5.10. Povezljivost (integracija) sistema z obstoječimi informacijskimi sistemi .....	44
6. Sklepne ugotovitve.....	45
7. Viri .....	46

## Slike

Slika 1: Definicija porazdeljenega sistema.....	22
Slika 2: Porazdeljen sistem povezan z vodilom .....	23
Slika 3: Porazdeljen sistem povezan s stikalom .....	24
Slika 4: Pregled programske opreme porazdeljenih sistemov .....	25
Slika 5: Sistem sporočilnih vrst s transformacijo sporočil .....	26
Slika 6: Arhitektura sistema IBM WebSphere MQ.....	28
Slika 7: Osnovna arhitektura sistema IBM Content Manager .....	31
Slika 8: Struktura sporočila SOAP .....	32
Slika 9: Uporabniške in zunanje storitve sistema eHramba.si .....	35
Slika 10: Arhitektura sistema eHramba.si .....	37
Slika 11: Struktura sistema eHramba.si - aplikativni model .....	38
Slika 12: Seznam funkcij SOAP storitve eHramba.si .....	41
Slika 13: Uporabniški vmesnik sistema eHramba.si - portal.....	43
Slika 14: Uporabniški vmesnik sistema eHramba.si - aplikacija .....	44

## Seznam uporabljenih kratic in simbolov

ZVDAGA	Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih
ZAGA	Zakon o arhivskem gradivu in arhivih
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu
SOA	Service-Oriented Architecture – storitveno orientirana arhitektura
SOAP	Simple Object Access Protocol – protokol za spletne storitve, ki temelji na XML
VPN	Virtual Private Network – telekomunikacijska storitev, ki zagotavlja naročniku zasebno omrežje, realizirano z viri javnega omrežja
XML	Extensible Markup Language – okrajšava za razširljivi označevalni jezik
FTP	File Transfer Protocol – protokol za prenos datotek
MQ	Message Queueing – sistem sporočilnih vrst
ETZ	Enotne tehnološke zahteve
DOS	Distributed Operating System – tesno povezan operacijski sistem
NOS	Network Operating System – šibko povezan operacijski sistem
LAN	Local area network – lokalno računalniško omrežje, ki pokriva manjše območje
WAN	Wide area network – prostrano omrežje, ki pokriva večje geografsko področje
ESB	Enterprise service bus – storitveno vodilo
IDS	Intrusion Detection System – sistem za zaznavanje vdorov
ESQL	Extended Structured Query Language – programski jezik za okolje WebSphere Message Broker
ERP	Enterprise Resource Planning - načrtovanje virov podjetja
ERS	Evidence Record Syntax – tehnološki standard za dolgoročno hranjenje elektronskih dokumentov
ISO	International Organization for Standardization – mednarodna organizacija za standardizacijo





## Povzetek

Diplomska naloga nas vodi skozi glavne točke poti do realizacije zakonsko skladnega elektronskega arhiva: od zakona do končne storitve elektronskega arhiviranja s pomočjo raznih informacijskih tehnologij.

V uvodu bomo na kratko pojasnili razlog za nastanek elektronskih arhivov in z njimi povezanega zakona.

V drugem poglavju uvedemo bralca v osnovne naloge arhiviranja, ki veljajo tako za klasično kot za elektronsko arhiviranje. Odgovorili si bomo na vprašanja kot so “zakaj uporaba elektronskega arhiva?”, podali njegove prednosti, slabosti ter cilje.

Tretje poglavje ponuja pregled skozi Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA), kateri nam podaja navodila in smernice za realizacijo zakonsko skladnega elektronskega arhiva. Pregledali bomo vsebinska področja zakona, njegova notranja pravila ter usklajenost z ostalimi zakoni in standardi. Opisali bomo tudi zahteve za strojno in programsko opremo ter primerne nosilce in oblike zapisov za elektronski arhiv.

V četrtem poglavju so opisane tehnologije, orodja, storitve in sistemi, ki tvorijo konkreten primer zakonsko skladnega elektronskega arhiva eHramba.si. Spoznali bomo storitveno orientirano arhitekturo in z njo povezana orodja IBM-ovega programskega paketa WebSphere. Sprehodili se bomo čez osnove porazdeljenih sistemov ter opisali ostale gradnike dotičnega sistema.

V petem poglavju je opisana zgradba in arhitektura sistema eHramba.si. Opisano je kako so posamezne tehnologije med seboj povezane in kakšne funkcije imajo v sistemu. Navedene so še nekatere glavne značilnosti sistema.

Ključne besede:

- elektronski arhiv
- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih
- eHramba.si
- storitveno orientirana arhitektura



## Abstract

This diploma thesis leads us through the main points of making a coherent legal electronic archive: from law, by means of various information technologies, to the final service of electronic archiving.

In the introduction we will briefly explain the reason for the emergence of electronic archives and the law that is related to it.

In the second chapter we will introduce to the basic archiving functions, applicable to both classical and electronic archiving. We will answer to questions such as "Why use an electronic archive?", list its good sides, bad sides and goals.

The third chapter gives us an overview over the law ZVDAGA, which gives us instructions and guidance for the realization of a coherent legal electronic archive. We will review the content of the law, its internal rules and the compliance with other laws and standards. We will also describe software and hardware requirements and the appropriate media and formats for electronic archiving.

In the fourth chapter we will describe the technologies, tools, services and systems that forms a concrete example of a coherent legal electronic archive eHramba.si. We will comprehend service-oriented architecture and related IBM WebSphere software packages. We will walk through the basics of distributed systems, SOAP technology and other blocks which form the affected system.

The fifth chapter describes the system architecture of eHramba.si. We will show how individual technologies are connected and linked together and what is their function in the system.

Keywords:

- electronic archive
- ZVDAGA
- eHramba.si
- Service-oriented architecture



## 1. Uvod

S prihodom novih tehnologij se je zagotovo spremenil tudi način medsebojnega komuniciranja in našega poslovanja. Že nekaj let je jasno, da se elektronskim dokumentom praktično ne moremo več izogniti, saj postajajo del našega vsakdana. Zato moramo poiskati načine, kako jih bomo ohranjali skozi čas ter za čas, ki je potreben zaradi zakonskih ali pogodbenih določil.

Elektronsko arhiviranje je eden izmed načinov ohranjanja elektronskih dokumentov. Osnovni namen elektronskega arhiva je urejena hramba dokumentov, ki so že od svojega nastanka izključno v elektronski obliki ali pa so bili kasneje digitalizirani. Poleg hrambe dokumentov pa mora zagotavljati nadzor, visoko stopnjo varnosti in zanesljivost delovanja sistema.

Vendar elektronski arhiv sam po sebi ni dovolj za odpravo vseh papirnih dokumentov. Tukaj vstopi v igro zakon. S pomočjo zakona in določil zakonodaje lahko arhiv pripravimo za hrambo dokumentov, katerih v arhivu brez zakonske podlage ne bi mogli hraniti oziroma ne bi imeli verodostojnosti. Z uporabo zakonsko skladnega elektronskega arhiviranja lahko podjetja in ustanove v veliki meri odpravijo uporabo papirnih dokumentov v postopkih ter tako pocenijo in pohitrijo poslovanje.

Za doseganje striktnih ciljev zakonsko skladnega elektronskega arhiviranja se moramo posluževati najnovejših informacijskih tehnologij, računalniških orodij in pristopov.

## 2. Elektronsko arhiviranje

Arhive lahko na splošno opredelimo kot zbirko listin in dokumentov, ki imajo poslovno, zgodovinsko, kulturno in znanstveno vrednost oz. kot prostor (tudi ustanovo), kjer so shranjene te listine in dokumenti. Arhivirana pisna gradiva vsebujejo pomembna dejstva, podatke, informacije, risbe in slike, katere s splošnim izrazom imenujemo dokumenti. Arhiv jih prejme v trajno last, s čimer sprejme obvezo, da je vsebina teh dokumentov ustrezna in dostopna vsem skupinam uporabnikov, hkrati pa mora zagotavljati tudi dolgoročno nespremenljivost in verodostojnost vseh hranjenih informacij. Dokumentarno gradivo arhiviramo zaradi različnih potreb in hranimo v arhivu ustanove, dokler ne potečejo roki hranjenja, ki jih narekujejo predpisi in potrebe poslovanja ali dokler dela dokumentarnega gradiva, ki ima značaj arhivskega gradiva (trajni pomen za zgodovino, znanost ali kulturo), ne izločimo pristojnemu arhivu.

### 2.1. Zakaj elektronski arhiv, zakaj digitalni dokument in zakaj digitaliziranje?

S pojavom elektronskih dokumentov in s tem elektronskih arhivov se je spremenila tudi sama logika arhiviranja. Ta ne temelji več samo na vzdrževanju in ohranjanju nosilcev in na njih zapisanih sporočilih, ampak predvsem na vzpostavljanju, vzdrževanju in razumevanju kontekstov, v katerih so zapisi nastali ali bili uporabljeni. Brez njih digitalni dokumenti izgubijo veljavnost in pomen.

Glavna težava klasičnih arhivov je njihova okornost oziroma togost. Upravljanje s papirnimi in drugimi dokumenti v analogni obliki je v primerjavi z digitalnimi dokumenti veliko bolj komplicirano in nepregledno, še posebej, če razpolagamo z večjimi količinami podatkov, ki zahtevajo zelo velike tehnične in prostorske kapacitete, kar nas pripelje do višjih stroškov. S pojavom elektronskih arhivov so glavne pomankljivosti klasičnega arhiva odpravljene, saj omogočajo mnogo preprostejše iskanje zelenih vsebin po raznih atributih dokumentov, arhivski prostor ter dostopni časi do vsebin pa se znatno zmanjšajo.

Ne glede na tip arhiva je potrebno zagotoviti:

- verodostojnost vsebine dokumenta;
- avtentičnost dokumenta in subjekta, ki je dokument ustvaril;
- celovitost oziroma garancijo, da dokument ni bil spremenjen delno ali v celoti;
- uporabnost oziroma berljivost dokumenta, ter v primeru podpisanih dokumentov tudi verifikacijo podpisa v daljšem ali trajnem časovnem obdobju;
- pravno veljavnost arhiviranega dokumenta.

Pri hranjenju in zagotavljanju dostopa do kulturnega spomina ima digitalna tehnologija številne prednosti in nam lahko pomaga rešiti tradicionalni konflikt med ohranjanjem in dostopom. Pri gradivu, shranjenemu digitalno, lahko uporabnik dela na enakem dokumentu, kot je original in ga ima shranjenega na lokalnem računalniku. S tem, da ločuje hranjenje in uporabljanje, digitalna tehnologija omogoča hkratno uporabo istega dokumenta na način, ki ga dokumenti shranjeni v drugačni obliki ne omogočajo. Digitalna tehnologija hkrati omogoča tudi dodatne možnosti

dostopa. V dokumentu z besedilom lahko bralec hitro najde potrebno informacijo z iskanjem po besedah, kombinaciji besed, frazah itd. Prav tako lahko bralec po želji oblikuje izgled dokumenta na zaslonu, ga shrani na disk, drugi zunanji nosilec ali pa ga natisne na papir. Potrebno je poudariti razliko med arhiviranjem digitalnih dokumentov in digitalizacijo arhivskih dokumentov. Poznamo dokumente, ki so bili "rojeni digitalno" (born digital) in tiste, ki so digitalno obliko pridobili šele kasneje.

Dokumente, podatke, zapise ter informativne in kulturne stvaritve vseh vrst lahko spremenimo v drugo obliko - jih digitaliziramo. S tem pridobimo prednosti, kot so:

- možnost ustvarjanja popolnih kopij digitalnih zapisov;
- možnost njihovega oglaševanja na številnih medijih;
- možnost distribuiranja in širjenja na omrežjih;
- možnost preoblikovanja v drugo obliko;
- možnost iskanja po vsebini;
- lahko jih obdelamo z avtomatiziranimi (avtomatskimi) in polavtomatiziranimi orodji.

Digitalni dokumenti so drugačni od klasičnih, papirnatih. Drugače so proizvedeni, shranjeni, prenešeni, in vzdrževani ter drugače se z njimi upravlja in do njih dostopa. Največja razlika je v zelo skrajšani življenjski dobi digitalnega dokumenta, če le-ta ni primerno hranjen.

Elektronski arhiv ima številne prednosti pred klasičnim sistemom arhiviranja, saj med drugim omogoča učinkovitejšo kontrolo nad uporabo dokumentov (beleži se lahko vsak vpogled, sprememba ali izpis dokumenta, kar zagotavlja revizijsko sledljivost skozi ves čas hrambe), časovno in krajevno neodvisno dostopnost do dokumentov ter njihovo varno hranjenje. Ker lahko zaposleni dostopajo do dokumentov preko spletnega vmesnika, odpadejo stroški posredovanja, razmnoževanja in razpošiljanja dokumentov, ki jih srečujemo pri klasičnem načinu arhiviranja dokumentov.

Elektronsko arhiviranje dokumentov zagotavlja podjetju tudi velike prihranke denarja in časa, saj se lahko zaposleni zaradi učinkovitejšega dostopa do dokumentov in preprostega ter hitrega iskanja informacij posvečajo pomembnejšim opravilom ter tako povečujejo tudi učinkovitost celotnega poslovanja podjetja. Če so papirni dokumenti tudi po nekaj deset letih v arhivu popolnoma berljivi, pa na žalost tega za elektronske dokumente ne moremo trditi. Zaradi omejene obstojnosti pomnilniških medijev in spreminjajočih se standardov, se pri elektronskem arhivu zahteva nenehna skrb in vzdrževanje. Ker se za dokumente, ki se nahajajo na začetku življenjske poti, pričakuje večje število dostopov oziroma vpogledov v njihovo vsebino, je zaželeno, da se nahajajo na hitrih magnetnih medijih (npr. računalniški diski). Po določenem časovnem obdobju, ko se zmanjša njihova "popularnost", pa jih lahko prenesemo na počasnejše medije (npr. na magnetne trakove), ki zagotavljajo daljšo obstojnost zapisanih objektov.

## 2.2. Prednosti in slabosti elektronskega arhiva

V primerjavi s klasičnimi imajo elektronski arhivi številne prednosti in seveda tudi slabosti. Najpogosteje navajane prednosti so [2]:

- nižji stroški hranjenja in transporta arhiviranih gradiv;
- varnejše in preglednejše okolje arhiva;
- lažje upravljanje in vzdrževanje poenotene podatkovne baze dokumentov;
- hitrejša prilagodljivost novim standardom na področju digitalnega arhiviranja;
- indeksiranje vsebin z možnostjo iskanja po različnih tipih datotek;
- pri rednem ustvarjanu rezervnih kopij veliko manjša verjetnost izgube vsebin;
- razpoložljivost dokumentov kadarkoli in kjerkoli;
- zmanjšani stroški tiskanja, vsaka natisnjena kopija je maksimalno kvalitetna.

Najpogostejše slabosti in problemi s katerimi se pri elektronskih arhivih srečujemo so:

- spreminjanje in zastarelost tehnologije;
- problem dolgoročnega hranjenja elektronskih vsebin;
- problem migracije vsebin;
- tehnična in pravna vprašanja.

## 2.3. Pot do popolnega elektronskega poslovanja

Elektronsko poslovanje predstavlja v najširšem pomenu preslikavo poslovnih procesov v elektronsko obliko na osnovi uporabe informacijskih tehnologij. Pisno obliko dokumentov, kot neposreden produkt številnih poslovnih in proizvodnih procesov, nadomeščajo zapisi v elektronski obliki. Pravila za upravljanje z elektronskimi zapisi se v osnovi ne razlikujejo bistveno od klasičnih in so podana tudi v slovenski zakonodaji. Zakon o elektronskem poslovanju in elektronskem podpisu prepozna elektronsko ustvarjene zapise in elektronske podpise kot formalno sredstvo poslovanja in v določenih primerih enači elektronski zapis in elektronski podpis s pisno obliko in lastnoročnim podpisom.

### **3. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih**

Krovni zakon, ki določa, kaj je arhivski dokumentarni material in kako ga ustrežno hraniti, je Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA).

Ta ureja:

- način, organizacijo, infrastrukturo in izvedbo hrambe dokumentarnega gradiva v fizični in elektronski obliki, vključno s pravnimi učinki takšne hrambe;
- varstvo javnega in zasebnega arhivskega gradiva kot kulturnega spomenika, ne glede na vrsto, obliko ali nosilec zapisa oziroma medij;
- pogoje za njegovo dostopnost in uporabo;
- naloge in organizacijo javne arhivske službe v Republiki Sloveniji;
- nadzor nad izvajanjem zakona.

Leta 1997 je bil sprejet Zakon o arhivskem gradivu in arhivih (ZAGA), ki ureja varstvo arhivskega gradiva, pogoje za uporabo arhivskega gradiva ter pristojnosti in naloge arhivov.

V letu 2000 je Slovenija s sprejetjem Zakona o elektronskem poslovanju in elektronskem podpisu (ZEPEP), izenačila veljavnost papirnatih in elektronskih dokumentov, vendar le tistih, za katere ni določen rok hrambe.

Leta 2004 je bil sprejet Zakon o terjatvah. Ta je razširil pravno veljavnost elektronske dokumentacije na pogodbe, matične dokumente in podobno, s čimer je odpravil popolnoma vse ovire za elektronsko poslovanje.

V letu 2006 je Slovenija sprejela še zakonodajo na področju upravljanja z dokumentarnim in arhivskim gradivom t.j. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). Le-ta predstavlja celovit predpis, ki ureja možnost in pravno veljavnost elektronske hrambe dokumentarnega gradiva v digitalni obliki ne glede na njegovo obliko nastanka (fizična ali elektronska oblika) in roke hrambe (gradivo z določenim rokom hrambe in arhivsko gradivo). Možnost zakonsko skladne hrambe dokumentarnega gradiva v digitalni obliki tako predstavlja ključni in še zadnji element na poti do popolnega elektronskega poslovanja. Poleg optimizacije poslovanja (hitrejši, enostavnejši dostop do podatkov, možnost povečanja varnosti naših podatkov itd.) pa lahko govorimo tudi o vplivu tega še na druge plati kakovosti našega življenja.

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih celovito ureja varstvo dokumentarnega in arhivskega gradiva v fizični in elektronski obliki. Zakon med drugim predpisuje pogoje, ki jih mora izpolnjevati strojna in programska oprema za elektronsko arhiviranje, pogoje in postopke spreminjanja papirne dokumentacije v elektronsko obliko ter ureja način, organizacijo, infrastrukturo in izvedbo hrambe dokumentarnega gradiva v fizični in elektronski obliki, vključno s pravnimi učinki takšne hrambe. Ker elektronske digitalne zapise ni mogoče trajno ohranjati v izvorni obliki, kot je to značilno za fizične dokumente na papirju, je z novim zakonom poskrbljeno tudi za to, da bo v primeru hrambe elektronskega gradiva dovoljeno

ohranjanje enakovrednih in verodostojnih reprodukcij gradiva namesto dosedanjega izključnega ohranjanja izvirnega gradiva. Način izvajanja ter tehnološke zahteve oziroma standardi za zajem, pretvorbo, hrambo, dostop, reproduciranje oziroma ohranjanje digitalnih zapisov bodo določeni s predvidenimi podzakonski akti, ki bodo sprejeti na podlagi novega zakona.

ZAGA je sicer predstavljal dobro pravno podlago za varstvo arhivskega gradiva kot kulturnega spomenika, ni pa urejal področja varstva elektronskega dokumentarnega in arhivskega gradiva, ki je zaradi tehnološkega razvoja informacijske družbe, postalo prevladujoče in izjemno pomembno. Nova zakonska ureditev varstva elektronskih zapisov in posledično s podzakonskimi akti standardizirana hramba je bila zato več kot nujna.

ZVDAGA je bistveno nadgradil dotedanjo ureditev varstva gradiva s celovitim in učinkovitim varstvom elektronskega dokumentarnega in elektronskega arhivskega gradiva. V obstoječo pravno ureditev varstva arhivskega gradiva je prinesel nekatere spremembe in dopolnitve v zvezi z varstvom filmskega arhivskega gradiva, arhivskim informacijskim sistemom in dostopom do arhivskega gradiva v javnih arhivih. Razen na področju standardiziranega zajema in hrambe oziroma arhiviranja elektronskega gradiva v digitalni obliki predlagane rešitve ne posegajo bistveno v dosednji koncept varstva dokumentarnega in arhivskega gradiva oziroma v načela do tedaj veljavnega zakona. Tako bodo tudi s sedanjim zakonom (ZVDAGA) ostala v veljavi zaradi tehnološkega razvoja in razvoja arhivistike nekoliko dopolnjena temeljna načela, kot jih je določal ZAGA in so že desetletja uveljavljena v arhivski stroki pri nas in v tujini, zlasti v državah Evropske unije.

### **3.1. Vsebina področja ZVDAGA**

Vsebina zakona se deli na deset glavnih delov:

1. Uvodne določbe
2. Temeljna načela zakona
3. Dokumentarno gradivo
4. Arhivsko gradivo
5. Arhivska javna služba
6. Zagotavljanje infrastrukture in storitev
7. Nadzor
8. Izdajanje predpisov, enotnih tehnoloških zahtev in priporočil za akreditirane ponudnike
9. Kazenske določbe
10. Prehodne in končne določbe

#### **3.1.1. Temeljna načela zakona**

Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih pomembno opredeljuje tudi načela shranjevanja [3]. Ta so:

- načelo ohranjanja dokumentarnega gradiva oziroma uporabnosti njegove vsebine;

- načelo trajnosti;
- načelo celovitosti;
- načelo dostopnosti;
- načelo varstva kulturnega spomenika.

### **Načelo ohranjanja dokumentarnega gradiva oziroma uporabnosti njegove vsebine (ZVDAGA, 3. člen)**

Hramba dokumentarnega gradiva pomeni ohranjanje izvirnega dokumentarnega gradiva ali uporabnosti vsebine tega gradiva. Hrambi izvirnega dokumentarnega gradiva je zato enaka hramba zajetega gradiva, če zagotavlja zajetemu gradivu vse učinke izvirnega gradiva (uporabnost vsebine gradiva).

### **Načelo trajnosti (ZVDAGA, 4. člen)**

Hramba dokumentarnega gradiva mora zagotavljati trajnost tega gradiva oziroma trajnost reprodukcije njegove vsebine.

### **Načelo celovitosti (ZVDAGA, 5. člen)**

Hramba dokumentarnega gradiva mora zagotavljati nespremenljivost in integralnost dokumentarnega gradiva oziroma reprodukcije njegove vsebine, urejenost dokumentarnega gradiva oziroma njegove vsebine ter dokazljivost izvora dokumentarnega gradiva (provenience).

### **Načelo dostopnosti (ZVDAGA, 6. člen)**

Dokumentarno gradivo oziroma reprodukcija njegove vsebine mora biti ves čas trajanja hrambe zavarovana pred izgubo ali okrnitvijo celovitosti ter dostopna pooblaščenim uporabnikom ali uporabnicam (v nadaljnjem besedilu: uporabnikom).

### **Načelo varstva kulturnega spomenika (ZVDAGA, 7. člen)**

Arhivsko gradivo je kulturni spomenik in mora biti varovano kot takšno.

#### **3.1.2. Dokumentarno gradivo**

V poglavju "Dokumentarno gradivo" so predpisani pogoji za zajem, pretvorbo in uničenje dokumentarnega gradiva. Sledi uredba za pripravo oseb na hrambo, ki zajema vsebine kot so: organizacija dela, priprava, sprejem in kontrola izvajanja notranjih pravil. Dalje je v več točkah razporejena vsebina, ki zajema izvajanje hrambe dokumentarnega gradiva v vseh oblikah, še posebej dolgoročna hramba in nazadnje pogoji za zagotovitev veljavnosti in dokazne vrednosti gradiva.

### **3.1.3. Arhivsko gradivo**

Pod to točko so navedena pravila za določanje arhivskega gradiva, postopek izročanja javnim arhivom ter uredbe za različna arhivska gradiva kot so javna arhivska gradiva, zasebna arhivska gradiva in filmska gradiva.

### **3.1.4. Arhivska javna služba**

Poglavje narekuje uredbe za organizacijo in delovanje javne arhivske službe. Navedene so dejavnosti arhivske javne službe, izvajalci arhivske javne službe ter pravila o uporabi arhivskega gradiva v arhivih.

### **3.1.5. Zagotavljanje infrastrukture in storitev**

Pod to točko so navedeni splošni pogoji, ki jih mora izpolnjevati strojna in programska oprema, splošni pogoji za opravljanje storitev hrambe ter posebni pogoji za specifične storitve.

### **3.1.6. Nadzor**

Poglavje "Nadzor" vsebuje uredbe za vršitev nadzora nad izvajanjem zakona. Deli se na tri točke, katere urejajo inšpekcijski nadzor nad izvajanjem tega zakona, drug nadzor arhivske javne službe ter nadzor, ki ga izvaja državni arhiv.

### **3.1.7. Novosti**

V primerjavi s starim zakonom (ZAGA) se Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih ne osredotoča več le na arhivsko gradivo v fizični obliki, temveč vsebuje dodatne, širše določbe, ki se nanašajo na varstvo dokumentarnega gradiva v elektronski obliki. Dodane so tudi zahteve za storitve, ki so povezane s hrambo ter uredbe za nadzor nad trgom ponudnikov opreme in storitev za namen elektronske hrambe dokumentarnega gradiva.

## **3.2. Notranja pravila ZVDAGA**

Notranja pravila o hrambi dokumentarnega gradiva morajo vsebovati najmanj določbe o:

- notranji organizaciji, vlogah in pooblastilih ter številu, sestavi in usposobljenosti osebja,
- upravljanju dokumentarnega gradiva,
- infrastrukturi informacijskega sistema za hrambo, njeni varnosti in zanesljivosti (fizično in tehnično varovanje, dostopi, varnostne nastavitve strežnikov, varnostne kopije, itd)

- periodičnem spreminjanju in dopolnjevanju notranjih pravil ter njihovi veljavnosti (ob spremembi vzorčnih notranjih pravil, spremembi veljavnih predpisov, tehnološki napredek ali spoznanja stroke, zaradi pomanjkljivosti notranjih pravil).

Pravilnik o strokovni usposobljenosti delavcev, javnopравnih oseb ter ponudnikov opreme in storitev, ki ravnajo z dokumentarnim gradivom, določa podrobnejša merila za strokovno usposobljenost, program poteka strokovnega usposabljanja in potek preizkusa strokovne usposobljenosti delavk in delavcev javnopравnih oseb ter ponudnikov opreme in storitev, ki delajo z dokumentarnim gradivom. V postopku strokovnega usposabljanja pridobi delavec znanja s področja pravnih predpisov, s področja upravljanja z dokumentarnim gradivom v fizični in v digitalni obliki, s področja informatike ter s področja arhivistike v najširšem smislu.

Notranja pravila o hrambi arhivskega gradiva morajo poleg prej naštetih točk vsebovati še določbe o zajemu in pretvorbi arhivskega gradiva, dolgoročni hrambi arhivskega gradiva, zagotavljanju neprekinjenega delovanja oziroma varstva arhivskega gradiva in njegovi izročitvi pristojnim arhivom ter izročanju arhivskega gradiva in sodelovanju s pristojnim arhivom.

### **3.3. Usklajenost z drugimi zakoni, predpisi in standardi**

ZVDAGA je usklajen še z vrsto drugih zakonov, predpisov in standardov [4]:

- Zakon o varstvu osebnih podatkov ZVOP-1;
- Zakon o splošnem upravnem postopku ZUP in Uredba o upravnem poslovanju (UUP);
- Zakon o varovanju tajnih podatkov ZTP in Uredba o varovanju tajnih podatkov;
- Zakon o elektronskem poslovanju in elektronskem podpisu in Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje;
- Zakon o davčnem postopku;
- Slovenski računovodski standardi SRS.

Usklajen je tudi z varnostnimi standardi:

- ISO/IEC 27001:2005 Specification for an Information Security Management System;
- ISO/IEC 17799:2005. Code of Practice for Information Security Management;
- ISO 18044:2004 - Information technology Security techniques Information Security incident management;

ter ostalimi:

- standardi za ravnanje s storitvami IT;
- standardi, ki urejajo pisarniško poslovanje in organizacijo arhivske službe;
- smernice in tehnične specifikacije, veljavne v EU;
- strokovna spoznanja in izkušnje, dostopne v okviru dokumentov, priporočil, dogovorov in standardov Mednarodnega arhivskega sveta, Sveta Evrope in drugih mednarodnih in nacionalnih združenj (npr. MoReq);

### **3.4. Strojna in programska oprema**

Strojna oziroma programska oprema za zajem oziroma hrambo gradiva v digitalni obliki je vsaka strojna oziroma programska oprema, katere namen je v celoti ali delno omogočiti zajem ali hrambo gradiva v digitalni obliki ter s tem povezana opravila.

Ponudnik strojne in programske opreme za hrambo gradiva v digitalni obliki je vsaka oseba, ki drugim osebam odplačno ali neodplačno omogoči uporabo strojne ali programske opreme za zajem oziroma hrambo gradiva v digitalni obliki.

#### **3.4.1. Strojna oprema**

Strojna oprema mora izpolnjevati vrsto zahtev:

- Skladna mora biti z enotnimi tehnološkimi zahtevami [5], mednarodnimi, državnimi in drugimi splošno priznanimi standardi;
- dokazljiva mora biti s certifikati, veljavnimi v EU ali drugimi svetovno poznanimi certifikati ali certifikati, ki so uveljavljeni v drugih državah;
- mednarodno mora biti uveljavljena (uveljavljena v najmanj treh državah EU, v katerih proizvajalec to opremo prodaja ter vzdržuje) – izjava proizvajalca;
- ponudnik strojne opreme mora zagotoviti podporo in vzdrževanje v RS (odzivni čas, dokazan z ustreznim dokazilom – pogodba, splošni pogoji).

#### **3.4.2. Programska oprema**

Programska oprema za zajem gradiva, hrambo gradiva v digitalni obliki in spremljevalne storitve mora izpolnjevati naslednje pogoje:

- Programska oprema mora biti široko priznana in uveljavljena oziroma uporabljena ali posebej razvita za zajem gradiva, hrambo gradiva v digitalni obliki ali spremljevalne storitve po zakonu in uredbi;
- uporaba programske opreme mora biti podprta s strojno in programsko opremo, uveljavljeno na trgu;
- skladna mora biti z mednarodnimi, državnimi in drugimi splošno priznanimi standardi ter z določbami zakona, uredbe in enotnimi tehnološkimi zahtevami;
- dokazljiva mora biti s certifikati, veljavnimi v EU ali drugimi svetovno poznanimi certifikati ali certifikati, ki so uveljavljeni v drugih državah.

### 3.5. Nosilci in oblike zapisa za dolgoročno hrambo dokumentarnega gradiva

V zakonu se pod terminom dokumentarno gradivo opredeljuje izvorno in reproducirano (pisano, risano, tiskano, fotografirano, filmano, fonografirano, magnetno, optično ali kako drugače zapisano) gradivo, ki je bilo prejeta ali je nastalo pri delu pravnih oziroma fizičnih oseb.

Elektronski dokumenti, ki se hranijo dolgotrajno, so izpostavljeni tveganju zaradi propadanja nosilca zapisa, zastarevanja strojne opreme ter zastarevanja oblike zapisa. Zato v zakonu srečamo poglavje o obliki ter nosilcu zapisa v katerem so predpisane smernice za izbiro le teh.

#### 3.5.1. Oblika zapisa

Oblika zapisa so tiste organizacijske in tehnološke značilnosti zapisa, ki določajo, kako je vsebina zapisana, hranjena in prikazana v procesu hrambe. Smernice za primerno obliko zapisa za dolgoročno hrambo so:

- Oblika zapisa mora biti široko priznana in uveljavljena oziroma uporabljena ter njena uporaba podprta z na trgu uveljavljeno strojno in programsko opremo (zaželeno je, da je oblika zapisa standard ISO);
- neposredno mora biti uporabna za reprodukcijo vsebine ali enostavno pretvorjena v obliko, ki je neposredno uporabna;
- omogočati mora samodejno pretvorbo iz najpogostejše uporabljanih izvornih oblik zapisa s samodejno zaznavo in poročanjem o nepredvidenih dogodkih oziroma napakah pri pretvorbi;
- neodvisna mora biti od posamezne programske ali strojne opreme oziroma okolja;
- omogočati mora po današnjih strokovnih predvidevanjih po obdobju petih let pretvorbo v novo, takrat določeno obliko zapisa za dolgoročno hrambo;
- temeljiti mora na mednarodnem, državnem ali splošno priznanem in praviloma odprtem standardu, če ta obstaja.

#### 3.5.2. Nosilec zapisa

Nosilec zapisa je klasičen ali elektronski nosilec zapisa, na katerega se zapiše vsebina v skladu z obliko zapisa. Primeren nosilec zapisa za dolgoročno hrambo:

- omogoča pogoje varne dolgoročne hrambe – dostopnost, uporabnost, avtentičnost, celovitost;
- omogoča ohranitev zapisa podatkov na nosilcu zapisa tudi ob prekinitvi dobave energije ali drugi spremembi okoljskih pogojev (nihanje temperature, vlažnosti itd.) za čas, ki je potreben, da se zagotovi prenos podatkov na drug nosilec zapisa;
- je široko priznan in uveljavljen oziroma uporabljan ter njegova uporaba podprta z na trgu uveljavljeno strojno in programsko opremo;

- zapis na takem nosilcu temelji na mednarodnem, državnem ali splošno priznanem in praviloma odprtem standardu, če obstaja;
- njegovo delovanje omogoča vse pogoje varne dolgoročne hrambe gradiva iz 16. člena uredbe;
- omogoča večje število prepisov s sedanjih na bodoče nosilce zapisa.

### 3.6. Varovanje in zaščita informacij

Pri poslovanju modernega podjetja so informacije ključnega pomena. V primeru ogroženosti informacij je v nevarnosti obstoj podjetja kot celote. Informacije bi lahko opredelili kot "življensko tekočino, ki, podobno kot pri človeku, omogoča obstoj organizacije".

Naša družba prehaja v informacijsko dobo, ki je odvisna od pretoka informacij in s tem posledično uporabe omrežij, v pretežni meri interneta, za komunikacijo s strankami, dobavitelji, izvajalci, zastopniki in zaposlenimi. Tovrstna povezljivost prinaša podjetjem naštetu prednosti, hkrati pa jih sili v nove izzive, povezane z varovanjem informacij, ki so ključni faktor pri novem načinu poslovanja. Dejavniki, ki ogrožajo informacije prihajajo tako od zunaj (virusi, trojanski konji, napadi hekerjev), kot iz podjetja samega (okvare strojne opreme, napake uporabnikov, neučinkovita uporaba opreme, zlonamerne akcije uporabnikov).

Pri varovanju in zaščiti informacij gre v osnovi za [6]:

- razpoložljivost informacij: informacije in storitve so na voljo pooblaščenim uporabnikom takrat, ko jih potrebujejo;
- neoporečnost informacij: informacije so takšne, kot so, in niso bile nepooblaščenno spremenjene;
- zaupnost informacij: dostop do informacij imajo le pooblaščenci, torej osebe katerim so v osnovi namenjene.

Za zagotavljanje zgoraj navedenih zahtev so v uporabi različni mehanizmi, kot so avtentifikacija, avtorizacija, šifriranje, varnostne kopije, ločevanje funkcij, itd. Samo varovanje informacij se izvede z implementacijo varnostnih kontrol na informacijskih virih.

### 3.7. Informacijska infrastruktura - varnost

Informacijsko varnost zagotavljamo z uvajanjem celovitega, učinkovitega sistema upravljanja varovanja informacij ter na osnovi zakonodaje, predpisov, direktiv, uredb, standardov in dobre prakse. Sistem upravljanja varovanja informacij delimo na dva vidika:

- organizacijski vidik
- tehnološki vidik

### 3.7.1. Organizacijski vidik

Organizacijski vidik se ukvarja s področji kot so:

- ocena tveganja (redno revidirana);
- sprejem ustreznih načel varovanja, ki so zapisana v hierarhično organizirani varnostni dokumentaciji (poslovnik in politika o varovanju informacij, pravilniki, navodila, postopki);
- jasna razmejitev odgovornosti in dolžnosti pri izvajanju načel varovanja informacij;
- uvajanje nalog s področja varovanja informacij v poslovne procese organizacije;
- dvig varnostne kulture zaposlenih in poslovnih partnerjev (šolanje in osveščanje iz področja informacijske varnosti);
- upravljanje z varnostnimi dogodki in incidenti (vdori, virusi).

### 3.7.2. Tehnološki vidik

Tehnološki vidik zajema implementacijo številnih varnostnih tehnologij in kritičnih postopkov, ki omogočajo izvedbo varnostnih načel in nalog varovanja informacij kot so:

- požarni zidovi (firewalls);
- navidezna zasebna omrežja (VPN);
- protivirusna zaščita;
- sistemi za detekcijo vdorov (sistemi IDS - Intrusion Detection Systems);
- sistemi za nadzor dostopa do sistemov in mrež (pametne kartice, generatorji gesel za enkratno uporabo);
- rešitve infrastrukture javnih ključev (digitalna potrdila in omogočanje uporabe teh tehnologij v aplikacijah);
- nastavljanje varnostnih parametrov v opremi;
- varnostno kopiranje dokumentov;
- uvajanje sistemov fizične varnosti – alarmi, video nadzor, pristopne kontrole;
- zagotovitev visoke razpoložljivosti sistema – neprekinjeno poslovanje.

## 3.8. Razvoj in vzdrževanje (aplikacijskih) informacijskih sistemov

Razvoj informacijskih sistemov je proces, ki poteka od strateškega planiranja in skozi vse obdobje delovanja informacijskega sistema. V tem procesu je v skladu z zakonodajo potrebno upoštevati naslednje zahteve:

- Vzpostavljeno mora biti posebno razvojno in testno okolje, ločeno od operativnega okolja;
- opisan in določen mora biti postopek razvoja informacijskih sistemov;
- upoštevati je potrebno zahteve glede varovanja podatkov in usklajenostjo z zakonodajo ter zahteve glede zanesljivosti ter ustrezne kakovosti sistemov;

- informacijski sistemi (ki se uporabljajo pri hrambi dokumentarnega in arhivskega gradiva) morajo biti pred uporabo overjeni oz. preverjeni na podlagi dokumentiranega postopka;
- določen mora biti postopek upravljanja s spremembami;
- poskrbljeno mora biti za varno uporabo testnih podatkov iz produkcijskega okolja;
- zagotovljena mora biti tehnična in uporabniška dokumentacija za vse sisteme v uporabi;
- pred redno uporabo moramo zagotoviti ustrezno izobraževanje uporabnikov in skrbnikov novih sistemov.

### 3.9. Zagotavljanje neprekinjenega delovanja

Namen postopkov za zagotavljanje neprekinjenega delovanja je v tem, da se zagotovi izpolnjevanje dogovorjenih zahtev glede razpoložljivosti sistema tudi v primeru izpada katere od komponent sistema. Upravljalca sistema mora, po potrebi v sodelovanju z udeleženci sistema, pripraviti načrte ravnanja v izrednih razmerah, ki opisujejo scenarije za različne vrste in ravni možnih operativnih težav.

Za uspešno zagotavljanje neprekinjenega delovanja morajo upravljalci ter udeleženci v sistemu slediti naslednjim točkam:

- Bistven poudarek mora biti na ohranjanju gradiv, njihove celovitosti in dostopnosti;
- postopek za restavracijo gradiv in vzpostavitev stanja mora biti zasnovan tako, da zagotavlja celovitost in potrebno zaupnost gradiv tudi v posebnih razmerah. Skladno s temi zahtevami in oceno poslovnih vplivov mora biti pripravljen celovit načrt za zagotavljanje neprekinjenega delovanja;
- načrt mora biti v skladu s poslanstvom organizacije (izvaja hrambo le zase ali tudi za druge) ter obsegom in kritičnostjo gradiv v hrambi;
- načrt mora biti ažuriran in preverjen najmanj enkrat letno;
- s sistemom mora upravljati za le tega strokovno usposobljeno osebje;
- za arhivsko gradivo mora biti poleg glavne lokacije hrambe zagotovljena tudi varna hramba najmanj dveh dodatnih kopij arhivskega gradiva na dveh geografsko oddaljenih lokacijah (lokacije morajo biti oddaljene najmanj 50 km zračne linije).

### 3.10. Elektronski podpis

Na področju informacijskih tehnologij smo bili v zadnjih dveh desetletjih priča izjemno hitremu tehnološkemu razvoju, kar je v veliki meri spremenilo tudi nekatere zadeve v arhivistiki kot so tehnika arhiviranja in varnost, predvsem pa odnos samih ustvarjalcev do dokumentarnega in arhivskega gradiva. To področje je bilo potrebno urediti s pravnega vidika. Tako je bil v Sloveniji leta 2000 sprejet Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP), ki opredeljuje elektronsko poslovanje z uporabo informacijske in komunikacijske tehnologije ter uporabo elektronskega podpisa v sodnih, upravnih in drugih postopkih. Največji pomen zakona je

v izenačitvi elektronskega podpisa z ročnim. Nesprejetje tega zakona bi pripreljalo do velikih ovir pri uvajanju elektronskega poslovanja v vse segmente gospodarstva.

### **3.11. eHramba.si kot primer dolgoročne elektronske hrambe**

Po tem, ko sta bila objavljena ZEPEP in ZVDAGA, so bile dane smernice, kako je potrebno hraniti elektronske dokumente oz. kaj je potrebno zagotoviti za revizijsko varen elektronski arhiv. Zahteve za hranjenje so tako striktne, da so vlaganja za vzpostavitev elektronskega arhiva zelo velika. Podjetje ZZI d.o.o. se je odločilo, da bo ponudilo storitev arhiviranja dokumentov podjetjem. Tako se vlaganja v razvoj in infrastrukturo lahko porazdelijo med več podjetij in tako postane elektronsko arhiviranje dostopnejše. Storitev se imenuje eHramba.si.

eHramba.si je storitev elektronske hrambe dokumentov, ki temelji na informacijskem sistemu za hrambo dokumentarnega gradiva in omogoča zakonsko skladno elektronsko hranjenje vseh vrst dokumentov, tako poslovne kot druge dokumentacije na enem mestu. V sistemu se lahko hranijo tako dokumenti, ki so izvorno nastali v elektronski obliki kot dokumenti, ki so nastali na papirju in so bili kasneje pretvorjeni (skenirani) v elektronsko obliko.

Sistem eHramba.si je porazdeljen sistem in ima storitveno orientirano arhitekturo.

## 4. Tehnologije sistema eHramba.si

### 4.1 Storitveno orientirana arhitektura

Poslovni informacijski sistemi so bili v preteklosti največkrat načrtovani funkcionalno. Takšni sistemi, včasih imenovani tudi silosi, vsebujejo velike količine podatkov in množico funkcionalnosti. Njihov osnovni problem je v tem, da naslavlajo podporo določeni funkciji oziroma aktivnosti, ne pa celotnemu poslovnemu procesu. Celoviti poslovni procesi morajo torej delovati nad več takšnimi aplikacijami – silosi. S tehničnega vidika to pomeni integracijski problem, kjer je potrebno ustrezno povezati različne aplikacije, izdelane v različnih tehnologijah in poskrbeti za ustrezno zaporedje izvajanja. Pri tem ne gre pozabiti, da je tudi funkcionalnost takega poslovnega procesa razpršena med več obstoječih sistemov – z drugimi besedami, funkcionalnost je fragmentirana in tesno sklopljena. Izhajajoč iz tega spoznanja je očitno, da je že razvoj poslovnih procesov, ki morajo povezati množico obstoječih sistemov, zamuden in kompleksen. Enako velja za dopolnjevanje in spreminjanje. Več kot očitno je, da na tak način informatiki ne morejo zadostiti potrebam po fleksibilnih in hitro spreminjajočih se poslovnih procesih [7].

Storitveno orientirane arhitekture ponujajo odgovor na ta problem in ponujajo načine razvoja in integracije poslovnih aplikacij na osnovi modularnih, šibko sklopljenih storitev. Ključni poudarek storitvenih arhitektur je torej na definiciji načina integracije samostojnih obstoječih ali novo razvitih aplikacij – imenovanih storitev – v celovit sistem. Poseben poudarek je na modelu komunikacije, podpori različnih transportnih mehanizmov, zagotavljanju varnosti in transakcijske identitete, zanesljivosti sporočanja ter koordinaciji in kompoziciji. S tehnološkega vidika storitvene arhitekture posebna vrsta porazdeljenih sistemov, pri katerih so komponente sistema storitve. Svojo pravo vrednost pa storitvene arhitekture razkrijejo, ko pogledamo na njih z vsebinskega vidika.

#### 4.1.1. Tehnološki vidik SOA

Storitveno orientirana arhitektura je posebna vrsta porazdeljenega sistema, pri kateri so komponente sistema storitve. Storitve opravlja neko natančno določeno operacijo, ki jo lahko uporabimo tudi izven konteksta aplikacije, v kateri je ponujena. Pomembno je tudi, da ima takšna storitev natančno definiran vmesnik, do katerega lahko dostopimo preko omrežja z uporabo standardnih protokolov in podatkovnih tipov. Vmesnik storitve je pravzaprav le natančen opis sporočil, ki si jih lahko izmenjamo.

Storitvene arhitekture temeljijo na naslednjih konceptih [8]:

- podpora za sinhrono in asinhrono komunikacijo;
- različnih tipih storitev: podatkovnih, komponentnih, konverzijskih, sporočilnih;
- storitvenem vodilu (ESB – Enterprise Service Bus);
- obravnavi izjem in kompenzaciji delnih učinkov procesov;

- prestrežanju zahtev in razširljivosti;
- povezljivosti;
- varnosti.

SOA udejanja spremembo načina razvoja aplikacij. Iz modela načrtovanja, kodiranja, testiranja, nameščanja prehajamo v model sestavljanja, konfiguriranja, testiranja, nadzora. To omogočajo poslovne storitve, ki morajo biti izdelane na ustreznem nivoju granularnosti in ki so najpomembnejši katalizator povezovanja poslovnih zahtev z zmožnostmi informatike. Zato predstavlja razvoj storitev prvi ključni korak v smeri realizacij SOA.

Vpeljava SOA poteka v dveh ključnih korakih, ki do neke mere lahko potekata vzporedno:

- Prvi korak je izpostavljanje funkcionalnosti obstoječih aplikacij v obliki storitev (najpogosteje spletnih storitev – Web services, v kompleksnejših sistemih pa uporabimo ESB – Enterprise Service Bus).
- Drugi korak je kompozicija storitev v poslovne procese.

Svojo pravo vrednost pokaže SOA šele po realizaciji drugega koraka, ki eksplicitno definira povezave in sodelovanje storitev v poslovnih procesih ter sodelovanje procesov v poslovnih protokolih. Šele z realizacijo drugega koraka lahko pričakujemo uresničitev ciljev, povezanih s SOA, kot so: izboljšana učinkovitost poslovnih procesov, hitrejša odzivnost na spremembe in boljša prilagodljivost, bolje integrirani in fleksibilni informacijski sistem in aplikacijski sistemi ter zmanjšana kompleksnost.

Pri tem pa je smiselno opozoriti, da je koncepte SOA potrebno aplicirati premišljeno, saj razvoj storitvenih arhitektur skriva tudi precej pasti. Najpogostejše med njimi so:

- storitve, ki uporabljajo preveč fino granulacijo vmesnikov;
- uporaba tehnologij za oddaljen dostop do storitev, ki so nameščene lokalno;
- pretirana uporaba jezika XML in neustrezna struktura sporočil;
- uporaba šibke sklopljenosti tam, kjer je potrebna tesna sklopljenost.

Realizacija storitvene arhitekture je povezana z uporabo ustreznih tehnologij. Spletne storitve so najprimernejša tehnologija za implementacijo storitvenih arhitektur.

## 4.2. Porazdeljeni sistemi

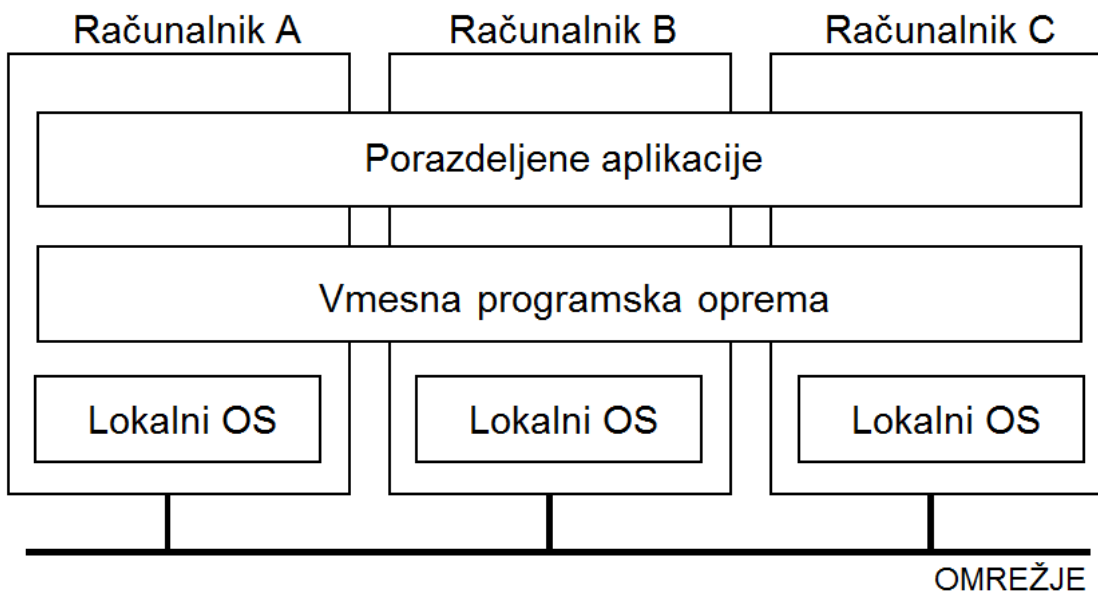
Pri brskanju po literaturi o porazdeljenih sistemih, se srečujemo z različnimi definicijami o le teh. Za naše namene, bo dovolj naslendja ohlapna definicija [9]:

“Porazdeljen sistem je zbirka medsebojno neodvisnih računalnikov, ki se uporabniku predstavlja kot en sam sistem.”

Definicija ima dva vidika. Prvi vidik govori o strojni opremi: računalniki so samostojni. Drugi pa o programski opremi: uporabniki mislijo, da delajo na enem samem sistemu. Obe sta bistvenega pomena.

Pomembna karakteristika porazdeljenega sistema je ta, da so razlike med računalniki in načini njihove medsebojne komunikacije skrite pred uporabniki. Enako velja za notranjo organizacijo porazdeljenih sistemov. Druga pomembna karakteristika je ta, da lahko aplikacije in uporabniki komunicirajo s porazdeljenim sistemom na konsistenten in enak način, ne glede na to od kje in kdaj dostopajo do njega. Pri gradnji porazdeljenega sistema se teži k temu, da bo sistem v prihodnosti relativno lahko razširili ali nadgradili. Ta karakteristika je posledica tega da imamo v sistemu samostojne računalnike ter da hkrati prikrijemo, kje se v sistemu nahajajo. Aplikacije in uporabniki ne smejo opaziti, da so deli sistema v popravilu ali pravkar v menjavi.

Za podporo heterogenih računalnikov in omrežij, medtem ko uporabniku ponujamo pogled v en sam sistem, so porazdeljeni sistemi pogosto organizirani s pomočjo plasti programske opreme, ki je postavljena med uporabnike in aplikacije na višjih nivojih in operacijske sisteme na nižjih nivojih kot prikazuje slika 1. V skladu s tem se porazdeljenemu sistemu včasih reče middleware.



Slika 1: Definicija porazdeljenega sistema

#### 4.2.1. Cilji pri načrtovanju porazdeljenega sistema

Samo zaradi tega, ker je porazdeljen sistem možno zgraditi, ni nujno da je to vedno dobra ideja. S trenutno tehnologijo bi načeloma lahko v računalnik vstavili štiri enote DVD-ROM, toda poteza bi bila nesmiselna. Zato obstajajo štirje pomembni cilji, katere si postavimo pred sestavo porazdeljenega sistema, da bo ta služil namenu. Porazdeljen sistem naj:

- z lahkoto poveže uporabnike z viri;
- prikrije dejstvo da so viri porazdeljeni po omrežju;

- je odprt;
- je razširljiv.

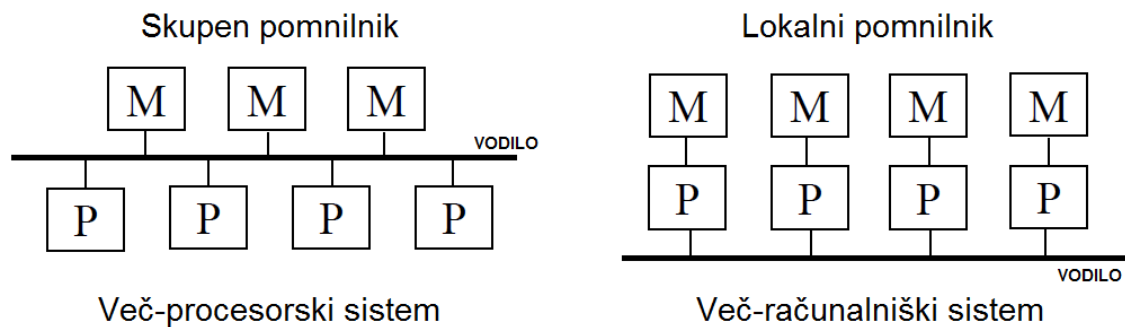
#### 4.2.2. Zasnova strojne opreme porazdeljenih sistemov

Čeprav vse porazdeljene sisteme tvori več centralno procesnih enot (CPE), obstajajo različni načini organizacije strojne opreme. Najbolj izpostavljena sta načina kako so CPE med seboj povezane ter kako med seboj komunicirajo. Vse računalnike delimo v dve skupini: več-procesorske (multiprocessors), ki si delijo skupni pomnilnik in več-računalniške (multicomputers), ki nimajo skupnega pomnilnika.

Glavna razlika je sledeča: pri več-procesorskemu sistemu je en sam pomnilniški naslovni prostor, ki si ga delijo vse CPE (če katerakoli CPE zapiše vrednost 4 na naslov 100, bo nato, katerakoli CPE, ki bo brala iz naslova 100, dobila vrednost 4. Vse CPE si delijo skupni pomnilnik).

Pri več-računalniškemu sistemu ima vsaka CPE svoj lasten pomnilnik, z lastnim naslovnim prostorom. Tipičen primer več-računalniškega sistema je skupina osebnih računalnikov povezanih v skupno omrežje.

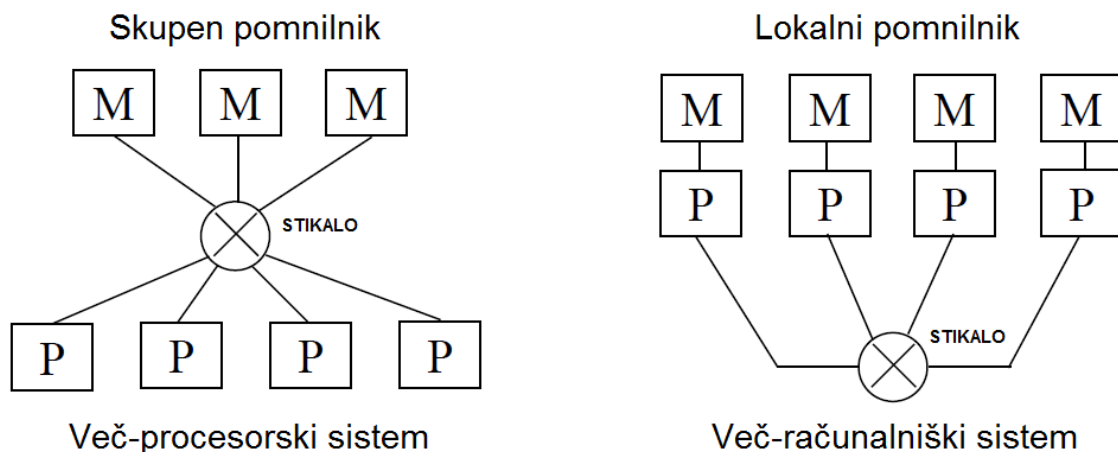
Obe skupini se naprej delita glede na arhitekturo povezave v omrežje. Delita se na povezave z vodilom in povezave s stikalom. Kot vodilo mislimo na eno omrežje, hrbtno povezavo ('backplane'), vodilo, kabel ali drug medij, ki povezuje vse računalnike. Tak primer je kabelska televizija, katera uporablja opisan način povezave: en kabel potuje po ulici na katerega so priključeni naročniki.



P - procesor  
M - pomnilnik

Slika 2: Porazdeljen sistem povezan z vodilom

Sistemi s povezavo s stikalom imajo za razliko od enega samega vodila vsak svojo povezavo od računalnika do računalnika. Informacije potujejo od računalnika po povezavah do stikal, kjer se naprej usmeri na naseljno povezavo. Svetovni javni telefonski sistem je organiziran na ta način.



Slika 3: Porazdeljen sistem povezan s stikalom

Več-računalniški sistemi se nadaljno delijo na homogene in heterogene sisteme. Pri homogenih več-računalniških sistemih so vsi procesorji enaki in imajo tudi enako velik pomnilnik, povezani so v eno povezovalno omrežje z enako tehnologijo. Vsi procesorji so enaki ter dostopajo do enake količine pomnilnika. Uporablja se jih predvsem za paralelno procesiranje (ukvarjajo se z enakim problemom). Heterogeni več-računalniški sistemi vsebujejo različne samostojne računalnike, ki so povezani preko različnih omrežij.

#### 4.2.3. Zasnova programske opreme porazdeljenih sistemov

Strojna oprema je za porazdeljene sisteme pomembna, toda programska oprema je tista, ki določi, kako bo sistem izgledal. Programska oprema porazdeljenih sistemov je v osnovi zelo podobna klasičnim operacijskim sistemom. Deluje kot upravljalca virov, kar omogoča uporabnikom in aplikacijam delitev virov kot so CPE, pomnilniki, periferne naprave, omrežje ter podatki različnih vrst. Bolj pomembno pa je, da porazdeljeni sistemi s pomočjo programske opreme prikrijejo zapleteno povezanost in heterogeno naravo strojne opreme.

Operacijske sisteme za porazdeljene sisteme delimo v tri kategorije:

- Tesno povezani operacijski sistemi za več-procesorske in homogene več-računalniške sisteme - DOS ('Distributed Operating System').
- Šibko povezani operacijski sistemi za heterogene več-računalniške sisteme (LAN in WAN) NOS ('Network Operating System').
- Vmesna programska oprema (middleware)

Naloga tesno povezanega porazdeljenega operacijskega sistema je, da prikrije zapletenost upravljanja s strojnimi viri in tako omogoča, da si jih lahko delijo različni procesi.

Da pravzaprav iz navadnega operacijskega sistema dobimo porazdeljen sistem so potrebna dodatna orodja. Ta orodja so splošno znana kot vmesna programska oprema ali "middleware". To je programska oprema, ki leži med operacijskim sistemom ter aplikacijami in katero sestavlja

nabor storitev, ki omogočajo interakcijo raznim procesom in aplikacijam, ki so porazdeljeni po sistemu.

Na sliki 4 so zbrana osnovna dejstva o treh različnih zasnovah programske opreme porazdeljenih sistemov.

Sistem	Opis	Osnovni cilj
DOS	Tesno povezan operacijski sistem za več-procesorske in homogene več-računalniške sisteme	Prikrivanje povezav – upravljanja s strojnimi viri
NOS	Šibko-povezan operacijski sistem za heterogene več-računalniške sisteme (LAN, WAN)	Omogoča lokalne storitve oddaljenim odjemalcem
Middle-ware	Dodatna plast med NOS in splošnimi storitvami	Omogoča nevidnost porazdeljenosti

Slika 4: Pregled programske opreme porazdeljenih sistemov

### 4.3. Sistem sporočilnih vrst

V sistemu sporočilnih vrst (Message-Queuing MQ) aplikacije komunicirajo med seboj s pošiljanjem sporočil v določene vrste. Sporočila potujejo preko komunikacijskih strežnikov in so sčasoma dostavljena prejemniku, tudi če je bil ta izključen, ko je bilo sporočilo poslano. Sporočilo je običajno poslano direktno prejemnikovemu strežniku. Vsaka aplikacija ima svojo privatno vrsto, v katero lahko pošiljajo sporočila druge aplikacije. Sporočila v vrsti lahko bere le aplikacija, ki ji vrsta pripada, lahko pa si tudi več aplikacij deli eno samo vrsto.

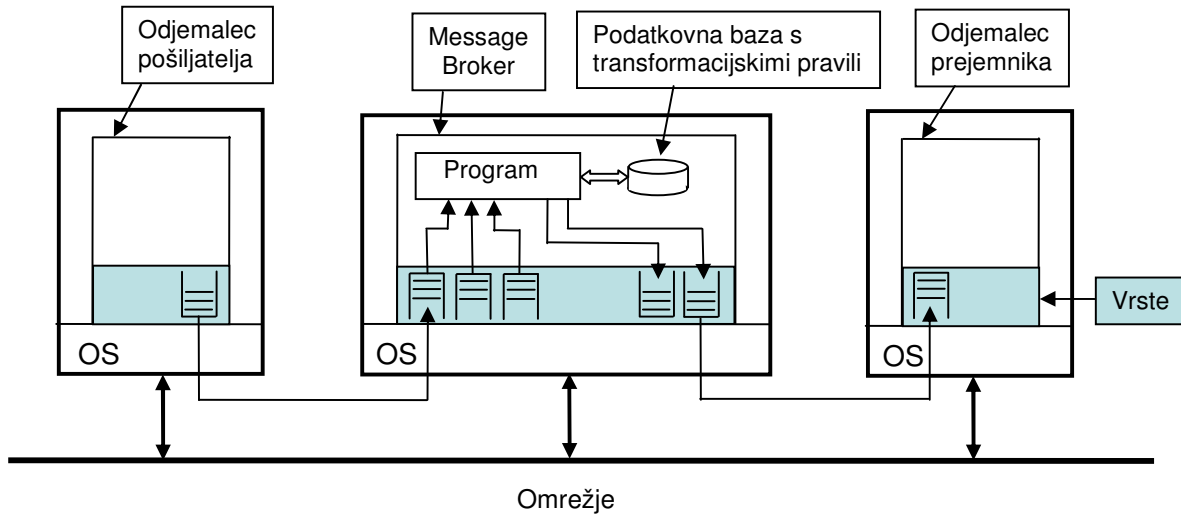
Pomembna lastnost sistema sporočilnih vrst je, da ima pošiljatelj le zagotovilo, da bo sporočilo sčasoma dostavljeno v prejemnikovo vrsto. Pošiljatelj nima nobenega zagotovila, kdaj bo sporočilo prebrano, oziroma če sploh bo prebrano, ker je to določeno z delovanjem prejemnika.

Tako lahko pošiljatelj in prejemnik sporočila delujeta popolnoma neodvisno drug od drugega in ni potrebno, da prejemnik deluje, ko je sporočilo poslano v njegovo vrsto. Prav tako lahko tudi pošiljatelj ne deluje, ko prejemnik prebere sporočilo.

Sporočila lahko v splošnem vsebujejo kakršnekoli podatke, važno je le, da so pravilno naslovljena. Naslavljanje je v praksi izvedeno z enoličnim imenom vrste, ki ji je sporočilo namenjeno. Dolžina sporočila je v določenih primerih lahko omejena, vendar sistem sam poskrbi za razstavljanje in ponovno sestavljanje zelo dolgih sporočil, kar je v aplikaciji popolnoma nevidno.

Dodajanje novih aplikacij v sistem sporočilnih vrst zahteva enak format sporočil, kar pa ni vedno mogoče ali smiselno. Čeprav so za določene aplikacijske domene definirani skupni formati sporočil, je v splošnem potrebno v sistem sporočilnih vrst dodati mehanizem za prilagajanje različnih formatov sporočil imenovan message broker.

Njegova naloga je pretvarjati prihajajoča sporočila v format, ki ga bo razumela aplikacija prejemnika sporočila. Za sistem sporočilnih vrst je message broker samo še ena od aplikacij in se običajno ne smatra kot integralni del sistema. Vloga aplikacije za pretvarjanje sporočil je razvidna na sliki 5.



Slika 5: Sistem sporočilnih vrst s transformacijo sporočil

Primer sistema sporočilnih vrst je sistem IBM WebSphere MQ firme IBM, ki je sestavni del programske opreme IBM WebSphere.

#### 4.4. IBM WebSphere

IBM WebSphere je programska oprema oziroma skupina programskih paketov za SOA okolja. Namenjen je vzpostavitvi, upravljanju in integraciji elektronskih poslovnih aplikacij po različnih računalniških okoljih, z uporabo javanskih spletnih tehnologij. Vsebuje tako izvajalno okolje kot razvojna orodja za aplikacije.

Najbolj znani programski paketi so :

- IBM WebSphere Application Server
- IBM WebSphere DataPower SOA Appliances
- IBM WebSphere ESB
- IBM WebSphere Message Broker
- IBM WebSphere MQ

## 4.5. IBM WebSphere MQ

IBM ponuja več različnih možnosti povezovanja zahtevnih okolij. Različna zahtevna okolja lahko povežemo med seboj na nivoju aplikacij in na nivoju poslovnih procesov. Na nivoju aplikacij IBM ponuja programsko opremo WebSphere MQ, ki lahko povezuje zahtevna okolja znotraj podjetja ali med podjetji. IBM WebSphere MQ je asinhroni, sporočilno usmerjen middleware s funkcionalnostjo enkratne in zanesljive (transakcijske) dostave sporočil (podatkov). Lahko ga uporabljamo na najrazličnejših platformah. Omogoča omrežno komunikacijo med programi, ki tečejo na različnih operacijskih sistemih z različnimi komponentami, podsistemi ter komunikacijskimi protokoli.

IBM WebSphere MQ je torej IBM-ov produkt za prenašanje podatkov med različnimi platformami. Njegove najpomembnejše lastnosti so:

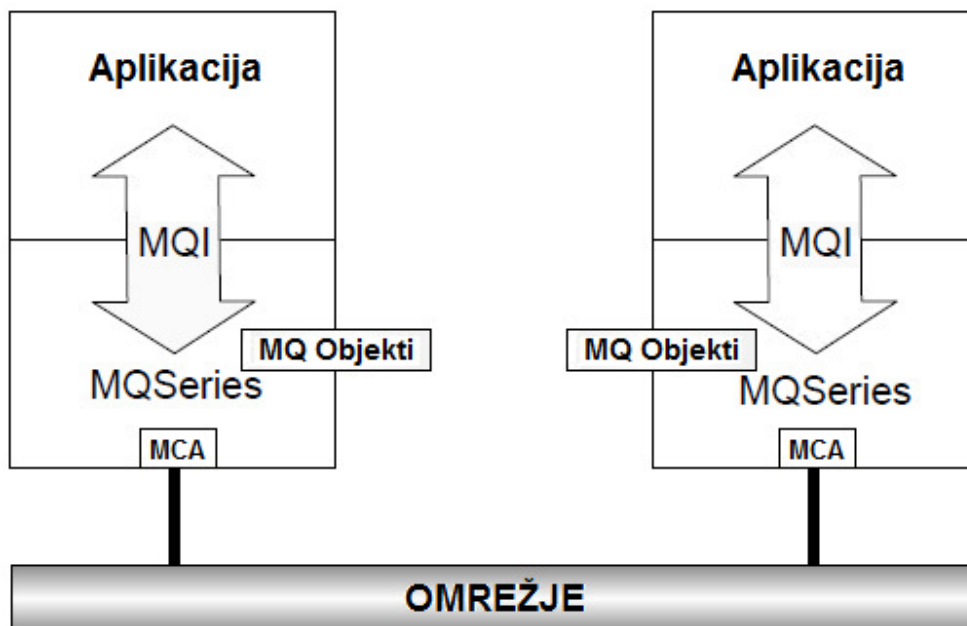
- Uporablja se za pošiljanje sporočil. Deluje podobno kot FTP (vendar ima več dodanih vrednosti), ter ni medij za shranjevanje podatkov.
- Asinhrona povezava (časovna neodvisnost - ni potrebe, da je ciljni sistem ob prenosu dosegljiv).
- Proženje - ko določeno število sporočil prispe v vrsto se lahko sproži obdelava ali proces, definira ga MQ Administrator.
- Sporočila se ne izgubljajo ali podvajajo. Podprt praktično za vse platforme, tako omogoča povezljivost med različnimi okolji in podatkovnimi bazami.
- Persistenca - beleženje sporočil (restavriranje v primeru prekinitve).

### 5.5.1. Arhitektura sistema IBM WebSphere MQ

Osnovna arhitektura sistema IBM WebSphere MQ je povsem enostavna. Imamo dva glavna gradnika:

- vrsta,
- sporočilni kanal.

Vse vrste upravljajo upravljavci vrst (ang. queue managers). Ti so zadolženi za pobiranje sporočil iz njihovih vrst za odhodna sporočila ter posredovanje sporočil drugim upravljavcem. Prav tako so zadolženi sprejemati sporočila iz omrežja ter jih posredovati naslovljeni vrsti. Upravljavci vrst so v paru povezani preko sporočilnih kanalov. Sporočilni kanal je neusmerjena, zanesljiva povezava med oddajnim in sprejemnim upravljavcem vrst, po kateri se prenašajo sporočila. Vsak konec kanala upravlja MCA ('Message Channel Agent'). Oddajni agent preverja svojo oddajno vrsto za sporočila, jih ovije v paket za transportni nivo ter pošlje do sprejemnega agenta. Obratno je naloga sprejemnega agenta poslušati za prihodne pakete, jih odviti ter shraniti sporočilo v primerno vrsto.



Slika 6: Arhitektura sistema IBM WebSphere MQ

Slika 6 prikazuje glavne dele IBM WebSphere MQ. Aplikacije uporabljajo MQI - 'Message Queue Interface' (vmesnik MQ) za komunikacijo z upravljavci vrst. Upravljalci vrst upravlja z objekti MQ, kot so vrste in kanali.

#### 4.6. IBM WebSphere Message Broker

Storitveno vodilo, narejeno za transformiranje in povezovanje podatkov med heterogenimi informacijskimi okolji. Deluje kot vmesnik za podatke in protokole med neskladnimi okolji in platformami.

Gre za prilagodljivo in dinamično infrastrukturo, ki nam poenostavi integracijo poslovnih aplikacij. S pomočjo WebSphere Message Broker-ja lahko SOA-o vpeljujemo po fazah in to iz katerekoli startne pozicije – bodisi gre za integracijo dveh aplikacij, med katerima postavimo Message Broker (1 v 1) ali pa integracijo širšega spektra aplikacij (n na n).

Broker je množica aplikacijskih procesov, ki gostijo in poganjajo sporočilne tokove. Kadar sporočilo prispe iz določene aplikacije v broker, ga ta obdela preden ga pošlje naprej na eno ali več aplikacij. Broker preusmerja, transformira in manipulira s sporočili po logiki ki je definirana v njegovem sporočilnem toku. Uporablja WebSphere MQ kot transportni mehanizem za komunikacijo med sporočilnimi tokovi ter z ostalimi brokerji. Vsak broker ima bazo podatkov, v kateri hrani informacije, ki jih potrebuje za procesiranje sporočil v času delovanja.

Funkcionalnosti:

- Podpora je širok spekter protokolov za delo s sporočili in podatkovnih formatov;
- Veliko je možnosti prilagoditve posredovanja, ki jo odigra Message Broker med aplikacijami;
- Uporablja enostavne programske modele za delo s sporočili in posredovanje (vključenih je veliko prednastavljenih posredovalnih/mediacijskih funkcij);
- Podprte transformacijske možnosti: preslikave, Java, ESQ, XSL in WebSphere Transformation Extender;
- Širok spekter možnosti administracije;
- Omogoča podobne zmogljivosti kot tradicionalni transakcijski sistemi;
- Izboljšana podpora za SOA;
- Razširjen je nabor podprtih platform;
- Podpora za spletne storitve;
- Integracija z orodjem IBM WebSphere Service Registry and Repository;
- Podpora za integracijo s ključnimi ERP-ji (načrtovanje virov podjetja): SAP, Siebel, PeopleSoft s pomočjo adapterjev WebSphere;
- Podpora za FTP, elektronsko pošto;
- Avtentifikacija in avtorizacija uporabnikov s podporo strežnikov LDAP;
- Razčlenjevalnik kode (parser) XML, z možnostjo validacije shem.

#### 4.7. Časovno žigosanje

Če želimo za neko pomembno pogodbo ali oporoko prepričati, da bi kdo kasneje oporekal njeni veljavnosti, si zagotovimo nepristransko pričjo, ki bo prav tako, kot vpletene stranke, podpisala dokument. Podobno vlogo kot nepristranska pričja za običajne dokumente ima izdajatelj časovnih žigov za elektronske dokumente. V angleščini se je zanj uveljavil naziv "Time Stamp Authority" oziroma kratica TSA.

Gre za dobro zaščiten strežnik – podobno kot za izdajatelja digitalnih potrdil morajo biti izpolnjeni strogi varnostni ukrepi, sicer bi lahko dvomili v njegovo verodostojnost oziroma nepristranskost. Sinhroniziran je s časovnimi strežniki in tako zagotavlja točen čas.

Ko želimo v neki aplikaciji časovno žigosati nek elektronski dokument oziroma podatke, pošljemo strežniku z zgoščitveno funkcijo narejen "povzetek" (hash) dokumenta oziroma podatkov. To je fiksni niz bitov, ki enolično določa dokument. Strežnik temu povzetku dopiše čas in vse skupaj podpiše s svojim zasebnim ključem - to je časovni žig, ki ga vrne aplikaciji. Aplikacija časovni žig shrani za bodoča preverjanja podpisanega dokumenta. Tako je dokazano, da je elektronski dokument obstajal pred časom, navedenim v časovnem žigu, poleg tega pa se da preveriti, da se od časa žigosanja ni spremenil (naredimo ponovni povzetek dokumenta in se mora ujemati s tistim, ki je del časovnega žiga).

#### 4.7.1. Sistem eKeeper

eKeeper je rešitev podjetja SETCCE, ki rešuje probleme zakonsko skladnega elektronskega arhiviranja. Omogoča obvladovanje poslovne dokumentacije in zagotavlja dolgoročno avtentičnost in verodostojnost hranjenih elektronskih dokumentov, ne glede na izvor (papirni ali elektronski). Vgrajeni postopki elektronskega arhiviranja upoštevajo stroga določila zakonodaje (ZVDAGA in ZEPEP).

eKeeper elektronskim dokumentom dodaja in vzdržuje varnostne vsebine skladno z zakonodajo, enotnimi tehnološkimi zahtevami in tehnološkim standardom ERS (Evidence Record Syntax), ki ga definira organizacija IETF [10]. Na podlagi varnostnih vsebin je mogoče kadarkoli v času hrambe na tehnološki način nedvoumno dokazati [11]:

- čas obstoja arhiviranih elektronskih dokumentov v preteklosti;
- neokrnjenost vsebine elektronskih dokumentov;
- veljavnost digitalnih podpisov elektronskih dokumentov;
- podaljševanje veljavnosti digitalnih podpisov.

V obdobju arhiviranja eKeeper v skladu z zakonskimi zahtevami po periodičnem potrjevanju avtentičnosti in celovitosti gradiva samodejno vzdržuje dodane varnostne vsebine. Z varnostnimi vsebinami upravlja ločeno od dokumentov in ne posega v njihovo vsebino. Priprava in vsakokratna osvežitev varnostnih vsebin se zaključijo s časovnim žigosanjem, kar omogoča preverjanje veljavnosti arhiviranih dokumentov v kasnejšem času. Pridobivanje časovnega žiga eKeeper izvaja samodejno, z uporabo akreditiranih zunanjih storitev (npr. pri SI-TSA ali POŠTA@CA [12]).

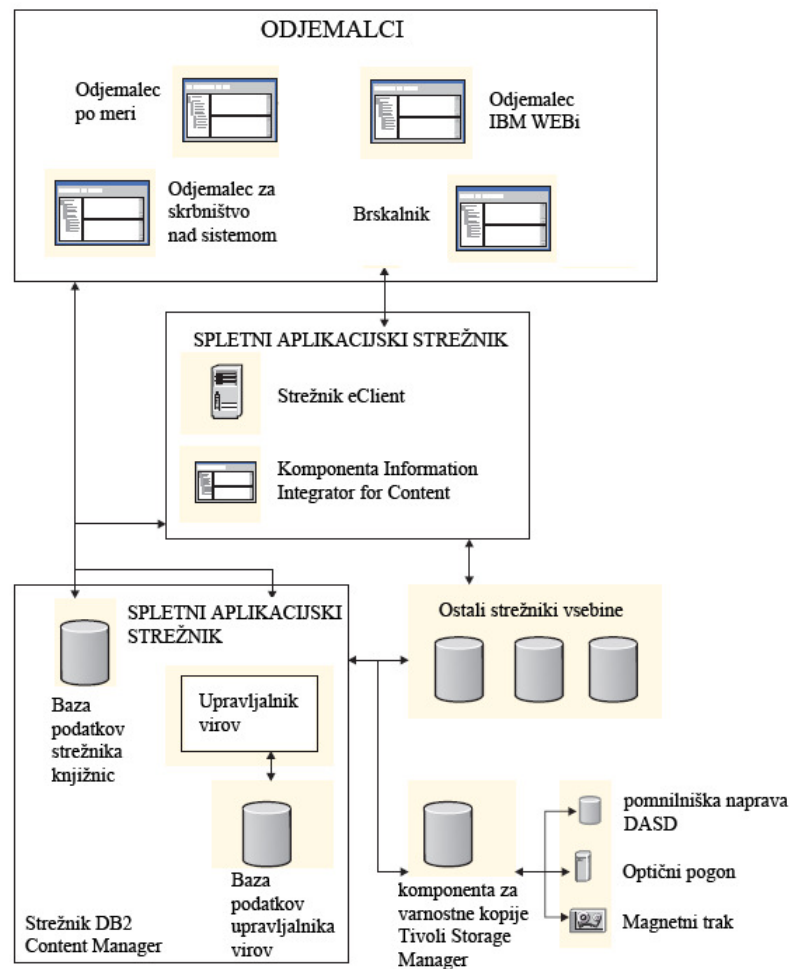
#### 4.8. Sistem IBM Content Manager

IBM Content Manager (IBM CM) predstavlja splošno uporabno orodje za upravljanje z digitalizirano vsebino vseh tipov, vključno s spletno vsebino HTML in XML, slike dokumentov, elektronske pisarniške dokumente, avdio in video.

Orodje omogoča [13]:

- shranjevanje in dostop do vsebine,
- verzioniranje vsebine,
- varnostni sistem za vsebino,
- upravljanje dela z dokumenti (workflow),
- ter iskanje elektronske vsebine v poljubnem formatu.

Programska oprema je podprta za več operacijskih sistemov in omogoča dostop do vsebine preko spletnega brskalnika. Sistem Content Manager je sestavljen iz odjemalskih programov, integriranih aplikacij, strežniških programov in repozitorija vsebine. Slika 7 kaže osnovno arhitekturo sistema Content Manager.



Slika 7: Osnovna arhitektura sistema IBM Content Manager

## 4.9. Simple Object Access Protocol

Simple Object Access Protocol (SOAP) je specifikacija protokola za izmenjavo strukturiranih informacij z implementacijo spletnih storitev. Strukturirane informacije so najpogosteje predstavljene v formatu XML, za izmenjavo in prenos informacij pa se najpogosteje poslužuje protokolov kot so RPC ali HTTP. Z drugimi besedami lahko rečemo da je SOAP standard za spletne storitve, ki temelji na formatu XML.

SOAP protokol je sestavljen iz treh delov [14]:

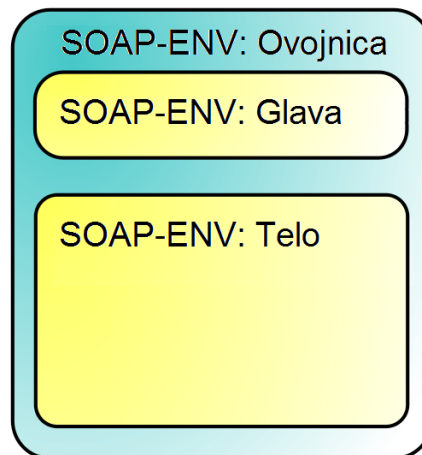
- ovojnica SOAP, ki definira vsebino sporočila ter način kako ga procesirati
- nabor pravil kodiranja
- podatki o klicih procedur in odzivov

SOAP deluje neodvisno glede na računalniško okolje in je povezljiv s katerikoli protokolom. Načrtovalcem SOAP-a sta cilj predstavljali dve poglavitni točki - preprostost in razširljivost.

#### 4.9.1. Struktura SOAP sporočila

Veljavno sporočilo SOAP je pravilno oblikovan dokument XML. Uvodno polje XML je lahko prisotno vendar lahko vsebuje samo deklaracijo XML (ne sme vsebovati nobenih pravil za strukturiranje dokumenta ali ukaze za procesiranja). Sestavljeno je iz ovojnice SOAP ter nabora pravil kodiranja in ima sledečo obliko [15]:

- deklaracijo XML (opcijsko)
- ovojnica SOAP (korenski element)
  - glava SOAP (opcijsko)
  - telo SOAP



Slika 8: Struktura sporočila SOAP

#### 4.9.2. Primer zahteve in odgovora SOAP

Primer je podan z enostavno metodo ki vrne dvakratnik podanega števila:

```
int doubleAnInteger (int numberToDouble);
```

##### Zahteva SOAP:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<SOAP-ENV:Envelope
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/1999/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/1999/XMLSchema">
  <SOAP-ENV:Body>
    <ns1:doubleAnInteger xmlns:ns1="urn:MySoapServices">
      <param1 xsi:type="xsd:int">123</param1>
    </ns1:doubleAnInteger>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

##### Odgovor SOAP:

```
<?xml version="1.0" encoding="UTF-8" ?>
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/1999/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/1999/XMLSchema">
  <SOAP-ENV:Body>
    <ns1:doubleAnIntegerResponse xmlns:ns1="urn:MySoapServices"
SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
">
      <return xsi:type="xsd:int">246</return>
    </ns1:doubleAnIntegerResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

V obeh primerih vidimo ogrodje ki objema celotni sporočili. Kot vidimo sta zgradbi zahteve in odgovora na prvi pogled enaki, kar nam pove, da je zgradba SOAP-a neodvisna in nevtralna ker tip ni eksplicitno podan. Potrebno je pogledati polje znotraj polja "Body" in definicijo tega polja, da vidimo razliko.

## 5. Storitve eHramba.si

eHramba.si je storitev elektronske hrambe dokumentov, ki temelji na informacijskem sistemu za hrambo dokumentarnega in arhivskega gradiva. Omogoča zakonsko skladno elektronsko hranjenje dokumentov, ki so izvorno nastali v elektronski obliki ter dokumentov, ki so nastali na papirju in so bili kasneje pretvorjeni v elektronsko obliko.

Cilji e-hrambe so zagotovitev zakonsko skladnega elektronskega arhiva čim večim podjetjem. Arhiv mora biti cenovno dostopen in mora pokriti vse zahteve podjetij po elektronskem arhivu.

Hranjeno dokumentarno gradivo je zaščiteno na nivoju strojne in programske opreme. V sistem so vgrajene tehnologije, ki onemogočajo nepooblaščen dostop in nenadzorovano uničenje ali izgubo hranjenega gradiva. Sistem tudi beleži vse dostope in izvedene akcije nad hranjenim gradivom po posameznih uporabnikih (revizijska sled).

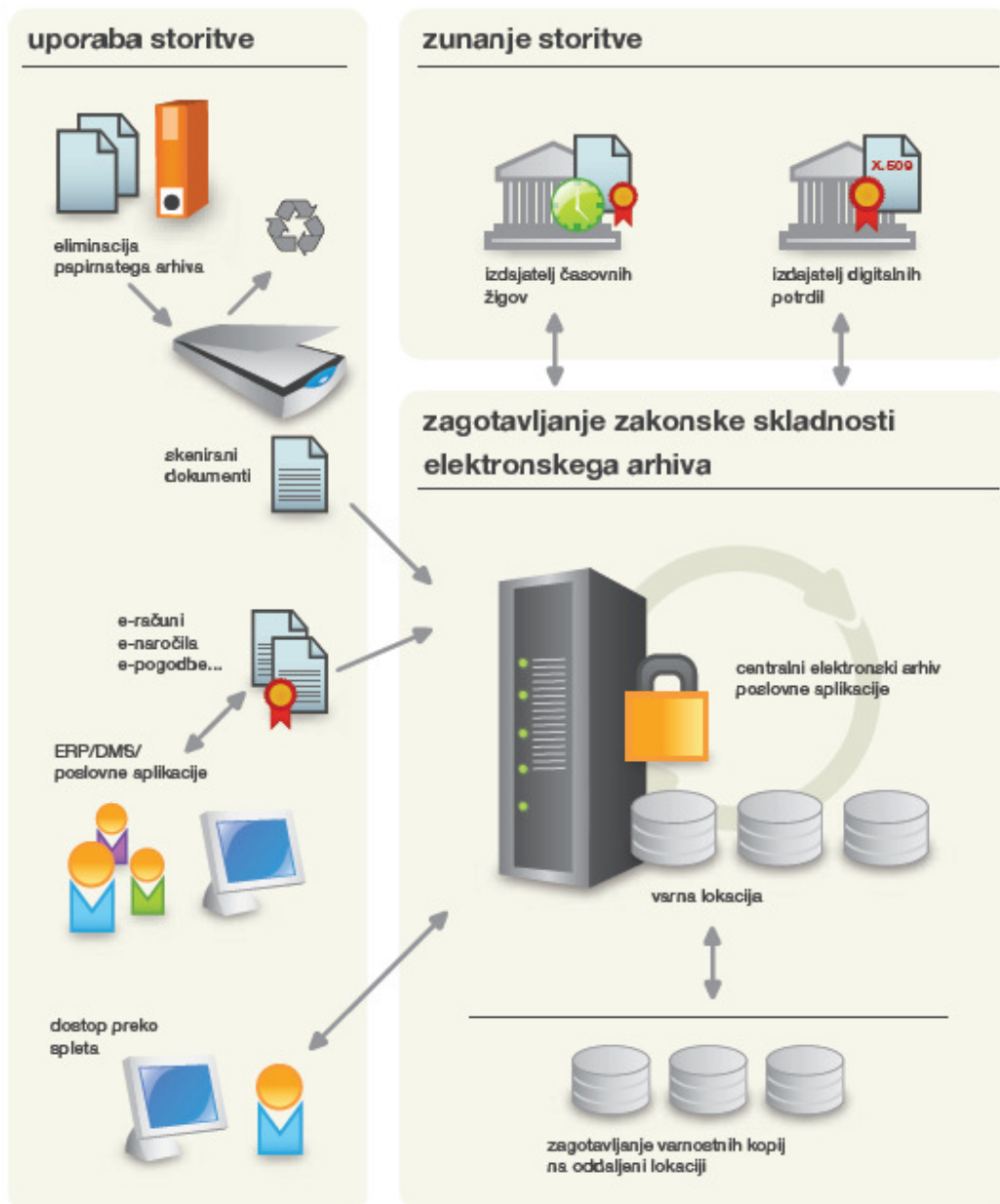
Storitve eHramba.si podpira osnovne aktivnosti v procesu arhiviranja dokumentarnega gradiva v elektronski obliki kot so:

- zajem dokumentov,
- pretvorba med različnimi formati zapisa,
- kratkoročna in dolgoročna hramba,
- iskanje hranjenih dokumentov in
- uničenje dokumentov po izteku roka hrambe.

Lastnosti eHramba.si storitev elektronskega arhiviranja dokumentarnega in arhivskega gradiva:

- Varna in zanesljiva hramba dokumentov
- Preglednost in hiter dostop do dokumentov
- Zagotovljena nespremenljivost in trajnost dolgoročno hranjenih dokumentov.
- Univerzalna dostopnost in neprekinjeno delovanje (preko portalnega uporabniškega vmesnika od kjerkoli in kadarkoli)
- Široka uporabnost na različnih področjih poslovanja.
- Integracija z različnimi poslovno-informacijskimi sistemi.
- Iskanje preko različnih atributov (metapodatkov dokumenta)
- Dokazljivost obstoja določenega dokumenta ob nekem času.

Slika 9 prikazuje storitve uporabnika in zunanje storitve sistema. Uporabnikom je omogočen dostop do sistema preko spleta in preko poslovnih aplikacij. Sistem se poslužuje zunanjih storitev kot so izdajanje časovnih žigov ter digitalnih potrdil.



Slika 9: Uporabniške in zunanje storitve sistema eHramba.si

## 5.1. Skladnost z zakonodajo

Struktura in delovanje sistema eHramba.si sta skladna z veljavno zakonodajo na tem področju, z Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA) in Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP). Poleg tehnoloških zahtev glede dolgoročne varnosti dokumentarnega gradiva so v sistemu upoštevani tudi standardi, ki urejajo organizacijo arhivske službe, poslovanje z elektronskimi dokumenti in podpisovanje arhivskega gradiva. Skladnost z zakonodajo, upoštevanje standardov in akreditacija ponudnika zagotavljajo

uporabniku enakovreden pravni status (dokazno vrednost) dokumentov, hranjenih v sistemu eHramba.si, z dokumenti, hranjenimi v materialni obliki (na papirju). Storitev je registrirana, ima potrjena notranja pravila in je v postopku akreditacije pri Arhivu Republike Slovenije (RS), ki je pooblaščen organ za registracijo in akreditacijo tovrstnih storitev v RS.

## **5.2. Varnost hranjenega gradiva**

Vsa infrastruktura, ki je potrebna za delovanje storitev eHramba.si se nahaja v za to posebej prirejenem prostoru, (standardi, protipožarna, protipoplavna, protivlomna zaščita). Prva paralelna lokacija, ki ustreza varnostnim standardom, zagotavlja nemoteno delovanje tudi v primeru naravnih nesreč in drugih katastrof. Tretja varnostna lokacija, pa se nahaja na oddaljeni lokaciji v obliki sefa.

Za preprečevanje okužbe z virusi je na vseh delovnih postajah, prenosnikih in strežnikih v podjetju ZZI d.o.o. nameščen protivirusni program, ki se centralno upravlja (nadzor, prenos definicij). Poskrbljeno je tudi za zaščito s požarnim zidom.

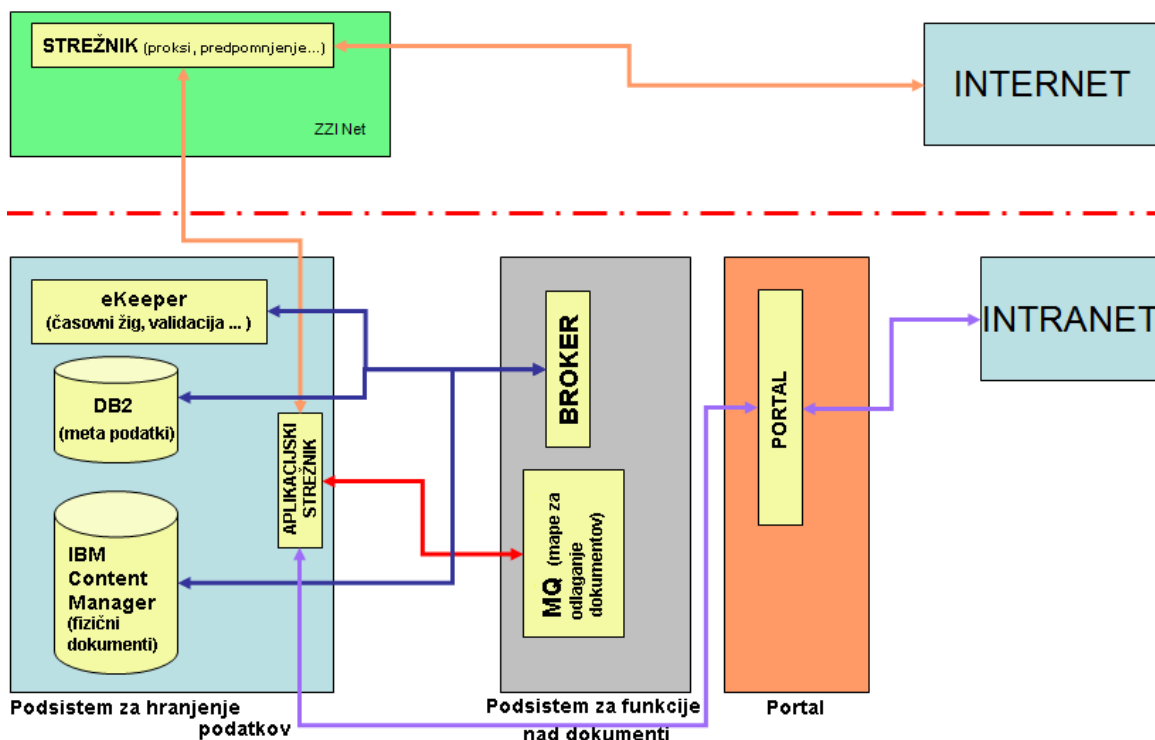
Storitev vsebuje uporabnikom prilagojen sistem pooblastil za dostop po uporabnikih in skupinah uporabnikov samo do določenih vrst dokumentov, nad katerimi se lahko izvajajo samo predpisane akcije.

## **5.3. Arhitektura sistema eHramba.si**

Sistem je porazdeljen - sestavljen iz več podsistemov. Delimo ga na [16]:

- podsistem za hranjenje podatkov;
- podsistem za funkcije nad dokumenti;
- portal.

Na sliki 10 je prikazana arhitektura sistema eHramba.si.



Slika 10: Arhitektura sistema eHramba.si

## 5.4. Podsystem za hranjenje podatkov

Dokument, ki je vložen v e-hrambo, je sestavljen iz več delov:

- Prvi del je vsebina dokumenta.
- Drug del je revizijska sled dokumenta (podpisi dokumenta, časovni žigi).
- Tretji del so opisni podatki dokumenta, ki so pa ločene od vsebine.

Podatki dokumenta se shranjujejo v tri podsisteme:

- podsistem za hranjenje opisnih podatkov;
- podsistem za hranjenje vsebine dokumentov (datoteke);
- podsistem za hranjenje revizijske sledi dokumentov.

### 5.4.1. Podsystem za hranjenje opisnih podatkov

V opisnih podatkih lahko določimo kdo je dokument izdelal, kje, kdaj, kdaj je bil vnesen v arhiv, kakšen je tip dokumenta, itd. S tem modulom je bilo doseženo, da lahko sistem omogoča iskanje

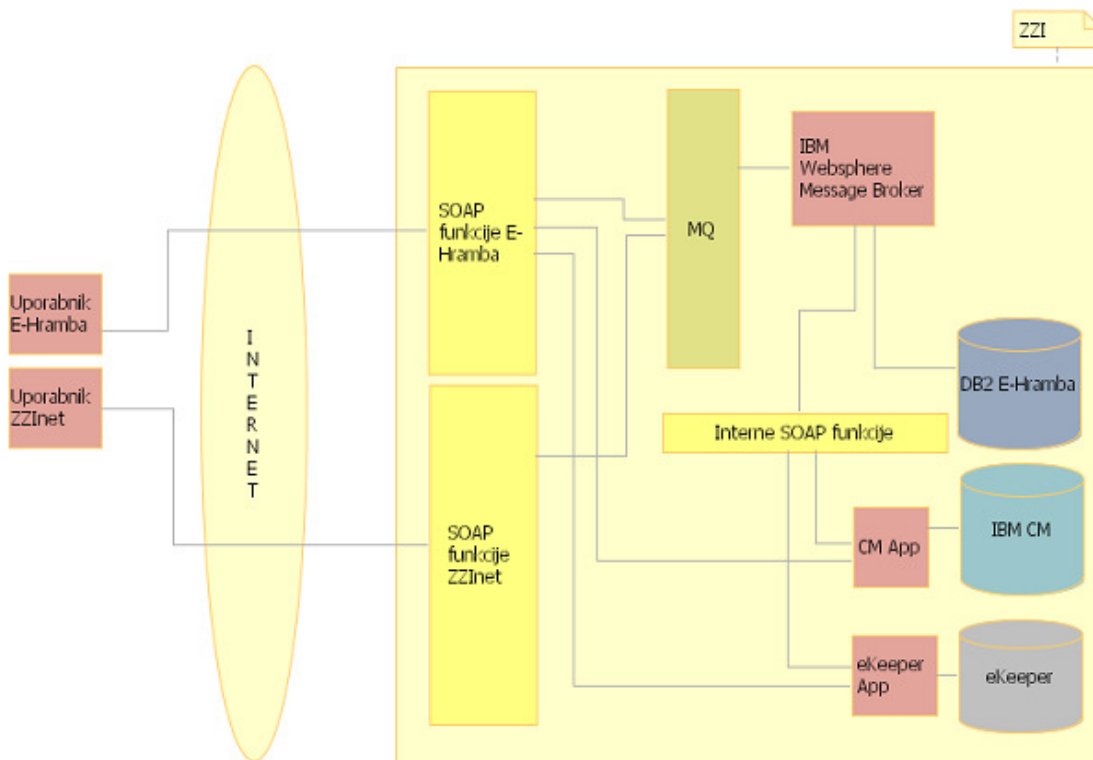
dokumentov po opisnih podatkih. Opisni podatki se zapisujejo v tabele relacijske baze podatkov IBM DB2

#### 5.4.2. Podsystem za hranjenje vsebine dokumentov

Podsystem za shranjevanje vsebin temelji na orodju IBM Content Manager. To zagotavlja sistemu e-hrambe razširljivost in zanesljivost hrambe. System je zasnovan tako, da je uporabnik neodvisen od količine dokumentov in načina hrambe.

#### 5.4.3. Podsystem za hranjenje revizijskih sledi

Za podsystem za zagotavljanje revizijske varnosti se uporablja rešitev eKeeper podjetja SETCCE. Rešitev je registrirana in zagotavlja vso potrebno funkcionalnost. Podatki za zagotavljanje revizijske sledi dokumentov se shranjuje v sistem eKeeper



Slika 11: Struktura sistema eHramba.si - aplikativni model

## 5.5. Podsystem za funkcije nad dokumenti

IBM Websphere Message Broker je okolje, s katerim rešujemo vnos dokumenta v podsisteme. Zagotavlja robustnost in sigurnost sistema. Broker zajema podatke iz sporočilnih vrst IBM MQ in jih razporeja v podsisteme. V Message Broker-ju se izvajajo vse funkcije, ki posegajo v vsebino dokumentov, kot so vnos dokumenta v podsisteme in brisanje dokumenta iz arhiva.

### 5.5.1. Vnos dokumenta

Za uspešen vnos dokumenta v sistem je potreben vnos dokumenta v vse podsisteme. Tako si funkcije pri toku dokumenta skozi Broker sledijo:

- Pridobitev interne identifikacije dokumenta v sistemu
- Vnos lastnosti dokumenta v relacijsko bazo
- Glede na klasifikacijo dokumenta ugotovimo politiko hranjenja. Politika hranjenja nam omogoča, da določimo:
  - Čas hranjenja
  - Ali se dokument hrani kot revizijsko varen elektronski dokument
  - Ali shranjujemo tudi vsebino dokumenta

Glede na zgornje ugotovitve krmilimo dokument v podsisteme. Če shranjujemo vsebino dokumenta, vstavimo vsebino (datoteko) v sistem IBM CM, ki nam vrne interno identifikacijo dokumenta v sistem IBM CM. Uspešnost vnosa beležimo v relacijski bazi. Če shranjujemo revizijsko sled dokumenta, vstavimo dokument v eKeeper, ki nam vrne interno identifikacijo eKeeper-ja. Uspešnost vnosa beležimo v relacijski bazi.

### 5.5.2. Brisanje dokumenta

#### Brisanje dokumenta po pretečenem roku hranjenja

Vsaka politika hranjenja ima določen rok hranjenja dokumenta. Ima tudi določeno, ali naj se brisanje dokumenta izvaja avtomatsko po pretečenem roku, ali naj se samo spremeni status dokumenta na "pretečen rok trajanja". Če je označeno, da naj se po pretečenem roku dokumenti brišejo, jih zajame obdelava "Avtomatsko brisanje pretečenih dokumentov". Obdelava se izvaja vsako noč in "počisti" arhiv starih – pretečenih dokumentov. Obdelava pripravi zahteve za brisanje dokumentov, ki jih pa potem izvaja Message Broker.

Broker izvaja brisanje dokumenta po vrstnem redu:

- Preveri, če je dokument res primeren za brisanje
- Izbriše sled dokumenta iz sistema eKeeper
- Izbriše vsebino dokumenta iz sistema IBM CM
- V primeru, da se vse prejšnje operacije pravilno izvedejo, izbriše tudi opisne podatke iz relacijske baze.

Funkcija brisanja dokumenta je asinhrona funkcija. Asinhrono funkcije podajo sistemu zahtevo ter ne počakajo na rezultat. Brisanje izvede Message Broker, ko prebere zahtevo iz svoje sporočilne vrste.

### **Ročno brisanje dokumenta**

Dokument lahko pobrišemo iz sistema tudi ročno. To lahko izvede oseba, ki ima za to pooblastila. Funkcija brisanja dokumenta pripravi zahtevek za brisanje dokumenta in ga po sporočilni vrsti preda Message Brokerju. Broker briše dokumente enako kot pri brisanju z avtomatsko obdelavo.

### **Ostale funkcije nad dokumentom**

Ostale funkcije nad dokumentom se izvajajo sinhrono. To pomeni, da funkcija SOAP sinhrono izvede zahtevo v podsistem in čaka rezultat. Te funkcije ne spreminjajo vsebine arhiva in so zato manj kritične za stabilnost sistema. Seznam ostalih funkcij je opisan v poglavju 5.7. Funkcije SOAP.

## **5.6. Asinhrona obdelava**

Struktura sistema E-Hramba.si je zasnovana tako, da zagotavlja visoko stopnjo zanesljivosti in razpoložljivosti sistema, tudi pri sočasni uporabi večjega števila uporabnikov. V sistem eHramba.si je vgrajen asinhronski sistem sporočilnih vrst (IBM WebSphere MQ), kar omogoča zanesljiv vnos dokumentov v podsisteme. Tudi v primeru odpovedi katerega od podsistemov se dokument ne izgubi, temveč počaka v vrsti do ponovne vzpostavitve podsistema, ko se postopek vnašanja nadaljuje.

Sistem je zasnovan na osnovi dokumentov XML. Tako lahko vsako poizvedbo oz. akcijo opišemo v dokumentu XML. Osnovni funkciji, ki ju je potrebno implementirati v poslovni sistem sta `setDocument` in `getDocument`. To sta funkciji za vlaganje dokumenta in pregled dokumenta. Pri vlaganju dokumenta dobi dokument enolično šifro `DocID`. To je številka, ki jo dodeli sistem eHramba.si.

## 5.7. Funkcije SOAP

Spletne funkcije storitve eHramba.si, so preko različnih protokolov dostopne uporabnikom preko spleta.

Seznam nekaterih funkcij SOAP:

Funkcija	Povratna vrednost	Opis
setDocument( java.lang.String guid, java.lang.String accountName, java.lang.String clasificationName, java.lang.String archiveDataXML, boolean compressed)	int	Funkcija sprejema dokument XML, s katerim dodajamo dokument v sistem. Dokument vsebuje tako vse metapodatke, kot tudi samo vsebino dokumenta.  Funkcija je sinhrona.
getDocument( java.lang.String guid, int docID, boolean compressed)	java.lang.String	Funkcija vrača dokument XML, v katerem so vsi podatki o izbranem dokumentu. Funkcija lahko vrača kompresiran dokument v zip formatu. V dokumentu so tako metapodatki dokumenta, kot tudi sam dokument.  Funkcija je sinhrona.
getDocumentMetaData( java.lang.String guid, int docID)	java.lang.String	Funkcija vrača dokument XML, v katerem so vsi podatki o izbranem dokumentu. Funkcija ne vrača vsebine dokumenta, ampak samo lastnosti dokumenta.  Funkcija je sinhrona.
deleteDocument( java.lang.String guid, int docID)	void	Funkcija omogoča brisanje dokumenta. Za parameter uporablja interno številko dokumenta.  Funkcija je asinhrona.
archive( java.lang.String guid, java.lang.String accountName, java.lang.String classificationName, si.zzi.ws.Itap.ArchiveData archiveData)	int	Omogoča vlaganje dokumenta preko strukture in ne preko xml. Funkcionalno je funkcija enaka setDocument. Funkcija vrne interno številko dokumenta.  Funkcija je asinhrona.

Slika 12: Seznam funkcij SOAP storitve eHramba.si

Ostale funkcije SOAP so: exportDocument, getAccounts, getActions, getActionsGroups, getClassifications, getClassificationsGroups, getDocumentRawData, getDocuments, getDocumentStatus, getFirms, getGroups, getGroupsUsers, getMyActions, getMyClassifications, getMyFunByClassification, getPolicies, getTransaction, getUsers, isUserSessionAvailable, login, logout, setAccount, setActionGroup, setClassification, setClassificationGroup, setFirm, setGroup, setGroupUser, setTransaction, setUser, verifyDocument, verifyDocument,

## **5.8. Ostali sistemi**

### **5.8.1. Sistem pooblastil**

Sistem pooblastil zagotavlja kontroliran dostop do funkcij arhiva. Podjetja imajo v sistemu odprte predale. Za vsak predal je mogoče nastaviti, katera skupina uporabnikov v podjetju lahko izvaja katere funkcije. Definira se lahko tudi pooblastila glede na klasifikacijo dokumenta.

### **5.8.2. Sistem za razvrščanje dokumentov**

Klasifikacijski sistem za dokumente je sistem razvrščanja dokumentov. Vsak dokument mora biti razvrščen v klasifikacijski načrt. Vsaka klasifikacija ima določeno tudi politiko hranjenja. Politika hranjenja nam omogoča nastavitve v sistemu, kot so:

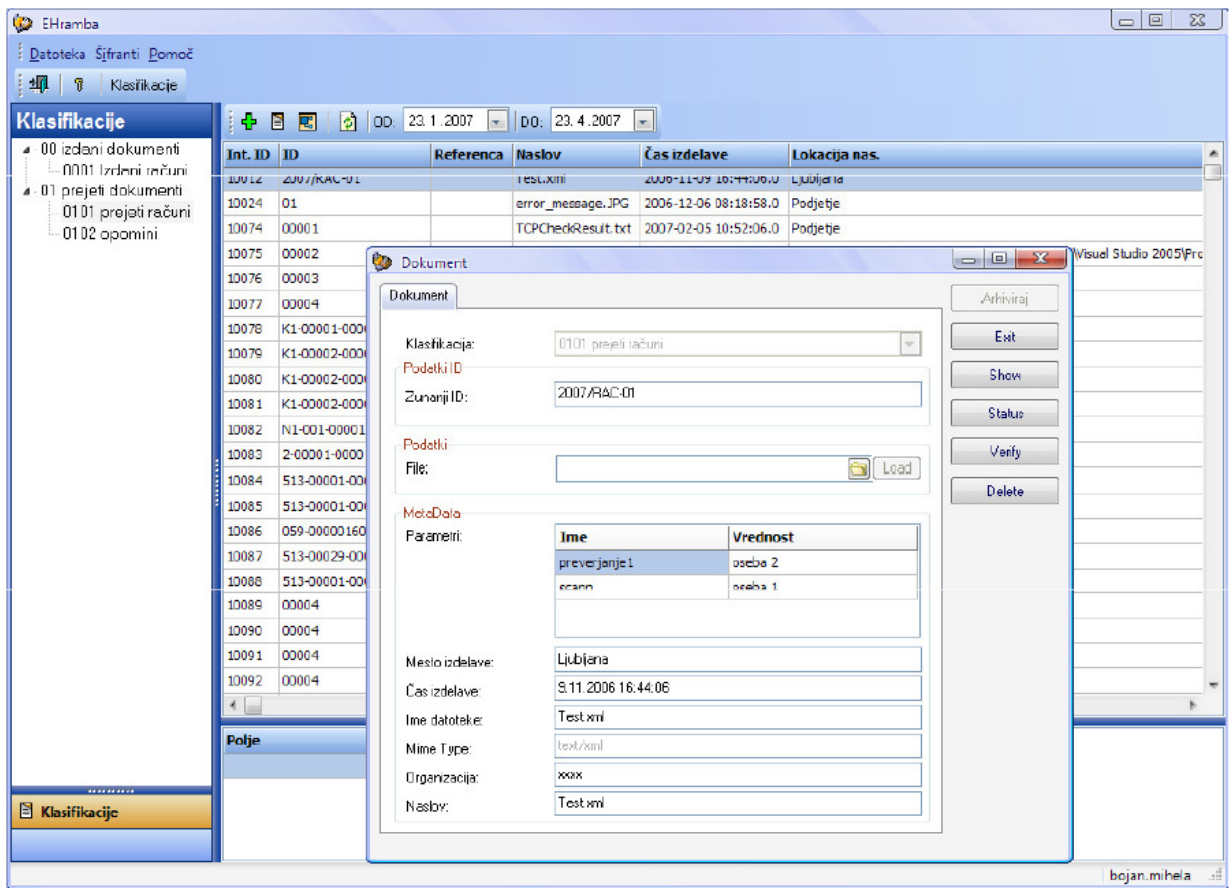
- Čas hrambe
- Ali želimo shranjevati vsebino dokumenta
- Ali želimo shranjevati revizijsko sled
- Ali želimo po predvidenem času hrambe avtomatsko brisanje dokumenta, ali pa samo označitev dokumenta z statusom “pretečen čas hrambe”

## **5.9. Uporabniški vmesnik**

Tehnološka zasnova storitve eHramba.si ponuja uporabnikom različne možnosti dostopa do spletnih funkcij. Do hranjenega gradiva je mogoče dostopati iz obstoječih poslovnih aplikacij (Navision, Datalab Pantheon, SAP...) ali pa preko spletnega brskalnika. Uporaba spletnega brskalnika omogoča dostop do arhiva s katerekoli lokacije. Spletne funkcije pa omogočajo integracijo z obstoječimi aplikacijami.

### **5.9.1. Portal**

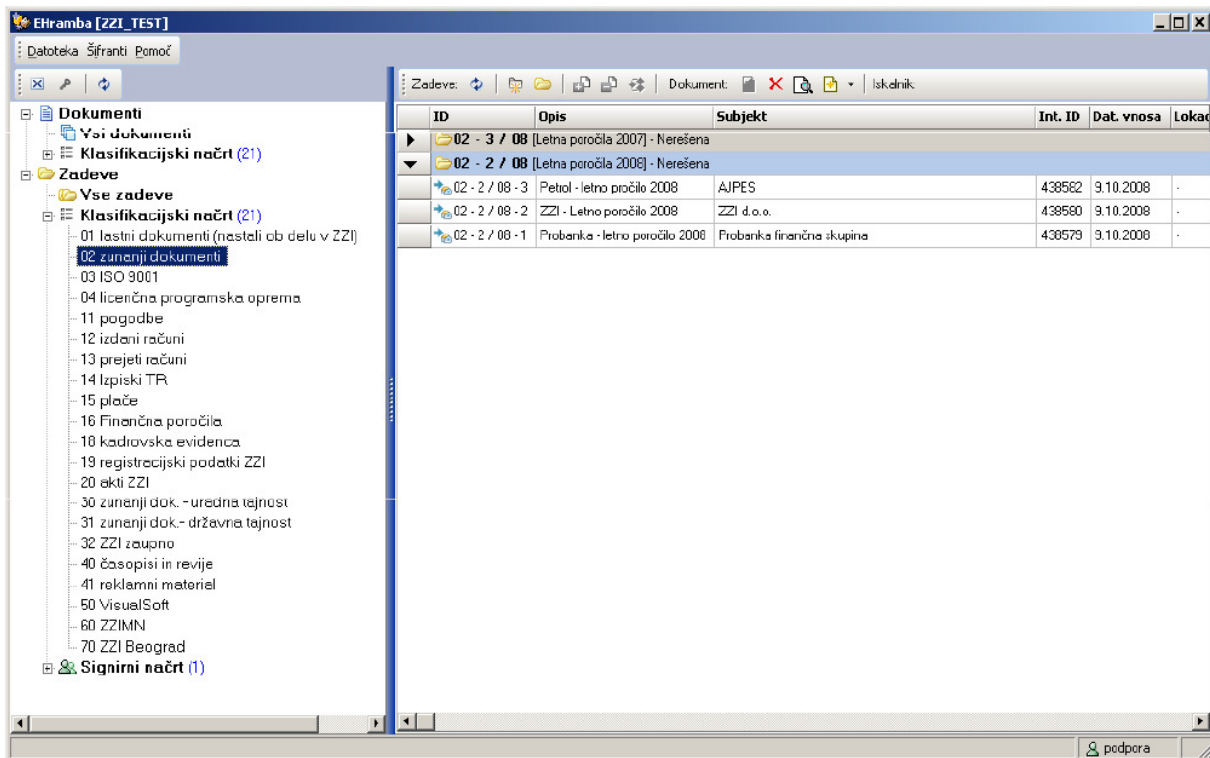
Uporabniški vmesnik, ki je razvit za spletno portalsko okolje, dostopa do spletnih storitev preko vmesnika SOAP. Portalski vmesnik omogoča vpogled v arhiv s katerekoli lokacije preko kateregakoli brskalnika. V portal so implementirane vse funkcije storitve eHramba.si. Na sliki 13 je prikazan pogled v uporabniški vmesnik razvit za portalsko okolje.



Slika 13: Uporabniški vmesnik sistema eHramba.si - portal

### 5.9.2. Odjemalec

Uporabniški vmesnik, ki je razvit v okolju Borland Delphi 7.0, dostopa do storitve preko vmesnika SOAP. Omogoča uporabo vseh spletnih funkcij storitve eHramba.si, hkrati pa služi kot prototip za razvijalce oziroma vpeljevalce storitve eHramba.si. Na sliki 14 je prikazan pogled v uporabniški vmesnik razvit v okolju Borland Delphi 7.0.



Slika 14: Uporabniški vmesnik sistema eHramba.si - aplikacija

### 5.9.3. Ostali uporabniški vmesniki

Storitev eHramba.si je zasnovana tako, da je uporaba storitev neodvisna od uporabniškega vmesnika. Spletne storitve omogočajo neodvisnost posameznih delov aplikacije in posledično tudi razvoj aplikacij. Uporabniški vmesnik lahko predstavlja tudi obstoječ poslovni informacijski sistem podjetja (npr. SAP, Navision, Pantheon...), če ta sistem podpira uporabo (oz. aktiviranje, klicanje) spletnih funkcij storitve eHramba.si. Vpeljava storitve eHramba.si v podjetje je v tem primeru osredotočena (usmerjena) le na vsebinska vprašanja, brez obremenjevanja vpeljevalcev s tehničnimi problemi.

## 5.10. Povezljivost (integracija) sistema z obstoječimi informacijskimi sistemi

Storitev je prilagojena uporabi v okoljih SOA in združljiva s poslovnimi okolji uporabnikov. Uporabniške vmesnike obstoječih informacijskih sistemov se le dopolni z novimi funkcijami. Način dela ostane nespremenjen, obstoječ informacijski sistem pa pridobi novo funkcionalnost brez uvedbe novih rešitev.

## 6. Sklepne ugotovitve

S tem diplomskim delom smo se sprehodili od teoretične podlage za snovanje zakonsko skladnega elektronskega arhiva do praktičnega primera eHramba.si, ki se danes uporablja na trgu.

Storitev eHramba.si je v uporabi od maja 2008. Storitev uporablja 20 podjetij s skupaj 150 uporabniki. Povprečni vnos dokumentov vseh podjetij v sistem se giblje okoli vrednosti 10.000 vnosov na leto. Podjetje z največ vnosi pa sega do številke 300.000 vnosov na leto. Povprečen dokument, ki je nastal v elektronski obliki zasede 50 kilobajtov, največji pa dosežejo od 2 do 3 megabajte. Povprečen skeniran dokument je velik okoli 500 kilobajtov, največji pa dosežejo tudi do 30 megabajtov.

Dobra izkušnja snovalcev sistema je ta, da je bila elektronska hramba dokumentov ponujena kot storitev in ne rešitev. Ker pomeni, da namesto, da bi imeli posamezne elektronske hrambe razpršene okoli po strankah, imajo v celotno okolje vpogled in dostop od doma. To omogoča lažjo podporo uporabnikom in hitrejšo odpravo morebitnih napak.

Težave sistema izvirajo iz velike odgovornosti in striktne varnosti. Za vzpostavitev varnega okolja hrambe je bilo potrebno vložiti veliko dela. Varnost in odgovornost za hranjene dokumente potrebujejo neprestan nadzor in vlaganje v razvoj sistema.

Z neprestanim razvojem tehnologij tako v računalništvu kot ostalih panogah, bo potrebno vedno in pravočasno uvajati nove načine in pristope za zagotavljanje varnosti in ohranjanje dokumentov.

## 7. Viri

- [1] Problematika in možne rešitve arhiviranja elektronskih dokumentov. Zadnji dostop: 5. marec 2010. Dostopno na: [http://ibmi.mf.uni-lj.si/~jure/pred\\_bib/i2/seminarji01/problematika-e-arhiviranja.pdf](http://ibmi.mf.uni-lj.si/~jure/pred_bib/i2/seminarji01/problematika-e-arhiviranja.pdf)
- [2] Primož Berger, Vloga elektronskega arhiva v sodobnem podjetju. Zadnji dostop: 5. marec 2010. Dostopno na: [http://www.cek.ef.uni-lj.si/u\\_diplome/berger1796.pdf](http://www.cek.ef.uni-lj.si/u_diplome/berger1796.pdf)
- [3] Uradni list Republike Slovenije. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). Zadnji dostop: 5. marec 2010. Dostopno na: <http://www.uradni-list.si/1/objava.jsp?urlid=200630&stevilka=1229>
- [4] SETCCE, Tehnično priporočilo za varno elektronsko arhiviranje. Zadnji dostop: 5. marec 2010. Dostopno na: [http://www.gzs.si/e-poslovanje/dokumentacija/eSLOG-Elektronski\\_arhiv\\_0.99%28v\\_pripravi%29.pdf](http://www.gzs.si/e-poslovanje/dokumentacija/eSLOG-Elektronski_arhiv_0.99%28v_pripravi%29.pdf)
- [5] Arhiv Republike Slovenije, Enotne tehnološke zahteve. Zadnji dostop: 5. marec 2010. Dostopno na: <http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/E-ARHIVI/obrazci/ETZ.pdf>
- [6] Šalej Andrej, *Vzpostavitev sistema za varovanje in zaščito informacij*. DOK\_SIS 2004 Ljubljana: Media.doc, 2004, str. VI-17 - VI-23
- [7] Matjaž B. Jurič, Storitvena arhitektura - zgolj kompozicija spletnih storitev? Zadnji dostop: 5. marec 2010. Dostopno na: [http://lisa.uni-mb.si/~juric/SOA\\_ss.pdf](http://lisa.uni-mb.si/~juric/SOA_ss.pdf)
- [8] Service-oriented architecture - Wikipedia, the free encyclopedia. Zadnji dostop: 5. marec 2010. Dostopno na: [http://en.wikipedia.org/wiki/Service-oriented\\_architecture](http://en.wikipedia.org/wiki/Service-oriented_architecture)
- [9] Andrew S. Tanenbaum, Maarten van Steen, *Distributed systems principles and paradigms*, Upper Saddle River, New Jersey : Prentice Hall, cop. 2002, pogl. 1.
- [10] Evidence Record Syntax. Zadnji dostop: 5. marec 2010. Dostopno na: <http://www.ietf.org/rfc/rfc4998.txt>
- [11] SETCCE eKeeper, Varen elektronski arhiv. Zadnji dostop: 5. marec 2010. Dostopno na: [http://www.setcce.si/images/download/ekeeper\\_brochure\\_slo.pdf](http://www.setcce.si/images/download/ekeeper_brochure_slo.pdf)
- [12] POŠTA®CA. Zadnji dostop: 5. marec 2010. Dostopno na: <http://postarca.posta.si/>
- [13] IBM Content Manager, Vodič za hiter začetek. Zadnji dostop: 5. marec 2010. Dostopno na: <http://www-01.ibm.com/support/docview.wss?uid=swg27016540&aid=41>
- [14] SOAP - Wikipedia, the free encyclopedia. Zadnji dostop: 5. marec 2010. Dostopno na: <http://en.wikipedia.org/wiki/SOAP>

[15] SOAP Basics 3 : SOAP Messages. Zadnji dostop: 5. marec 2010. Dostopno na: <http://www.soapuser.com/basics3.html>

[16] Interno gradivo, projekt eHramba.si - ZZI d.o.o.