# Delta arhitektuur

|  |  |  |  |
| --- | --- | --- | --- |
| **Versioon** | **Muutja** | **Muutmise kuupäev** | **Muudatus** |
| 1.0 | Erko Hansar | 22.04.2010 | Täisversioon |

## Sissejuhatus

Käesolev dokument kirjeldab Delta dokumendihaldussüsteemi tehnilist arhitektuuri.

### Dokumendi sihtrühm

Dokument on mõeldud kasutamiseks kirjeldatava dokumendihaldussüsteemi arendamise, paigaldamise ja haldamisega kokkupuutuvatele tehnilise valdkonna inimestele.

### Kasutatud mõisted ja lühendid

DHS – Dokumendihaldussüsteem

Java EE – Java Enterprise Edition platvorm

WAR – Java web archive failiformaat

SVN – Subersion koodirepositoorium

SMTP - Simple Mail Transfer Protocol

IMAP - Internet Message Access Protocol

NTLM - Microsoft authentication protocol

### Viited

RITKR2 – Riigi IT koosvõime raamistik, versioon 2.0 http://www.riso.ee/et/koosvoime/raamistik2\_0.pdf

RITA – Riigi IT arhitektuur http://www.riso.ee/et/koosvoime/RITA1\_01.pdf

IYA2013 – Eesti infoühiskonna arengukava 2013 http://www.riso.ee/et/files/Infoyhiskonna\_arengukava\_2013.pdf

## Süsteemi kontseptuaalne arhitektuur

### Arhitektuurselt olulised nõuded

Arhitektuurilisi valikuid tehes on esmajärjekorras silmas peetud vajadust rahuldada kliendi püstitatud mittefunktsionaalsed nõuded nii, et oleks loodud võimalikult optimaalne platvorm, kuhu peale arendada infosüsteem, mis täidab kliendi funktsionaalsed nõuded ja tagab hilisema mugava halduse ja laiendatavuse.

Arvesse on võetud riigi koostöövõime ja tarkvaraarhitektuuri soovitusi ning pakutud lahendus põhineb maailmas levinud dokumendihalduslahenduste ja Java veebirakenduste arendamise headel tavadel. Valitud teegid ja vahendid on küpsed ning laialt kasutatavad ja uusi vahendeid ega tehnoloogiad projekti käigus katsetama ei hakata.

Prioriteedid:

• Kasutatavus

• Turvalisus

• Käideldavus

• Muudetavus

• Süsteemi kasutatakse läbi veebilehitsejate Microsoft Internet Explorer versioon 7 ja kõrgem ja Mozilla Firefox versioon 3.0 ja kõrgem.

• Süsteemi kasutamine funktsionaalsetes nõuetes kirjeldatud ulatuses ei tohi vajada kasutaja arvutisse eritarkvara paigaldamist.

• Süsteem peab paigalduma kolmekihilisse (andmesalvestuskiht, loogikakiht, esitluskiht) turvaarhitektuuuri kus kihid on omavahel eraldatud tulemüüridega.

o Esitluskiht mida esitatakse kasutaja arvutis peab võtma loogikakihiga ühendust HTTPS protokolli kasutades. Krüpteeritud HTTP päringud võtab vastu turvaserver ning edastab need tavaliste HTTP päringutena loogikakihi rakendusserverile.

o Tarkvaralahendus peab suutma tuvastada kasutajat turvaserveri poolt HTTP päringu päisesse lisatud autentimisinfo alusel.

• Lisaks kasutajatele peab teenindama loogikakiht ka välisveebi päringuid ning võtma vastu dokumendihaldusesse suunatud e-posti.

• Süsteemi andmesalvestuskiht peab dokumentide info säilitamiseks kasutama jagatud salvestusseadet (Storage Area Network).

• Süsteem peab võtma organisatsiooni struktuuri ning kasutajate info Active Directoryst.

• Süsteem peab riikliku dokumendivahetuskeskusega suhtluseks kasutama X-tee turvaserverit.

• ID-kaardi sertifikaatide kehtivuse kontrollimiseks peab süsteem kasutatama Sertifitseerimiskeskuse kehtivuskontrolli teenust.

• Süsteem peab võimaldama tagada kõrget käideldavust (99,9%) aktiivsete õlgadega või automaatse tõrkesiirdega klastrit kasutades.

• Süsteemi regulaarsed haldusprotseduurid (s.h. varundamine) ei tohi vajada süsteemi töö seiskamist.

• Süsteem peab võimaldama varukoopiast ajahetkeni (point in time) taastamist.

• Süsteem peab väljastama tarkvaralahenduses vigade tuvastamiseks vajalikus ulatuses logi.

• Funktsionaalsete nõuete realiseerimisel tuleb kasutada lahenduse arendusplatvormi tehnoloogiaid, vahendeid, arhitektuuri ja arendustavasid (s.h. nõudeid koodi vormistamisele).

• Realiseeritud lisafunktsionaalsused peavad olema piiranguteta kasutatavad teistes avaliku halduse asutustes.

• Lisafunktsionaalsuste realiseerimiseks peab olema moodulsüsteem mis võimaldab arendada eraldiseisvaid funktsionaalsusi üksteisest sõltumatult.

o Lisafunktsionaalsuste arendamiseks ette nähtud programmaatilised liidesed peavad olema piisavalt dokumenteeritud jätkuarenduste teostamiseks kolmandate osapoolte poolt.

o Vastav dokumentatsioon peab olema inglise keeles, et tagada rahvusvaheline konkurents.

• Süsteem peab töötama eesti lokaadiga.

• Dokumentide digiallkirjastamine peab toimuma veebibrauserist ning platvormist sõltumatuna. (IYA2013)

• Kasutajaliidese Eesti keelde tõlkimine peab olema realiseeritud eraldiseisvate tõlkeressurssidega (näiteks tõlkefailidena).

• Rakenduste serveripoolne kood peab töötama JVM 6.0 ja kõrgemates keskkondades.

• Rakendused peavad töötama PostgreSQL 8.4+ andmebaasiplatvormil.

• Rakendused töötavad Tomcat 6+ rakendusserverites.

• Rakenduste poolt kasutatavaid infrastruktuuriteenuseid peab olema võimalik hallata rakenduseväliste, soovituslikult JMXi vahenditega.

• Rakendust peab olema võimalik monitoorida väliste, soovituslikult JMX vahenditega. Jälgitavad peavad olema vähemalt järgnevad ressursid rakendusserveri tasemel: Mälukasutus, JVM heapi kasutus, CPU kasutus, Võrgu I/O, Ketta I/O, Lõimed, Andmebaasiühendused, HTTPSessioonid, JMS Queued ja Topicud, Andmebaasiserveri tasemel, Päringud, Andmemaht.

### Süsteemi dekompositsioon

DHS rakendus põhineb Alfresco Community Edition 3.2 vabavaralisel dokumendihalduse süsteemil ja kõik arhitektuurilised kihid ja komponendid pärinevad Alfresco arhitektuurist. Dokumendihalduse funktsionaalsete nõuete täitmiseks, rakenduse juurutamiseks ja liidestamiseks teiste infosüsteemidega on tehtud hulganisti täiendusi Alfresco rakenduse teenuskihis ja Alfresco Explorer kasutajaliidese kihis.

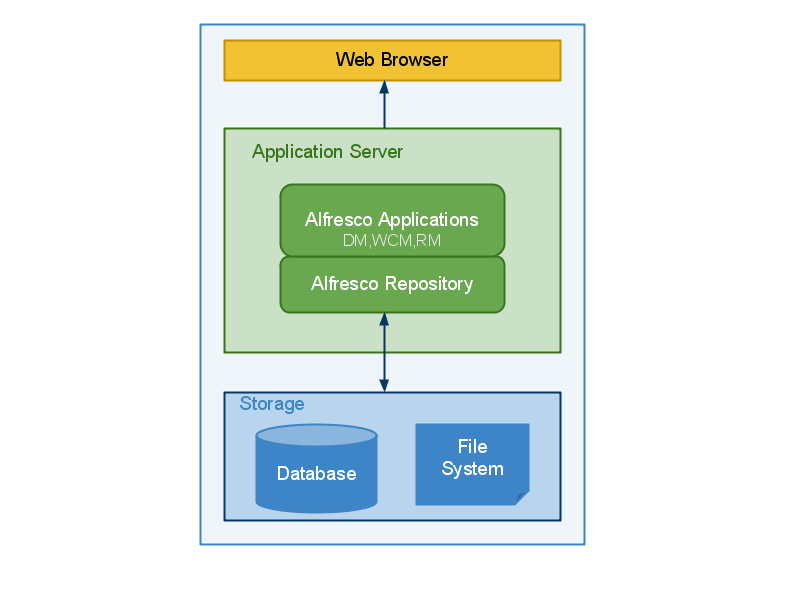
Rakenduse kihid:

• Andmekiht – Andmed ja failid

• Teenuskiht – Andmekihiga suhtlus, äriloogika, teenuste liidesed

• Kasutajaliidese kiht – Kasutaja sisendi töötlemine ja väljundi kuvamine, suhtlemine teenuskihiga

• Veebibrauser kasutaja arvutis – Suhtleb üle turvaprotokolli DHS rakenduse kasutajaliidese kihiga



### Arhitektuurselt olulised mehhanismid

• Autentimine – Kirjeldatud peatükis „3.8 Turvalisuse vaade“

• Autoriseerimine – Kirjeldatud peatükis „3.8 Turvalisuse vaade“. Ärikihi teenuste autoriseerimine seadistatakse aspektidega.

• Logimine – Kasutatakse Apache Log4j teeki. Logimise tasemed on seadistatavad. Toodangukeskkonnas on üldised tasemed seadistatud INFO või WARN peale, vajadusel saab funktsionaalsuse kaudu seadistada täpsemaid tasemeid.

• Transaktsioonid – Ärikihi teenuste transaktsioonid töötavad aspektidena ja seadistatakse teenuste seadistusfailides.

• Veahaldus – Kõik tehnilised veaolukorrad logitakse ja lisaks kuvatakse kasutajale veateadet. Tehnilised vead peavad eelistatult olema unchecked exceptionid. Vajadusel võib sisuliste eriolukordade jaoks kasutada checked exceptioneid.

• Klasterdamine – Kasutatavad komponendid on kergekaalulised ja ise klasterdamise tehnoloogiad ei sisalda. Klasterdamine on toetatud rakendusserveri tasemel.

• Taustatööd (job-id) – Seadistatakse jooksma DHS veebirakendusega samasse Spring application context-i (paigaldub rakendusserveri sisse ühisesse JVM-i).

• Versioneerimine – Lähtekood ja seadistusfailid paigaldatakse Subversion (SVN) koodirepositooriumisse.

### Arhitektuurimustrite kasutamine

DHS lahendus põhineb Alfresco dokumendihaldusplatvormil ja seega kasutab samu mustreid, mida Alfresco. Realiseeritud lisafunktsionaalsuste realiseerimisel tuleb lähtuda Alfresco platvormist ja kasutada üldlevinud tavasid. Konkreetseid arhitektuurimustreid ette määratud ei ole.

## Süsteemi tehniline arhitektuur

Kuna DHS rakendus põhineb Alfresco olemasoleval tooteplatvormil, siis põhifunktsionaalsuse osas ei tulnud arhitektuurilisi otsuseid ja valikuid teha. Teiste süsteemidega liidestamisel tehtud valikud on tingitud nende süsteemide pakutavatest liidesest (näiteks X-tee, SOAP jne.) ja valikuid samuti teha vaja ei olnud.

### Kasutuslugude realisatsioonivaade

Kasutuslood on lahti kirjutatud kasutuslugude ja spetsifikatsioonide dokumentides.

### Loogiline vaade

DHS rakenduse kogu funktsionaalsus:

• Dokumendi metaandmete ja failide haldus

• Täistekstiotsing

• Registreerimine

• Töövood

• Allkirjastamine

• Administreerimisvaated (kontaktid, kasutajad, klassifikaatorid, parameetrid, registrid, mallid, dokumendi liigid, teavitused, ...)

• Liidestused (Active Directory, e-post, DVK, dokumentide avalikustamine ADR kaudu)

• ...

asub põhimoodulis, on ülesse ehitatud ühtse arhitektuuri peale ja töötab samas JVM-is ning suhtleb omavahel lokaalväljakutsetega.

### Tehnoloogiate vaade

Kõik kasutatud komponendid ja tehnoloogiad on vabavaralised ning ei sõltu kasutatavast operatsioonisüsteemist, võimaldades toodangukeskkonna loomisel paindlikku füüsilist infrastruktuuri. Platvorm võimaldab keskenduda maksimaalselt loodava lisafunktsionaalsuse realiseerimisele ning jättes infrastruktuursed operatsioonid kasutatava alustarkvara hoolde.

• Java SE – Java Standard Edition, konkreetses käsitluses Java virtuaalmasin. DHS lahenduses kasutatakse Sun JDK 6 viimast stabiilset parandustepakki.

• Java EE – Java Enterprise Edition, spetsifikatsioon Java ärirakenduste realiseerimiseks. DHS rakendus on ühilduv Java EE 5.0 spetsifikatsiooniga.

• Tomcat – Vabavaraline Java EE rakendusserver. Rakenduses kasutatakse Tomcat v6.0 stabiilset versiooni.

• PostgreSQL – Kasutatav relatsiooniline andmebaas haldusandmestiku ning dokumendi metadata tarbeks. Rakenduses kasutatakse Postgres 8.4 või uuemat viimast stabiilset versiooni.

• Alfresco – Lahendusse integreeritud dokumendihaldustarkvara. Vahendisse sisse ehitatud funktsionaalsust kasutatakse dokumentide registreerimisel, versioneerimisel, arhiveerimisel, autoriseerimisreeglite rakendamisel ning töövoogude loomisel. Lahenduses kasutatakse Alfresco Community 3.2 versiooni.

• Spring Framework – IoC konteiner ja AOP raamistik. Java EE maailmas tänapäeval de facto standard ärirakenduste loomisel.

• Spring Security – Teek autentimiseks ja autoriseerimiseks.

• MyFaces JSF – Alfresco Explorer kasutajaliidese kiht põhineb MyFaces JSF veebiraamistikul. Vaated on realiseeritud JSP lehtedena.

• Lucene – Täisteksti indeksid otsingute jaoks.

• Hibernate – ORM raamistik andmekihi ja teenuskihi vahel andmete teisendamiseks.

• Ant, SVN, JUnit, JMeter – Töövahendid projekti kasutajaliidese testimiseks, käideldavusnõuete kontrollimiseks ja sujuva arendusprotsessi tagamiseks.

### Liidestusvaade

Süsteemi välised seosed on toodud järgneval diagrammil:



ADR - Väliseveebi avalike dokumentide register. Dokumentide pärimiseks on DHS-il SOAP veebiteenuse liides

DVK – Dokumendivahetuskeskuse liidestus üle X-tee.

Active Directory– Liidestus kasutajate info saamiseks.

E-posti server – Liidestus üle SMTP.

### Levitusvaade

Komponentide topoloogia (kuidas komponendid paiknevad füüsiliselt/virtuaalselt, st millisel riistvaral/virtuaalmasinates), kasutuselevõtmise ja paigaldamise esialgsed põhimõtted on kirjeldatud eraldi paigaldusskeemi dokumendis.

### Realiseerimise vaade

DHS rakenduse realisatsiooni tulem on kokkuehitatud dhs.war fail - Java WAR formaadis pakend. See pakend sisaldav tervet rakendust ja paigaldatakse koos seadistusfailiga Java rakendusserverisse. Eraldi komponentideks on cas.war ja adr.war.

### Andmevaade

DHS rakendus talletab andmeid järgmiste kogumitena:

• Andmebaas – Dokumentide metaandmestik, rakenduse ja kasutajate andmed ning töövoogude seisundid salvestatakse Alfresco puustruktuuriga repositooriumisse, mis salvestab andmed relatsioonilisse andmebaasi PostgreSQL. Andmebaas on levitusskeemi järgi kõikidel klastri serveritel ühine.

• Failid – Dokumentide failid salvestatakse failisüsteemi jagatud salvestusseadmele, mis on kõikidel klastri serveritel ühine.

• Indeksid – Otsingu jaoks genereeritavad Lucene indeksid kirjutatakse failisüsteemi iga rakendusserveri kohalikule kettale eraldi.

### Turvalisuse vaade

DHS rakenduse turvalisus põhineb esmalt välisel turvaserveril ja CAS single sign-on autentimiskihil. DHS veebiliideses autentimiseks kasutatakse turvaserveri poolt rakendusele edastatava HTTP päringu päisesse lisatavat autentimismärki.

Kasutajategevuste autoriseerimiseks kasutatakse Alfresco arendusplatvormi siseseid võimalusi.

• Autentimata kasutajal ligipääs süsteemile puudub.

• Kasutajakonto tekib automaatselt kõikidele Active Directory’s olemasolevatele kasutajatele (luuakse konto ja lisatakse töötajate gruppi) kui nad esmakordselt sisse logivad või kui toimub kasutajate perioodiline sünkroniseerimine üks kord ööpäevas.

• Õiguste määramine toimub rollipõhiselt: Administraator, Dokumendihaldur, Tavakasutaja

• Sarjade tasemel on võimalik seadistada eraldi ligipääsuõiguseid failide lugemiseks kasutajate ja gruppide lõikes.

• Lisaks on veel erireegleid rakenduse teatud funktsionaalsuste juures, kus dokumendi omanikustaatus või töövoo vastutava täitja staatus annab kasutajale eriõiguseid. Kõik sellised eritingimused on kirjeldatud vastavate funktsionaalsuste spetsifikatsioonides ja põhinevad tehniliselt Alfresco õigustesüsteemil.