# MV DHS 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 |

## Sissejuhatus

MV DHS on Java EE tehnoloogial põhinev ja Alfresco (Community Edition 3.2 final) põhjal ehitatud dokumendihaldustarkvara.

Käesolev dokument kirjeldab MV DHS tarkvara paigaldamist kliendi testkeskkonda ja on mõeldud kasutamiseks Andmevara administraatoritele.

## Sõnastik

*MV* Maavalitsus

*DHS* Dokumendihaldussüsteem

*MIS* Maajärelmaksu Infosüsteem

*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. Andmevara administraatorid 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 Andmevara administraatorid paigaldavad DHS rakenduse rakendusserverisse.

Rakenduse pakk koosneb:

* DHS paigaldusjuhend
* Näidis konfiguratsioonifailid DHS, CAS, Tomcat jaoks
* DHS rakenduse WAR fail – dhs.war
* Autentimis rakenduse (CAS) WAR fail – cas.war
* MSO teenuse paigaldusjuhend
* MSO teenuse rakenduse failid – mso-service.zip

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 paigaldatakse käesoleva projekti levitusskeemi järgi samasse Tomcat’i rakendusserverisse. Kasutaja arvutist ei pöörduta otse Tomcat’i poole, vaid selle ette proxy-ks paigaldatud Apache httpd 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. Kui DHS rakendus on ligipääsetav lisaks asutuse sisevõrgule ka kusilt avalikust võrgust, siis URLile algusega /dhs/service/ peab piirama ligipääsu! Selle algusega URLile lõppkasutajal ligipääseda vaja ei ole. Sellel URLil asuvad:
  + /dhs/service/adr – Avaliku Dokumendiregistri (ADR) veebiteenus – sellele veebiteenusele on vaja ligi pääseda ainult ADR rakendusel.
* Ülejäänud DHS rakenduse URLidele pääseb ligi ainult autenditult.
* DHS rakenduse pakutavale IMAP teenusele (pordil TCP/143) pääseb ligi ainult autenditult.

Käesolev juhend eeldab, et DHS ja MIS jaoks on kummalegi eraldi Tomcat rakendusserveri instants. Kui DHS (koos selle juurde käiva autentimisrakendusega CAS) paigaldatakse omaette Tomcat’i, siis on see MIS’i 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\_22 või uuem)
  + Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6
* Apache Tomcat 6.0 (versioon 6.0.29 või uuem)
* OpenOffice.org 3 (versioon 3.2.1 või uuem)
* Apache httpd
* Kerberos klienttarkvara

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

* PostgreSQL 8.4 andmebaas (versioon 8.4.5 või uuem) – 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 autentimiseks – aadress ja port (tavaliselt TCP/88) määratavad konfist
* Active Directory server kasutajate/gruppide info tõmbamiseks – aadress ja port (tavaliselt TCP/389) 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 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. Perioodiline restartimine – TODO!

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 serveri kell peab 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/
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 port 4443 peale; vajalik lisada VirtualHost blokist väljapoole ka rida  
      Listen 4443
   3. ProxyPass ja ProxyPassReverse read jäävad samaks, mis eelmisel VirtualHost’il
   4. muuta veel vajalikud read, näiteks logifailide asukohad
   5. seadistada VirtualHost kasutama ID-kaardiga autentimist (juhendi alusena on kasutatud http://code.google.com/p/esteid/wiki/AuthConfApache#Apache\_seadistamine):
      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/files/JUUR-SK.PEM.cer
      5. wget -O "ESTEID-SK.crt" http://www.sk.ee/files/ESTEID-SK.PEM.cer
      6. wget -O "ESTEID-SK 2007.crt" http://www.sk.ee/files/ESTEID-SK%202007.PEM.cer
      7. for f in \*.crt;do ln -sf "$f" $(openssl x509 -hash -noout -in "$f").0; done

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. 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
5. 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
6. 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.
7. 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/"); %>
8. 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. 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.
* 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 viitab OpenOffice.org käivitusfailile.
* 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.
* 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).
* ldap.\* seaded viitavad Active Directory serverile, millelt kasutajate ja gruppide infot tõmbama hakatakse.
  + 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  
    OU=Domain Controllers,DC=viljandi,DC=maavalitsus
  + ldap.synchronization.groupSearchBase viitab Active Directory alamosa nimetusele, mille alt gruppe otsitakse, näiteks  
    OU=Domain Controllers,DC=viljandi,DC=maavalitsus
* 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 – isikukood, mida kasutatakse üle X-tee DVK päringute tegemisel

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
* mso.url viitab MSO veebiteenuse SOAP aadressile. Kui väärtus jätta tühjaks, siis rakendus ei kasuta MSO veebiteenust ja samad tegevused teostatakse OpenOffice abil.
  + 1. Digiallkirjastamise kehtivuskinnituspäringud juurdepääsutõendi alusel

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

* jdigidoc.pkcs12.container [mittekohustuslik] 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] juurdepääsutõendi faili parool
* jdigidoc.pkcs12.cert\_serial [mittekohustuslik] 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.

### 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.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
* kerberos.principal viitab Active Directory serveris loodud SPN nimetusele, 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 OU=Domain Controllers,DC=viljandi,DC=maavalitsus
* ldap.mapToAttribute viitab Active Directory serveris kasutajate info all oleva välja nimetusele, millele on sisestatud isikukood, näiteks pager
* jdigidoc.test peab olemas kas false või true. False kasutada toodangkeskkonnas, kus kehtivuskinnituspäring (OSCP) tuleb teha vastu Sertifitseerimiskeskuse serverit. True kasutada testkeskkonnas, kus kehtivuskinnituspäring tuleb teha vastu OpenXAdES serverit.
* idcard.authurl viitab URL’ile, mida kasutatakse ID-kaardiga autentimise lingiks. Sellel URL’il peab olema Apache httpd 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.

## 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 versiooniuuendusega (s.t. Tomcat’is on varem paigaldatud dhs.war), siis kustutage eelneva paigaldusega seotud kõik failid:  
   cd /home/dhs/tomcat  
   dhs.war versiooniuuenduse puhul:  
   rm -rf webapps/dhs webapps/dhs.war work/Catalina/localhost/dhs temp/Alfresco  
   cas.war versiooniuuenduse 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.
3. Paigutage dhs.war ja/või cas.war fail kataloogi /home/dhs/tomcat/webapps/
4. Kui tegemist on versiooniuuendusega ja kaasa on tulnud eraldi juhend versiooni­uuendusega seotud tegevuste kohta, siis teostage need tegevused.
5. Käivitage Tomcat rakendusserver: /home/dhs/tomcat/tomcat.sh start

### Rakenduse seire

Rakenduse seireks HTTP kaudu ei ole loodud eraldi lehekülge/URL’i. Selleks et kontrollida, kas rakendus on „üleval“, võib seirata URL’i https://dhs.example.com/dhs/service/adr - see URL vastab HTTP staatusega 200 OK. DHS rakenduse kasutajaliidese URL’id suunavad (302 Moved Temporarily) CAS rakenduse lehele, kuna ei olda sisselogitud.

## 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.
3. Kui andmebaasi varundamine on lõppenud, siis teha varukoopia järgmistest data (dir.root parameetriga viidatav kaust) alamkaustadest:
   1. audit.contentstore
   2. backup-lucene-indexes
   3. contentstore
   4. contentstore.deleted

Varukoopiat ei tohi teha järgmistest data alamkaustadest:

* 1. lucene-indexes
  2. 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.
3. Teha varukoopia järgmistest data (dir.root parameetriga viidatav kaust) alamkaustadest:
   1. audit.contentstore
   2. lucene-indexes
   3. backup-lucene-indexes
   4. contentstore
   5. contentstore.deleted

Varukoopiat ei tohi teha järgmistest data alamkaustadest:

* 1. oouser

1. DHS rakenduse võib käivitada.

### Varukoopiast taastamine

1. DHS rakendus peab olema seisatud.
2. Liigutage olemasolev data kaust (dir.root parameetriga viidatav kaust) teise nimega või teise kohta.
3. Taastage varukoopiast data kausta 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.
6. Käivitage DHS rakendus.

## Active Directory serveri seadistamine

1. Selleks, et DHS rakendus saaks tõmmata kasutajate ja gruppide infot Active Directory serverist, on vaja AD serveris luua kasutajakonto, mille kaudu DHS rakendus infole ligi pääseb:
   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.
   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 DHS rakendusse sisenemiseks.  
      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 serveri ja klientarvutite kellad peaksid olema mitte rohkem kui 5 minutise erinevusega Active Directory serveri kellast! Vastasel juhul Kerberos autentimine ei tööta.

AD serverist tõmmatakse üle seadistusfailis määratud alamosade alt:

* Kõik kasutajad, kellel isikukood on täidetud. Kasutajad, kellel isikukood on täitmata, ignoreeritakse.
* Kõik grupid. Grupis ei tohi sisalduda kasutajat kellel isikukood on täitmata, muidu gruppide tõmbamine tervikuna ebaõnnestub!

## 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 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 Local Intranet Sites nimekirjas. Selleks tuleb:
   1. Käivita Internet Explorer
   2. Mine *Tools* -> *Internet Options* -> *Security*
   3. Vali *Local intranet*, vajuta *Sites* ja *Advanced*
   4. Sisesta https://dhs.example.com ja vajuta *Add*
   5. Vajuta *Close*, *OK*, *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

### 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 Local Intranet Sites nimekirjas – sama mis punkt 9.3.1
   3. *Tools* -> *Internet Options* -> *Security* -> *Local intranet* -> *Custom level* -> *User authentication* -> *Logon* valikuks peab olema *Automatic logon only in Intranet Zone*
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“.

DHS toetab e-maile vormingutes „Plain Text“ ja „HTML“. E-mailid vormingus „Rich Text“ ei ole toetatud. Kui lohistada „Rich Text“ vormingus e-mail DHS’i, siis DHS’is tekib kirja sisu faili asemel fail winmail.dat.

## Probleemid

### Veateade „ObjID already in use“

Kui DHS rakenduse käivitamine ebaõnnestub veateatega

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

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 masina küljes oleva võrguliidese 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 6.

### 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 Local Intranet 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“. E-mailid vormingus „Rich Text“ ei ole toetatud. Kui lohistada „Rich Text“ vormingus e-mail DHS’i, siis DHS’is tekib kirja sisu faili asemel fail winmail.dat.

### 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.