



Instal·lació de PortaFIB

Guia Ràpida d'Instal·lació de PortaFIB



Govern de les Illes Balears

Vicepresidència i Conselleria
d'Innovació, Recerca i Turisme

Direcció General de Desenvolupament Tecnològic



Govern de les Illes Balears

Fundació Balear d'Innovació i Tecnologia



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	18/04/2016
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 custòdia 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 Custòdia-Fitxers	A. Nadal	07/04/2015
Taula de tamany de PDF suportat	A. Nadal	23/06/2015
Noves propietats (firmatperformat, automaticredirect i motiudelegacioformat)	A. Nadal	02/07/2015
Millorar Documentació sobre connexió HTTPS	A. Nadal	09/09/2015
Actualitzar a versió 1.1	A. Nadal	03/02/2016
Migració GitHub	A. Nadal	26/02/2016

Font documental.



Index de Contingut

1.-Introducció.....	5
2.-Configurar JBOSS.....	5
2.1.-Instal·lació de JBoss.....	5
2.2.-Configurar Servidor JBoss.....	6
2.2.1.-Directori de PortaFIB.....	6
2.2.2.-Port Segur HTTPS.....	7
2.2.3.-Publicar Ports a peticions externes.....	7
2.2.4.-Requeriments de memòria.....	7
2.2.5.-Permetre consultes sobre múltiples Datasources.....	8
2.2.6.-Autenticador WSBASIC.....	8
2.3.-Fitxers de Configuració.....	8
2.3.1.-Fitxer JDBC d'accés a BBDD.....	8
2.3.1.1.-Oracle.....	8
2.3.1.2.-PostgreSQL.....	8
2.3.2.-Fitxer de Propietats.....	9
2.3.2.1.-Propietats Generals PortaFIB.....	9
2.3.2.2.-Plugins.....	16
2.3.3.-Configurar Coes.....	16
2.3.4.-Configurar Servidor de Correu.....	17
2.3.5.-Autenticació i Autorització per Usuaris Persona.....	17
2.3.6.-Autenticació i Autorització per Usuaris Aplicació.....	18
2.4.-Copia de binaris.....	18
2.5.-DataSources.....	19
3.-Plugins.....	19
3.1.-Plugin de Conversió de Documents.....	20
3.2.-Plugin de Certificat.....	20
3.2.1.-Plugin Fake.....	20
3.2.2.-Plugin @firma CXF.....	20
3.2.3.-Plugin @firma.....	21
3.3.-Plugin de Informació d'Usuari.....	22
3.3.1.-Plugin de UserInformation via DataBase.....	22
3.3.2.-Plugin de UserInformation via LDAP.....	23
3.4.-Plugin de Custòdia Documental.....	25
3.5.-Plugins de Firma WEB.....	25
4.-Gestió de BBDD.....	25
4.1.-Crear usuari i BBDD per PortaFIB.....	25
4.1.1.-Connectar-se a la BBDD.....	25
4.1.2.-Crearem l'usuari portafib:.....	25
4.1.3.-Crear la BBDD.....	26
4.2.-Crear esquema de taules i inserir dades.....	26
4.2.1.-Connectar-se al servidor de BBDD amb l'usuari portafib:.....	26
4.2.2.-Donam permisos al usuari:.....	26
4.2.3.-Importam l'estructura de taules i dades dins la BBDD.....	26
4.2.4.-Sortir.....	27
4.3.-Crear usuari i BBDD per la gestió d'usuaris PortaFIB.....	27
5.-Annexes.....	28
5.1.-Compilar PortaFIB des de Git de GitHub.....	28



5.1.1.-Git Clone.....	28
5.1.2.-Llibreries sense repositori a Internet.....	28
5.1.3.-Firma del jar l'Applet o Applet firmat per defecte.....	28
5.1.3.1.-Utilitzar Applet ja Firmat.....	29
5.1.3.2.-Compilar i Firmar l'Applet	29
5.1.4.-Compilació.....	29
5.2.-Connexions HTTPS i ClientCert en JBoss.....	31
5.2.1.-Magatzem amb el certificats de client acceptats.....	31
5.2.1.1.-Crear KeyStore Built.....	31
5.2.1.2.-Incorporar certificats de confiança.....	32
5.2.1.3.-Copiar fitxer de truststore a JBOSS.....	32
5.2.2.-Magatzem amb la identitat del servidor per connexions https.....	32
5.2.2.1.-Certificat d'Identitat de proves per connexions https.....	33
5.2.2.2.-Certificat d'Identitat d'una Autoritat de Confiança per connexions https.....	33
5.2.3.-Configurar https en el JBOSS.....	34
5.2.3.1.-Configurar Port 8443 (https) del JBOSS.....	34
5.2.3.2.-Afegir autenticador sobre Certificats.....	35
5.2.4.-Compilar PortaFIB per ClientCert.....	35
5.2.5.-Exemple d'Accés.....	35
5.3.-Creació d'un certificat de proves de Client.....	37
5.3.1.-Introducció.....	37
5.3.2.-Crear Autoritat de Certificació.....	37
5.3.3.-Afegir certificat arrel de l'Autoritat de Confiança dins jboss.truststore.....	38
5.3.4.-Crear un certificat d'usuari de l'autoritat certificadora de proves.....	38
5.4.-Configurar OpenOffice com a servei en Linux.....	40
5.4.1.-Instal·lar OpenOffice.....	40
5.4.2.-Arrancar OpenOffice com a Servei.....	40
5.4.3.-Script per Arrancar OpenOffice com a Servei.....	41
5.5.-Tamany de PDF suportat.....	42
5.5.1.-Pujada de PDF des de entorn WEB.....	42
5.5.2.-Pujada de PDF des de entorn WebServices.....	42
5.5.3.-Firma de Fitxers des del Mòdul de firma MiniApple com Applet.....	43
5.6.-Gestió de Rols a través de triggers Oracle.....	43
5.7.-Configuració Apache 2.2.14 o superior per connectar amb PortaFIB.....	44
5.7.1.-Crear Certificats de Prova per Apache.....	44
5.7.2.-Instal·lació i Configuració Apache 2.2.14 (o superior).....	45
5.7.2.1.-Instal·lació.....	45
5.7.2.2.-Afegir mòduls SSL i proxy.....	45
5.7.2.3.-Configurar Connexió SSL.....	45
5.7.2.4.-Activar Virtual Host 443.....	46
5.7.2.5.-Redirecció pel port 80.....	46
5.7.2.6.-Host permesos per atacar PortaFIB.....	47
5.7.2.7.-Obrir firewall pels ports 80 i 443.....	47
5.7.2.8.-Reiniciar l'apache.....	47



1.- Introducció

Aquest document exposa les passes per posar en marxa una instància 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 través 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.-Compilar PortaFIB des de Git de GitHub" d'aquest document per generar el binari a partir del codi font

(B) DESCARREGAR BINARI: Accedint al projecte portafib de GitHub, podem descarregar el binaris corresponents. Accedir via web a la següent adreça <https://github.com/GovernIB/portafib/tree/binaris/portafib-1.0/portafib-1.0.0/bin> i descarregar el fitxer de la versió desitjada. 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 emprem un JBoss 5.1.0 GA que podem descarregar de <http://sourceforge.net/projects/jboss/files/JBoss/JBoss-5.1.0.GA/>. D'aquesta adreça descarregarem el següent fitxer jboss-5.1.0.GA-jdk6.zip i el descomprimem dins un directori /usr/local/jboss-as. Aquesta versió de JBoss conté un petit bug² que es soluciona descarregant una versió més moderna del jar jboss-metadata.jar (https://repository.jboss.org/nexus/content/repositories/root_repository/jboss/metadata/1.0.6.GA-brew/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): jboss-patch-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/default/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>



```
...  
property name="applicationURIs">  
  <list elementClass="java.net.URI">  
    <value>${jboss.server.home.url}deploy</value>  
    <value>${jboss.server.home.url}deployportafib</value>  
  </list>  
</property>  
...
```

I finalment crearem el nou directori deployportafib:

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

2.2.2.- Port Segur HTTPS

Per defecte JBoss fa feina sobre el port 8080 amb protocol HTTP. Podem afegir comunicació segura i/o autenticació via ClientCert afegint un port addicional 8443 amb protocol HTTPS.

Com que aquest punt és opcional, descrivim les passes a seguir per afegir un port segur en el punt "5.2.-Connexions HTTPS i ClientCert en JBoss".

2.2.3.- Publicar Ports a peticions externes

Si volem que el nostre jboss sigui accessible des de fora del nostre propi ordinador llavors heu d'editar el fitxer run.conf (o run.conf.bat si estem amb Windows) de \$JBASS/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 recomana donar la major memòria possible al JBoss ja que Portafib és una aplicació web bastant pesada. Obrir run.conf (o run.conf.bat si estem amb Windows) de \$JBASS/bin i editar els parametres -Xms i Xmx i posar-li aquests valors:

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

Segons el tamany de Fitxers a ser enviats via WebServices s'haurà de modificar aquesta condifuració segons les taules descrites en el punt "5.5.2.-Pujada de PDF des de entorn WebServices"



2.2.5.- Permetre consultes sobre múltiples Datasources

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

```
<property 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:

```
<entry>
  <key>WSBasic</key>
  <value>org.apache.catalina.authenticator.BasicAuthenticator</value>
</entry>
```

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 nostra 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 \$JBASS/server/default/deployportafib:

```
$ sudo cp $HOME/portafib/scripts/config/portafib-properties-service.xml
$JBASS/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
├─ META-INF
│   └─ jboss-service.xml
└─ MANIFEST.MF
```

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

```
Manifest-Version: 1.0
Archiver-Version: Plexus Archiver
Created-By: Apache Maven
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.*	<p>Propietats de Configuració Hibernate: Estableix les propietats de configuració de Hibernate. Les dues propietats més importants són:</p> <ul style="list-style-type: none"> • es.caib.portafib.hibernate.dialect • es.caib.portafib.hibernate.query.substitutions <p>En PostgreSQL la propietat 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.</p>
es.caib.portafib.filesdirectory	<p>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.</p>
es.caib.portafib.url (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	<p>És l'adreça pública d'accés al portafirmes: es.caib.portafib.url=http://localhost:8080/portafib</p>
es.caib.portafib.email.from (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	<p>És l'adreça d'email des d'on s'enviaran les notificacions per correu als usuaris: es.caib.portafib.email.from=portafib@portafib.org</p>
es.caib.portafib.defaultlanguage	<p>Idioma per defecte. Valors possibles poden ser “ca” per català i “es” per castellà. es.caib.portafib.defaultlanguage=ca</p>



<p>es.caib.portafib.defaultentity (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)</p>	<p>Si val null indicam que l'Administrador d'Entitat ha de donar d'alta la persona i després l'usuari-entitat associat a aquella persona. Si aquest valor conté l'identificador d'una entitat, llavors els usuaris autenticats, automàticament seran registrats com a persones i associats a aquesta entitat.</p> <div data-bbox="750 573 1436 788">  <p><i>En l'entorn de la CAIB (Govern Balear) quan la propietat es.caib.portafib.iscaib=true, llavors sempre l'usuari es dona d'alta automàticament en l'entitat "caib" independentment del valor d'aquesta propietat.</i></p> </div>
<p>es.caib.portafib.defaultrolesincreation (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)</p>	<p>S'utilitza conjuntament amb la propietat "es.caib.portafib.defaultentity". Indica els rols virtuals a assignar per defecte a l'usuari-entitat quan aquest es crea automàticament. Es tracta d'una llista de rols separats per comes. Els valors possibles són:</p> <ul style="list-style-type: none"> • Sol·licitant: ROLE_SOLI • Destinatarí: ROLE_DEST • Delegat: ROLE_DELE • Col·laborador: ROLE_COLA <div data-bbox="750 1205 1436 1420">  <p><i>En l'entorn de la CAIB (Govern Balear) quan la propietat es.caib.portafib.iscaib=true, llavors a l'usuari-entitat sempre se li assigna el rol Destinatarí (ROLE_DEST) independentment del valor d'aquesta propietat.</i></p> </div>
<p>es.caib.portafib.development</p>	<p>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</p>
<p>es.caib.portafib.checknifcertificate (PortaFIB 1.1.0 Deprecat 13/11/2015: Mirar propietat "Comprovar NIF després de Firmar" dins l'Entitat)</p>	<p>Si val true quan es firma un document comprova que el DNI de la persona que ha firmat (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</p>



es.caib.portafib.maxuploadsizeinbytes ³ (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	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 ⁴ (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	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 (PortaFIB 1.1.0 Deprecat 12/01/2016: Eliminada ja que no s'usava)	Nom de l'aplicació PortaFIB: es.caib.portafib.name=PortaFIB
es.caib.portafib.editableuser (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	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.defaultsignalalgorithmid (PortaFIB 1.1.0 Deprecat 13/11/2015: Mirar camp "Algorisme de Firma" dins l'Entitat)	Camp opcional. Defineix l'identificador de l'algorisme a utilitzar per defecte durant la firma de documents o fitxers. Fa referència al camp ID de la taula pfi_algorismedefirma. Els valors possibles d'una instal·lació per defecte són: <ul style="list-style-type: none"> • 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.plugins.exportdata.csv.CSVPlugin,org.fundaciobit.plugins.exportdata.ods.ODSPlugin,org.fundaciobit.plugins.exportdata.excel.ExcelPlugin
es.caib.portafib.numberoferrorsinnotificationtosendmail (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	Opcional. 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.

³ Revisar punt 5.5.-Tamany de PDF suportat

⁴ Revisar punt 5.5.-Tamany de PDF suportat



es.caib.portafib.numberoferrorstopausenotification (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	Opcional. 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.notificationtimelapse (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	Opcional. Valor per defecte 60000ms (1 minut). Ha de ser major de 15000. Temps mínim que s'espera abans de reintentar una notificació ws fallida en ms Exemple (15 segons):- es.caib.portafib.notificationtimelapse=15000
es.caib.portafib.applet.signerClass (PortaFIB 1.1.0 Deprecat 10/11/2015: S'usen els Mòduls de Firma)	Indica al PortaFIB quina API emprarem per firmar els documents. Valors possibles són: <ul style="list-style-type: none"> • Firma de documents emprant @firma: es.caib.portafib.applet.signers.AfirmaSigner • Firma emprant IB-KEY: es.caib.portafib.applet.signers.IBKeySigner
es.caib.portafib.automatredirect (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	Si el valor és true llavors redirecciona segons el contexte: — (a) Si entra amb http dins /portafib/s llavors redirecciona a /portafib — (b) Si entra amb https dins /portafib i existeix /portafib/s llavors redirecciona a /portafib/s Si el valor és false, llavors no intenta fer cap redirecció.



<p>es.caib.portafib.firmatperformat.{entitat_id}. {idioma} (PortaFIB 1.1.0 Deprecat 13/11/2015: Mirar propietat "Format de 'Firmat Per'" de l'Entitat)</p>	<p>Opcional. Format del camp "Firmat Per" de la taula de firmes definit per entitat i per idioma. Els camps disponibles són (s'obtenen del certificat amb el que s'ha firmat):</p> <ul style="list-style-type: none"> • {0} = NOM • {1} = LONGITUD NIF • {2} = NIF • {3} = EMISSOR • {4} = LONGITUD CARREC_CERTIFICAT • {5} = CARREC_CERTIFICAT • {6} = LONGITUD UNITAT_ADMINISTRATIVA • {7} = UNITAT_ADMINISTRATIVA <p>Exemple de formats per l'entitat caib pels idiomes català i castellà:</p> <pre>es.caib.portafib.firmatperformat.caib.ca={0} {4,choice,0#11&lt;C\u00E0rrec {5}} {6,choice,0#11&lt;Unitat {7}} es.caib.portafib.firmatperformat.caib.es={0} {4,choice,0#11&lt;Cargo {5}}{6,choice,0#11&lt;Unidad {7}}</pre> <p>NOTA: S'han d'escapar els accents i caràcters especials a XML. Per exemple 'à' → \u00E0 o '<' → &lt;</p>
<p>es.caib.portafib.motiudelegacioformat. {entitat_id}. {idioma} (PortaFIB 1.1.0 Deprecat 13/11/2015: Mirar propietat "Format del motiu per delegació" de l'Entitat)</p>	<p>Opcional. Format del camp "Motiu" de la taula de firmes quan es tracta d'una delegació definit per entitat i idioma. Els paràmetres disponibles són:</p> <ul style="list-style-type: none"> • {0} Nom del delegat • {1} NIF del delegat • {2} Nom del destinatari • {3} NIF del destinatari • {4} Motiu de la delegació • {5} Motiu de la petició de firma <p>Exemple de formats per l'entitat caib pels idiomes català i castellà:</p> <pre>es.caib.portafib.motiudelegacioformat.caib.ca=F irma {0} ({1}) per delegaci\u00F3 de {2} ({3}). Motiu: {4} es.caib.portafib.motiudelegacioformat.caib.es=F irma {0} ({1}) por delegaci\u00F3n de {2} ({3}). Motivo: {4}</pre> <p>NOTA: S'han d'escapar els accents i caràcters especials a XML emprant Unicode. Per exemple 'ó' → \u00F3</p>



es.caib.portafib.entitadforagentssql (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	Opcional excepte en entorns de la CAIB. Entitat sobre la qual s'aplicaran les accions del "Agents-Seycon". Veure punt "5.6. Gestió de Rols a través de triggers Oracle" per més informació.
es.caib.portafib.passwordforagentssql (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	Opcional excepte en entorns de la CAIB. Contrasenya (o clau de pas) per comprovar que les peticions http realment provenen d'un trigger de BBDD. Veure punt "5.6. Gestió de Rols a través de triggers Oracle" per més informació.
es.caib.portafib-maxitemstoshowinautocomplete (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats d'Entitat del menú d'Administrador d'Entitat)	Opcional. Valor per defecte 10. En els formularis de cerques dinàmiques d'usuari, indica el màxim de resultats permesos per mostrar resultats de l'usuari. Modificar dades de Persona Seleccioni la Persona de la que vol modificar les seves dades <div> <div>Usuari (*)</div> <div> <input type="text"/> <div> <div>Escriui part del nom, del NIF i/o del username, o tria un favorit pitjant sobre ★</div> <div>★ ▼</div> </div> </div> <div>Ha d'escriure com a mínim 2 caràcters i que els criteris seleccionin manco de 10 usuaris per mostrar-se la cerca.</div> <div> <div>Continuar</div> <div>Cancel·lar</div> </div> </div>
es.caib.portafib-mincharstostartautocomplete (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats d'Entitat del menú d'Administrador d'Entitat)	Opcional. Valor per defecte 2. En els formularis de cerques dinàmiques d'usuari, indica el mínim de caràcters que ha d'escriure l'usuari abans de que li apareguin els resultats de la cerca. En entitats amb molts d'usuaris es recomana incrementar aquest valor a 3 o 4 amb la finalitat de reduir càrrega de xarxa, processador i bbdd. Relacionat amb la propietat <i>es.caib.portafib-maxitemstoshowinautocomplete</i>
es.caib.portafib.defaultcustodymessage-: {entitat_id}-{idioma} (PortaFIB 1.1.0 Deprecat 13/11/2015: Mirar camp "Cutòdia per Defecte" de l'Entitat)	Indica un missatge per defecte de la custòdia de les peticions de Firma, definit per entitat i per idioma. Exemple: <i>es.caib.portafib.defaultcustodymessage.fundacio bit.ca=Data:{3} URL de validaci\u00F3: {0}</i> <i>es.caib.portafib.defaultcustodymessage.fundacio bit.es=Fecha:{3} URL de validaci\u00F3n: {0}</i>
es.caib.portafib.maxtimelockedsigninms (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats d'Entitat del menú d'Administrador d'Entitat)	Opcional. Indica Temps de validesa del Token de Firma només quan hi ha múltiples firmes en un bloc o hi ha delegats definits. Es a dir, el temps màxim que un firmant pot tenir bloquejat un document mentre es realitza el procés de firma. Valor per defecte 3*60*1000, o sigui 3 minuts. Quan la firma és única en el bloc i no hi ha delegats definits llavors no hi ha bloqueig de temps



es.caib.portafib.emailsgroupedsendercronexpression (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	Opcional. Expressió cron que indica cada quan s'ha d'executar l'enviador de correus quan s'han definit enviaments d'avisos agrupats. Per defecte s'executa cada dia a les 6:00 (-). Exemple:- • L'executa cada dos minuts: 0 0/2 * 1/1 * ? * • L'executa cada dia a les 6:00: 0 0 6 1/1 * ? * Veure www.cronmaker.com per altres valors.
es.caib.portafib.checkcertificateincllientcert	Opcional. Indica si s'ha de validar el certificat emprant el Plugin de CheckCertificate quan l'autenticació es realitza emprant ClientCert. Valor per defecte false. Exemple: es.caib.portafib.checkcertificateincllientcert=true
es.caib.portafib.signaturemodule.absoluteurl (PortaFIB 1.1.0 Deprecat 12/01/2016: Migrat a Propietats Globals del menú d'Administrador)	Opcional. Si no es defineix llavors obté la URL absoluta de la petició (Pot haver hi problemes si el Apache Proxy no té activat "ProxyPreserveHost On"). Si és defineix s'utilitzarà aquesta URL com ruta absoluta en els plugins de firma web que ho requereixin (JavaWebStart, SIA, ...). Serveix per Plugins de Firma que han d'accedir externament al Servidor de PortaFIB. Exemple: es.caib.portafib.signaturemodule.absoluteurl= http://portafib.ibit.org/portafib

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 notifiacions 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
$JBOSSE/server/default/deployportafib

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




2.3.4.- Configurar Servidor de Correu

Per l'enviament de correus necessitem 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 rols guardats dins una base de dades, per això a continuació configurarem el JBoss per accedir a aquestes dades.

Obrim 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"
flag="sufficient">
    </login-module>
    <!-- DATABASE -->
    <login-module code="org.jboss.security.auth.spi.DatabaseServerLoginModule"
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 mòduls 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 empen 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:

```
<application-policy name = "seycon">  
  <authentication>  
  
    ...  
  
    <!-- DATABASE -->  
    <login-module code="org.jboss.security.auth.spi.DatabaseServerLoginModule"  
flag="sufficient">  
      <module-option name="dsJndiName">java:/es.caib.portafib.db</module-option>  
      <module-option name="principalsQuery">  
        SELECT contrasenya FROM pfi_usuariaplicacio WHERE usuariaplicacioid = ?  
      </module-option>  
      <module-option name="rolesQuery">  
        SELECT roleid, 'Roles' FROM pfi_roleusuariaplicacio where usuariaplicacioid = ?  
      </module-option>  
    </login-module>  
  
  </authentication>  
</application-policy>
```

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, les 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 es podrà definir autenticació CLIENT-CERT dins un context /portafib/s

Amb qualsevol combinació necessitem l'ear portafib:

```
$ sudo cp $HOME/portafib/ear/target/portafib.ear $JBOSSE/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 fitxer:

```
$ sudo cp $HOME/portafib/earplugins/target/portafib_plugins.ear  
$JBOSSE/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  
$JBOSSE/server/default/deployportafib
```

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

3.- Plugins

Les propietats que es descriuen a continuació 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 “5.4.-Configurar OpenOffice com a servei en Linux” es mostra com posar un OpenOffice en 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 `es.caib.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:

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: <ul style="list-style-type: none"> MODE_VALIDACIO_SIMPLE = 0 MODE_VALIDACIO_AMB_REVOCACIO = 1 MODE_VALIDACIO_CADENA = 2
COMUNICACIO VIA USUARI CONTRASENYA⁵	
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.
COMUNICACIO 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-dgiddt.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 després es desconfiguren.
es.caib.portafib.plugins.certificate.afirma.authorization.ks.password	Contrasenya d'accés al KeyStore. Aquesta contrasenya s'utilitza per accedir al keystore c
es.caib.portafib.plugins.certificate.afirma.authorization.ks.cert.alias	Defineix l'alias 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.

⁵ Aquest tipus d'establiment de connexió ja no és vàlid quan s'ataca a la web de producció de @firma

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 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/O ⁶	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
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

⁶ R = Requerit | O = Opcional



es.caib.portafib.plugins.userinformation.database.surname_column	O	Nom de la columna que conté els llinatges de la persona
es.caib.portafib.plugins.userinformation.database.language_column	O	Nom de la columna que conté l'idioma de la persona (ca, es, en, ...)
es.caib.portafib.plugins.userinformation.database.telephone_column	O	Nom de la columna que conté el telefon de la persona
es.caib.portafib.plugins.userinformation.database.email_column	R	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.database.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.database.username_column_in_roles_table=UGR_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.database.rolename_column=UGR_CODGRU

(*) Aquests camps són opcionals sí des de l'aplicació que empra el plugin no realitza 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 ⁷	Descripció
es.caib.portafib.plugins.userinformation.ldap.host_url	R	Servidor de LDAP.Exemple: es.caib.portafib.plugins.userinformation.ldap.host_url=ldap://ldap.fundaciobit.org:389

⁷ R = Requerit | O = Opcional



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.security_authentication=simple
es.caib.portafib.plugins.userinformation.ldap.users_context_dn	R	Context on es troben els usuaris. es.caib.portafib.plugins.userinformation.ldap.users_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.search_scope=onelevel
es.caib.portafib.plugins.userinformation.ldap.search_filter	R	Filtre de cerca. Exemple: es.caib.portafib.plugins.userinformation.ldap.search_filter=((memberOf=CN=@PFI_ADMIN,CN=Users,DC=ibitnet,DC=lan) (memberOf=CN=@PFI_USER,CN=Users,DC=ibitnet,DC=lan))
es.caib.portafib.plugins.userinformation.ldap.attribute.username	R	Nom de l'usuari. Exemple: es.caib.portafib.plugins.userinformation.ldap.attribute.username=sAMAccountName
es.caib.portafib.plugins.userinformation.ldap.attribute.mail	R	Correu de l'usuari. Exemple: es.caib.portafib.plugins.userinformation.ldap.attribute.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.attribute.administration_id=postOfficeBox
es.caib.portafib.plugins.userinformation.ldap.attribute.name	R	Nom de l'usuari. Exemple: es.caib.portafib.plugins.userinformation.ldap.attribute.name=givenName
es.caib.portafib.plugins.userinformation.ldap.attribute.surname	O	Llinatges de l'usuari. Exemple: es.caib.portafib.plugins.userinformation.ldap.attribute.surname=sn
es.caib.portafib.plugins.userinformation.ldap.attribute.telephone	O	Telefon de l'usuari. Exemple: es.caib.portafib.plugins.userinformation.ldap.attribute.telephone=telephoneNumber
es.caib.portafib.plugins.userinformation.ldap.attribute.memberof	R(*)	Atribut que conté els rols. Exemple: es.caib.portafib.plugins.userinformation.ldap.attribute.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.prefix_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.suffix_role_match_memberof=,CN=Users,DC=ibitnet,DC=lan

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

3.4.- Plugin de Custòdia Documental

S'ha mogut a entorn Web. L'Administrador de PortaFIB ha de donar d'alta el Plugin i després l'Administrador d'Entitat ha de crear una plantilla base. Veure Manual d'Usuari.

3.5.- Plugins de Firma WEB

S'ha de tenir en compte que els plugins de MiniApplet en Client (com Applet o JavaWebStart) i de MiniApplet en Servidor s'adjunten automàticament dins cada distribució de PortaFIB.

Si es desitja el Mòdul de Firma SIA s'ha de compilar PortaFIB emprant el paràmetre -Psia.

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.sql8  
\i $HOME/portafib/scripts/bbdd/[x.y]/oracle/portafib_carrecs_caib.sql9
```

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.-Compilar PortaFIB des de Git de GitHub”);

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

⁸ portafib_create_data_caib.sql: incorpora els tipus de documents del Portafirmas de la CAIB

⁹ 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.



sc_wl_usuarii associar-li el role PFI_ADMIN dins la taula sc_wl_usugru.

5.- Annexes

5.1.- Compilar PortaFIB des de Git de GitHub

Aquest manual explica com compilar l'aplicació PortaFIB a partir del repositori de git de GitHub. 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.- Git Clone

Estant en el home de l'usuari fer clone d'una branca o un tag executant la següent comanda (per exemple branca portafib-1.1:

BRANCA

```
$git clone --branch portafib-1.1 http://github.com/GovernIB/portafib
```

TAG

```
$git clone --branch portafib-1.1.1 http://github.com/GovernIB/portafib
```

5.1.2.- Llibreries sense repositori a Internet

Anar a \$HOME/portafib-x.y/lib i executar les següents comandes:

```
$ install_afirma_miniapplet_jar.sh
$ install_plugin_signatureweb_miniappletui_jar.sh
$ install_axis_jaxrpc_jar.sh
```

Aquestes comandes serveixen per afegir 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 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 deixar que Maven obtengui el jar del repositori local al projecte del codi font.



5.1.3.1.- Utilitzar Applet ja Firmat

No s'ha de fer res ja que maven obté el jar d'un directoi del codi font i el copia al repositori maven de la màquina-usuari local.

5.1.3.2.- Compilar i Firmar l'Applet

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

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 escriuiu 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
-Pbuild	Nomes emprar en desenvolupament. Sistema manual de revisions. Marca una nova data de revisió.
-Psqlgen	Genera scripts SQL dins /scripts/sqlgenerator. Més informació a /scripts/sqlgenerator/readme.txt
-Pminiappletui	Compila l'applet i el firma amb el afirma.keystore. Sinó s'ha d'executar install_portafib_applet_signed_jar.sh/bat
-Psia	Compila i inclou dins l'ear el Modul de Firma de SIA. Requereix llibreries addicionals (llegir plugins-signatureweb\miniappletinserver\sia\requirements.txt)
-Pclientcert	Genera un segon context web amb autenticacio CLIENT-CERT (context a /portafib/s)
-Pws-portafib	Crea WS per atacar a PortaFIB. Els WS definits són /portafib/ws/v1/PortaFIBPeticioDeFirma /portafib/ws/v1/PortaFIBUsuariEntitat /portafib/ws/v1/PortaFIBUsuariAplicacio /portafib/ws/v1/PortaFIBHelloWorld També compila exemples de cridada a ws\portafib_api.
-Pws-portafib-callback-server	Crea 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 versió 1. Per veure les cridades accedir a http://HOST:8080/portafib/portafibcb
-Pws-portafirmas	Crea WS compatible amb l'API del PortaFirmas antic de la CAIB. El WS es accessible des de /portafib/portafirmasws/web/services/CWS. Exemple de cridada a ws\indra_api.
-Pws-portafirmas-callback-server	Crea WS per provar la recepcio dels Callback del PortaFirmas antic de la CAIB. Els usuaris aplicacio han de tenir calback url http://HOST:8080/portafib/portafirmascb/v0/PortafirmasCallBack i callback versió 0. Per veure les cridades accedir a http://HOST:8080/portafib/portafirmascb
clean	Neteja els projectes abans de compilar.



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

```
$ mvn -Pdesenvolupament -Pclientcert -Pminiappletui clean install
```

O emprant els scripts

```
$ deploydev.sh -Pclientcert -Pminiappletui
```

5.2.- Connexions HTTPS i ClientCert en JBoss

A continuació veurem com configurar JBoss per emprar connexions https i connexions https/ClientCert, és a dir emprant http segur i autenticació emprant Certificats.

Abans de res crearem dos fitxers que contenen certificats. El primer que anomenarem jboss.keystore conté un certificat que representa la identitat de la nostra web quan l'usuari hi accedeix via https. El segon fitxer, anomenat jboss.truststore conté certificats arrel d'autoritats de confiança que serviran per indicar al navegador quins tipus de certificats de client acceptam.

Després indicarem a JBoss com convertir els Certificats rebuts en credencials vàlides per autenticar els usuaris i finalment com compilar PortaFIB per suportat ClientCert.

Crearem un directori net on fer feina.

5.2.1.- Magatzem amb el certificats de client acceptats

El truststore, o magatzem amb el certificats de client acceptats pel servidor, serveix per filtrar el tipus de certificats acceptats en la part client o navegador. A continuació es descriu com crear-ne un.

5.2.1.1.- Crear KeyStore Buit

Anirem al directori de feina i executarem les següents comandes:

```
$ keytool -genkey -alias buit -storetype jks -keystore jboss.truststore  
$ keytool -delete -alias buit -storetype jks -keystore jboss.truststore
```

Després de la primera comanda demanarà una contrasenya que ha de ser "fundaciobit". La resta de valors poden ser qualsevol ja que el certificat generat s'esborrarà posteriorment.



Per comprovar que els keystore està buit executar ...

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

Ha de retornar "0 entries"

5.2.1.2.- Incorporar certificats de confiança

Dins el directori [PORTAFIB_CODE]\scripts\certificats_jboss hi ha un subdirectorí anomenat root on hi ha un conjunt de certificats arrel. Copiarem aquest directori "root" al nostre directori de feina.

Ara incorporarem alguns dels certificats arrel més coneguts. La vostra entitat ha d'elegir quins desitja. Executarem les següent comandes:

```
$ keytool.exe -import -keystore jboss.truststore -storepass fundaciobit -file  
.\root\DNI-AC003-RAIZ.crt.cer -alias AcRaizDNIE  
  
$ keytool.exe -import -keystore jboss.truststore -storepass fundaciobit -file  
.\root\FNMT_CLASSE_2_CA.cer -alias AcRaizFNMT  
  
$ keytool.exe -import -keystore jboss.truststore -storepass fundaciobit -file  
.\root\CAMERFIRMA-ROOT-CHAMBERS.crt -alias AcRaizCamerfirma
```

Si tinguéssim algun altre certificat arrel de confiança llavors repetiríem la comanda anterior modificant el paràmetre *-file* i *-alias*.

5.2.1.3.- Copiar fitxer de truststore a JBOSS

Copiar fitxer jboss.truststore a JBOSS\server\default\conf.

5.2.2.- Magatzem amb la identitat del servidor per connexions https

Aquest certificat servirà com a carta de presentació enfront del navegador del client. Podem crear-ne un de proves o podem comprar un certificat de servidor a alguna de les Autoritats Certificadores. A continuació s'expliquen els dos casos.



5.2.2.1.- Certificat d'Identitat de proves per connexions https

Podem ometre aquest punt si tenim un certificat de servidor d'alguna autoritat de confiança i anar directament al punt "5.2.2.2.-Certificat d'Identitat d'una Autoritat de Confiança per connexions https".

Crearem un keystore i emprarem el certificat per defecte que es genera. Per això executarem la següent comanda:

```
$ keytool -genkey -alias jboss -keyalg RSA -keystore ./jboss.keystore
Enter keystore password: fundaciobit
Re-enter new password: fundaciobit
What is your first and last name?
[Unknown]: Oficina Tecnica Administracio Electronica HA DE SER localhost?????
What is the name of your organizational unit?
[Unknown]: Administracio Electronica
What is the name of your organization?
[Unknown]: FundacioBit
What is the name of your City or Locality?
[Unknown]: Palma
What is the name of your State or Province?
[Unknown]: Illes Balears
What is the two-letter country code for this unit?
[Unknown]: ES
Is CN=Oficina tecnica administracio electronica, OU=Administracio Electronica,
O=FundacioBit, L=Palma, ST=Illes Balears, C=ES correct?
[no]: yes
Enter key password for <jboss>
(RETURN if same as keystore password): ↵
```

Finalment copiarem el fitxer jboss.keystore a JBOSS\server\default\conf.

5.2.2.2.- Certificat d'Identitat d'una Autoritat de Confiança per connexions https

Si hem pogut adquirir o comprar un certificat d'alguna de les autoritats de confiança, llavors a continuació s'expliquen les passes per crear el fitxer jboss.keystore. Si no tenim un certificat llavors anar al punt "5.2.2.1.-Certificat d'Identitat de proves per connexions https".

Anirem al directori de feina i executarem les següents comandes per crear un keystore buit:

```
$ keytool -genkey -alias buit -storetype jks -keystore jboss.keystore
$ keytool -delete -alias buit -storetype jks -keystore jboss.keystore
```

Després de la primera comanda demanarà una contrasenya que ha de ser "fundaciobit". La resta de valors poden ser qualsevol ja que el certificat generat s'esborrarà en la següent comanda.

Ara el certificat de confiança el podem tenir en un fitxer de certificat (.cer, .crt, .der, ...) o dins d'un magatzem de claus amb format PKCS12 (.p12)

Si l'autoritat certificadora ens ha passat un fitxer de certificat llavors hem d'executar la següent comanda:



```
$ keytool.exe -import -keystore jboss.keystore -storepass fundaciobit -file  
[FITXER_CERTIFICAT_DE AUTORITAT CONFIANÇA] -alias serveridentity
```

Si l'autoritat certificadora ens ha passat un fitxer de magatzem de claus (.p12) llavors hem d'executar les següents comandes:

- Llistarem els certificats del magatzem .p12

```
keytool -list -keystore [MAGATZEM_AUTORITAT_CONFIANÇA].p12 -storetype PKCS12
```

- De la llista anterior mirarem l'alias del certificat que volem emprar ([ALIAS_P12]) i executarem la següent comanda per moure el certificat del magatzem p12 al keystore

```
keytool -v -importkeystore -srckeystore [MAGATZEM_AUTORITAT_CONFIANÇA].p12 -srcstorepass  
[PASSWORD_P12] -srcalias [ALIAS_P12] -srcstoretype PKCS12 -destkeystore jboss.keystore  
-deststorepass fundaciobit -destalias serveridentity -deststoretype JKS
```

- Ara la contrasenya del keystore (fundaciobit) i la contrasenya del certificat importat ([PASSWORD_P12]) són diferents i hem de fer que siguin iguals. Això es fa executant la següent comanda:

```
keytool -keypasswd -alias serveridentity -keypass [PASSWORD_P12] -new fundaciobit  
-keystore jboss.keystore -storepass fundaciobit
```

Finalment copiarem el fitxer jboss.keystore a JBOSS\server\default\conf.

5.2.3.- Configurar https en el JBOSS

5.2.3.1.- Configurar Port 8443 (https) del JBOSS

Necessitam obrir un nou port al JBoss per on entraran les peticions https i aquest serà el 8443. En producció el port https és el 443. Editar el fitxer [JBOSS]\server\default\deploy\jbossweb.sar\server.xml i afegir el següent bloc després del comentari "<!-- SSL/TLS Connector ...":

```
<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"  
  
    ciphers="TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA,  
    TLS_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_RC4_128_SHA,  
    SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_DES_CBC_SHA"  
  
    />
```



5.2.3.2.- Afegir autenticador sobre Certificats

Ara hem d'indicar al JBoss com autenticar els usuaris a partir dels certificats que enviïn els navegadors. Això es fa editant el fitxer [JBoss]\server\default\conf\login-config.xml i dins del bloc xml "<application-policy name = "seycon"><authentication>" afegir la següent línia:

IMPORTANT: Aquest login-module ha de ser el darrer del <application-policy>, en cas contrari els WS no funcionaran.

```
<!-- HTTPS CLIENT-CERT -->  
<login-module code="es.caib.portafib.back.security.BaseCertLoginModule"  
flag="sufficient">  
</login-module>
```

5.2.4.- Compilar PortaFIB per ClientCert

Tal i com s'ha vis al punt 5.1.4.-Compilació existeix un paràmetre de configuració que compila PortaFIB afegint un un mòdul d'accés emprant https+ClientCert: -Pclientcert.

```
$ ./deploydev.sh clean -Pclientcert
```

5.2.5.- Exemple d'Accés

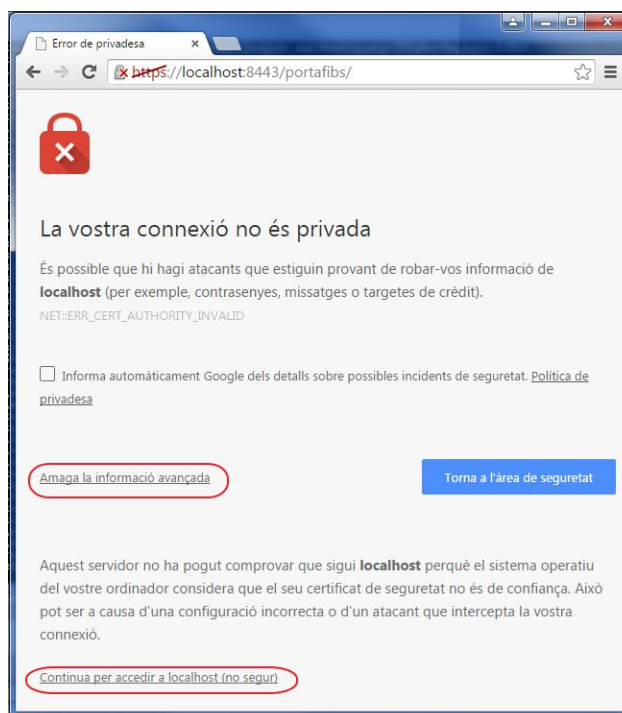
Per les proves següents necessitem que l'usuari tingui un certificat (software o de targeta) on el DNI d'aquest Certificat correspongui amb el DNI de l'usuari donat d'alta al PortaFIB. En cas de que l'usuari no tingui cap certificat, llavors se'n pot crear un de proves visitant el punt "5.3.-Creació d'un certificat de proves de Client".

Per començar, hem de posar en marxa el nostre JBoss i des d'un navegador accedir a la següent adreça: <https://localhost:8443/portafib/s>.

Si em emprat un certificat de identitat de proves tot d'una ens apareixerà una finestra com la de la captura següent, indicant que la identitat del servidor no és de confiança (cosa totalment normal ja que hem emprat un certificat de proves) i per continuar acceptarem la connexió fent clic sobre els llocs marcats en vermell.



Missatge d'Alerta en Firefox



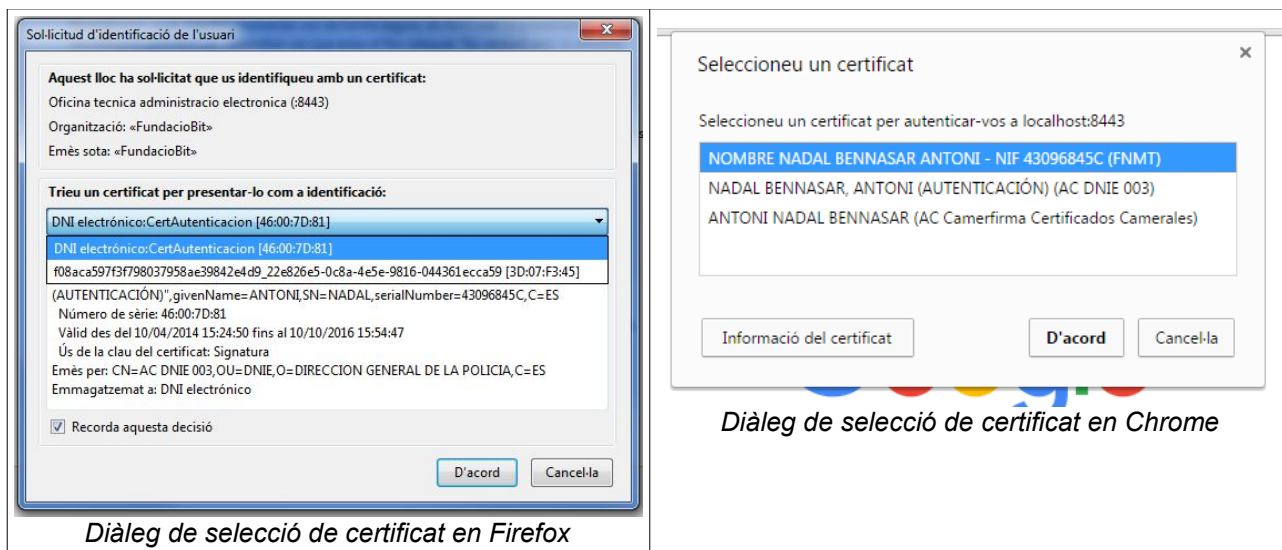
Missatge d'Alerta en Chrome

Si no volem que apareguin aquestes pantalles llavors haurem d'importar el certificat de servidor en totes les màquines client que es vulguin fer proves. Això es fa seguint aquestes passes:

```
keytool -export -keystore jboss.keystore -storepass fundaciobit -alias jboss -file  
certificatdeservidor.cer
```

Aquest certificat `certificatdeservidor.cer` l'hem d'instal·lar en els magatzems de certificats de tots els clients que accedeixin al servidor. Recordar que Firefox gestiona el seu propi magatzem de certificats, per la qual cosa també s'haurà de donar d'alta en aquest navegador si es fa feina amb ell.

Després ja ens apareixerà una finestra amb un llistat de certificats que podem emprar per aquella connexió:



5.3.- Creació d'un certificat de proves de Client

Per continuar amb aquest punt es pressuposa que hem seguit totes les passes del punt "5.2.-Connexions HTTPS i ClientCert en JBoss".

5.3.1.- Introducció

En aquest apartat simularem la creació d'una autoritat de certificació i a partir d'aquesta generarem un certificat d'usuari i donarem d'alta el certificat de client en la màquina de l'usuari l/o navegador. També afegirem el certificat arrel de la nova autoritat dins del fitxer de jboss.truststore. Després de fer tot això si des d'un navegador de l'ordinador de l'usuari intentam obrir una pàgina emprant https del servidor JBOSS llavors dins del llistat de certificats disponibles per autenticar-nos cap aquella web apareixerà el de l'usuari de proves.

Les passes s'han reproduït d'una pàgina web on s'expliquen aquests passos amb més detall: <http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=JBossClientCert>.

5.3.2.- Crear Autoritat de Certificació

Hem d'obrir una consola i anar al directori del codi font de PortaFIB següent: [PORTAFIB_CODE]\scripts\certificats_client. Aquí executarem l'script "1_CrearAutoritatCertificadora.bat" per obtenir dos fitxers: fundaciobit_ca.crt i fundaciobit_ca.key, és a dir el certificat públic i la clau privada de l'autoritat.



5.3.3.- Afegir certificat arrel de l'Autoritat de Confiança dins jboss.truststore

Obtindrem l'actual jboss.truststore o el copiarem de [PORTAFIB_CODE]\scripts\certificats_jboss\jboss.truststore al directori [PORTAFIB_CODE]\scripts\certificats_client. Amb una consola en aquest darrer directori executarem la següent comanda que afegeix el certificat arrel al truststore:

```
$ keytool.exe -import -keystore jboss.truststore -storepass fundaciobit -file  
.\fundaciobit_ca.crt -alias AcRaizFundacioBitCA
```

Per finalitzar copiarem el fitxer jboss.truststore a JBOSS\server\default\conf.

5.3.4.- Crear un certificat d'usuari de l'autoritat certificadora de proves

Ara ens queda crear un certificat per l'usuari. Dins el fitxer [PORTAFIB_CODE]\scripts\certificats_client\infousuari.cfg hi ha les dades amb les que es crearà el certificat de la persona. Amb una consola accedirem al directori [PORTAFIB_CODE]\scripts\certificats_client executarem la comanda "2_CrearCertificatUsuari.bat".

La primera contrasenya que ens demana és de la clau privada del certíficat arrel, o sigui "fundaciobit" i la segona és la del magatzem de claus p12.

Al final del procés obtindrem dos fitxers que ens interessin: certificatusuari.crt i certificatusuari.p12, que són el certificat públic i el certificat privat dins un magatzem p12.

El següent pas es importar el certificat que acabam de crear en els magatzems de claus (mostram com fer-ho en el navegadors de Windows):

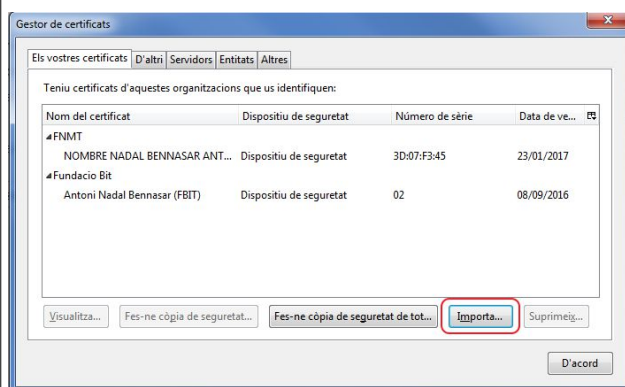
Internet Explorer i Chrome

Només hem de copiar el fitxer certificatusuari.p12 a la màquina de l'usuari i fer doble clic. Apareixerà un diàleg com el de més abaix i pitjarem sobre el boto "Endavant >". Col·locarem el certificat en la carpeta "Personal".



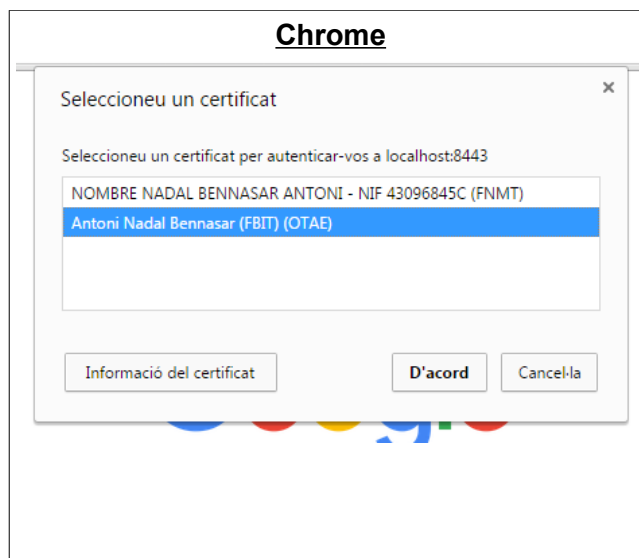
Firefox

Anirem al menú Opcions / Avançat / Visualitza Certificats i pitjarem el boto "Importa ...". Seleccionarem el fitxer certificatusuari.p12.

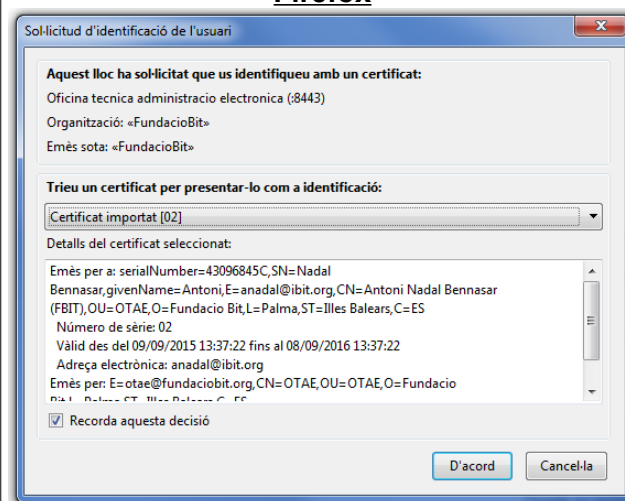


Després d'haver fet això si accedim al servidor amb https, ens apareixerà dins la llista de certificats disponibles el certificat que acabam de donat d'alta als magatzems:

Chrome



Firefox





5.4.- Configurar OpenOffice com a servei en Linux

5.4.1.- Instal·lar OpenOffice

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

```
# apt-get install openoffice.org
```

5.4.2.- Arrancar OpenOffice com a Servei

Crearem el fitxer “openoffice” en el directori /etc/init.d amb el contingut que es descriu en el punt “5.4.3.-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
```




5.4.3.- 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. Tomaszczik
#
OOo_HOME=/usr/bin
SOFFICE_PATH=$OOo_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
fi
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
```

5.5.- Tamany de PDF suportat

A continuació es mostren els resultats de Peticions de Firma amb diferents tamany de PDF així com diferents configuracions de de memòria reservada a JBoss.

5.5.1.- Pujada de PDF des de entorn WEB

Servidor amb següent configuració: **-Xms512m -Xmx1024m -XX:MaxPermSize=256m**

<i>Tamany Fitxer PDF</i>	<i>Resultat</i>
19MB	OK
30MB	OK
40MB	OK
45MB	OK
51MB	OK
54MB	OK
60MB	OK
65MB	OK
70MB	OK

5.5.2.- Pujada de PDF des de entorn WebServices

Les proves s'han fet sobre un màquina Windows 7, amb processador Intel Core i5 a 3.30GHz i 12GB de RAM. El servidor és un JBoss 5.1.GA. Les proves han consistit en enviar tant des de l'API de PortaFIB 1.0 com des de l'API de Portafirmas de CAIB tres peticions de firma al servidor i arrancar-la separades per u interval d'entre 30 i 60 segons. La configuració inicial del servidor: **-Xms512m -Xmx1024m -XX:MaxPermSize=256m**.

<i>Tamany Fitxer PDF</i>	<i>Memòria de Servidor requerida</i>			
19MB	-Xmx1024m			
30MB	-Xmx1024m			
40MB		-Xmx1303m		
45MB		-Xmx1303m		
51MB		-Xmx1303m		
54MB		-Xmx1303m		
60MB			-Xmx1512m	
65MB			-Xmx1512m	
70MB				-Xmx2048m



5.5.3.- Firma de Fitxers des del Mòdul de firma MiniApple com Applet

En aquest cas s'han provat en dos clients:

- (1) Un windows XP, processador Intel Core2 Duo amb 2GB de RAM
- (2) Un Windows 7, processador Intel Core i5 a 3.30GHz i 12GB de RAM

S'han fet les proves amb JDK 1.6 i navegador Firefox 38.0.5 i Chrome 43.0.2357.130.

<i>Tamany Fitxer PDF</i>	<i>Resultat</i>
19MB	OK
30MB	OK
40MB	OK
45MB	OK
51MB	OK
54MB	OK
60MB	OK
65MB	OK
70MB	Error Java Heap Space

5.6.- Gestió de Rols a traves de triggers Oracle

El departament de Informàtica de la CAIB empra un sistema anomenat "Agents Seycon" per sincronitzar informació del seu sistema centralitzat d'usuaris i rols, anomenat seycon, amb la resta d'aplicacions existents. Aquest sistema funciona de la següent forma:

- 1) Hi ha un canvi (alta, modificació o eliminació) en un rol (seycon també utilitza rols per gestionar càrrecs)
- 2) Un "Agent Seycon" específicament implementat per escoltar canvis en rols que representen càrrecs i canvis del rol PFI_USER, actualitza taules creades específicament per aquest fi en la BBDD Oracle de PortaFIB
- 3) Hi ha uns Triggers associats a aquestes taules que es connecten a PortaFIB a través d'una URL emprant un simple cridada HTTP amb paràmetres i aquest controlador del servidor PortaFIB actualitza informació de càrrecs o dona d'alta (o baixa) usuaris als que se li han assignat el rol PFI_USER

Com s'ha pogut observar en la presentació inicial hi ha dues accions ben diferenciades que són gestió de càrrecs i donada d'alta/baixa d'usuaris escoltant accions sobre el rol PFI_USER. Dins la carpeta [portafib]\scripts\bdd\1.0\oracle trobareu dos scripts sql encarregats de crear les



taules i els triggers que són `portafib_carrecs_caib.sql` (per la gestió de càrrecs) i `portafib_usuaris_caib.sql` (per la gestió d'usuaris). Aquests scripts han de ser modificats abans de ser executats en una BBDD Oracle modificant l'adreça del servidor PortaFIB i la contrasenya per accedir al controlador web de peticions `http` de PortaFIB.

Com que PortaFIB és multientitat s'ha d'indicar sobre quina entitat es realitzaran els canvis de càrrecs i d'usuaris, per això s'ha de definir la propietat `es.caib.portafib.entitatidforagentssql` i assignar-li l'identificador de l'entitat. Amb la finalitat d'oferir un poc de seguretat al sistema s'ha de definir una altra propietat anomenada `es.caib.portafib.passwordforagentssql` i assignar-li la contrasenya definida dins dels scripts, d'aquesta forma evitarem que només des dels triggers es puguin fer efectives les peticions via HTTP. Veure punt "2.3.2.1.-Propietats Generals PortaFIB".

Encara que aquest sistema estigui pensat per l'Entorn de la CAIB, pot ser emprat per altres entitats sense cap problema. També es podria emprar des d'una base de dades PostgreSQL si s'implementessin els triggers corresponents.

5.7.- Configuració Apache 2.2.14 o superior per connectar amb PortaFIB

5.7.1.- Crear Certificats de Prova per Apache

Si tenguéssim algun certificat emès per una entitat de confiança llavors empraríem aquest enlloc del de proves.

```
$ openssl genrsa -des3 -passout pass:x -out apache.pass.key 2048
$ openssl rsa -passin pass:x -in apache.pass.key -out apache.key
$ rm apache.pass.key
$ openssl req -new -key apache.key -out apache.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:IB
Locality Name (eg, city) []:Palma
```



```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:FundacioBit
Organizational Unit Name (eg, section) []:OTAE
Common Name (eg, YOUR name) []:<<IP_HOSTNAME_O_DOMINI>>
Email Address []: <<ADMIN_EMAIL>>
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

$ openssl x509 -req -days 365 -in apache.csr -signkey apache.key -out
apache.crt
```

5.7.2.- Instal·lació i Configuració Apache 2.2.14 (o superior)

Configurarem l'apache per emprar AJP (proxy) i a més configurarem SSL per les comunicacions HTTPS-CLIENTCERT

5.7.2.1.- Instal·lació

```
sudo apt-get install apache2
```

5.7.2.2.- Afegir mòduls SSL i proxy

```
sudo a2enmod ssl proxy proxy_ajp
```

5.7.2.3.- Configurar Connexió SSL

Crear el fitxer portafib-ssl dins /etc/apache2/sites-available. S'ha de canviar cadena <<PATH_TO_CERT>> per la ruta als fitxers de certificats generats en el punt "5.7.1.-Crear Certificats de Prova per Apache". El contingut de l'arxiu ha de ser el següent:



```
<IfModule mod_ssl.c>
<VirtualHost *:443>

    ServerAdmin <<ADMIN_EMAIL>>

    CustomLog /var/log/apache2/portafibs_access.log combined
    ErrorLog /var/log/apache2/portafibs_error_log

    ServerName <<IP_HOST>>:443
    SSLEngine on

    SSLProtocol all -SSLv2
    SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW

    SSLCertificateFile      <<PATH_TO_CERT>>/apache.crt
    SSLCertificateKeyFile   <<PATH_TO_CERT>>/apache.key

    # CLIENT CERT REQUIRED
    <Location /portafib/s >
        SSLVerifyClient optional_no_ca
        SSLOptions +ExportCertData
        SSLVerifyDepth 1
    </Location>

    <Proxy *>
        AddDefaultCharset Off
        Order deny,allow
        Allow from all
    </Proxy>

    ProxyPass /portafib ajp://<<IP_TO_PORTAFIB>>:8009/portafib timeout=600 keepalive=on
    ProxyPassReverse /portafib ajp://<<IP_TO_PORTAFIB>>:8009/portafib

</VirtualHost>
</IfModule>
```

Activarem aquest site executant la següent comanda

```
sudo a2ensite portafib-ssl
```

5.7.2.4.- Activar Virtual Host 443

Farem un VirtualHost del port 443. Editarem el fitxer /etc/apache2/ports.conf i damunt de "Listen 443" afegirem la següent línia "NameVirtualHost *:443":

```
<IfModule mod_ssl.c>
    NameVirtualHost *:443
    Listen 443
</IfModule>
```

5.7.2.5.- Redirecció pel port 80



Obrem el fitxer `/etc/apache2/sites-available/default` i abans del `</VirtualHost>` afegirem les següent línies:

```
ProxyPass /portafib ajp://<<IP_TO_PORTAFIB>>:8009/portafib timeout=600 keepalive=on
ProxyPassReverse /portafib ajp://<<IP_TO_PORTAFIB>>:8009/portafib
```

5.7.2.6.- Host permesos per atacar PortaFIB

Editar el fitxer `/etc/apache2/mods-enabled/proxy.conf` i comentar amb `#` tot el bloc `<Proxy *> ... </Proxy>` si no està ja comentat.

```
#      <Proxy *>
#      AddDefaultCharset off
#      Order deny,allow
#      Deny from all
#      Allow from localhost
#      #Allow from .example.com
#      </Proxy>
```

5.7.2.7.- Obrir firewall pels ports 80 i 443

Si tenim firewall llavors obrir els ports 80 i 443. Per exemple per Ubuntu és:

```
sudo ufw allow 80
sudo ufw allow 443
```

5.7.2.8.- Reiniciar l'apache

```
sudo service apache2 restart
```