# Delta paigaldusjuhend

|  |  |  |  |
| --- | --- | --- | --- |
| **Versioon** | **Muutja** | **Muutmise kuupäev** | **Muudatus** |
| 1.0 | Alar Kvell | 08.12.2010 | Dokumendi algversioon |
| 1.1 | Alar Kvell | 03.01.2011 | Täiendatud varundamise ja taastamise juhendit |
| 1.2 | Alar Kvell | 07.04.2011 | Lisatud juhised paki ehitamiseks lähtekoodist. Täiendatud rakenduse versioonivahetuse juhendit. |
| 1.3 | Alar Kvell | 20.10.2011 | Lisatud peatükk mitme DHS rakenduse samasse masinasse paigaldamise kohta |
| 1.4 | Alar Kvell | 22.11.2011 | Täiendatud varundamise juhendit, peamiselt andmebaasi varundamise ja taastamise detailsemate juhiste osas |
| 1.5 | Alar Kvell | 22.12.2011 | Lisatud klasterdamise seadistamise juhend PPA paigalduse jaoks |
| 1.6 | Alar Kvell | 03.07.2012 | Lisatud nginx puudutavad juhised |
| 1.7 | Kaarel Jõgeva | 05.09.2012 | Lisatud OpenOffice toega seotud juhised |

## Sissejuhatus

Delta on Java EE tehnoloogial põhinev ja Alfresco (Community Edition 3.2 final) põhjal ehitatud dokumendihaldussüsteem ehk DHS.

Käesolev dokument kirjeldab DHS tarkvara paigaldamist kliendi testkeskkonda ja on mõeldud kasutamiseks süsteemiadministraatoritele.

## Sõnastik

*DHS* Dokumendihaldussüsteem

*WAR* Java web archive failiformaat

*Java EE* Java Enterprise Edition platvorm

*FTP* File Transfer Protocol

*CAS* Central Authentication Service

*SMTP* Simple Mail Transfer Protocol

*IMAP* Internet Message Access Protocol

*MSO* Microsoft Office

## Kirjeldus

Webmedia laeb rakenduse paki ülesse FTP serverisse. Süsteemiadministraatorid valmistavad ette infrastruktuuri, paigaldavad ja seadistavad vajaliku kolmandate osapoolte tarkvara (andmebaas, rakendusserver, ehitusvahendid, single sign-on jne.) ning paigaldavad DHS rakenduse rakendusserverisse.

Hiljem uue versiooni korral laeb Webmedia viimase versiooni paki ülesse FTP serverisse ja süsteemiadministraatorid paigaldavad DHS rakenduse rakendusserverisse.

Rakenduse pakk koosneb:

* DHS rakenduse WAR fail – dhs.war
* DHS paigaldusjuhend (kui on muutunud võrreldes viimases pakis sisaldunuga)
* Näidis konfiguratsioonifailid ja skriptid DHS, CAS, Tomcat jaoks (kui on tegemist kõige esimese paigaldusega)Autentimis rakenduse (CAS) WAR fail – cas.war (kui on muutunud võrreldes viimases pakis sisaldunuga)
* MSO teenuse paigaldusjuhend (kui on muutunud võrreldes viimases pakis sisaldunuga)
* MSO teenuse rakenduse failid – mso-service.zip (kui on muutunud võrreldes viimases pakis sisaldunuga)

Koos DHS rakendusega tuleb kaasa autentimise rakendus (CAS), mille kaudu kasutajad hakkavad DHS rakendusse sisse logima, aga mis ise on realiseeritud eraldi rakendusena. Mõlema rakenduse WAR failid, vastavalt dhs.war ja cas.war peab paigaldama käesoleva projekti levitusskeemi järgi samasse Tomcat’i rakendusserverisse (DHS rakenduse IMAP autentimine Kerberos kaudu sõltub sellest et CAS rakendus oleks käivitatud samas Java virtuaalmasinas). Kasutaja arvutist ei pöörduta otse Tomcat’i poole, vaid selle ette proxy-ks paigaldatud Apache httpd või nginx serveri poole. Kasutaja jaoks hakkavad välja paistma aadressid:

* https://dhs.example.com/ - suunab https://dhs.example.com/dhs rakenduse lehele
* https://dhs.example.com/dhs - DHS rakenduse
* https://dhs.example.com/cas - autentimise rakendus
* https://dhs.example.com:4443/cas - sama autentimise rakendus, aga nõuab kasutaja brauserilt ID-kaarti

DHS rakendus on ette nähtud asutuse siseseks kasutamiseks. Elementaarse turvalisuse tagamiseks peab piirama juurdepääsu kogu DHS rakenduse domeenile (dhs.example.com kõikidele teenuste portidele – TCP/80, TCP/443, TCP/4443, TCP/143) ainult asutuse sisevõrgust.

Ligipääsud:

* DHS rakenduse URLile algusega /dhs/service pääseb ligi ilma autentimata. Selle algusega URLile peab piirama ligipääsu kõigile (nii kasutajatele kui teistele süsteemidele), seadistades vastava keelu DHS rakenduste ees olevas koormusjaoturis-proxy's (Apache / nginx). Seadistada, et ligipääs lubatakse konkreetsetele URL'idele ainult konkreetsetele liidestuvatele süsteemidele. Sellel URLil asuvad:
  + /dhs/service/adr – Avaliku Dokumendiregistri (ADR) veebiteenus – sellele veebiteenusele on vaja ligi pääseda ainult ADR rakendusel.
  + /dhs/service2/addDocument – Dokumendi lisamise veebiteenus – sellele veebiteenusele on vaja ligi pääseda ainult kokkulepitud süsteemidel.
  + /dhs/service/monitor – [DHS 3.6 versioonis puudub] Monitooringu info teenus – sellele veebiteenusele on vaja ligi pääseda ainult kokkulepitud süsteemidel.
* Ülejäänud DHS rakenduse URLidele pääseb ligi ainult autenditult.
* DHS rakenduse pakutavale IMAP teenusele (pordil TCP/143) pääseb ligi ainult autenditult.

Teised rakendused peale CAS rakenduse (nt. ADR jm) ei ole käesoleva projekti levitusskeemi järgi ette nähtud paigaldamiseks samasse Tomcat rakendusserveri instantsi. Kui DHS (koos selle juurde käiva autentimisrakendusega CAS) paigaldatakse omaette Tomcat’i, siis on see teistest rakendusest sõltumatu – probleemid või *downtime* ühe Tomcat instansti juures ei mõjuta teist Tomcat instantsi. See on vajalik seepärast, et DHS rakendus ei toeta undeploy’mist/redeploy’mist – uue versiooni paigaldamiseks (või mingil muul põhjusel rakenduse (uuesti) käivitamiseks) peab eelnevalt Tomcat rakendus­serveri seiskama!

## Infrastruktuur ja serveri tarkvara

Rakendusserverisse peab olema paigaldatud:

* Sun JDK 6 (versioon 1.6.0\_31 või uuem 1.6.0\_x)
  + Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 (kui soovitakse kasutada OCSP kehtivuskinnitusteenusele ligipääsuks juurdepääsutõendi faili)
* Apache Tomcat 6.0 (versioon 6.0.29 või uuem 6.0.x)
* OpenOffice.org 3.2.x või 3.3.x (LibreOffice / Apache OpenOffice versioonid 3.4 ja kõrgemad ei tööta, vt. peatükk 10.17)
* Apache httpd või nginx (võib ka mujal serveris paikneda)
* Kerberos klienttarkvara (kui soovitakse kasutada Active Directory Kerberos autentimist (JuM/MV puhul))

Teenusena peab mõnest serverist olema kättesaadav (võib ka sama server olla):

* PostgreSQL 9.1 andmebaas (versioon 9.1.3 või uuem 9.1.x) – aadress ja port (tavaliselt TCP/5432) määratavad konfist
* X-tee turvaserver – aadress ja port (tavaliselt TCP/80 määratavad konfist)
* SMTP server e-mailide välja saatmiseks – aadress ja port (tavaliselt TCP/25) määratavad konfist
* Active Directory server Kerberos protokolli kaudu autentimiseks – aadress ja port (tavaliselt TCP/88) määratavad konfist
  + SiM/SMIT/PPA puhul selle asemel Active Directory server NTLM „passthrough“ protokolli kaudu autentimiseks – aadress määratav konfist
* Active Directory server LDAP protokolli kaudu kasutajate/gruppide info tõmbamiseks – aadress ja port (tavaliselt TCP/389) määratavad konfist
  + SiM/SMIT/PPA puhul selle asemel Ametnikuregister veebiteenus – aadress ja port määratavad konfist
* Kehtivuskinnitusteenus (OCSP) digiallkirjastamiseks ja ID-kaardiga autentimiseks – http://ocsp.sk.ee
* MSO teenus, mis jookseb Windowsi masinas – aadress ja port määratavad konfist

Sun JDK

1. Paigaldada Sun JDK
2. Veenduda, et keskkonnamuutuja JAVA\_HOME viitaks paigaldatud JDK kataloogile
3. Veenduda, et käsk java oleks käivitatav, s.t. PATH’is
4. Paigaldada Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6. Kui seda ei ole paigaldatud, siis tuleb juurdepääsutõendi kasutamisel viga (vt. peatükk 10.3).

OpenOffice.org

1. Paigaldada OpenOffice.org. Näiteks RedHat/CentOS 6 või uuema distributsiooni puhul saab seda teha järgnevalt:  
   yum install openoffice.org-writer openoffice.org-calc openoffice.org-impress openoffice.org-headless  
   Vanema RedHat/CentOS distributsiooni puhul saab seda teha järgnevalt:  
   wget http://openoffice.offline.ee/stable/3.2.1/OOo\_3.2.1\_Linux\_x86\_install-rpm\_en-US.tar.gz  
   tar zxpf OOo\_3.2.1\_Linux\_x86\_install-rpm\_en-US.tar.gz  
   cd OOO320\_m18\_native\_packed-1\_en-US.9502/RPMS  
   rm \*integration\*.rpm  
   yum --nogpgcheck localinstall \*.rpm
2. OpenOffice.org monitoorimiseks ja perioodiliseks restartimiseks on soovitav kasutada skripti soffice-monitor.sh . Skript ise käivitab OpenOffice.org protsessi, seega peab DHS rakenduse seadistusfailis määrama ooo.exe tühja väärtusega, et DHS rakendus ei käivitaks OpenOffice.org protsessi. Seadistada soffice-monitor.sh skripti alguses olevad seaded enda keskkonnale sobivaks ning käivitada (soovitavalt serveri käivitumisel automaatselt) skript, näiteks:  
   /path/to/soffice-monitor.sh 8100 /home/dhs/data/local/oouser >> /home/dhs/data/local/soffice-monitor.log &

Kerberos

1. Paigaldada Kerberos kliendi tarkvara (RedHat/CentOS distributsioonis pakett nimega krb5-workstation, Debian distributsioonis pakett nimega krb5-user).
2. Asendada /etc/krb5.conf faili sisu järgnevaga (terve faili sisuks pannagi järgnevad 3 rida):  
   [libdefaults]  
    # Force Kerberos to use TCP. Default is to use UDP.  
    udp\_preference\_limit = 1
3. DHS ja CAS serverite kellad peavad olema mitte rohkem kui 5 minutise vahega Active Directory serveri kellast! Vastasel juhul Kerberos autentimine ei tööta.

Apache httpd

1. Paigaldada Apache httpd, mod\_ssl, mod\_proxy\_ajp
2. Luua https://dhs.example.com aadressi jaoks vajalik konfiguratsioon, selleks:
   1. võtta SSL virtualhosti vaikekonfiguratsioon
   2. lisada VirtualHost bloki lõppu järgnevad read:  
      ProxyPass / ajp://127.0.0.1:8009/  
      ProxyPassReverse / ajp://127.0.0.1:8009/  
      ProxyTimeout 3600
3. Luua https://dhs.example.com:4443 ehk ID-kaardiga autentimise aadressi jaoks vajalik konfiguratsioon. Selleks:
   1. kopeerida eelmises punktis määratud VirtualHost konfiguratsioon
   2. muuta vajalikud read (port, logifailide asukohad, vajadusel ProxyPass ja ProxyPassReverse, vajadusel lisada ka VirtualHost blokist väljapoole rida Listen 4443)
   3. seadistada VirtualHost kasutama ID-kaardiga autentimist (juhendi alusena on kasutatud http://code.google.com/p/esteid/wiki/AuthConfApache#Apache\_seadistamine ja http://www.id.ee/public/Configuring\_Apache\_web\_server\_to\_support\_ID.pdf):
      1. lisada VirtualHost bloki sisse read  
         SSLCACertificatePath /etc/pki/esteid/ca  
         SSLVerifyClient require  
         SSLVerifyDepth 2  
         SSLOptions +StdEnvVars +ExportCertData
      2. mkdir -p /etc/pki/esteid/ca
      3. cd /etc/pki/esteid/ca
      4. wget -O "JUUR-SK.crt" http://www.sk.ee/upload/files/JUUR-SK.PEM.cer
      5. wget -O "ESTEID-SK 2007.crt" http://www.sk.ee/upload/files/ESTEID-SK%202007.PEM.cer
      6. wget -O "ESTEID-SK 2011.crt" http://www.sk.ee/upload/files/ESTEID-SK%202011.pem.cer
      7. wget -O "EECCRCA.crt" http://www.sk.ee/upload/files/EECCRCA.pem.cer
      8. for f in \*.crt;do ln -sf "$f" $(openssl x509 -hash -noout -in "$f").0; done
   4. Kui CAS rakenduses ID-kaardiga sisselogimisel kehtivuskinnituspäringuid ei sooritata (peatükis 5.2 määrate seade jdigidoc.ocsp.enabled=false), siis peab siin lisaks seadistama Apache kasutama tühistusnimekirjasid (CRL) ning realiseerima nende perioodilise uuendamise. Samuti peab serveri kellaaeg olema korrektne, kuna CAS rakendus ise kontrollib sertifikaatide aegumist.
      1. Punktis e defineeritud ID-kaardiga autentimise VirtualHost bloki sisse lisada rida  
         SSLCARevocationPath /etc/pki/esteid/crl
      2. mkdir -p /etc/pki/esteid/crl
      3. Punktis e viidatud esimeses ja/või teises juhendis kirjeldatud skripti alusel koostada skript, mis perioodiliselt tõmbaks CRL failid, teisendaks need antud kaustas PEM vormingusse, genereeriks sinna räsi symlingid ning restardiks Apache. Panna see skript iga 12 tunni tagant käivituma. CRL failid, mida on vaja tõmmata, on järgnevad:
         1. http://www.sk.ee/crls/juur/crl.crl
         2. http://www.sk.ee/crls/esteid/esteid2007.crl
         3. http://www.sk.ee/repository/crls/esteid2011.crl
         4. http://www.sk.ee/crls/eeccrca/eeccrca.crl

nginx (alternatiiv Apache’le)

1. Paigaldada nginx
2. Vt. näidisfaile nginx-\*.conf.example; märkuseks, et näidisfailides on DHS ja CAS rakendus eraldi virtualhost’idesse seadistatud (nii nagu JuM paigaldusskeemis ette nähtud); järgnevas tekstis on kirjeldatud DHS ja CAS rakenduse vaikimisi sama virtualhosti alla seadistamist.
3. Luua https://dhs.example.com aadressi jaoks vajalik konfiguratsioon, selleks:
   1. võtta SSL server vaikekonfiguratsioon
   2. lisada server blokki järgnevad read  
      location / { proxy\_pass http://127.0.0.1:8080; }  
      proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;  
      proxy\_read\_timeout 3600s;
   3. määrata DHS rakenduse seadistusfailis useClientIpFromXForwardedForHttpHeader=true (vt. täpsemalt peatükk 5.1 ja selle alampunkt useClientIpFromXForwardedForHttpHeader)
   4. kui CAS rakendus on samas virtuaalserveris, siis lisada server blokki järgnev rida  
      proxy\_set\_header Host $host:$server\_port;
   5. kui kasutusel on klasterdamine, siis DHS rakendus vajab sticky sessioone; selleks lisada upstream blokki rida  
      ip\_hash;  
      kui klientide IP aadressid ei muutu päringute vahepeal. Kui muutuvad, siis selle asemel tuleb kasutusele võtta küpsise-põhised sticky sessioonid (http://code.google.com/p/nginx-sticky-module/)
4. Luua https://dhs.example.com:4443 ehk ID-kaardiga autentimise aadressi jaoks vajalik konfiguratsioon. Selleks:
   1. kopeerida eelmises punktis määratud server konfiguratsioon
   2. muuta vajalikud read (port, domeeni nimi, logifailide asukohad, vajadusel proxy\_pass)
   3. seadistada VirtualHost kasutama ID-kaardiga autentimist
      1. lisada server blokki järgnevad read  
         ssl\_verify\_client on;  
         ssl\_verify\_depth 2;  
         ssl\_client\_certificate /etc/pki/esteid/ca-all.crt;  
         proxy\_set\_header SSL\_CLIENT\_CERT $ssl\_client\_cert;
      2. Teostada peatüki „Apache httpd“ alampunktid 3.c.ii kuni 3.c.viii
      3. Tõmmatud crt failid kombineerida kokku üheks failiks, selliselt:  
         cat /etc/pki/esteid/ca/\*.crt > /etc/pki/esteid/ca-all.crt
   4. Kui CAS rakenduses ID-kaardiga sisselogimisel kehtivuskinnituspäringuid ei sooritata (peatükis 5.2 määrate seade jdigidoc.ocsp.enabled=false), siis peab siin lisaks seadistama nginx kasutama tühistusnimekirjasid (CRL) ning realiseerima nende perioodilise uuendamise. Samuti peab serveri kellaaeg olema korrektne, kuna CAS rakendus ise kontrollib sertifikaatide aegumist.
      1. Punktis c defineeritud ID-kaardiga autentimise server bloki sisse lisada rida  
         ssl\_crl /etc/pki/esteid/crl-all.crl;
      2. Teostada peatüki „Apache httpd“ alampunktid 3.d.ii kuni 3.d.iii
      3. Täiendada perioodilise uuendamise skripti selliselt, et tõmmatud crl failid kombineeritaks kokku üheks failiks, selliselt:  
         cat /etc/pki/esteid/crl/\*.crl > /etc/pki/esteid/crl-all.crl
5. Luua IMAP jaoks vajalik konfiguratsioon. Selleks:
   1. kasutada nginx juures moodulit https://github.com/yaoweibin/nginx\_tcp\_proxy\_module/
   2. lisada seaded näidisfaili nginx-dhs01-imap.conf.example põhjal, vajadusel neid muutes
6. Kui soovitakse kasutada kasutaja arvutist OpenOffice.org / LibreOffice / Apache OpenOffice kaudu failide avamist muutmiseks ja tagasi salvestamist DHS rakendusse (s.t. kui peatükis 5.1 kirjeldatud seade conf.openoffice-client-extensions väärtus on mittetühi), siis luua http://dhs.example.com jaoks vajalik konfiguratsioon, mis suunab (302 redirect) kõik päringud ümber https://dhs.example.com peale sama URL'iga, ainult https protokolliga.

Tomcat

1. Pakkida lahti apache-tomcat-6.0.29.tar.gz. Siin juhendis kasutame Tomcat’i kataloogina näidisväärtust /home/dhs/tomcat
2. Apache httpd server hakkab Tomcat’iga ühendust võtma AJP protokolli kaudu (mod\_proxy\_ajp) – see on vajalik selleks, et Tomcat’ini jõuaks ID-kaardi autentimise puhul kliendi sertifikaat. Seega /home/dhs/tomcat/conf/server.xml failis peab rida  
   <Connector port="8009" protocol="AJP/1.3"...  
   olema sisse lülitatud, mis vaikimisi ongi; kuna httpd ja Tomcat asuvad samas masinas, siis ei pea seda protokolli väljapoole serveerima, seega võib rea lõppu panna address="127.0.0.1". Kokkuvõtteks, terve rida oleks:  
   <Connector port="8009" protocol="AJP/1.3" address="127.0.0.1" />
3. Kuna Tomcat’iga võetakse ühendust AJP protokolliga, siis ei ole vajadust et Tomcat serveeriks välja HTTP protokolli, seega rea  
   <Connector port="8080" protocol="HTTP/1.1"...  
   võib kustutada või välja kommenteerida.
4. Kui Tomcat’iga, milles töötab CAS rakendus, võetakse ühendust HTTP protokolli kaudu (nt. nginx kaudu), siis on vajalik sooritada järgnev:
   1. server.xml failis elemendile <Connector port="8080" protocol="HTTP/1.1" lisada atribuudid scheme="https" secure="true"
   2. server.xml failis elemendi <Engine>...</Engine> sisse lisada rida <Valve className=“org.apache.catalina.valves.SSLValveFixed“/>
   3. kopeerida fail tomcat-sslvalve-fixed.jar kausta tomcat/lib
5. Genereerida HTTPS serveri sertifikaadi põhjal Java Keystore fail:  
   keytool -v -importcert -keystore truststore.jks -file myserver.crt  
   parooliks sisestada changeit  
   ning paigutada saadud fail asukohta /home/dhs/tomcat/truststore.jks
6. Tomcat’i käivitamiseks soovitame kasutada antud juhendiga kaasas olevat faili tomcat.sh. Paigutada see fail asukohta /home/dhs/tomcat/tomcat.sh ning muuta selle sisu:
   1. Määrata Java virtuaalmasina poolt kasutava heap mälu ülempiir võtmega  
       -Xmx1024m
7. Java virtuaalmasin on võimalik seadistada selliselt, et kui tekib fataalne viga, siis käivitatakse operatsioonisüsteemis etteantud programm või skript. Kasulik on lasta käivitada selline skript, mis logib vea tekkimise aja, seejärel saadab e-mailiga teavituse süsteemi administraatorile ning seejärel tapab Tomcat’i protsessi ning käivitab selle uuesti. Võtta antud juhendiga kaasas olev fail jvm-error.sh ning paigutada see fail asukohta /home/dhs/tomcat/jvm-error.sh ning muuta selle sisu enda vajadustele sobivaks.  
   NB! Kui rakenduse töö ajal tekib OutOfMemoryError, siis kindlasti peab koheselt Java virtuaalmasinat restartima, s.t. Tomcat’i sulgema ning uuesti käivitama – muidu võib rakendus jääda vigasesse seisu! Selleks ongi vajalik eelpoolmainitud skript, sest see käivitatakse ka OutOfMemoryError puhul. Selle skripti kaudu peab tegema automaatse teavitamise, soovitavalt ka Tomcat’i automaatse taaskäivitamise.
8. Kustutada Tomcat’i vaikimisi juur-rakenduse failid  
   rm –rf /home/dhs/tomcat/webapps/ROOT/\*  
   ning tekitada fail /home/dhs/tomcat/webapps/ROOT/index.jsp järgneva sisuga:  
   <?xml version="1.0" encoding="UTF-8"?>  
   <%@ page session="false" %>  
   <% response.sendRedirect("/dhs/"); %>
9. Kui teised Tomcat’iga vaikimisi kaasa tulnud rakendused (docs, examples, host-manager, manager) ei ole vajalikud, siis kustutada need:  
   rm –rf /home/dhs/tomcat/webapps/{docs,examples,host-manager,manager}

PostgreSQL

1. Peale andmebaasi tarkvara installeerimist tekitage login role:

CREATE ROLE dhs LOGIN PASSWORD 'dhs' NOSUPERUSER NOINHERIT NOCREATEDB NOCREATEROLE;

Password väärtus võib olla teistsugune, see tuleb rakenduse seadistusfailis hiljem ära määrata.

1. Ja tekitage andmebaas:

CREATE DATABASE dhs WITH OWNER = dhs ENCODING = 'UTF8';

Kui DHS rakendus käivitatakse, siis DHS rakendus ise loob andmebaasi vajalikud tabelid, muud objektid ja andmed.

## Rakenduse seadistamine

Kui teete muudatusi kummagi rakenduse seadistusfailis, siis muudatusi arvestatakse alles rakenduse järgmisel käivitumisel.

### DHS rakenduse seadistamine

DHS rakenduse seadistusfail on alfresco-global.properties ning see peab asuma DHS rakenduse classpath’i juurkaustas. Kui sisestada mitte-ASCII tähemärke (näiteks täpitähti), siis peavad need olema pagendatud vastavalt http://docs.oracle.com/javase/specs/jls/se5.0/html/lexical.html#3.3 kirjeldatule (Näiteks sõna näidis tuleb sisestada kujul n\u00E4idis). Võtke juhendiga kaasasolev näidisfail alfresco-global.properties ning paigutage see asukohta /home/dhs/tomcat/lib/alfresco-global.properties ning muutke selle sisu. Vaadake üle kõik järgnevad seaded ja vajadusel tehke muudatusi (failis sees on samuti kõikide nende seadistusparameetrite kohta olemas näiteväärtused ja selgitavad kommentaarid):

* dir.root viitab kaustale kus DHS rakendus hakkab hoidma dokumendi failide sisu ja täistekstiotsinguindeksite andmeid (näiteks /home/dhs/data). Kui seda kausta ei eksisteeri, siis DHS rakendus loob selle ise. Kui kustutate selle kausta sisu, siis peate kustutama ka järgnevate seadetega viidatud andmebaasi sisu. NB! Kettal, kus dir.root alamkaust lucene-indexes asub, peab lisaks lucene-indexes kausta suurusele olema veel vaba ruumi vähemalt 2 korda sama palju, selleks et DHS rakendus saaks lucene indeksite faile töö käigus ümber kirjutada (näiteks kui lucene-indexes kausta suurus on parajasti 5 GB, siis peab samal kettal olema vaba ruumi veel vähemalt 10 GB, ehk ruumi kokku vähemalt 15 GB. Ja sellele lisaks peab kettal, kus dir.root asub, olema 5 GB backup-lucene-indexes kausta jaoks.).
* dir.root.shared [DHS 3.6 versioonis puudub] [mittekohustuslik, vaikimisi ${dir.root}/shared] viitab kaustale, mis peab olema klastris kõikide rakendusserverite vahel ühine.
* dir.root.local [DHS 3.6 versioonis puudub] [mittekohustuslik, vaikimisi ${dir.root}/local] viitab kaustale, mis peab olema klastris igal rakendusserveril eraldi.
* db.\* seaded viitavad PostgreSQL andmebaasiserverile ja sisaldavad õiget andmebaasi nime, kasutajanime ja parooli. Kui kustutate andmebaasi sisu, siis peate kustutama ka eelmise seadega viidatud andmekausta sisu.
* ooo.exe [mittekohustuslik, vaikimisi tühi] viitab OpenOffice.org käivitusfailile. Kui tühi, siis DHS rakenduse käivitumisel ei käivitata OpenOffice.org protsessi. Kui mittetühi, siis käivitatakse. Kui OpenOffice.org protsess käivitatakse mujalt (näiteks välise monitoorimise skripti kaudu, vt. peatükk 4, alampeatükk OpenOffice.org punkt 2), siis jätta tühjaks.
* ooo.port [mittekohustuslik, vaikimisi 8100] viitab TCP pordile, millel OpenOffice.org protsess kuulama pannakse ning millele DHS rakendus ühendab. DHS rakendus kontrollib OpenOffice.org ühenduse kättesaadavust antud pordil iga 60 sekundi tagant (olenemata sellest kas ooo.exe on tühi või mitte).
* mail.host viitab SMTP serverile, mille kaudu saab e-maile välja saata. NB! E-maili serveris tuleb seada e-kirja suuruse piirang vastavaks DHS’is maxAttachedFilesSize parameetri (administraatori kasutajaliideses) väärtusele, lähtudes järgnevast näitest:
  + Kui maxAttachedFilesSize väärtus on 10, siis see tähendab et kasutajal lubatakse dokumendi väljasaatmisel kaasa panna maksimaalselt 10 MB kogusuuruses faile.
  + Kui dokumendi väljasaatmisel pannakse kaasa faile kogusuuruses 10 MB, siis see teisendub e-kirja suuruseks 13,3 MB (kuna failid on base64 kodeeringus 33% suuremad). Pluss mõnikümmend kilobaiti kirja sisule ja päistele.
  + Seega peab e-maili serveris e-kirja suuruse piiranguks panema minimaalselt (rohkem võib ka olla) 14 MB kui DHS-is on maxAttachedFilesSize parameetri väärtus on 10.
* mail.messageFolder [mittekohustuslik, vaikimisi tühi] kui mittetühi, siis salvestatakse kõik väljasaadetud e-mailid originaalformaadis antud seadega määratud kausta. Kasulik probleemide lahendamiseks.
* cas.casServerUrl viitab autentimise (CAS) rakenduse aadressile. Väärtus peab lõppema kaldkriipsuga, näiteks https://dhs.example.com/cas/
* external.authentication.defaultAdministratorUserNames sisaldab komaga eraldatud nimekirja kasutajatunnustest (isikukoodidest), kes sisselogimise järel rakenduse administraatori rolli külge saavad.
* server.url viitab URL-ile, kus DHS rakendus jooksma hakkab (sinna tulevad päringud CAS-ist tagasi ning seda kasutatakse väljasaadetavates e-mailides dokumendi linkides).
* useClientIpFromXForwardedForHttpHeader [mittekohustuslik, vaikimisi false] määrata true siis kui proxy (Apache või nginx) ühendub rakendusserveri (Tomcat) külge http:// või https:// protokolli kaudu, sest siis proxy paigutab kasutaja IP aadressi X-Forwarded-For HTTP päisesse. Määrata false siis kui kasutajad ühenduvad otse rakendusserveri külge või kui proxy ühendub rakendusserveri külge ajp:// protokolli kaudu.
* ldap.\* seaded [DHS 3.6 versioonis puudub] viitavad Active Directory serverile, millelt kasutajate ja gruppide infot tõmbama hakatakse. Järgnevalt on välja toodud ainult kohustuslikud seaded (kõik Active Directory’ga seotud seaded, s.h. mittekohustuslikud seaded, on täpsemalt dokumenteeritud spetsifikatsioonidokumendis Liidestused - Active Directory.docx):
  + ldap.authentication.java.naming.provider.url viitab Active Directory serverile ja pordile, mida kasutada LDAP protokolli kaudu kasutaja ja gruppide info tõmbamiseks, näiteks ldap://fw.viljandimaa.ee:389
  + ldap.synchronization.java.naming.security.principal viitab Active Directory serveris olevale kasutajanimele, koos domeeniga, näiteks   
    dhs-test@viljandi.maavalitsus
  + ldap.synchronization.java.naming.security.credentials viitab eelmise seadega määratud kasutaja paroolile Active Directory serveris
  + ldap.synchronization.userSearchBase viitab Active Directory alamosa nimetusele, mille alt kasutajaid otsitakse, näiteks  
    CN=Users,DC=viljandi,DC=maavalitsus
  + ldap.synchronization.groupSearchBase viitab Active Directory alamosa nimetusele, mille alt gruppe otsitakse, näiteks  
    CN=Users,DC=viljandi,DC=maavalitsus
  + ldap.synchronization.organizationalUnitSearchBase viitab Active Directory alamosa nimetusele, mille alt struktuuriüksuste tippe järgmise päringuga otsitakse, näiteks OU=Haldusala,DC=viljandi,DC=maavalitsus
  + ldap.synchronization.organizationalUnitSearchQuery määrab päringu, millega leitakse struktuuriüksuste alamosade tipud, näiteks (|(distinguishedName=OU=Alamosa1,OU=Haldusala,DC=viljandi,DC=maavalitsus)(distinguishedName=OU=Alamosa2,OU=Haldusala,DC=viljandi,DC=maavalitsus))
  + ldap.synchronization.organizationalUnitSecondarySearchQuery määrab päringu, millega otsitakse struktuuriüksuseid, kasutades eelneva päringuga leitud tippusid baasidena, näiteks (&(objectClass=organizationalUnit)(! (|(distinguishedName=OU=Alamosa1,OU=Haldusala,DC=viljandi,DC=maavalitsus)(distinguishedName=OU=Alamosa2,OU=Haldusala,DC=viljandi,DC=maavalitsus))))
* SiM/SMIT/PPA puhul ldap.\* seadete asemel kasutada amr.\* seadeid, mis viitavad Ametnikuregistri veebiteenusele
  + amr.service.url viitab Ametnikuregistri veebiteenuse SOAP aadressile
  + amr.org.id on DHS rakendust kasutava asutuse ID Ametnikuregistris
* x-tee.\* seaded viitavad X-tee turvaserverile, mille kaudu DVK päringuid teostatakse.
  + x-tee.security-server - X-tee turvaserveri URL. See X-tee turvaserver peab olema liitunud soovitud X-tee keskkonnaga (toodang või test), mille kaudu on ligipääs soovitud DVK keskkonnale (toodang või test).
  + x-tee.institution – asutuse äriregistri kood, mida kasutatakse üle X-tee DVK päringute tegemisel
  + x-tee.id-code – kahekohaline riigi kood, mille järel on isikukood, mida kasutatakse üle X-tee DVK päringute tegemisel. Väärtus peab olema kujul EE01234567890
  + x-tee.receivedDocumentsFolder [mittekohustuslik, vaikimisi tühi] kui mittetühi, siis salvestatakse kõik DVK kaudu vastuvõetud sõnumid originaalformaadis antud seadega määratud kausta. Kasulik probleemide lahendamiseks.
  + x-tee.sentDocumentsFolder [mittekohustuslik, vaikimisi tühi] kui mittetühi, siis salvestatakse kõik DVK kaudu väljasaadetud sõnumid originaalformaadis antud seadega määratud kausta. Kasulik probleemide lahendamiseks.

Nii see äriregistri kood kui ka isikukood peavad olema registreeritud selles DVK keskkonnas (toodang või test), mille külge X-tee turvaserveri kaudu ühendatud ollakse – äriregistri koodi ja isikukoodi alusel lubab DVK keskkond sooritada päringuid.

* imap.server.port määrab DHS rakenduse sees serveeritava IMAP teenuse pordi.  
  Kasutaja arvuti jaoks peab IMAP teenus olema kättesaadav pordil 143. Kui DHS rakendust jooksutada Unix'is tavakasutaja õigustes, siis pole privileege kasutada porte < 1024. Siis tuleks seada IMAP teenus töötama mõnel kõrgemal pordil, nt. 1143 ning lisada serveri tulemüüri pordi suunamine 143 -> 1143, näiteks selliselt:  
  iptables -t nat -A PREROUTING -p tcp -d 192.168.41.61 --dport 143 -j DNAT --to-destination 192.168.41.61:1143
* imap.messageFolder [mittekohustuslik, vaikimisi tühi] kui mittetühi, siis salvestatakse kõik IMAP teenuses vastuvõetud e-mailid originaalformaadis antud seadega määratud kausta. Kasulik probleemide lahendamiseks.

mso.url viitab MSO veebiteenuse SOAP aadressile. Kui väärtus jätta tühjaks, siis rakendus ei kasuta MSO veebiteenust ja samad tegevused teostatakse OpenOffice.org abil.

* kerberos.\* seaded [DHS 3.6 versioonis puudub] viitavad Active Directory serverile, mida kasutatakse Kerberos protokolli kaudu kasutajate autentimiseks, kui kasutajad IMAP kaudu DHS rakendusse ühendavad
  + kerberos.conf viitab operatsioonisüsteemis paigaldatud Kerberos klienttarkvara konfiguratsioonifailile, näiteks /etc/krb5.conf . Kerberos protokolli kaudu kasutajate autentimise korrektseks toimimiseks peavad DHS rakenduse masinas olema tehtud peatükk 4 alampeatükis Kerberos kirjeldatud tegevused.
  + kerberos.kdc viitab Active Directory serverile ja pordile, mida kasutada Kerberos protokolli kaudu kasutajate autentimiseks, näiteks fw.viljandimaa.ee:88
  + kerberos.realm viitab Active Directory serveris olevale Windows domeeni täispikale nimetusele, kirjutada suurtähtedega, näiteks VILJANDI.MAAVALITSUS . NB! Siin olev domeeni Domeeni nimetus peab kindlasti olema täispikk ja kindlasti olema kirjutatud suurtähtedega. Näiteks kuigi kasutajad võivad saada Windowsisse autentida ka lühema domeeniga VILJANDI\username (ja ka LDAP ligipääsul võib töötada kasutajanime lõpus lühem domeen (CAS seade ldap.userDn, DHS seade ldap.synchronization.java.naming.security.principal)), siis siin peab Kerberos autentimise jaoks kindlasti olema täispikk domeeni nimi VILJANDI.MAAVALITSUS, muidu autentimine ebaõnnestub. Samuti, kui täispikk domeeni nimi peab olema kirjutatud suurtähtedega, muidu autentimine ebaõnnestub.
* SiM/SMIT/PPA puhul kerberos.\* seadete asemel kasutada passthru.authentication.servers seadet, mis viitavad Active Directory serverile, mida kasutatakse NTLM „passthrough“ protokolli kaudu kasutajate autentimiseks, kui kasutajad IMAP kaudu DHS rakendusse ühendavad; väärtuseks määrata Active Directory serveri aadress või komaga eraldatult mitu aadressi
* jdigidoc.test [mittekohustuslik, vaikimisi false] Toodangkeskkonnas kasutada false, siis tehakse digiallkirjastamisel kehtivuskinnituspäringud (OSCP) vastu Sertifitseerimis-keskuse serverit ja Mobiil-ID jaoks päringuid vastu Sertifitseerimiskeskuse DigiDocService toodangteenust. Testkeskkonnas võib kasutada true, siis tehakse digiallkirjastamise kehtivuskinnituspäringud vastu OpenXAdES testserverit ja Mobiil-ID jaoks päringuid vastu OpenXAdES DigiDocService testteenust. Kui kasutada false, siis test ID-kaarte ei saa digiallkirjastamisel kasutada ning test ID-kaartidega antud allkirju ja vastu test kehtivuskinnitusteenust antud allkirju näidatakse kehtetuna.
* mobile-id.service-name [mittekohustuslik, vaikimisi tühi] kui tühi, siis mobiil-ID on välja lülitatud. Kui mittetühi, siis mobiil-ID on sisselülitatud ja antud seadega määratud väärtust kasutatakse DigiDocService’ile päringuid tehes ServiceName välja väärtusena. ServiceName on telefonil kuvatav teenuse nimetus, maksimaalne pikkus 20 tähemärki. Eelnevalt on vajalik kasutatava teenuse nimetuse kokkuleppimine Sertifitseerimiskeskusega. Lisaks vt. peatükk 5.1.2 HTTPS sertifikaatide kohta.
* SiM/SMIT/PPA puhul email.\* seaded viitavad DHS rakenduse sees serveeritavale SMTP teenusele. Kasutaja arvuti jaoks peab SMTP teenus olema kättesaadav pordil 25. Kui DHS rakendust jooksutada Unix'is tavakasutaja õigustes, siis pole privileege kasutada porte < 1024. Siis tuleks seada SMTP teenus töötama mõnel kõrgemal pordil, nt. 1025 ning lisada serveri tulemüüri pordi suunamine 25 -> 1025. SMTP teenus on mõeldud selleks, et skanner saaks saata e-maili otse DHS rakendusse. SMTP teenus võtab vastu ainult ühele kindlale aadressile saadetud e-maile, ülejäänutest keeldub. Aadress, millele saadetud kirju vastu võetakse (näiteks scan@dhs.example.com) pannakse kokku kahest osast, @-märgist vasakpoolne osa defineeritakse seadega email.to.scanned.local-part ning parempoolne osa seadega email.server.domain.
* SiM/SMIT/PPA puhul ocr.url viitab tekstituvastuse veebiteenuse SOAP aadressile. Kui väärtus jätta tühjaks, siis rakendus ei kasuta tekstituvastuse veebiteenust.
* PPA puhul archivals-additional [mittekohustuslik, vaikimisi tühi] kui mittetühi, siis semikoolonitega eraldatult sisaldab arhiivimoodustajate seadeid; iga arhiivimoodustaja seade peab olema ID + „/“ + kirjeldus; ID tohib sisaldada [a-zA-Z0-9] ja seda kasutatakse hoidla nime suffiksina, kirjeldus võib sisaldada kõiki tähemärke (täpitähed peavad olema pagendatud vastavalt peatüki alguses viidatule); PPA puhul määrata väärtuseks näiteks PPA/PPA;PohjaPref/P\u00F5hja PREF;LounaPref/L\u00F5una PREF;IdaPref/Ida PREF;LaanePref/L\u00E4\u00E4ne PREF
* PPA puhul imap-folders.\*.subfolderType [mittekohustuslik, vaikimisi kõigil fixed] määrab Outlooki kaustade alamkaustade tekkimise (fikseeritud kaustad või kasutajapõhised), täpsemalt vaata spetsifikatsioonidokument; PPA puhul määrata kõigil (imap-folders.incomingLetters.subfolderType, imap-folders.attachments.subfolderType, imap-foders.outgoingLetters.subfolderType, imap-folders.sendingFailed.subfolderType) väärtuseks näiteks fixed;PPA;P\u00F5hi;L\u00F5una;Ida;L\u00E4\u00E4s
* logo.file [DHS 3.6 versioonis puudub] [mittekohustuslik, vaikimisi tühi] kui tühi, siis DHS rakenduse veebilehe päises kuvatakse vaikelogo. Kui mittetühi, siis loetakse brauserist logo URL’i poole pöördumisel antud seadega viidatud faili sisu. Kui faili lugemisel tuleb viga, siis logitakse hoiatus. Faili tüüp leitakse faili laiendi põhjal. Sobiv logo peab olema PNG formaadis, suurusega 184 x 57 pikslit ning läbipaistva taustaga.
* system.usages.enabled [mittekohustuslik, vaikimisi true] Muuta false-iks pärast seda kui rakendus on esmakordselt paigaldatud ja käivitatud ja vähemalt ühe korra on suvaline kasutaja edukalt sisse loginud. False-iks muutmine lülitab välja Alfrescos ebavajaliku funktsionaalsuse kasutajate poolt tarbitud kettaruumi arvutamise kohta; kahjuks ei saa Alfresco vea tõttu see väärtus olla juba vaikimisi false.
* jobs.enabled [mittekohustuslik, vaikimisi true] vt. klasterdamine
* alfresco.cluster.name [mittekohustuslik, vaikimisi tühi] vt. klasterdamine
* project.test [mittekohustuslik, vaikimisi false] kui määrata true, siis rakendub järgnev:
  + Kasutaja andmete uuendamisel määratakse e-maili aadressiks mail.from.default seadega määratud väärtus
  + Rakendusse luuakse süsteemsete meiliteavituste jaoks testmallid – ainult uue paigalduse puhul (rakenduse esmakordsel käivitamisel tühja baasi pealt)
  + Veebilehe resurssid (JavaScript, pildid, CSS) laetakse brauserisse igal päringul uuesti
  + Teatud funktsionaalsuse juures rakenduvad debugimiseks mõeldud lisakontrollid või lisateated
* index.tracking.disableInTransactionIndexing=false [mittekohustuslik, vaikimisi true] Muuta false-iks suuremahuliste tegevuste (importimised, tühjaks kustutamised) ajaks. Rakenduse esmase paigaldamise ajaks (kui baas ja andmekaust on tühi) muuta samuti false-iks. Tava töö (sealhulgas koormustestide) ajaks kommenteerida see seade välja, siis rakendub vaikeväärtus true .
* conf.\* seaded muudavad DHS rakenduses rohkem sisulist käitumist ja on vähem olulised infrastruktuuri ja halduse seisukohast; sellised seaded on täpsemalt kirjeldatud spetsifikatsioonidokumentides.
  + conf.openoffice-client-extensions [DHS 3.6 versioonis puudub] [mittekohustuslik, vaikimisi tühi] Sisaldab komaga eraldatud faililaiendeid (ilma punktita ja ilma tühikuteta; nt. odt,ods,rtf,doc,docx), mille puhul kasutaja arvutis avatakse fail muutmiseks OpenOffice.org programmiga. Kasutaja arvutis peab olema paigaldatud OpenOffice.org 3.2 või uuem OpenOffice.org / LibreOffice / Apache OpenOffice ning vastavalt kasutatavale programmile registreeritud *vnd.sun.star.webdav* protokoll. Protokolli registreerimiseks saab kasutada tarnega kaasas olevat faili OpenOffice\_WebDAV\_Protocol.reg, milles tuleb korrigeerida rakenduse asukohta. Lisaks, kui server.url alguses on https://, siis kõikidele URLidele peab vastama ka http:// alternatiiv, mis suunab päringu https:// URLile (vt. peatükk 4 alampeatükk nginx punkt 6).
    1. Digiallkirjastamise kehtivuskinnituspäringud juurdepääsutõendi alusel

Kui soovite, et digiallkirjastamise OCSP päringud tehtaks juurdepääsutõendi alusel, siis lisage seadistusfaili järgnevad seaded:

* jdigidoc.pkcs12.container [mittekohustuslik, vaikimisi tühi] kui tühi, siis juurdepääsutõendit ei kasutata. Kui mittetühi, siis kasutatakse kehtivuskinnituspäringute (OCSP) puhul juurdepääsutõendit sellest failist, mis on väärtusega määratud, näiteks /path/to/47315.p12d Kui mittetühi, siis peavad mittetühjad olema ka järgnevad seaded.
* jdigidoc.pkcs12.passwd [mittekohustuslik, vaikimisi tühi] juurdepääsutõendi faili parool
* jdigidoc.pkcs12.cert\_serial [mittekohustuslik, vaikimisi tühi] juurdepääsutõendi faili sees asuva sertifikaadi seerianumber (serial number)

Need seaded on mittekohustuslikud, s.t. kui juurdepääsutõendit ei kasutata, siis ei pea neid seadeid lisama, neil on vaikimisi tühjad väärtused.

Juurdepääsutõendi faili sees asuva sertifikaadi seerianumbrit saab leida järgnevalt:

1. Käivitage  
   openssl pkcs12 -info -in 47315.p12d  
   Kuvatakse 2 sertifikaati (üks on välja antud juurdepääsutõendi saajale, teine on juurdepääsutõendi väljaandja ehk Sertifitseerimiskeskuse enda sertifikaat) ja 1 privaatvõti.
2. Valige õige sertifikaat ja salvestage see eraldi faili, seejärel käivitage:  
   openssl x509 -text -in my\_file.crt  
   Otsige väljundist „Serial Number“ väärtust.

NB! DHS rakenduse käivitumisel ei kontrollita juurdepääsutõendi korrektsust. Kui juurdepääsutõendiga on probleem, siis see tuleb välja alles esimesel kasutaja poolt rakenduses sooritataval tegevusel, mis on seotud id-kaardiga või digiallkirjaga (vt. peatükid 10.3 ja 10.4). Seega peate ise jälgima, millal juurdepääsutõend aeguma hakkab.

* + 1. DigiDocService ühendamiseks vajalike HTTPS sertifikaatide lisamine

Kui Mobiil-ID on sisse lülitatud (vt. peatükk 5.1 seade mobile-id.service-name), siis Mobiil-ID tegevuste puhul tehakse päringuid DigiDocService veebiteenusele aadressil https://digidocservice.sk.ee (või testteenusele aadressil https://www.openxades.org:8443). Antud HTTPS sertifikaadid on signeeritud Sertifitseerimiskeskuse poolt, mille juursertifikaadid ei ole Java’ga kaasas, seega vaikimisi HTTPS ühendused nimetatud aadressidele ebaõnnestuvad veaga *SSLHandshakeException: javax.net.ssl.sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target*.

Selleks, et HTTPS ühendused nimetatud aadressidele õnnestuksid, tuleb lisada vajalikud sertifikaadid usaldatud sertifikaatide hulka:

1. Laadida alla failid http://www.sk.ee/upload/files/KLASS3-SK.PEM.cer ja http://www.sk.ee/upload/files/KLASS3-SK\_2010.pem
2. Käivitada käsud

keytool -v -importcert -keystore /home/dhs/tomcat/truststore.jks -alias mykey1 -file KLASS3-SK.PEM.cer

keytool -v -importcert -keystore /home/dhs/tomcat/truststore.jks -alias mykey2 -file KLASS3-SK\_2010.pem

parooliks sisestada changeit

Fail truststore.jks võib eelnevalt olemas olla peatükk 4 alapeatükk Tomcat punkt 5 tegevuse tulemusena. Kui fail truststore.jks ei ole eelnevalt olemas, siis keytool käsk loob selle ise.

1. Kontrollida, et Tomcat käivitusskriptis /home/dhs/tomcat/tomcat.sh oleks Java käivitusargumentide hulgas olemas -Djavax.net.ssl.trustStore=truststore.jks

### CAS rakenduse seadistamine

CAS rakenduse seadistusfail on cas-config.properties ning see peab asuma CAS rakenduse classpath’i juurkaustas. Võtke juhendiga kaasasolev näidisfail cas-config.properties ning paigutage see asukohta /home/dhs/tomcat/lib/cas-config.properties ning muutke selle sisu. Vaadake üle kõik järgnevad seaded ja vajadusel tehke muudatusi (failis sees on samuti kõikide nende seadistusparameetrite kohta olemas näiteväärtused ja selgitavad kommentaarid):

* kerberos.conf viitab operatsioonisüsteemis paigaldatud Kerberos klienttarkvara konfiguratsioonifailile, näiteks /etc/krb5.conf . Kerberos protokolli kaudu kasutajate autentimise korrektseks toimimiseks peavad CAS rakenduse masinas olema tehtud peatükk 4 alampeatükis Kerberos kirjeldatud tegevused.
* kerberos.kdc viitab Active Directory serverile ja pordile, mida kasutada Kerberos protokolli kaudu kasutajate autentimiseks, näiteks fw.viljandimaa.ee:88
* kerberos.realm viitab Active Directory serveris olevale Windows domeeni täispikale nimetusele, kirjutada suurtähtedega, näiteks VILJANDI.MAAVALITSUS . NB! Siin olev domeeni Domeeni nimetus peab kindlasti olema täispikk ja kindlasti olema kirjutatud suurtähtedega. Näiteks kuigi kasutajad võivad saada Windowsisse autentida ka lühema domeeniga VILJANDI\username (ja ka LDAP ligipääsul võib töötada kasutajanime lõpus lühem domeen (CAS seade ldap.userDn, DHS seade ldap.synchronization.java.naming.security.principal)), siis siin peab Kerberos autentimise jaoks kindlasti olema täispikk domeeni nimi VILJANDI.MAAVALITSUS, muidu autentimine ebaõnnestub. Samuti, kui täispikk domeeni nimi peab olema kirjutatud suurtähtedega, muidu autentimine ebaõnnestub.
* kerberos.principal viitab Active Directory serveris loodud SPN nimetusele (peab olema sama mis peatükis 8.2.c määratud väärtus), vajalik selleks et Single Sign-On töötaks, näiteks HTTP/dhs.example.com@VILJANDI.MAAVALITSUS
* kerberos.password viitab eelmise seadega määratud SPN’i kasutaja paroolile Active Directory serveris
* ldap.url viitab Active Directory serverile ja pordile, mida kasutada LDAP protokolli kaudu kasutaja ja gruppide info tõmbamiseks, näiteks ldap://fw.viljandimaa.ee:389
* ldap.userDn viitab Active Directory serveris olevale kasutajanimele, koos domeeniga, näiteks dhs-test@viljandi.maavalitsus
* ldap.password viitab eelmise seadega määratud kasutaja paroolile Active Directory serveris
* ldap.searchBase viitab Active Directory alamosa nimetusele, mille alt kasutajaid otsitakse, näiteks CN=Users,DC=viljandi,DC=maavalitsus
* ldap.mapToAttribute viitab Active Directory serveris kasutajate info all oleva välja nimetusele, millele on sisestatud isikukood, näiteks pager
* jdigidoc.ocsp.enabled peab olema kas false või true. True kasutada siis, kui soovitakse et igal ID-kaardiga autentimisel tehtaks ID-kaardi sertifikaadi kontrollimiseks kehtivuskinnituspäring (OSCP) vastu Sertifitseerimiskeskuse serverit. False kasutada siis, kui soovitakse, et kehtivuskinnituspäringuid üldse ei tehtaks; siis teisi jdigidoc.\* seadeid ignoreeritakse; siis peab veebiserver (Apache httpd või nginx) olema seadistatud kontrollima ID-kaardi sertfikaadi kehtivust vastu tühistusnimekirjasid (CRL, <http://www.sk.ee/repositoorium/crl/> ). Samuti peab serveri kellaaeg olema korrektne, kuna CAS rakendus ise kontrollib sertifikaatide aegumist.
* jdigidoc.test peab olema kas false või true. False kasutada toodangkeskkonnas, kus kehtivuskinnituspäring (OSCP) tuleb teha vastu Sertifitseerimiskeskuse serverit. True kasutada testkeskkonnas, kus kehtivuskinnituspäring tuleb teha vastu OpenXAdES testserverit. Kui kasutada false, siis test ID-kaarte ei saa ID-kaardiga autentimisel kasutada.
* idcard.authurl viitab URL’ile, mida kasutatakse ID-kaardiga autentimise lingiks. Sellel URL’il peab olema Apache httpd või nginx seadistatud nõudma kliendi brauserilt ID-kaarti, näiteks https://dhs.example.com:4443
  + 1. ID-kaardiga autentimise kehtivuskinnituspäringud juurdepääsutõendi alusel

Kui soovite, et ID-kaardi autentimise OCSP päringud tehtaks juurdepääsutõendi alusel, siis lisage seadistusfaili järgnevad seaded:

* jdigidoc.pkcs12.container
* jdigidoc.pkcs12.passwd
* jdigidoc.pkcs12.cert\_serial

Seadete kirjeldus on sama, mis peatükis 5.1.1. Välja arvatud asjaolu, et cas-config.properties seadistusfailis on need seaded kohustuslikud, s.t. kui juurdepääsutõendit ei kasutata, siis tuleb need seaded lisada tühjade väärtustega.

### DHS rakenduse seadistamine klastris

Selleks, et kasutada kahte DHS rakenduse instantsi klastris, on vajalik:

1. Tagada, et mõlemal rakendusserveril on sünkroniseeritud sama kellaaeg.
2. Määrata mõlema rakenduse paigalduse juures alfresco-global.properties failis  
   alfresco.cluster.name=minginimi  
   Väärtuse sisu ei ole oluline, kontrollitakse ainult seda kas väärtus on tühi või mittetühi.
3. Määrata mõlema rakenduse paigalduse juures alfresco-global.properties failis dir.root.shared viitama kaustale, mis on mõlema rakenduse peale ühine.
4. Määrata mõlema rakenduse paigalduse juures alfresco-global.properties failis dir.root.local viitama kaustale, mis on kummagi rakenduse kohta eraldi.
5. Ühe rakenduse paigalduse juures peavad taustatööd olema sisse lülitatud (vaikimisi on); teise rakenduse paigalduse juures peavad taustatööd olema välja lülitatud, selleks peab teise rakenduse paigalduse juures lisama faili alfresco-global.properties rea  
   jobs.enabled=false
6. Selleks, et toimuks EHCache replitseerimine kahe rakendusserveri vahel, on vaja mõlema rakenduse paigalduse juures kopeerida SVN’ist fail delta/common/etc/ehcache-custom.xml.sample.cluster failiks tomcat/lib/alfresco/extension/ehcache-custom.xml
7. Mõlema rakenduse paigalduse juures asendada failis ehcache-custom.xml kõik "otherserver" teksti esinemised teise klastri rakendusserveri domeeninimega või IP aadressiga. Vaikimisi TCP pordiks ehcache suhtlusel on pandud 40001.
8. EHCache replitseerimise õnnestumise kontrollimiseks peab sisse lülitama täiendavat logimist – lisama faili tomcat/lib/alfresco/extension/dev-log4j.properties rea  
   log4j.logger.net.sf.ehcache.distribution=debug
   1. Kui EHCache replitseerimine õnnestub, siis tuleb rakenduse töötamise ajal logisse sarnaseid teateid:  
      *DEBUG [net.sf.ehcache.distribution.RMICachePeer] Remote remove received for key ...  
      DEBUG [net.sf.ehcache.distribution.RMICachePeer] Remote put received...*
   2. Kui EHCache replitseerimisel ei ole teine rakendusserver kättesaadav, siis tuleb logisse sarnaseid teateid:  
      *DEBUG [net.sf.ehcache.distribution.ManualRMICacheManagerPeerProvider] Looking up rmiUrl //otherserver:40001/...Cache through exception Connection refused to host: otherserver; nested exception is:  
       java.net.ConnectException: Connection refused. This may be normal if a node has gone offline. Or it may indicate network connectivity difficulties  
      java.rmi.ConnectException: Connection refused to host: otherserver; nested exception is:  
       java.net.ConnectException: Connection refused*

NB! Rakenduse uue versiooni paigaldamisel peab toimima järgmiselt:

1. Mõlemas rakendusserveris peab rakendused peatama
2. Uut rakenduse versiooni ei tohi samal ajal mõlemas rakendusserveris käivitada, vaid peab kõigepealt käivitama ühes rakendusserveris uue versiooniga rakenduse ning ootama selle eduka käivitumise lõpuni. Pärast seda saab käivitada teises rakendusserveris uue versiooniga rakenduse.

## Rakenduse paigaldamine

1. Kui Tomcat rakendusserver töötab, siis esmalt seisake Tomcat: /home/dhs/tomcat/tomcat.sh stop  
   Seiskamine on vajalik seepärast, et DHS rakendus ei toeta undeploy’mist/redeploy’mist – uue versiooni paigaldamiseks (või mingil muul põhjusel rakenduse (uuesti) käivitamiseks) peab eelnevalt Tomcat rakendusserveri seiskama! Üheks põhjuseks on see, et rakenduse mahukuse tõttu võib redeploy ilma serverit seiskamata (vana versiooni otsa deploytakse uus versioon nii et server kogu aeg töötab) tekitada vea OutOfMemoryError: PermGen space, mis tuleneb levinud Java EE rakenduste probleemist, kus paljud teegid jätavad undeploy järel osa ressursse PermGen mälualasse alles.
2. Kui tegemist on versioonivahetusega, siis teostada andmete varundamine (vt. peatükk 7).
3. Kui tegemist on versioonivahetusega, siis paigaldatava DHS rakenduse versiooninumber peab olema sama või suurem, kui oli sama andmebaasi ja andmekausta peal varem käivitatud DHS rakenduse versiooninumber. Vastasel juhul vt. peatükk 6.2.
4. Kui tegemist on versioonivahetusega (s.t. Tomcat’is on varem paigaldatud dhs.war), siis kustutage eelneva paigaldusega seotud kõik failid:  
   cd /home/dhs/tomcat  
   dhs.war versioonivahetuse puhul:  
   rm -rf webapps/dhs webapps/dhs.war work/Catalina/localhost/dhs temp/Alfresco  
   cas.war versioonivahetuse puhul:  
   rm -rf webapps/cas webapps/cas.war work/Catalina/localhost/cas   
   Kui mõned vanad failid alles jäävad, siis teatud juhtudel on oht, et Tomcat jääb mõnda vana faili kasutama.
5. Kui dhs.war ja/või cas.war failinimi ei ole täpselt sellisel kujul (näiteks on dhs-2.1.1.46.war vms), siis nimetada failid ümber et nimi oleks kujul dhs.war ja cas.war
6. Paigutage dhs.war ja/või cas.war fail kataloogi /home/dhs/tomcat/webapps/
7. Kui tegemist on versioonivahetusega ja kaasa on tulnud eraldi juhend versiooni­vahetusega seotud tegevuste kohta, siis teostage need tegevused.
8. Käivitage Tomcat rakendusserver: /home/dhs/tomcat/tomcat.sh start
9. Kui tegemist on versioonivahetusega ja DHS rakenduse uus versioon mingi vea tõttu ei käivitu ning on vaja minna tagasi eelmisele versioonile, siis:
   1. Järgida käesoleva peatüki punkte 1-2.
   2. Taastada varukoopiast DHS rakenduse andmed, mida kasutati eelmise versiooni või sellest vanema versiooni ajal (vt. peatükk 7.3). See on vajalik, sest versiooni uuendamise käigus võidi muuta olemasolevaid andmeid ning selle tõttu ei ole vanemale versioonile tagasi minek toetatud kui andmed on uuendatud (või andmete uuendamist on alustatud).
   3. Järgida käesoleva peatüki punkte 4-9.

### Rakenduse seire [DHS 3.6 versioonis puudub]

Rakenduse seireks HTTP kaudu on loodud lehekülg https://dhs.example.com/dhs/service/monitor - see URL vastab HTTP staatusega 200 OK ning väljastab mitmesugust infot XML kujul. Kui DHS rakendus on klastris, siis tuleb jälgida iga rakendusserveri seirelehekülge eraldi, sest seirelehekülg väljastab ainult konkreetse rakendusserveri kohta infot.

DHS rakenduse kasutajaliidese URL’id ei ole seireks sobivad, sest suunavad (302 Moved Temporarily) CAS rakenduse lehele, kuna ei olda sisselogitud.

### Rakenduse viimine madalamale versioonile

Kui on alustatud DHS rakenduse mingi versiooni Y käivitamist, siis sellest väiksema numbriga versiooni X enam ei tohi käivitada sama andmebaasi ja andmekausta peal. Selle kohta teeb DHS rakendus käivitumisel ka kontrolli, aga see kontroll toimub ainult juhul kui versioon Y varem käivitus edukalt. Aga kui alustati DHS rakenduse mingi versiooni Y käivitamist ja see ebaõnnestus, ning siis käivitati sellest väiksema numbriga versioon X, siis kirjeldatud kontrolli ei toimunud. Seega kuigi kirjeldatud juhul DHS rakenduse poolne kontroll puudub, siis sellest olenemata ei tohi väiksema numbriga versiooni käivitada.

Väiksema numbriga versiooni X käivitamiseks peab taastama varukoopiast DHS rakenduse andmed, mida kasutati versiooni X või sellest vanema versiooni ajal (vt. peatükk 6 punkt 9).

## Varundamine

Varukoopia tuleb teha samal ajal nii andmebaasist kui ka DHS rakenduse andmete kaustast /home/dhs/data (ainult teatud alamkaustad) ning neid tuleb säilitada üksteisega koos.

Vt. ka varundamise originaaljuhend:

http://wiki.alfresco.com/wiki/Backup\_and\_Restore#Backing\_up\_the\_File\_system

### Kuumvarundamine (hot backup)

Kuumvarundamist tehakse samal ajal kui DHS rakendus töötab. Kuumvarundamine peab kindlasti toimuma sellises järjestuses:

1. DHS rakendus teeb igal öösel kell 03:00 lucene-indexes kaustast ise koopia kausta backup-lucene-indexes, seega peab järgnevate punktide teostamine toimuma hiljem, näiteks kell 04:00.
2. Teha varukoopia andmebaasist (täpsemalt vt. peatükk 7.4).
3. Kui andmebaasi varundamine on lõppenud, siis teha varukoopia järgmistest data (dir.root / dir.root.shared / dir.root.local parameetritega viidatavate kaustade) alamkaustadest:
   1. shared/audit.contentstore
   2. local/backup-lucene-indexes
   3. shared/contentstore
   4. shared/contentstore.deleted
   5. shared/updater

Varukoopiat ei tohi teha järgmistest data alamkaustadest:

* 1. local/lucene-indexes
  2. local/oouser

### Külmvarundamine (cold backup)

Külmvarundamist tehakse siis, kui DHS rakendus on seisatud. Külmvarundamise puhul tegevuste järjekord ei ole oluline, teostada tuleb:

1. DHS rakendus peab olema seisatud.
2. Teha varukoopia andmebaasist (täpsemalt vt. peatükk 7.4).
3. Teha varukoopia järgmistest data (dir.root / dir.root.shared / dir.root.local parameetritega viidatavate kaustade) alamkaustadest:
   1. shared/audit.contentstore
   2. local/lucene-indexes
   3. local/backup-lucene-indexes
   4. shared/contentstore
   5. shared/contentstore.deleted
   6. shared/updater

Varukoopiat ei tohi teha järgmistest data alamkaustadest:

* 1. local/oouser

1. DHS rakenduse võib käivitada.

### Varukoopiast taastamine

1. DHS rakendus peab olema seisatud.
2. Liigutage olemasolevad data kaustad (dir.root / dir.root.shared / dir.root.local parameetritega viidatavad kaustad) teise nimega või teise kohta.
3. Taastage varukoopiast data kaustade sisu.
4. Kui tegemist oli kuumvarukoopiaga, siis nimetage backup-lucene-indexes kaust ümber lucene-indexes kaustaks. Kui tegemist oli külmvarukoopiaga, siis ei ole vaja midagi ümber nimetada.
5. Taastage varukoopiast andmebaasi sisu (täpsemalt vt. peatükk 7.5).
6. Käivitage DHS rakendus.

### Andmebaasist varukoopia tegemine

Teha andmebaasist varukoopia faili järgmise vahendiga (nurksulgudega sõnad asendada reaalsete väärtusega, mis viitavad andmebaasile ja tekitatavale väljundfailile; andmebaasi külge ühendamiseks saab kasutada sama kasutajanime, mida DHS rakendus kasutab):

pg\_dump -f <dumpfile> -F c -b -h <hostname> -p <port> -U <username> <dbname>

Ning tekkinud väljundfail kaasata varundatavate failide hulka.

(pg\_dump vahendi kohta on täpsemalt kirjutatud PostgreSQL ametlikus juhendis peatükis „SQL Dump“.)

Kui pg\_dump küsib andmebaasiga ühendamisel parooli, siis parooli küsimist saab vältida .pgpass faili abil nagu on kirjeldatud PostgreSQL ametlikus juhendis peatükis „The Password File“.

### Andmebaasi taastamine varukoopiast

Enne andmebaasi taastamist tuleb luua tühi andmebaas (vt. peatükk 4 alampeatükk „PostgreSQL“ punkt 2). Kui soovitud nimega andmebaas eksisteerib, siis enne tuleb vana andmebaas ümber nimetada (ALTER DATABASE <dbname> RENAME TO <olddbname>;) või kustutada (DROP DATABASE <dbname>;) ja siis luua tühi andmebaas.

Varundatud andmebaasi failist taastada andmebaasi sisu järgmise vahendiga (nurksulgudega sõnad asendada reaalsete väärtusega, mis viitavad andmebaasile ja olemasolevale sisendfailile; andmebaasi külge ühendamiseks saab kasutada sama kasutajanime, mida DHS rakendus kasutab):

pg\_restore -d <dbname> -h <hostname> -p <port> -U <username> <dumpfile>

(pg\_restore vahendi kohta on täpsemalt kirjutatud PostgreSQL ametlikus juhendis peatükis „SQL Dump“.)

Kui pg\_restore küsib andmebaasiga ühendamisel parooli, siis parooli küsimist saab vältida .pgpass faili abil nagu on kirjeldatud PostgreSQL ametlikus juhendis peatükis „The Password File“.

## Active Directory serveri seadistamine

1. Selleks, et DHS ja CAS rakendused saaks tõmmata kasutajate ja gruppide infot Active Directory serverist, on vaja AD serveris luua kasutajakonto, mille kaudu DHS ja CAS rakendused infole ligi pääsevad:
   1. Luua kasutajakonto dhs-test
   2. Parooli võib panna suvalise genereeritud pika sümbolite jada
   3. Määrata kasutajakontol *Password never expires*
2. Selleks, et töötaks Single Sign-On autentimine, on vajalik eelmises punktis loodud kasutajakontole teha järgmised tegevused:
   1. Veenduda, et Windows Server 2003 on vähemalt Service Pack 2 peal. Paigaldada Windows Support Tools, mis ise peab ka olema vähemalt Service Pack 2. Windows Server 2008 puhul on ktpass tööriist olemas ning Windows Support Tools paigaldada vaja ei ole.
   2. cd C:\Program Files\Support Tools
   3. ktpass /out dhs-test.keytab /princ HTTP/dhs.example.com@VILJANDI.MAAVALITSUS /pass \* /mapuser dhs-test@VILJANDI.MAAVALITSUS /ptype KRB5\_NT\_PRINCIPAL /crypto RC4-HMAC-NT  
      Siin määratud dhs.example.com asemel tuleb panna domeeninimi, mida kasutaja brauseri aadressireal kasutama hakkab CAS rakendusse sisenemiseks.  
      Siin määratud HTTP peab olema HTTP, kuigi reaalne protokoll CAS’ile ligipääsemiseks on HTTPS.  
      Siin määratud VILJANDI.MAAVALITSUS peab kindlasti olema Active Directory domeeni täispikk nimetus; näiteks kuigi kasutajad võivad saada Windowsisse autentida ka lühema domeeniga VILJANDI\username (ja ka LDAP ligipääsul võib töötada kasutajanime lõpus lühem domeen (CAS seade ldap.userDn, DHS seade ldap.synchronization.java.naming.security.principal)), siis siin peab Kerberos autentimise jaoks kindlasti olema täispikk domeeni nimi VILJANDI.MAAVALITSUS, muidu autentimine ebaõnnestub.  
      Kui küsitakse parooli, sisestage suvaline parool.
   4. Teha kasutajale dhs-test *Reset Password* ja määrata parooliks uuesti sama mis punktis 1.b
   5. dhs-test.keytab vaja ei lähe, selle võib kustutada.
   6. DHS ja CAS serverite ja klientarvutite kellad peaksid olema mitte rohkem kui 5 minutise erinevusega Active Directory serveri kellast! Vastasel juhul Kerberos autentimine ei tööta.

## Kasutaja arvuti seadistamine

### ID-kaart

ID-kaardiga sisselogimise ning digiallkirjastamise jaoks peavad olema kasutaja arvutis paigaldatud uusimad ID-kaardi draiverid.

Digiallkirjastamine on toetatud ainult Windows operatsioonisüsteemis ning ainult Internet Explorer ja Mozilla Firefox brauseries.

### DHS’is failide üleslaadimine

DHS’is toimub failide üleslaadimine Java applet’i kaudu. Selleks peab kasutaja arvutis olema paigaldatud uusim Sun JRE (Java Runtime Environment).

### DHS’is failide avamine muutmiseks (Microsoft Word’i või OpenOffice.org kaudu WebDAV protokolliga)

Selleks et Microsoft Wordis töötaks korrektselt failide avamine DHS’ist WebDAV protokolli kaudu, peavad kasutaja arvutis olema täidetud järgnevad nõuded:

1. DHS serveri URL (https://dhs.example.com) peab olema kasutaja arvutis Internet Exploreri seadetes Trusted Sites nimekirjas. Selleks tuleb:
   1. Käivita Internet Explorer
   2. Mine *Tools* -> *Internet Options* -> *Security*
   3. Vali *Trusted sites*, vajuta *Sites*
   4. Sisesta https://dhs.example.com ja vajuta *Add*
   5. Vajuta *Close*, *OK*
2. DHS serveri HTTPS sertifikaat peab olema kasutaja arvutis usaldatud Internet Exploreri poolt
   1. Lahendus 1: Signeerida DHS serveri HTTPS sertifikaat usaldatud juursertifitseerija poolt.
   2. Lahendus 2: Kui DHS serveri HTTPS sertifikaat on signeeritud juursertifitseerija poolt, mis ei ole kasutaja arvutis usaldatud, siis paigaldada see juursertifikaat kasutaja arvutis Internet Explorer brauserisse (näiteks Andmevara puhul http://it.andmevara.ee/avhosting.crt)
   3. Lahendus 3: Paigaldada DHS serveri HTTPS sertifikaat kasutaja arvutis Internet Explorer brauserisse. Selleks tuleb:
      1. Käivita Internet Explorer administraatori õigustes (*Run as Administrator*)
      2. Mine DHS rakenduse lehele, IE peaks ütlema et „*There is a problem with this website’s security certificate.*“, vajuta „*Continue to this website (not recommended).“*, aadressiriba peaks olema punane
      3. Vajuta aadressiriba paremas ääres nupule „*Certificate Error“*, vajuta „*View certificates*“
      4. Vajuta „*Install Certificate...“* ja „*Next >*“
      5. Vali „*Place all certificates in the following store“* ja vajuta „*Browse...*“
      6. Vali „*Trusted Root Certification Authorities“* ja vajuta „*OK*“
      7. Vajuta „*Next >“* ja „*Finish*“
      8. Küsitakse „*Do you want to install this certificate?“*, vajuta „*Yes*“, vajuta „*OK*“
      9. Vajuta „*OK*“
3. Kui fail avaneb Internet Exploreri akna sees (näiteks Office 2002 puhul), siis tuleks failid panna avanema uues aknas:
   1. Käivita Windows Explorer ja vali *Tools* -> *Folder Options* -> *File Types*
   2. Iga DHS-is muutmiseks avatava faili tüübi kohta (RTF, DOC, DOCX, XLS, XLSX, jne) valida *Advanced* ja eemaldada linnuke *Browse in same window* eest
4. Kui kasutusel on tulemüüre või proxy’sid vms tarkvara (ükskõik kas kohalikus arvutis või kohaliku arvuti ja DHS serveri vahele jäävas võrgus), mis sekkuvad HTTPS liiklusesse, siis peab DHS serveri HTTPS sertifikaat olema usaldatud ka kõikides nendes. Muidu võib tekkida probleeme muutmiseks avatud failide salvestamisel (näiteks MS Word veateade „There has been a network or file permission error. The network connection may be lost.“ või muudatusi ei salvestu või salvestub tühi faili sisu.)

Märkus: faili avamine muutmiseks töötab ainult Internet Explorer 32-bit versiooniga (täpsemalt vaata https://office.microsoft.com/en-us/web-apps-help/system-requirements-for-opening-files-from-office-web-apps-in-office-desktop-applications-HA010378334.aspx). Internet Explorer 64-bit versiooniga toimib funktsionaalsus samamoodi nagu teiste brauseritega – failile klikkides pakutakse seda allalaadimiseks või lugemiseks avamiseks.

Kasutaja arvutis OpenOffice.org / LibreOffice / Apache OpenOffice kaudu DHS rakenduses asuvate failide muutmiseks avamise ja tagasi salvestamise toeks [DHS 3.6 versioonis puudub] peab olema tehtud peatükk 4 alampeatükk nginx punkt 6 ja peatüki 5.1 seade conf.openoffice-client-extensions peab olema mittetühi. Samuti on vajalik kasutaja arvutis paigaldada OpenOffice.org 3.2 või uuem OpenOffice.org / LibreOffice / Apache OpenOffice ning protokoll vnd.sun.star.webdav peab olema registreeritud kasutaja arvutis. Protokolli registreerimiseks saab kasutada tarnega kaasas olevat faili OpenOffice\_WebDAV\_Protocol.reg, milles tuleb korrigeerida rakenduse asukohta.

### Single Sign-On (SSO)

Kui kasutaja on logitud sisse Windowsi domeeni, siis on võimalik Signle Sign-On funktsionaalsus – kui kasutaja läheb DHS rakenduse veebilehele, siis ei näidata talle sisselogimislehte, vaid sisselogimine toimub automaatselt (brauser edastab autentimisvõtmed ning kasutaja näeb juba DHS lehte, kus ta on sisse logitud). Selleks, et Single Sign-On töötaks, tuleb:

1. Kui kasutatakse Internet Explorerit, siis
   1. Tools -> Internet Options -> Advanced -> Enable Integrated Windows Authentication peab olema sisse lülitatud
   2. DHS serveri URL (https://dhs.example.com) peab olema kasutaja arvutis Internet Exploreri seadetes Trusted Sites nimekirjas – sama mis punkt 9.3.1
   3. *Tools* -> *Internet Options* -> *Security* -> *Trusted sites* -> *Custom level* -> *User authentication* -> *Logon* valikuks peab olema *Automatic logon with current user name and password*
2. Kui kasutatakse Mozilla Firefox brauserit, siis
   1. about:config parameetrite nimekirjas tuleb network.negotiate-auth.trusted-uris parameetri väärtuseks panna dhs.example.com

### E-mailide liidestus (IMAP)

Selleks, et kasutaja saaks e-maile lohistada postkastist DHS’i, tuleb kasutaja arvutisse paigaldatud Microsoft Outlook 2007 seadistada vastavalt dokumendis „Administraatori juhis“ toodud peatükile „Outlooki seadistamine“.

### PDF’ide kuvamine veebilehe sees

E-arve juures on võimalus kuvada PDF faili veebilehe sees. Selleks peab olema kasutaja arvutis paigaldatud brauserisse PDF lugeja plugin.

Kui brauseris PDF lugeja pluginat ei ole paigaldatud, siis PDF faili veebilehe sees kuvamise asemel pakutakse PDF faili allalaadimiseks.

Kui soovitakse PDF faili veebilehe sees kuvamiseks kasutada Adobe Reader PDF lugejat, siis peab selle paigaldama kasutaja arvutisse. Adobe Reader 10 paigaldamisel paigaldatakse PDF lugeja plugin nii Internet Explorer kui ka Firefox brauserite jaoks automaatselt ning vaikimisi on Adobe Reader seadetes sisse lülitatud *Display PDF in browser* seade.

### Osakonna töödokumendid lingi avamine Firefox’is

DHS rakenduses oleva lingi „Osakonna töödokumendid“ saab viitama panna soovitud URL’ile (URL võetakse parameetri workingDocumentsAddress väärtusest). Kui etteantav URL viitab kohalikule või võrguressurssile (kujul file://///servername/share/ ), siis Internet Explorer avab sellise lingi edukalt, aga Firefox vaikeseadetega selliseid linke ei ava (lingile klikkides ei juhtu mitte midagi, veateadet ei tule, jäädakse samale lehele). Selleks, et Firefox avaks selliseid linke, peab kasutaja arvutis Firefox’is selle lubama vastavalt http://kb.mozillazine.org/Links\_to\_local\_pages\_do\_not\_work kirjeldatud juhistele (Firefox’i seadetes määratava väärtuse http://www.example.com asemel kasutada DHS rakenduse URL’i algust kujul https://dhs.example.com ).

## Probleemid

### Veateade „ObjID already in use“ või “java.net.UnknownHostException: basename”

Kui DHS rakenduse käivitamine ebaõnnestub veateatega

*java.rmi.server.ExportException: internal error: ObjID already in use*

või veateatega

*java.net.UnknownHostException: basename*

siis peaks kontrollima, et masina täisdomeeninimi (FQDN) vastaks tema võrguliidese IP aadressile ja vastupidi.

* Kontrollige, et käsu „hostname -f“ väljastatud domeeninimi lahenduks IP aadressiks, mis on masina küljes oleval võrguliidesel.
* Kontrollige, et sama IP aadress lahenduks tagasi „hostname -f“ väljastatud domeeninimeks.

### Andmekausta ja andmebaasi sisu mittevastavus

Kui DHS rakenduse käivitamine ebaõnnestub ja veateadetes esineb mõni järgnevatest:

*SISU TERVIKLIKKUSE VIGA: Hoidla indekseid X ei leitud.*

*SISU TERVIKLIKKUSE VIGA: Sisu hoidlas ei leitud süsteemset sisu.*

*Veendu, et ’dir.root=/home/dhs/data’ tunnus osutab andmete õigele kohale.*

siis peaks kontrollima, et andmekausta ja andmebaasi sisu vastaksid üksteisele. DHS rakenduse haldamisel tuleb pidada meeles seda, et andmebaasi sisu (rakenduse seadistusfailis db.\* seadetega viidatud) ja andmekataloogi sisu (dir.root seadega viidatud) käivad üksteisega koos. Sellest lähtuvalt tuleb järgida järgnevaid põhimõtteid:

* Varundamisel tuleb varundada mõlemat korraga – nii andmebaasi kui ka andmekausta sisu.
* Kui soovitakse rakenduse andmed kustutada (nullist alustada), siis tuleb mõlema sisu korraga kustutada; kui kustutada üks, aga mitte teine, tuleb ülalmainitud veateade.

### Veateade „Illegal key size“

Kui DHS serveris ei ole Sun JDK juurde paigaldatud Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6, siis esimene kord kui rakenduses üritatakse sooritada tegevust, mis on seotud digiallkirjastamisega, tuleb rakenduse logisse veateade  
*java.io.IOException: exception decrypting data - java.security.InvalidKeyException: Illegal key size*  
ning sõltuvalt sellest, mis see esimene tegevus oli:

* Kui esimeseks tegevuseks oli, et kasutaja üritas digiallkirjastada, siis digiallkirjastamine ebaõnnestub ja kasutajale tuleb veateade: *Allkirjastamine ebaõnnestus: ERROR: 67 ERROR: 67java.io.IOException; nested exception is: java.io.IOException: exception decrypting data - java.security.InvalidKeyException: Illegal key size*
* Kui esimeseks tegevuseks oli sisenemine sellise dokumendi ekraanile, mille failide blokis sisaldub .ddoc fail, siis kasutajale veateadet ei kuvata, vaid .ddoc faili detailinfot ei näidata.

Järgnevate digiallkirjastamisega seotud tegevuste puhul tulevad juba teistsugused veateated, aga reaalne viga on ikkagi käesolevas probleemis.

### Ebasobiv juurdepääsutõend digiallkirjastamiseks

Kui digiallkirjastmiseks kasutatakse juurdepääsutõendit ja Sertifitseerimiskeskuse server keeldub OCSP päringust (näiteks on juurdepääsutõend aegunud), siis kasutajale kuvatakse digiallkirjastamisel, pärast PIN2 sisestamist, veateade: Allkirjastamine ebaõnnestus: OCSP response unsuccessful!

Rakenduse logisse tuleb samuti veateade: ERROR: 69 - OCSP response unsuccessfull!

### Veateade „OutOfMemoryError“

Kui rakenduse töö ajal tekib OutOfMemoryError, siis kindlasti peab koheselt Java virtuaalmasinat restartima, s.t. Tomcat’i sulgema ning uuesti käivitama – muidu võib rakendus jääda vigasesse seisu! Selle jaoks on tungivalt soovitav seadistada Java virtuaalmasina poolt fataalse vea puhul käivitatav skript, mis teavitaks süsteemiadministraatorit ning teeks Tomcat’i automaatse taaskäivitamise – vt. peatükk 4, alampeatükk Tomcat, punkt 7.

### Enne DHS-i sisselogimist kuvab Internet Explorer kasutajanime-parooli küsimise akna

Kui soovitakse siseneda DHS rakendusse, minnakse Internet Exploreris aadressile https://dhs.example.com ning Internet Explorer kuvab eraldi kasutajanime-parooli küsimise akna, siis on teostamata punkt 9.3.1 (DHS URLi lisamine Internet Exploreris Trusted Sites nimekirja). Kui see punkt teostada, siis Internet Explorer ei kuva eraldi kasutajanime-parooli küsimise akent. Infoks: selles aknas kasutajanime ja parooli sisestamisest ei ole kasu, pärast seda akent kuvatakse ikkagi tavapärane CAS rakenduse sisselogimisleht.

### Microsoft Office 2002 avab WebDAV kaudu faili kirjutuskaitsega (*read-only*) kui failinimes on täpitähti

Kui kasutaja arvutis on paigaldatud Microsoft Office 2002 ja DHS rakenduses avatakse muutmiseks fail, mille nimes esineb mitte-ASCII sümboleid, siis avaneb fail kirjutuskaitsega ning failis tehtavaid muudatusi ei ole võimalik DHS-i tagasi salvestada. Kui failinimi koosneb ainult ASCII sümbolitest, siis avaneb fail muutmiseks ning muudatused on võimalik DHS-i tagasi salvestada. Lahenduseks on kasutaja arvutis Microsoft Office uuendamine Office 2003 või uuema peale.

### E-mailide liidestuse (IMAP) kaudu kirja lohistamisel DHS’i tekib kirja sisu asemel fail winmail.dat

DHS toetab e-maile vormingutes „Plain Text“ ja „HTML“. Alates DHS versioonidest 3.6.29.10, 3.11.26.5, 3.13.11.3 on toetatud ka e-mailid vormingus „Rich Text“ ning winmail.dat faili ei teki.

### Dokumendi väljasaatmisel veateade „Dokumendi välja saatmine ebaõnnestus!“

Kui dokumendi väljasaatmisel tuleb veateade „Dokumendi välja saatmine ebaõnnestus!“ ning kui DHS rakenduse logis on veateade *com.sun.mail.smtp.SMTPSendFailedException: 552 4.3.1 Message size exceeds fixed maximum message size* (teate täpne sõnastus võib sõltuvalt e-maili serverist erineda), siis see tähendab et e-maili server keeldub sellise suurusega kirja edastamast. Palun järgida punktis 5.1 alampunkti mail.host juures kirjeldatud juhiseid.

### DHS rakenduses tegevused hanguvad

Kui DHS rakenduses tegevused hanguvad (jäävad pikaks ajaks ootama ja ei lõpe edukalt), siis peab kontrollima järgnevat:

1. Kas OpenOffice.org protsess (soffice) on kokku jooksnud (näiteks võtab 100% CPU pidevalt)? Kui jah, siis peab OpenOffice.org protsessi seiskama ja taaskäivitama samade võtmetega. Soovitav on selle vältimiseks kasutada OpenOffice.org välise monitoorimise skripti (vt. peatükk 4, alampeatükk OpenOffice.org punkt 2).
2. Kas Tomcat Java protsess on kokku jooksnud?
3. Kas PostgreSQL andmebaasiserver on kokku jooksnud?

### DVK kaudu välja saadetud dokumendi staatus ei muutu ning DVK kaudu ei saa vastu võtta andmeid

Kui:

* DVK kaudu välja saadetud dokument jõuab saajale kohale, aga DHS rakenduses näitab antud saatmise staatuseks jätkuvalt “saatmisel”
* DVK kaudu ei tule vastu
* Logi järgi on DVK päringud olnud edukad, veateateid ei ole

Siis peab kontrollima järgmist:

1. Et alfresco-global.properties failis olev seade x-tee.id-code väärtus oleks korrektne (vt. peatükk 5.1 antud seade kirjeldus).
2. Et eelmises punktis viidatud seades määratud isikukood oleks RIA juures vastava DVK keskkonna (toodang või test) juures vastava asutuse kohta lubatud isikukoodide nimekirjas.

Kui antud punktid ei ole täidetud, siis võib esineda järgnev probleem:

* Käesolevast asutuse DHS’ist dokumenti üle DVK saates teise asutusse jõuab dokument teise asutusse kohale, aga käesoleva asutuse DHS’is jääb saatmisel staatusesse.
* Teisest asutusest saates dokumenti üle DVK käesoleva asutuse DHS’i ei jõua dokument käesoleva asutuse DHS’i kohale.

RIA kinnitas (seisuga 04.05.2011), et teatud DVK päringud ei toimi kui isikukood on mittelubatud: receiveDocuments, markDocumentsReceived, getSendStatus, changeOrganizationData. Sel juhul tagastavad need päringud tühja vastuse, mitte veateate. Järelikult ülejäänud päringud (näiteks sendDocuments jm) töötavad mittelubatud isikukoodiga.

### Mobiil-ID tegevused ebaõnnestuvad, kuna HTTPS sertifikaat pole usaldatud

Kui Mobiil-ID tegevusel tuleb DHS kasutajaliideses veateade “Viga Sertifitseerimiskeskuse DigiDocService teenuse poole pöördumisel!” ning kui DHS rakenduse logis on selle kohta veateade *SSLHandshakeException: javax.net.ssl.sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target*, siis see tähendab et DigiDocService teenuse HTTPS sertifikaat pole usaldatud. Palun järgida peatükis 5.1.2 kirjeldatud juhiseid.

### Mobiil-ID tegevused ebaõnnestuvad, kuna teenuse nimetus on ebakorrektne

Kui Mobiil-ID tegevusel tuleb DHS kasutajaliideses veateade „Allkirjastamine ebaõnnestus: Telefoninumber mittekorrektsel kujul.“ ning sisestatud telefoninumber on kindlasti korrektsel kujul (5123456 või +3725123456), siis on alfresco-global.properties failis oleva seade mobile-id.service-name väärtus ebakorrektne. (DHS rakendus kuvab kasutajaliideses sellist veateadet, kuna ei ole võimalik eristada, millised DigiDocService teenuse päringu sisendiks antud andmed on ebakorrektsed.) Palun järgida peatükis 5.1 seade mobile-id.service-name juures kirjeldatud juhiseid.

### Osakonna töödokumendid link ei avane Firefox’is

Kui DHS rakenduses oleval lingil „Osakonna töödokumendid“ Firefox’iga klikkides ei juhtu mitte midagi, veateadet ei tule ja jäädakse samale lehele, siis palun järgidda peatükis 9.7 kirjeldatud juhiseid.

### CAS rakenduses kasutajanime ja parooliga autentimine ebaõnnestub; DHS rakenduses IMAP kaudu (Outlookist) kasutajanime ja parooliga autentimine ebaõnnestub

Kui muid veateateid ei ole ning ollakse kindel, et sisestatud kasutajanimi ja parool on korrektsed, siis kontrollida, et DHS rakenduses ja CAS rakenduses oleks seadega kerberos.realm viidatud Active Directory serveris oleva Windows domeeni nimetus kindlasti täispikk, näiteks VILJANDI.MAAVALITSUS . Kuigi näiteks kasutajad võivad saada Windowsisse autentida ka lühema domeeniga VILJANDI\username (ja ka LDAP ligipääsul võib töötada kasutajanime lõpus lühem domeen (CAS seade ldap.userDn, DHS seade ldap.synchronization.java.naming.security.principal)), siis siin peab Kerberos autentimise jaoks kindlasti olema täispikk domeeni nimi VILJANDI.MAAVALITSUS, muidu autentimine ebaõnnestub.

### Hoiatusteade „Error trying to query Open Office version information“

Kui DHS rakenduse logis on hoiatusteade (tavaliselt vahetult või natuke aega pärast käivitamist) „Error trying to query Open Office version information com.sun.star.uno.RuntimeException: com.sun.star.configuration.ConfigurationRegistry: not implemented“, siis on tegemist OpenOffice.org 3.3 versiooniga (OpenOffice.org 3.2 versiooniga sellist hoiatusteadet ei tule). OpenOffice.org 3.3 versiooniga sisuline funktsionaalsus (failide teisendamine) töötab samamoodi nagu OpenOffice.org 3.2 versiooniga, seega ignoreerida antud hoiatusteadet. Lisaks panna tähele, et DHS rakendusega töötavad ainult OpenOffice.org versioonid 3.2.x ja 3.3.x; LibreOffice / Apache OpenOffice versioonid 3.4 ja kõrgemad ei tööta (vt. peatükk 10.17).

### Veateade „OpenOfficeException: connection failed“

Kui DHS rakenduse logis on veateade (tavaliselt vahetult või natuke aega pärast käivitamist) „net.sf.jooreports.openoffice.connection.OpenOfficeException: connection failed: socket,host=localhost,port=8100,tcpNoDelay=1; com.sun.star.lang.DisposedException: java.io.IOException: com.sun.star.io.IOException: EOF reached“, siis on tegemist OpenOffice.org 3.4 või kõrgema versiooniga, mis DHS rakenduses pole toetatud. Kui OpenOffice.org ei ole DHS rakenduse jaoks kättesaadav / töökorras, siis DHS rakendus käivitub ja DHS rakenduses töötab kogu funktsionaalsus, välja arvatud failide sisu teisendamine indekseerimise jaoks, mis tähendab et selliste failide sisudest otsimine ei tööta, mis on lisatud või muudetud või mille dokumenti on muudetud sel ajal kui OpenOffice.org ei olnud DHS rakenduse jaoks kättesaadav / töökorras. Jälgida, et oleks paigaldatud OpenOffice.org versioon, mis on toetatud (vt. peatükk 4) ning et pärast rakenduse käivitamist (tavaliselt mõne minuti jooksul) tuleks logisse teade „The OpenOffice connection was re-established.“.

## Paki ehitamine lähtekoodist

Paki ehitamiseks lähtekoodist peab ehitamist teostavas masinas olema paigaldatud:

* Sun JDK 6 (versioon 1.6.0\_31 või uuem)
* Apache Ant 1.7.0 või uuem
* Apache Maven 3.0 või uuem

Teostada DHS rakenduse ehitamine järgnevalt:

1. Liikuda delta kausta
2. Defineerida järgmised kolm seadet:
   1. Kas käsureal, näiteks punktis 3 toodud käsu puhul:

ant -Dconf.name=smit-test -Dconf.organization.name=default -Dappserver=tomcat clean-all zip

* 1. Või luua fail conf-name.properties millesse lisada iga seade eraldi reale

Defineeritavad seaded (ehituse tulemusena tekkinud war faili sisu sõltub ii ja iii seadetest):

1. conf.name=smit-test

Seade conf.name väärtus viitab etc/conf all olevale kaustale, milles olevaid seadistusfaile kasutatakse andmebaasi ja rakendusserveriga seotud ant käskude puhul.

* + 1. JuM puhul määrata väärtuseks kindlasti jum-example
    2. Teiste puhul ehitustulemused sellest ei sõltu, võib määrata väärtuseks näiteks smit-test

1. conf.organization.name=default

Seade conf.organization.name väärtus viitab etc/conf-organization all olevale kaustale, milles olevaid seadistusfaile kasutatakse ehitamise puhul.

* + 1. SiM/SMIT ja teiste Siseministeeriumi allasutuste puhul (v.a. PPA) määrata väärtuseks kindlasti default
    2. PPA puhul määrata väärtuseks kindlasti ppa
    3. MV puhul määrata väärtuseks kindlasti mv
    4. Justiitsministeeriumi allasutuste puhul määrata väärtuseks kindlasti jum

1. appserver=tomcat

Seade appserver väärtus viitab rakendusserverist sõltuvatele teekide kaustadele (common/lib-${appserver} ja common/lib-dev-${appserver}), milles olevaid faile kasutatakse ehitamise puhul.

1. SiM/SMIT + DHS rakenduse 2.x versiooni puhul määrata väärtuseks glassfish
2. Teiste asutuste või DHS rakenduse uuemate versioonide puhul määrata väärtuseks tomcat
3. Defineerida keskkonnamuutuja ANT\_OPTS="-XX:MaxPermSize=128m"
4. Käivitada ant clean-all zip (kui seaded defineerida käsureal, siis  
   ant -Dconf.name=smit-test -Dconf.organization.name=mv -Dappserver=tomcat clean-all war)
5. Ehituse tulemusena tekib pakk build/delta-X.Y.Z.A.zip mis on ülalmääratud seadete spetsiifiline.

Kui CAS rakendus on muutunud võrreldes viimase pakiga, siis teostada CAS rakenduse ehitamine järgnevalt:

1. Liikuda cas kausta
2. Käivitada mvn clean package
3. Ehituse tulemusena tekkinud fail target/cas.war lisada eraldi tarnitavasse CAS pakki.
4. Lisada eelmises punktis loodud pakki ka näidis konfiguratsioonifailid:
   1. configuration/cas-config.properties
   2. configuration/krb5.conf

## Mitme DHS rakenduse paigaldamine samasse masinasse

1. Paigaldage iga DHS rakenduse jaoks eraldi Tomcat, näiteks

/home/dhs1/tomcat

/home/dhs2/tomcat

jne.

vastavalt peatükk 4 alampeatükile Tomcat. Lisaks peab iga Tomcat’i seadistusfailis tomcat/conf/server.xml määrama erinevad portide väärtused, järgnevatel ridadel:

<Server port="8005" ...

<Connector port="8009" ...

Kui kasutusel on ka HTTP connector (ei ole välja kommenteeritud), siis ka järgneval real:

<Connector port="8080" ...

1. Paigaldage ja seadistage DHS rakendus eraldi igasse Tomcat’i vastavalt peatükkidele 5.1 ja 6. Kuna kõikide asututuse DHS’ide puhul peavad kõik kasutajad saama autentida samamoodi, siis mitte paigaldada CAS rakendust igasse Tomcat’i, vaid eraldi ühte Tomcat’i. Lisaks peab iga DHS rakenduse seadistusfailis alfresco-global.properties määrama erinevad portide väärtused, järgnevatel ridadel:

ooo.port=8100

imap.server.port=1143

alfresco.rmi.services.port=50600

avm.rmi.service.port=50601

avmsync.rmi.service.port=50602

attribute.rmi.service.port=50603

authentication.rmi.service.port=50604

repo.rmi.service.port=50605

action.rmi.service.port=50606

deployment.rmi.service.port=50607

1. Seadistage iga DHS rakenduse jaoks eraldi andmebaas vastavalt peatükk 4 alampeatükile PostgreSQL. Lisaks peab iga DHS rakenduse seadistusfailis alfresco-global.properties määrama erinevad andmebaasi seaded ja samuti erinev andmekausta, järgnevatel ridadel:

db.name=...

(kui erinevad ka teised db.\* seaded, siis need samuti)

dir.root=...