

Instal·lació de PortaFIB

Guia Ràpida d'Instal·lació de PortaFIB



Conselleria d'Economia i Competitivitat Direcció General d'Innovació i Desenvolupament Tecnològic





Informació general del document.

Descripció.

Títol: Guia Ràpida d'Instal·lació de PortaFIB

Estat: Esborrany/Aprovat

Versió: 1.0

Autor/s: Antoni Nadal Bennasar

Creat: 13/01/2014 **Modificat** 24/04/2014

Fitxer: Manual_de_Instalacio_de_PortaFIB.odt

Històric de modificacions.

Comentari:	Autor/s:	Data:
Explicació detallada de propietats del fitxer portafib-properties- service.xml	A. Nadal	24/04/2014
Refactor dels noms de les propietats i plugin de custodia de CAIB	A. Nadal	25/06/2014
Noves propietats de plugins i errors en callback.	A. Nadal	08/09/2014
Adaptar Instal·lació a JBoss 5.1	A. Nadal	04/02/2015
Eliminar flag -Dcaib	A. Nadal	05/03/2015
Afegides propietats de hash al Plugins de Custodia-Fitxers	A. Nadal	07/04/2015

Font documental.



Index de Contingut

	Introduccio	
2.	Configurar JBOSS	
	2.1Instal·lació de JBoss	
	2.2Configurar Servidor JBoss	6
	2.2.1Directori de PortaFIB	
	2.2.2Port Segur HTTPS	
	2.2.3Publicar Ports a peticions externes	
	2.2.4Requeriments de memòria	
	2.2.5Permetre consultes sobre múltiples Datasources	
	2.2.6Autenticador WSBASIC	8
	2.3Fitxers de Configuració	
	2.3.1Fitxer JDBC d'accés a BBDD.	
	2.3.1.1Oracle	
	2.3.1.2PostgreSQL	
	2.3.2Fitxer de Propietats	
	2.3.2.1Propietats Generals PortaFIB	
	2.3.2.2Plugins	
	2.3.3Configurar Coes	
	2.3.4Configurar Servidor de Correu	. 12
	2.3.5Autenticació i Autorització per Usuaris Persona	
	2.3.6Autenticació i Autorització per Usuaris Aplicació	
	2.4Copia de binaris	
_	2.5DataSources	
ა.	Plugins	
	3.1Plugin de Conversió de Documents	
	3.2Plugin de Certificat	
	3.2.1Plugin Fake	
	3.2.2Plugin @firma CXF	
	3.2.3Plugin @firma	
	3.3Plugin de Informació d'Usuari	
	3.3.1Plugin de UserInformation via DataBase	
	3.3.2Plugin de UserInformation via LDAP	
	3.4Plugin de Custòdia Documental	.21
	3.4.1Plugin de Custòdia emprant el Sistema de Fitxers	
	3.4.1.1Com instal·lar un servidor de validació pel plugin de custòdia emprant el sister	
	de fitxers	
	3.4.2Plugin de Custòdia emprant Alfresco	.22
	3.4.3Plugin de Custòdia emprant Custodia de la CAIB	.22
4.	Gestió de BBDD	.24
	4.1Crear usuari i BBDD per PortaFIB	.24
	4.1.1Connectar-se a la BBDD	.24
	4.1.2Crearem l'usuari portafib:	.24
	4.1.3Crear la BBDD	
	4.2Crear esquema de taules i inserir dades	



4.2.1Connectar-se al servidor de BBDD amb l'usuari portafib:	25
4.2.2Donam permisos al usuari:	
4.2.3Importam l'estructura de taules i dades dins la BBDD	
4.2.4Sortir	
4.3Crear usuari i BBDD per la gestió d'usuaris PortaFIB	26
5Annexes	
5.1ANNEX I: Compilar PortaFIB des de subversion de sourceforge	26
5.1.1SVN CheckOut	
5.1.2Llibreries sense repositori a Internet	
5.1.3Firma del jar l'Applet o Applet firmat per defecte	
5.1.3.1Utilitzar Applet ja Firmat	27
5.1.3.2Compilar i Firmar l'Applet	
5.1.4Compilació	
5.2Annex II: Creació de Keystore i Truststore per JBoss	29
5.2.1Introducció	29
5.2.2Afegir certificats a keystore:	30
5.2.3Llistar certificats de keystore	
5.2.4Configurar Navegadors amb Certificats de Client	30
5.3Annex III Configurar OpenOffice com a servei en Linux	31
5.3.1Instal·lar OpenOffice	31
5.3.2Arrancar OpenOffice com a Servei	
5.3.3Script per Arrancar OpenOffice com a Servei	32



1.- Introducció

Aquest document exposa les passes per posar en marxa una instancia del producte PortaFIB tant si és a partir d'un binari (ear) o una compilació del codi sobre un servidor jboss i un sistema gestor de BBDD. A continuació descriurem amb més detall les característiques de la instal·lació:

- Com a SO emprarem un Linux (Ubuntu) i les comandes que es mostren són per aquest sistema, encara que són fàcilment exportable a altres SO com Windows.
- El sgbd serà PostgreSQL, encara que es poden fer algunes referències a altres com oracle.
- L'autenticació i autorització es realitzarà a traves de BBDD. En JBoss configurarem un mòdul de login de base de dades i per PortaFIB definirem un plugin de UserInformation per base de dades (aquest darrer servirà per obtenir informació dels usuaris: nom, nif, telefon, email, ..). Disponible també via LDAP.
- PortaFIB en mode JAAS, permet el login autenticant-se de forma BASIC i/o CLIENT-CERT (aquests modes depenen del tipus de compilació realitzada sobre el codi font)

Com a primera tasca, hem d'aconseguir un binari del producte PortaFIB. Per això hi ha dues alternatives.

- (A) COMPILAR CODI FONT: S'han de seguir les instruccions del punt "5.1.-ANNEX I: Compilar PortaFIB des de subversion de sourceforge" d'aquest document per generar el binari a partir del codi font
- (B) DESCARREGAR BINARI: Accedint al projecte portafib de sourceforge, podem descarregar el binaris corresponents. Accedir via web a la següent adreça https://sourceforge.net/projects/portafib/files/portafib-x.y.z/bin/ i descarregar el fitxer portafib-x.y.z.zip. Després descomprimir el zip en l'arrel del nostre home.

Una vegada seguides les passes del punt (A) o (B) obtindrem en el nostre "home" un directori \$HOME/portafib amb tots els fitxers necessaris per a la instal·lació.

2.- Configurar JBOSS

2.1.- Instal·lació de JBoss

Es requereix un JBoss 5.1 amb el parxe de CXF per poder córrer l'aplicació, i per això



necessitarem un JDK 1.6¹ per fer-ho funcionar. No s'ha provat si aquest producte funciona correctament en versions superiors tant de JBoss com de Màquina Virtual Java.

Concretament emprarem un **JBoss** 5.1.0 GA que podem descarregar http://sourceforge.net/projects/jboss/files/JBoss/JBoss-5.1.0.GA/. D'aguesta adreca descarregarem el següent fitxer jboss-5.1.0.GA-jdk6.zip i el descomprimirem dins un directori /usr/local/jboss-as. Aquesta versió de JBoss conté un petit bug² que es soluciona descarregant més moderna del jboss-metadata.jar jar (https://repository.jboss.org/nexus/content/repositories/root_repository/jboss/metadata/1.0.6.GAbrew/lib/) i copiant-ho als directoris de [JBOSS]/common/lib i [JBOSS]/client.

El patch CXF el podem descarregar de http://download.jboss.org/jbossws/jbossws-cxf-3.4.1.GA.zip. L'hem de descomprimir dins la carpeta arrel del JBoss i seguir les instruccions detallades dins la subcarpeta doc.

Tots aquests fitxers també els podem trobar dins el directori Files del projecte KitAnibal de Sourceforge (https://sourceforge.net/projects/kitanibal/files/jboss/jboss-5.1.0-GA/)

Per millorar els scripts farem ús d'una variable d'entorn per apuntar al nostre servidor JBoss:

\$ export JBOSS=/usr/local/jboss-as

Es deixa en mans de l'administrador de sistemes la instal·lació del JDK i la configuració del JBoss com a servei.



En l'entorn de la CAIB (Govern Balear) es requereixen els següents productes:

- JBoss 5.2.0 AS
- Llibreries de Serveis Web Apache CXF específiques per JBoss 5.2.0 AS (jboss-ep-ws-cxf-5.2.0-installer.zip)
- Aplicar el paquet d'adequació de l'entorn JBoss per a la CAIB (versió 1.6.2): jbosspatch-1.6.2

2.2.- Configurar Servidor JBoss

2.2.1.- Directori de PortaFIB

En JBoss el directori on es guarden per defecte les aplicacions (ears) és el directori de DEPLOY (\$JBOSS/server/defualt/deploy). En el nostre cas el que farem serà crear un altra directori de deploy per simplificar la instal·lació.

Editarem el fitxer \$JBOSS/server/default/conf/bootstrap/profile.xml i afegirem una nova línia tal i com és mostra a continuació:

¹ En el nostre cas empram 1.6.0 33-b05

² El bug en qüestió es descriu en la següent pàgina web https://issues.jboss.org/browse/JBMETA-207



I final ment crearem el nou directori deployportafib:

```
$ sudo mkdir -p $JBOSS/server/default/deployportafib
```

2.2.2.- Port Segur HTTPS

Per l'autenticació bàsica opcionalment potser volem connectar-nos al servidor emprant una connexió segura (https). Per autenticació Client-Cert forçosament necessitam obrir un port especial https.

Podem afegir aquest port al JBoss editant el fitxer \$JBOSS/server/default/deploy/jbossweb.sar/server.xml i descomentant el bloc xml titulat "SSL/TLS Connector..." i modificant-ho amb el següent text:

```
<Connector protocol="HTTP/1.1" SSLEnabled="true"
allowUnsafeLegacyRenegotiation="true"
    port="8443" address="${jboss.bind.address}"
    scheme="https" secure="true" clientAuth="false"
    keystoreFile="${jboss.server.home.dir}/conf/jboss.keystore"
    keystorePass="fundaciobit" sslProtocol = "TLS"
    truststoreFile="${jboss.server.home.dir}/conf/jboss.truststore"
truststorePass="fundaciobit"/>
```

S'han de copiar els arxius jboss.keystore i jboss.truststore dins el directori \$JBOSS\server\default\conf. Podeu trobar exemples d'aquests dos fitxers dins el directori \$HOME/portafib/scripts/certificats. Aquest dos fitxers contenen els certificat arrel del DNIe, Camerfirma i el certificat de proves de FundacioBit, per la qual cosa amb aquest arxius només es podrà autenticar via CLIENT-CERT amb certificats de DNIe, de Camerfirma o de FundacioBit.

La generació d'altres arxius jboss.keystore i jboss.truststore, amb certificats específics, es descriu al punt "5.2.-Annex II: Creació de Keystore i Truststore per JBoss".



2.2.3.- Publicar Ports a peticions externes

Si volem que el nostres jboss sigui accessible des de forà del nostre propi ordinador llavors heu d'ediar el fitxer run.conf (o run.conf.bat si estam amb Windows) de \$JBOSS/bin i afegir la següent línia:

```
set "JAVA OPTS=%JAVA OPTS% -Djboss.bind.address=0.0.0.0"
```

2.2.4.- Requeriments de memòria

Es recomada donar la major memòria possible al JBoss ja que Portafib és una aplicació web bastant pesada. Obrir run.conf (o run.conf.bat si estam amb Windows) de \$JBOSS/bin i editar els parametres -Xms i Xmx i posar-lis valors majors a 800m (es recomanen 1024m).

```
-Xms512m -Xmx1024m -XX:MaxPermSize=256m
```

2.2.5.- Permetre consultes sobre múltiples Datasources

S'ha d'editar el fitxer \$JBOSS\server\default\conf\jbossts-properties.xml i cercar l'entrada <properties depends="arjuna" name="jta"> i just després afegir la següent línia:

```
cproperty name="com.arjuna.ats.jta.allowMultipleLastResources" value="true" />
```

NOTA: Revisar que l'entrada anterior no estigui donada d'alta. Si hi fos canviar el valor a "true"

2.2.6.- Autenticador WSBASIC



En l'entorn de la CAIB (Govern Balear) aquest punt s'ha d'ometre ja que el patch de la CAIB ja configura els autenticadors.

S'ha d'obrir el fitxer \$JBOSS]/server/default/deployers/jbossweb.deployer/META-INF/war-deployers-jboss-beans.xml. S'ha de cercar un bloc xml "property name="authenticators">" i dins aquest bloc s'ha d'inserir un nou autenticador:



2.3.- Fitxers de Configuració

2.3.1.- Fitxer JDBC d'accés a BBDD

2.3.1.1.- Oracle

Accedir a http://www.oracle.com/technetwork/database/features/jdbc/index.html i descarregar el driver (fitxer jar) corresponent a la nostre versió d'oracle i copiar-ho dins \$JBOSS/server/default/lib/.

2.3.1.2.- PostgreSQL

Si estem emprant com a SGBD PostgreSQL llavors descarregar el fitxer de la següent adreça http://jdbc.postgresql.org/download/postgresql-8.4-703.jdbc3.jar i copiar-ho dins el directori de llibreries del JBOSS: \$JBOSS/server/default/lib/.

2.3.2.- Fitxer de Propietats

Aquest fitxer serveix per definir la configuració del PortaFIB. Podem trobar una plantilla d'aquest fitxer a \$HOME/portafib/scripts/config/portafib-properties-service.xml. Aquest fitxer el copiarem a \$JBOSS/server/default/deployportafib:

\$ sudo cp \$HOME/portafib/scripts/config/portafib-properties-service.xml \$JBOSS/server/default/deployportafib



En l'entorn de la CAIB (Govern Balear) aquest fitxer ha d'anar encapsulat dins un fitxer portafib.sar seguit la següent estructura:

```
portafib.sar

LMETA-INF

- jboss-service.xml

L MANIFEST.MF
```

on jboss-service.xml és el fitxer portafib-properties-service.xml renombrat i MANIFEST.MF és un fitxer que conté les dades bàsiquest d'un MANIFIEST:

Manifest-Version: 1.0
Archiver-Version: Plexus Archiver
Created-By: Apache Maven
Built-By: <<author>>

Built-By: <<author>>
Build-Jdk: 1.6.0 31



2.3.2.1.- Propietats Generals PortaFIB

En aquest fitxer hi ha algunes propietats que requereixen de la intervenció de l'administrador:

Nom	Descripció
es.caib.portafib.iscaib	Propietat que indica als projectes que activin les característiques especials requerides en l'entorn de la CAIB (Govern Balear) si val true. Si no estam dins l'entorn CAIB llavors ha de valer "false".
es.caib.portafib.hibernate.*	 Propietats de Configuració Hibernate: Estableix les propietats de configuració de Hibernate. Les dues propietats més importants són: es.caib.portafib.hibernate.dialect es.caib.portafib.hibernate.query.substitutions En PostgreSQL la propietats de substitutions no es definirà però en Oracle aquesta ha de valer "true 1, false 0" ja que s'ha de realitzar el mapeig de booleans a sencers ja que aquest SGBD no suporta booleans.
es.caib.portafib.filesdirectory	Directori d'emmagatzemament de Fitxers: PortaFIB necessita un directori on guardar tots els fitxers ja que aquests no es guarden en base de dades. Per això s'ha de definir la propietat es.caib.portafib.filesdirectory que apunti a un directori existent i amb espai suficient per guardar tots els fitxers. Crearem un directori /portafibfiles i inicialitzarem aquesta propietat a es.caib.portafib.filesdirectory=/portafibfiles. Un exemple de ruta windows podria ser la següent: es.caib.portafib.filesdirectory=c:\\tmp\\portafibfiles. Si estam carregant la BBDD de demo, llavors és el lloc on ficarem els fitxers associats amb les dades de prova, per això executarem la següent comanda \$unzip \$HOME/portafib/portafibfiles.zip -d /portafibfiles.
es.caib.portafib.url	És l'adreça pública d'accés al portafirmes: es.caib.portafib.url=http://localhost:8080/portafib
es.caib.portafib.email.from	És l'adreça d'email des d'on s'enviaran les notificacions per correu als usuaris: es.caib.portafib.email.from=portafib@portafib.org
es.caib.portafib.defaultlanguage	Idioma per defecte. Valors possibles poden ser "ca" per català i "es" per castellà. es.caib.portafib.defaultlanguage=ca



es.caib.portafib.development	Propietat que fa que es mostrin per pantalla i per log més informació de la requerida. Aquest valor es carrega en calent, per la qual cosa en qualsevol moment sense haver d'aturar el servidor es pot activar o desactivar per fer una depuració ràpida. Valors possibles són true o false: es.caib.portafib.development=false
es.caib.portafib.checknifcertificate	Si val true quan es firma un document comprova que el DNI de la persona que ha firma (DNI del certificat digital) s'ajusta al DNI de la persona que realment ha de firmar. S'assigna a false en mode desenvolupament per poder fer tests amb certificats i usuaris de proves. es.caib.portafib.checknifcertificate=true
es.caib.portafib.maxuploadsizeinbytes	Tamany màxim de pujada de fitxers en bytes. No definit o amb valors buit significa sense límit (es.caib.portafib.maxuploadsizeinbytes=)
es.caib.portafib.maxfitxeradaptatsizeinbytes	Tamany màxim del fitxer PDF una vegada se li han afegit els annexes i taula de firmes. No definit significa sense límit (es.caib.portafib.maxfitxeradaptatsizeinbytes=)
es.caib.portafib.encryptkey	Clau per encriptar l'identificador del fitxers a descarregar (IMPORTANT tamany de 16 caràcters): es.caib.portafib.encryptkey=portafibportafib
es.caib.portafib.name	Nom de l'aplicació PortaFIB: es.caib.portafib.name=PortaFIB
es.caib.portafib.editableuser	Si està a true permet als usuaris editar l'email dels usuari-persona i usuaris-entitats, així com el logo dels usuaris-entitat. En cas contrari, únicament és l'administrador d'entitat que pot fer canvis en aquest camps es.caib.portafib.editableuser=false
es.caib.portafib.defaultsignalgorithmid	Camp opcional. Defineix l'identificador de l'algorisme a utilitzar per defecte durant la firma de documents o fitxers. Fa referencia al camp ID de la taula pfi_algorismedefirma. Els valors possibles d'una instal·lació per defecte són: • 0 = SHA1withRSA • 1 = SHA256withRSA • 2 = SHA384withRSA • 3 = SHA512withRSA



es.caib.portafib.exportdataplugins	Llistat de Plugins pel l'exportació de dades en els llistats (excel, ods, csv,). Exemple: es.caib.portafib.exportdataplugins=org.fundaciobit.pl ugins.exportdata.cvs.CSVPlugin,org.fundaciobit.plu gins.exportdata.ods.ODSPlugin,org.fundaciobit.plugins.exportdata.excel.ExcelPlugin
es.caib.portafib.numberoferrorsinnotification tosendmail	Indica a partir de quants d'errors en una notificació callback s'enviarà un correu al responsable de l'usuari aplicació. Si no es defineix llavors no s'envia cap correu.
es.caib.portafib.numberoferrorstopausenotification	Indica a partir de quants d'errors en una notificació callback aquesta automàticament es pausarà. Si no es defineix llavors no es pausarà automàticament.
es.caib.portafib.applet.signerClass	Indica al PortaFIB quina API emprarem per firmar els documents. Valors possibles són: • Firma de documents emprant @firma: es.caib.portafib.applet.signers.AfirmaSigner • Firma emprant IB-KEY: es.caib.portafib.applet.signers.IBKeySigner

En aquest fitxer s'han de definir els plugins necessaris pel bon funcionament de PortaFIB. A continuació es descriuen aquests plugins:

2.3.2.2.- Plugins

La informació des plugins es defineix dins del fitxer \$HOME/portafib/scripts/config/portafib-properties-service.xml, però per la seva extensió i varietat s'explica en el punt "3.-Plugins".

2.3.3.- Configurar Coes

Per l'enviament massiu de correu i notificacions webservice, requerim de la definició de coes en el servidor jboss. Aquest pas és relativament senzill ja que únicament hem de copiar dos fitxers dins el directori deployportafib:

\$sudo cp \$HOME/portafib/scripts/config/portafib-mailsqueue-service.xml
\$JBOSS/server/default/deployportafib

\$sudo cp \$HOME/portafib/scripts/config/portafib-notificacionsqueue-service.xml \$JBOSS/server/default/deployportafib



2.3.4.- Configurar Servidor de Correu

Per l'enviament de correus necessitau un servidor de correu i en aquest fitxer és on s'ha de configurar. Trobareu una plantilla dins \$HOME/portafib/scripts/config/portafib-mail-service.xml, que copiarem dins \$JBOSS/server/default/deployportafib i després editarem per establir les dades del nostre servidor de correu:

```
$sudo cp $HOME/portafib/scripts/config/portafib-mail-service.xml
$JBOSS/server/default/deployportafib
```

2.3.5.- Autenticació i Autorització per Usuaris Persona



En l'entorn de la CAIB (Govern Balear) hem de saltar aquest punt ja que l'autenticació dels usuaris-persona ja es realitza automàticament al aplicar el patch de la CAIb sobre un servidor JBOSS.

Com hem dit al principi, tindrem els nostres usuaris i roles guardats dins una base de dades, per això a continuació configurarem el JBoss per accedir a aquestes dades.

Obrirem el fitxer \$JBOSS/server/default/conf/login-config.xml i abans del tag "</policy>" del final del fitxer, afegirem la següent entrada:

```
<application-policy name = "seycon">
  <authentication>
   <!-- CLIENT CERT -->
   <login-module code="es.caib.portafib.back.security.BaseCertLoginModule"</pre>
flag="sufficient">
    </login-module>
   <!-- DATABASE -->
   <login-module code="org.jboss.security.auth.spi.DatabaseServerLoginModule"</pre>
flag="sufficient">
            <module-option name="dsJndiName">java:/es.caib.seycon.db.wl</module-option>
            <module-option name="principalsQuery">
               select USU_PASS from SC_WL_USUARI where USU_CODI = ?
            </module-option>
            <module-option name="rolesQuery">
               select UGR CODGRU, 'Roles' from SC WL USUGRU where UGR CODUSU = ?
            </module-option>
    </login-module>
  </authentication>
 </application-policy>
```

(a) El bloc CLIENT-CERT només serveix si ens autenticam emprant https i CLIENT-CERT emprant un mecanisme JAAS. En la resta de casos podem comentar-ho. EXPLICAR Més EN DETALL. (b) Es poden consultar per internet altres mòdul d'autenticació JBoss com per exemple per LDAP, Fitxers de Propietats, ... Dins el fitxer \$HOME/portafib/scripts/config/login-config.xml trobarà l'exemple anterior de BBDD i altres exemple per LDAP i específics de la CAIB.



El fitxer associat a la connexió de bases de dades definida amb el nom d'atribut "dsJndiName" es troba en els propis fitxers d'scripts. Només hem de copiar-ho al JBoss:

```
$sudo cp $HOME/portafib/scripts/development/seycon-ds.xml
$JBOSS/server/default/deployportafib
```

La base de dades definida en aquest fitxer es crearà en l'apartat de "4.-Gestió de BBDD".

2.3.6.- Autenticació i Autorització per Usuaris Aplicació



En l'entorn de la CAIB (Govern Balear) hem de saltar aquest punt ja que l'autenticació dels usuaris-aplicació ja està integrada amb el sistema de login CAS.

Aquesta entrada s'utilitza per a que el usuaris aplicació en entorn no-CAIB, puguin validar la contrasenya i poder accedir als WebServices del PortaFIB (als WS propis de PortaFIB, el WS de Portafirmes antic de CAIB empren un altre mecanisme). En aquest cas, s'ha d'afegir una nova entrada al fitxer login-config.xml.

Obrirem el fitxer \$JBOSS/server/default/conf/login-config.xml i al final del bloc <application-policy> de seycon, afegirem la següent entrada:



2.4.- Copia de binaris

Els possibles binaris que existeixen es poden generar combinant dues variables amb dos valors possibles:

- Mode desenvolupament o producció: en el mode desenvolupament, las diferents implementacions dels plugins (tant de informació d'usuari com de validació de certificat) es guarden dins de l'ear generat. En producció, s'han de definir els plugins requerit dins del pom del directori earplugins.
- Sistema d'autenticació Basic o Basic&ClientCert: Sempre hi haurà un context web
 /portafib amb autenticació bàsica. Opcionalment, a més és podrà definir autenticació
 CLIENT-CERT dins un context /portafibs

Amb qualsevol combinació necessitam l'ear portafib:

\$ sudo cp \$HOME/portafib/ear/target/portafib.ear \$JBOSS/server/default/deployportafib

Si esta activat el mode Producció, significa que els plugins estan dins l'ear de portafib-plugins.ear, per la qual cosa també haurem de copiar aquest fitxers:

\$ sudo cp \$HOME/portafib/earplugins/target/portafib_plugins.ear \$JBOSS/server/default/deployportafib

2.5.- DataSources

Els datasources defineixen l'origen de les dades. Podem trobar una plantilla a \$HOME/portafib/scripts/datasources/portafib-ds.xml per PostgreSQL:

Aquest script es connecta a una BBDD anomenada portafib en un postgresql que es troba en el mateix servidor (localhost) emprant un usuari portafib (contrasenya portafib). Si les dades d'accés a la BBDD difereixen, llavors s'ha d'editar aquest fitxer i modificar el que calgui.

\$sudo cp \$HOME/portafib/scripts/datasources/portafib-ds.xml
\$JBOSS/server/default/deployportafib

Nota: Dins el datasource \$HOME/portafib/scripts/development/seycon-ds.xml podeu trobar un exemple comentat de datasource per Oracle.



3.- Plugins

Les propietats que es descriuen a continuacio han d'anar dins del fitxer \$HOME/portafib/scripts/config/portafib-properties-service.xml juntament amb les propietats generals descrites en el punt "2.3.2.-Fitxer de Propietats".

3.1.- Plugin de Conversió de Documents

Actualment només hi ha disponible una implementació que és la d'OpenOffice. Aquí el que es pot modificar és on es troba escoltant el servidor d'OpenOffice.

```
es.caib.portafib.documentconverterplugin=
org.fundaciobit.plugins.documentconverter.openoffice.OpenOfficeDocumentConverterPlugin
es.caib.portafib.plugins.documentconverter.openoffice.host=localhost
es.caib.portafib.plugins.documentconverter.openoffice.port=8100
```

En el punt "5.3.-Annex III Configurar OpenOffice com a servei en Linux" es mostra com posar un OpenOffice em mode servei en Linux.

3.2.- Plugin de Certificat

Serveix per verificar si els certificats són correctes. Actualment esta activat una verificació bàsica (plugin Fake). La propietat és portafib.certificateplugin. Per les administracions que tenguin configurada @firma és pot emprar la classe AfirmaCertificatePlugin (només s'ha de comentar el plugin Fake, descomentar el plugin de AfirmaCertificatePlugin i definir les propietats de connexió a @firma). Nota: Com és lògic no es compatible la comunicació BASIC i la de CERTIFICAT, se n'ha de triar una de les dues. La propietat que defineix aquest certificat és la següent:

es.caib.portafib.certificateplugin=[NOM DE LA CLASSE DEL PLUGIN DE CERTIFICAT]

3.2.1.- Plugin Fake

Aquest plugin només verifica de forma bàsica el certificat (data inici i final). Si es vol emprar s'ha de definir la següent propietat:

es.caib.portafib.certificateplugin=org.fundaciobit.plugins.certificate.fake.FakeCertificatePlugin



3.2.2.- Plugin @firma CXF

És idèntic al plugin @firma (3.2.3.-Plugin @firma) i té les mateixes propietats però realitza la comunicació WebServices emprant les classes CXF enlloc de la llibreria AXIS. Si es vol emprar s'ha de definir la següent propietat:

es.caib.portafib.certificateplugin=org.fundaciobit.plugins.certificate.afirmacxf.AfirmaCxfCertificate Plugin

3.2.3.- Plugin @firma

Aquest plugin es connecta amb @firma per validar el certificat d'una firma. Les propietats es classifiquen en tres: propietats generals, propietats per comunicació BASIC i propietats per comunicació via Certificat. Si es vol emprar s'ha de definir la següent propietat:

es.caib.portafib.certificateplugin=org.fundaciobit.plugins.certificate.afirma.AfirmaCertificatePlugin

Les propietats necessàries per configurar aquest plugin es descriuen a continuació:

,	<u> </u>		
es.caib.portafib.plugins.certificate.afirma. endpoint	Adreça dels serveis d'@firma. El valor normalment és: http://des-afirma.redsara.es/afirmaws/services/		
es.caib.portafib.plugins.certificate.afirma. applicationid	Identificador @firma associat a la nostra entitat		
es.caib.portafib.plugins.certificate.afirma. validationmode	Sencer que indica el mode de validació: • MODE_VALIDACIO_SIMPLE = 0 • MODE_VALIDACIO_AMB_REVOCACIO = 1 • MODE_VALIDACIO_CADENA = 2		
COMUNICAC	IO VIA USUARI-CONTRASENYA³		
es.caib.portafib.plugins.certificate.afirma. authorization.username	Nom d'usuari assignat a la comunicació BASIC		
es.caib.portafib.plugins.certificate.afirma. authorization.password	Contrasenya associada a l'usuari anterior.		
COMU	NICACIO VIA CERTIFICAT		
es.caib.portafib.plugins.certificate.afirma. authorization.ks.path	Ruta al KeyStore que conté el certificat per l'establiment de connexió amb @firma. En windows les barres s'han d'escriure com / : D:/plugins-certificate/afirma/proves-dgidt.jks		
es.caib.portafib.plugins.certificate.afirma. authorization.ks.type	És el tipus de KeyStore: JKS (de java) o PKCS12 (PKCS 12). Nota: Les proves amb P12 funcionen en el primer establiment i despres es desconfiguren.		
es.caib.portafib.plugins.certificate.afirma. authorization.ks.password			

³ Aquest tipus d'establiment de connexió ja no és vàlid quan s'ataca a la web de producció de @firma



es.caib.portafib.plugins.certificate.afirma. authorization.ks.cert.alias	Defineix l'àlies del certificat que volem utilitzar (serveix per quan dins el keystore hi ha varis certificats)
es.caib.portafib.plugins.certificate.afirma. authorization.ks.cert.password	Contrasenya d'accés al certificat.

3.3.- Plugin de Informació d'Usuari

S'utilitza per obtenir informació dels usuaris a partir del seu username o a partir de l'identificador de l'administració (nif). Aquest plugin està molt relacionat amb el mòdul de login de JBoss ja que normalment, els dos accediran a la mateixa font d'usuaris. Actualment hi ha dues implementacions:

- Accés a Base de Dades: Veure punt 3.3.1.-Plugin de UserInformation via DataBase
- Accés a LDAP: Veure punt 3.3.2.-Plugin de UserInformation via LDAP

La propietat que defineix el Plugin de de UserInformation és:

es.caib.portafib.userinformationplugin=[NOM DE LA CLASSE DEL PLUGIN DE USERINFORMATION]

3.3.1.- Plugin de UserInformation via DataBase

Si volem utilitzar aquest plugin llavors s'ha de definir la següent entrada:

es.caib.portafib.userinformationplugin=org.fundaciobit.plugins.userinformation.database.DataBaseUserInformationPlugin

I a més definir les següents propietats:

Nom	R/O⁴	Descripció
es.caib.portafib.plugins.userinformation.database .jndi	R	Nom jndi que defineix la connexió amb la BBDD. Exemple: es.caib.portafib.plugins.userinformation.data base.jndi=java:/es.caib.seycon.db.wl
es.caib.portafib.plugins.userinformation.database .users_table	R	Nom de la taula d'usuaris. Exemple: es.caib.portafib.plugins.userinformation.data base.users_table=SC_WL_USUARI
es.caib.portafib.plugins.userinformation.database .username_column	R	Nom d'usuari. Exemple: es.caib.portafib.plugins.userinformation.data base.username_column=USU_CODI

⁴ R = Requerit | O = Opcional



es.caib.portafib.plugins.userinformation.database .administrationid_column	R	Nom de la columna que conté el NIF o l'identificador de l'administració. es.caib.portafib.plugins.userinformation.data base.administrationid_column=USU_NIF
es.caib.portafib.plugins.userinformation.database .name_column	R	Nom de la columna que conté el nom de la persona (amb o sense llinatges) es.caib.portafib.plugins.userinformation.data base.name_column=USU_NOM
es.caib.portafib.plugins.userinformation.database .surname_column	0	Nom de la columna que conté els llinatges de la persona
es.caib.portafib.plugins.userinformation.database .language_column	0	Nom de la columna que conté l'idioma de la persona (ca, es, en,)
es.caib.portafib.plugins.userinformation.database .telephone_column	0	Nom de la columna que conté el telefon de la persona
es.caib.portafib.plugins.userinformation.database .email_column	0	Nom de la columna que conté l'email de la persona
es.caib.portafib.plugins.userinformation.database .roles_table	R(*)	Taula que conte els Roles associats a la persona. Exemple: es.caib.portafib.plugins.userinformation.data base.roles_table=SC_WL_USUGRU
es.caib.portafib.plugins.userinformation.database .username_column_in_roles_table	R(*)	Columna de la taula de roles que conté l'username de la persona. Exemple: es.caib.portafib.plugins.userinformation.data base.username_column_in_roles_table=UG R_CODUSU
es.caib.portafib.plugins.userinformation.database .rolename_column	R(*)	Columna de la taula de roles que conté el nom del role. Exemple: es.caib.portafib.plugins.userinformation.data base.rolename_column=UGR_CODGRU

^(*) Aquests camps són opcionals sí des de l'aplicació que empri el plugin no realitzi consultes per conèixer els roles de cert usuari.

3.3.2.- Plugin de UserInformation via LDAP

Si volem utilitzar aquest plugin llavors s'ha de definir la següent entrada:

es.caib.portafib.userinformationplugin=org.fundaciobit.plugins.userinformation.ldap.LdapUserInformationPlugin

I a més definir les següents propietats:



Nom	R/O ⁵	Descripció
es.caib.portafib.plugins.userinformation.ldap. host_url	R	Servidor de LDAP.Exemple: es.caib.portafib.plugins.userinformation.ldap.hos t_url=ldap://ldap.fundaciobit.org:389
es.caib.portafib.plugins.userinformation.ldap. security_principal	R	Usuari de amb permisos de lectura de LDAP
es.caib.portafib.plugins.userinformation.ldap.security_credentials	R	Contrasenya de l'usuari anterior
es.caib.portafib.plugins.userinformation.ldap. security_authentication	R	Tipus d'autenticació es.caib.portafib.plugins.userinformation.ldap.sec urity_authentication=simple
es.caib.portafib.plugins.userinformation.ldap.users_context_dn	R	Context on es troben els usuris. es.caib.portafib.plugins.userinformation.ldap.use rs_context_dn=cn=Users,dc=ibitnet,dc=lan
es.caib.portafib.plugins.userinformation.ldap.search_scope	R	Nivell de cerca. es.caib.portafib.plugins.userinformation.ldap.sea rch_scope=onelevel
es.caib.portafib.plugins.userinformation.ldap.search_filter	R	Filtre de cerca. Exemple: es.caib.portafib.plugins.userinformation.ldap.sea rch_filter=((memberOf=CN=@PFI_ADMIN,CN=Users,DC=i bitnet,DC=lan) (memberOf=CN=@PFI_USER,CN=Users,DC=ib itnet,DC=lan))
es.caib.portafib.plugins.userinformation.ldap. attribute.username	R	Nomde l'usuari.Exemple: es.caib.portafib.plugins.userinformation.ldap.attri bute.username=sAMAccountName
es.caib.portafib.plugins.userinformation.ldap. attribute.mail	R	Correu de l'usuari.Exemple: es.caib.portafib.plugins.userinformation.ldap.attri bute.mail=mail
es.caib.portafib.plugins.userinformation.ldap. attribute.administration_id	R	Nif o AdministrationID de l'usuari. Exemple: es.caib.portafib.plugins.userinformation.ldap.attri bute.administration_id=postOfficeBox
es.caib.portafib.plugins.userinformation.ldap. attribute.name	R	Nom de l'usuari. Exemple: es.caib.portafib.plugins.userinformation.ldap.attri bute.name=givenName
es.caib.portafib.plugins.userinformation.ldap. attribute.surname	0	Llinatges de l'usuari. Exemple: es.caib.portafib.plugins.userinformation.ldap.attri bute.surname=sn

⁵ R = Requerit | O = Opcional



es.caib.portafib.plugins.userinformation.ldap. attribute.telephone	0	Telefon de l'usuari. Exemple: es.caib.portafib.plugins.userinformation.ldap.attri bute.telephone=telephoneNumber
es.caib.portafib.plugins.userinformation.ldap. attribute.memberof	R(*)	Atribut que conté els roles. Exemple: es.caib.portafib.plugins.userinformation.ldap.attri bute.memberof=memberOf
es.caib.portafib.plugins.userinformation.ldap. prefix_role_match_memberof	R(*)	Prefix per obtenir el role de l'atribut: es.caib.portafib.plugins.userinformation.ldap.pref ix_role_match_memberof=CN=@
es.caib.portafib.plugins.userinformation.ldap.suffix_role_match_memberof	R(*)	Sufix per obtenir el role de l'atribut: es.caib.portafib.plugins.userinformation.ldap.suffi x_role_match_memberof=,CN=Users,DC=ibitnet ,DC=lan

(*) Aquests camps són opcionals sí des de l'aplicació que empri el plugin no realitzi consultes per conèixer els roles de cert usuari.

3.4.- Plugin de Custòdia Documental

Aquest plugins serveix per fer persistents, independentment de PortaFIB, els documents signats. La propietat que defineix el Plugin de Custòdia Documental és:

es.caib.portafib.documentcustodyplugin=[NOM DE LA CLASSE DEL PLUGIN DE CUSTODIA]

3.4.1.- Plugin de Custòdia emprant el Sistema de Fitxers

Aquesta implementació guarda els fitxers en un directori del sistema de fitxers. Si es vol emprar s'ha de definir la següent propietat:

es.caib.portafib.documentcustodyplugin=org.fundaciobit.plugins.documentcustody.filesystem.FileSystemDocumentCustodyPlugin

Les propietats necessàries per configurar aquest plugin es descriuen a continuació:

es.caib.portafib.plugins.documentcustody. filesystem.prefix	Defineix un prefix pels fitxers guardats. Es per si s'utilitza un directori on hi ha altres fitxers i es vol diferenciar fàcilment quins són els fitxers custodiats. Exemple: es.caib.portafib.plugins.documentcustody.filesystem.prefix =CUST_
--	---



es.caib.portafib.plugins.documentcustody. filesystem.basedir	Defineix el directori dels sistema de fitxers on es guardaràn els fitxers. Exemple: es.caib.portafib.plugins.documentcustody.filesystem.base dir=D:\\dades\\dades\\CarpetesPersonals\\Programacio\\PortaFIB-jboss-as\\server\\default\\deployportafib\\custodia.war
es.caib.portafib.plugins.documentcustody. filesystem.baseurl	Si s'ha enllaçat el directori definit anteriorment amb un servidor web, llavors indicarem la URL per descarregar/validar cer document. Els valors reemplaçables en el misstatge són els següents: • {0} = custodialD • {1} = URLEncoded(custodialD) • {2} = Hash Exemples: es.caib.portafib.plugins.documentcustody.filesystem.base url=http://localhost:8080/custodia/index.jsp?custodylD={0} es.caib.portafib.plugins.documentcustody.filesystem.base url=http://localhost:8080/custodia/index.jsp?hash={2}
es.caib.portafib.plugins.documentcustody. filesystem.hash.algorithm	(opcional) Algorisme emprat per la generació del Hash emprat en "baseurl". Valors posibles són MD2, MD5, SHA,SHA-256,SHA-384 i SHA-512
es.caib.portafib.plugins.documentcustody. filesystem.hash.password	(opcional) En angles s'anomena "s <i>alt</i> ". És l'afegit a la cadena custodylD a partir de la qual es genera el hash. Aquest valor evita l'obtenció de valors a partir del hash.

3.4.1.1.- Com instal·lar un servidor de validació pel plugin de custòdia emprant el sistema de fitxers

(1) Crear un directori anomenat custodia.war dins \$JBOSS/server/default/deployportafib:

\$mkdir \$JBOSS/server/default/deployportafib/custodia.war

- (2) Copiar dins el directori anterior el fitxer index.jsp que trobarem dins el zip de l'empaquetat o en el codi font en la següent ruta: plugins\plugins-documentcustody\filesystem\index.jsp
- (3) Reiniciar JBoss.

3.4.2.- Plugin de Custòdia emprant Alfresco

<< FALTA - NO IMPLEMENTAT>>

3.4.3.- Plugin de Custòdia emprant Custodia de la CAIB

Aquesta implementació guarda els fitxers en el sistema de Custòdia de la CAIB. Si es vol emprar s'ha de definir la següent propietat:



 $\verb|es.caib.portafib.documentcustodyplugin=org.fundaciobit.plugins.documentcustody.custodiacaibaxis.CustodiaCaibAxisPlugin|$

Les propietats necessàries per configurar aquest plugin es descriuen a continuació:

es.caib.portafib.plugins.documentcustody. custodiacaib.urlvalidation	Indica la plantilla de la URL de validació. Els valors reemplaçables en el l'adreça són els següents: • {0} = HASH • {1} = CodiExtern • {2} = CodiEspecial Exemple: es.caib.portafib.plugins.documentcustody.custodiacaib.urlvalidat ion=http://192.168.31.143:8080/signatura/sigpub/viewdoc?
es.caib.portafib.plugins.documentcustody. custodiacaib.server	Indica la ubicació dels Servidor de custòdia Exemple: es.caib.portafib.plugins.documentcustody.custodiacaib.server=h ttp://192.168.31.143:8080/signatura/services/CustodiaDocumen tos
es.caib.portafib.plugins.documentcustody. custodiacaib.username	Indica l'usuari amb el que autenticar-se al servidor de custòdia. Exemple: es.caib.portafib.plugins.documentcustody.custodiacaib.usernam e=valcust
es.caib.portafib.plugins.documentcustody. custodiacaib.password	Indica la contrasenya assicada a l'usuari amb el que autenticar-se al servidor de custòdia. Exemple: es.caib.portafib.plugins.documentcustody.custodiacaib.passwor d=valcust
es.caib.portafib.plugins.documentcustody.custodiacaib.defaultdocumenttype=PDF	És el tipus de document per defecte definit dins Custodia amb que es guardarà aquest document. Aquest tipus és pot modificar definint en el camp paràmetres del Plugin de Custòdia un paràmetre "documenttype=[TIPUS]" via web o via webservices. En cas contrari farà ús del tipus definit en aquesta propietat. Exemple: es.caib.portafib.plugins.documentcustody.custodiacaib.defaultd ocumenttype=PDF



es.caib.portafib.plugins.documentcustody. custodiacaib.defaultreserveprefix	fer la reserva. Aquest identificador es pot modificar
	definint en el camp paràmetres del Plugin de Custòdia un paràmetre "reserveprefix=[NOM]" via web o via webservices. En cas contrari farà ús de l'identificador
	definit en aquesta propietat. Exemple:
	es.caib.portafib.plugins.documentcustody.custodiacaib.defaultre serveprefix=PORTAFIB

4.- Gestió de BBDD

4.1.- Crear usuari i BBDD per PortaFIB

4.1.1.- Connectar-se a la BBDD

- \$ sudo bash
- \$ su postgres
- \$ psql -U postgres

4.1.2.- Crearem l'usuari portafib:

CREATE USER "portafib" WITH ENCRYPTED PASSWORD 'portafib' NOCREATEUSER;

4.1.3.- Crear la BBDD

CREATE DATABASE "portafib" WITH OWNER=portafib;

i sortirem

/q

4.2.- Crear esquema de taules i inserir dades



4.2.1.- Connectar-se al servidor de BBDD amb l'usuari portafib:

```
$ psql -h localhost -p 5432 -U portafib -W -d portafib
```

i si està en un altra servidor llavors executar

```
$ psql -h www.xxx.yyy.zzz -p 5432 -U portafib -W -d portafib
```

4.2.2.- Donam permisos al usuari:

```
GRANT ALL PRIVILEGES ON DATABASE "portafib" TO portafib;
GRANT ALL PRIVILEGES ON SCHEMA PUBLIC TO portafib;
```

4.2.3.- Importam l'estructura de taules i dades dins la BBDD

```
\i $HOME/portafib/scripts/bbdd/[x.y]/[sgbd]/portafib_create_schema.sql
\i $HOME/portafib/scripts/bbdd/[x.y]/[sgbd]/portafib_create_data.sql
```



En l'entorn de la CAIB (Govern Balear) els scripts a carregar són els següents:

```
\i $HOME/portafib/scripts/bbdd/[x.y]/[sgbd]/portafib_create_schema_caib.sql
\i $HOME/portafib/scripts/bbdd/[x.y]/[sgbd]/portafib_create_data.sql
\i $HOME/portafib/scripts/bbdd/[x.y]/portafib_create_data_caib.sql<sup>6</sup>
\i $HOME/portafib/scripts/bbdd/[x.y]/oracle/portafib_carrecs_caib.sql<sup>7</sup>
```

Important: Abans d'executar el fitxer portafib_carrecs_caib.sql aquest s'ha d'editar per configurar la IP del servidor de PortaFIB.

On **[sgbd]** pot ser oracle o postgresql i [x.y] és la versió que estam instal·lant. Si dins aquest directori no trobau el vostre sgbd, llavors comentar-vos que dins els directori \$HOME/portafib/scripts/sqlgenerator existeix un generador d'scripts sql a partir de les anotacions Hibernate-JPA per qualsevol BBDD que suporti Hibernate. Llegir el readme.txt del mateix directori (Requereix compilar el codi. Veure punt "5.1.-ANNEX I: Compilar PortaFIB des de subversion de sourceforge");

⁶ portafib_create_data_caib.sql: incorpora els tipus de documents del Portafirmas de la CAIB

⁷ portafib_carrecs_caib.sql: Conté una taula adicional on els agents de seycon actualitzaran les dades dels càrrecs i disparadors que cridaran a certes URL per actualitzar els corresponents càrrecs dins PortaFIB.



4.2.4.- Sortir

/q

4.3.- Crear usuari i BBDD per la gestió d'usuaris PortaFIB.

Aquest punt només és necessari si no tenim definida cap font d'usuaris amb que autenticar i autoritzar l'accés a portafirmes.

Per això realitzarem les mateixes passes descrites en el punt "4.1.-Crear usuari i BBDD per PortaFIB" però amb les següents dades:

- Nom de bbdd: seycon
- Usuari: seycon
- Contrasenya: seycon
- Script de creació de bbdd: \$HOME/portafib/scripts/development/seycon.sql
- Script de creació de dades: \$HOME/portafib/scripts/development/seycon-data.sql

Nota: Podem no voler donar d'alta el conjunt d'usuaris de dins seycon-data.sql, per la qual cosa no es necessari. Únicament per accedir a portafib requerim donar d'alta un usuari dins la taula sc wl usuarii associar-li el role PFI ADMIN dins la taula sc wl usugru.

5.- Annexes

5.1.- ANNEX I: Compilar PortaFIB des de subversion de sourceforge

Aquest manual explica com compilar l'aplicació PortaFIB a partir del repositori de subversion de sourceforge. Es requerix JDK 1.6, ant i maven (versió mínima 3.0.2). La compilació es realitzarà en un directori portafib del home de l'usuari (\$HOME/portafib).

5.1.1.- SVN CheckOut

Estant en el home de l'usuari fer check out d'una branca o un tag executant la següent



comanda:

BRANCA

\$svn co http://subversion.ibit.org/portafib/portafib-core/branches/portafib-x.y

BRANCA

\$svn co http://subversion.ibit.org/portafib/portafib-core/tags/portafib-x.y.z/

5.1.2.- Llibreries sense repositori a Internet

Anar a \$HOME/portafib/lib i executar les següents comandes:

```
$ install_ibkeyapi_jar.sh
$ install_afirma_miniapplet_jar.sh
$ install_axis_jaxrpc_jar.sh
```

Aquestes comandes serveixen per ficar dins del repositori MAVEN llibreries que no es poden descarregar de cap repositori d'Internet. Nota: trobareu també els fitxers .bat si feis feina amb Windows.

5.1.3.- Firma del jar l'Applet o Applet firmat per defecte

Applet del PortaFIB requereix que estigui firmat. A partir de la versió de java 1.7.0_45 requereix que aquesta firma estigui dins el repositori de d'entitats en que java confia. En cas contrari no executa l'applet.

La forma més senzilla es emprar l'applet ja firmat ubicat dins el directori \$HOME/portafib/lib, que s'explica en el punt

5.1.3.1.- Utilitzar Applet ja Firmat

Anar a \$HOME/portafib/lib i executar la següent comanda:

```
$ install_portafib_applet_signed_jar.sh
```

Aquesta comanda serveix per ficar dins del repositori MAVEN l'applet signat per a que sigui utilitzat en la resta del codi del PortaFIB. Nota: trobareu també el fitxer .bat si feis feina amb windows.

5.1.3.2.- Compilar i Firmar l'Applet



En cas que volguem desenvolupar l'applet llavors requerin de dues passes: primera, definir el certificar amb el que es firmarà l'applet i segona indicar a maven que volem compilar l'applet (utilitzar el paràmetre -Papplet).

Per definir el certificat amb el que firmar el jar de l'applet necessitem un keystore anomenat afirma.keystore amb contrasenya "afirma" situat en l'arrel del projecte. En aquest keystore hi ha d'anar el certificat amb amb alies "codesign" i contrasenya "afirma".

Teniu un exemple de keystore amb un certificat de firma dins el directori \$HOME/portafib/scripts/certificats/afirma.keystore executar la següent comanda:

\$ cp \$HOME/portafib/scripts/certificats/afirma.keystore \$HOME/portafib

El certificat contingut en aquest keystore és de proves, per lo que si alguna entitat vol utilitzar un certificat reconegut per firmat l'applet llavors no hi ha cap problema, només ha de seguir les instruccions abans descrites.

5.1.4.- Compilació

Tal i com s'ha explicat en la introducció, es poden generar ears amb diferents característiques segons el paràmetres emprats durant la compilació. Si escriviu help.sh /.bat vos apareixeran totes les opcions possibles excepte dues que sempre una o l'altra es requerida:

- -Pdesenvolupament: s'utilitza en desenvolupament i el que fa es carregar els plugins dins el propi ear de PortaFIB
- -Pproduccio: s'utilitza en producció i separa el codi de PortaFIB en un ear i els plugins en un altra ear.

Tipus	Paràmetres Maven	Output
Desenvolupament	-Pdesenvolupament	/ear/target/portafib.ear
Producció	-Pproduccio	/ear/target/portafib.ear /earplugins/target/portafib_plugins.ear

Existeixen dos scripts que ens ajuden en la tasca de compilació i que a més ens copien l'ear al JBoss i son deploydev.sh/.bat i deploypro.sh/.bat respectivament per desenvolupament i producció. Opcionalment emprant aquests scripts, si definim la variable d'entorn de sistema PORTAFIB_DEPLOY_DIR apuntant al directori de deploy de jboss, llavors després de cada execució es copiaran els ear/ears a aquest directori de deploy. A aquests scripts se li poden afegir els següent paràmetres (executar comanda help.sh/.bat per veure la llista actualitzada)



Paràmetre	Descripció
clean	Neteja el projecte abans de recompilar
-Psqlgen	Genera scripts SQL dins /scripts/sqlgenerator. Més informació a /scripts/sqlgenerator/readme.txt
-Papplet	Compila l'applet i el firma amb el afirma.keystore. Sinó s'ha d'executar install_portafib_applet_signed_jar.sh/bat
-Pclientcert	Si volem un segon context web amb autenticació CLIENT-CERT (context a /portafibs)
-Pws-portafirmas	WS compatible amb l'API del PortaFirmas antic de la CAIB (Context a /portafirmasws)
-Pws-portafirmas-callback- server	WS per provar la recepció dels Callback del PortaFirmas antic de la CAIB. Els usuaris aplicació han de tenir callback url apuntant a http://HOST:8080/portafib/portafirmascb/v0/PortafirmasCallBack callback versió 1. Per veure les cridades accedir a http://HOST:8080/portafib/portafirmascb
-Pws-portafib	WS per atacar a PortaFIB (Context /portafibws) (Exemple de cridada a ws\portafib_client)
-Pws-portafib-callback- server	WS per provar la recepcio dels Callback de PortaFIB. Els usuaris aplicacio han de tenir callback url http://HOST:8080/portafib/cb/v1/PortaFIBCallBack i callback versio 1. Per veure les cridades accedir a http://HOST:8080/portafib/portafibcb

Per exemple si volguéssim compilar amb mode Desenvolupament i afegir-hi un segon context amb autenticació ClientCert i a més l'applet llavors executaríem la següent comanda:

\$ mvn -Pdesenvolupament -Pclientcert -Papplet clean install

O emprant els scripts

\$ deploydev.sh -Pclientcert -Papplet

5.2.- Annex II: Creació de Keystore i Truststore per JBoss

5.2.1.- Introducció

Aquest fitxers també es poden generar seguint els scripts del fitxer



portafib/scripts/certificats (certificats.bat per generar els certificat de l'autoritat certificadora, certificats de servidor i certificats d'usuari, executar importdni.bat per afegir el certificat arrel del DNIe al certificats de servidor) o seguint les passes descrites a la pàgina web http://www.adictosaltrabajo.com/tutoriales/tutoriales.php? pagina=JBossClientCert. D'aquests fitxers hem de saber:

- Certificats de servidor(jboss.keystore i jboss.truststore): serveixen per indicar al navegador quins certificats son acceptats i per la qual cosa només es mostraran aquells que tenguin com a entitat pare els definits en el servidor.
- 2) Certificats d'usuari (anadal.crt i anadal.pcks12): corresponen al certificat public i la clau privada per l'usuari anadal. Serveixen per afegir-los al magatzems de certificats dels navegadors. Altres certificats que no requereixen afegir-los al magatzems són els certificats emmagatzemats en dispositius segurs com targetes intel·ligents.

5.2.2.- Afegir certificats a keystore:

```
keytool -importcert -file CamerFirma_Root.cer -keystore jboss.keystore -storepass fundaciobit keytool -importcert -file CamerFirma_Root.cer -keystore jboss.truststore -storepass fundaciobit
```

5.2.3.- Llistar certificats de keystore

```
keytool -list -keystore jboss.keystore -storepass fundaciobit
```

5.2.4.- Configurar Navegadors amb Certificats de Client

Amb els certificats de servidor configurats tal i com estan en els exemples es pot autenticar emprant el DNIe i si es vol utilitzar el certificat de l'usuari anadal llavors s'han de configurar els navegador d'aquesta forma:

- Firefox: Per firefox anirem a l'apartat de certificats i importarem el anadal.crt
- Chrome i lExplorer: requereixen la clau privada anadal.pcks i el certificat public de l'entitat certificador (fundaciobit_ca.crt). Anirem al Panell de Control, Opcions d'Internet (pipella de contingut) i dins l'apartat de certificats i importarem els dos.



5.3.- Annex III Configurar OpenOffice com a servei en Linux

5.3.1.- Instal·lar OpenOffice

Executar la següent comanda per instal·lar OpenOffice en un sistema Linux:

apt-get install openoffice.org

5.3.2.- Arrancar OpenOffice com a Servei

Crearem el fitxer "openoffice" en el directori /etc/init.d amb el contingut que es descriu en el punt "5.3.3.-Script per Arrancar OpenOffice com a Servei". Per fer que el sistema executi cada vegada que arranca aquest script s'ha d'executar la següent comanda dins del directori /etc/init.d/:

\$ sudo chmod 777 /etc/init.d/openoffice
\$ chkconfig -add openoffice



5.3.3.- Script per Arrancar OpenOffice com a Servei

```
#!/bin/bash
### BEGIN INIT INFO
### END INIT INFO
# openoffice.org headless server script
# chkconfig: 2345 80 30
# description: headless openoffice server script
# processname: openoffice
# Author: Vic Vijayakumar
# Modified by Federico Ch. Tomasczik
OOo HOME=/usr/bin
SOFFICE_PATH=$000_HOME/soffice
PIDFILE=/var/run/openoffice-server.pid
set -e
case "$1" in
start)
if [ -f $PIDFILE ]; then
echo "OpenOffice headless server has already started."
sleep 5
exitq
echo "Starting OpenOffice headless server"
$SOFFICE_PATH -headless -nologo -nofirststartwizard
-accept="socket, host=0.0.0.0, port=8100; urp" & > /dev/null 2>&1
touch $PIDFILE
;;
stop)
if [ -f $PIDFILE ]; then
echo "Stopping OpenOffice headless server."
killall -9 soffice && killall -9 soffice.bin
rm -f $PIDFILE
exit
fi
echo "Openoffice headless server is not running."
exit
*)
echo "Usage: $0 {start|stop}"
exit 1
esac
exit 0
```