Manual de Instalación @firma
Versión 4.0

Documento nº:	TI-20-1074-INS-001
Revisión:	2
Fecha:	24-02-2005
Período de retención:	Permanente durante su período de vigencia + 3 años después de su anulación

CONTROL DE COMPROBACIÓN Y APROBACIÓN

Documento nº: TI-20-1074-INS-001
Revisión: 2
Fecha: 24/02/05

REALIZADO

23/07/04

Javier Cerceda García
Analista

COMPROBADO

23/07/04

Javier Cerceda García	José Antonio Márquez Contreras
Analista	Director @firma

APROBADO

23/07/04

José Manuel Alanis Gamero	José Antonio Márquez Contreras
Director Proyecto	Director @firma

CONTROL DE MODIFICACIONES

Documento nº: TI-20-1074-INS-001
Revisión: 2
Fecha: 24/02/05

Rev. 1
Fecha 23/07/04
Autor/es JCG
Descripción Documentación inicial

Rev. 2
Fecha 24/02/05
Autor/es MMIG
Descripción Se modifica la configuración del componente Servidor Autenticación SSL

Rev. 3
Fecha 05/04/05
Autor/es ARB
Descripción Se modifica la configuración del componente Servidor Autenticación SSL

Rev. 4
Fecha 05/04/05
Autor/es MMIG
Descripción Se añade la configuración de los clusters de Firma

Rev. 5
Fecha 24/06/05
Autor/es ARB
Descripción Se corrigen varios errores en la configuración de la plataforma Linux

CONTROL DE DISTRIBUCIÓN

Documento nº: TI-20-1074-INS-001
Revisión: 2
Fecha: 24/02/05

Copias Electrónicas:

La distribución de este documento ha sido controlada a través del sistema de información.

Copias en Papel:

La vigencia de las copias impresas en papel está condicionada a la coincidencia de su estado de revisión con el que aparece en el sistema electrónico de distribución de documentos.

El control de distribución de copias en papel para su uso en proyectos u otras aplicaciones es responsabilidad de los usuarios del sistema electrónico de información.

Fecha de impresión 06/07/2005 12:37:00

Distribucion en Papel:

Nombre o Cargo y (Organización)	Nº de Ejemplares	Referencia de la carta de transmisión y fecha

Índice

1 Objeto

Es objeto de este documento describir el proceso de instalación de @firma Versión 4.0, la plataforma de Autenticación y Firma Digital de la Junta de Andalucía, utilizando certificados de usuario X.509.

Los objetivos globales de este proceso son:

- Describir el Proceso completo de Instalación de todos los componentes de la plataforma, junto con las Herramientas necesarias para su correcto funcionamiento y administración.
- Gestión y puesta en marcha de todos los componentes de la plataforma.

2 Alcance

El presente documento recoge la instalación de la solución propuesta por Telvent Interactiva ante las necesidades de creación de una plataforma de autenticación y firma digital mediante el uso de certificados digitales para la Consejería de Justicia y Administración Pública.

3 Siglas

AC	Autoridad de Certificación
CJAP	Consejería de Justicia y Administración Pública
CPD	CRL Distribution Point
CRL	Lista de Revocación de Certificados
DES	Data Encryption Standard
FNMT-RCM	Fábrica Nacional de Moneda y Timbre, Real Casa de la Moneda
LDAP	Lightweight Directory Access Protocol
PC	Ordenador Personal
RMI	Remote Method Invocation
RSA	Rivest Shamir Adleman
SID	Signer Identification
SSL	Secure Socket Layer
IIOP	Inter-Orb Protocol
EJB	Enterprise Java Bean
JSP	Java Server Pages
JDK	Java Develoment Kit
TI	Telvent Interactiva

4 Documentos de Referencia

- Documento TI-20-1074-ADM-001, Manual de Administración de la plataforma @Firma.
- Documento TI-20-1074-ARQ-001, Manual de Arquitectura de la plataforma @Firma

5 Introducción

El presente documento recoge la instalación de la plataforma de Autenticación y Firma Digital @firma Versión 4.0, utilizando certificados digitales de usuario que se proporciona como parte centralizada y fundamental dentro del Plan Director para la Calidad de los Servicios de la Junta de Andalucía.

@firma ha sido desarrollada bajo la plataforma JBoss, un servidor de aplicaciones J2EE que ejecuta componentes software desarrollados en Java. Estos componentes pueden ser tanto componentes Web (directorios Web, páginas JSP, servicios Web) como componentes EJB's. Es por ello que todo lo referente a la aplicación (directorios, puesta en marcha, configuración) depende en gran medida y está condicionada por el servidor de aplicaciones JBoss y las herramientas que le dan soporte.

6 Guía de Instalación

La plataforma @firma Versión 4.0 esta compuesta principalmente por tres elementos que se presentan a continuación:

- Sistema de Custodia: Representa la Base de Datos donde se almacenan las transacciones de firma realizadas y se custodian los documentos firmados. Por motivos de eficiencia, el Sistema de Gestión de Base de Datos permitido es ORACLE 8/9i. Este elemento debe colocarse en la red interna del organismo, sin visibilidad desde Internet.

- Servidor Centralizado @firma: Representa el núcleo de la plataforma y publica las interfaces necesarias para la comunicación con el mismo (RMI-IIOP, WEBSERVICES). Este elemento debe colocarse en la red interna del organismo, sin visibilidad desde Internet.

- Fachada de Comunicación @firma: Representa la parte de la plataforma encargada de atender las peticiones de Autenticación y Firma Web externas / internas y redirigirlas al Servidor de Firma. También publica los applets necesarios y componentes descargables. Este elemento debe colocarse en la DMZ del organismo, con visibilidad desde Internet / Intranet.

Para información más detallada sobre los componentes de la plataforma @firma, y las conexiones y comunicaciones de los mismos consultar detalladamente el Manual de Arquitectura de la plataforma @Firma (TI-20-1074-ARQ-001).

Adicionalmente, la plataforma @firma Versión 4.0 proporciona una Herramienta de Administración Remota, que permite administrar desde cualquier máquina de la Intranet varios servidores de firma.

A continuación en los siguientes apartados se describe la instalación de cada uno de los componentes descritos: Sistema de Custodia, Servidor de Firma, Fachada de Firma y Herramienta de Administración.

6.1 Instalación del Sistema de Custodia

El Sistema de Custodia representa la Base de Datos donde se almacenan las transacciones de firma realizadas y se custodian los documentos firmados. Por motivos de eficiencia, el Sistema Gestor de Base de Datos utilizado es ORACLE 8/9i. Este elemento debe colocarse en la red interna del organismo, sin visibilidad desde Internet.

El Sistema de Custodia está compuesto básicamente por los siguientes elementos:

- Tres Tablespaces: CU_NORMAL_TABLESPACE, CU_DATA_TABLESPACE, CU_LOB_TABLESPACE
- Dos Usuarios: CUOWNER, CUUSR01.
- Varias Tablas de datos.
- Un Rol: CUSTODIA_ROLE.
- Varios Sinónimos.

A continuación se describe cada uno de estos elementos:

1) Tablespace CU_NORMAL_TABLESPACE: Espacio de Datos utilizado para almacenar los tipos de datos normales (NUMBER,VARCHAR2,INTEGER,DATE). Por defecto, el tamaño indicado en los scripts de creación para este TableSpace es de 1 Gb.

2) Tablespace CU_DATA_TABLESPACE: Espacio de Datos utilizado para almacenar los tipos de datos BLOB de pequeño tamaño. Por defecto, el tamaño indicado en los scripts de creación para este TableSpace es de 1 Gb.

3) Tablespace CU_LOB_TABLESPACE: Espacio de Datos utilizado para almacenar los tipos de datos BLOB de gran tamaño. Por defecto, el tamaño indicado en los scripts de creación para este TableSpace es de 1 Gb.

4) Usuario CUOWNER: Propietario de las tablas de datos del sistema de custodia y con todos los permisos sobre las mismas. Este usuario es utilizado únicamente por el Administrador de Bases de Datos (DBA) y ninguna otra persona ha de tener acceso a él. Las tablas son las siguientes:

    a. Secuencia SEQ_SID: Generador de identificadores únicos del sistema

    b. Tabla ACCESO

    c. Tabla CERTIFICADOS

    d. Tabla NOTARIOELECTRONICO

    e. Tabla PLANTILLA

    f. Tabla DATOSFIRMA

g. Tabla DOCSENBLOQUE

h. Tabla PAGEURL

i. Tabla SIGNDATA

j. Tabla SIGNTRANSACTION

k. Tabla TEMPORALDATA

l. Tabla ATTACHMENT

m. Tabla IMAGE

- Role CUSTODIA_ROLE: Role con permisos de consulta, inserción, actualización y borrado restringido sobre las tablas de datos de CUOWNER. Básicamente este rol puede consultar, introducir y actualizar información pero no borrarla. El único borrado que puede realizar este rol está restringido a una tabla con datos temporales denominada TEMPORALDATA. Para mayor información consultar los scripts de creación de este rol.

- Usuario CUUSR01: Usuario utilizado para conectarse desde el Servidor de Firma al Sistema de Custodia, tiene asignado el role CUSTODIA_ROLE y el permiso de conexión. Será utilizado en la fase de instalación del Servidor de firma para configurar los parámetros de conexión a base de datos.

- Sinónimos: proporcionan facilidad para el acceso a las tablas de datos de CUOWNER, en concreto permiten referenciar una tabla sin precederla por el nombre usuario.

6.1.1 Consideraciones previas

Recomendamos encarecidamente que la instalación y el mantenimiento del sistema de custodia lo realice personal técnico cualificado en Base de Datos (preferiblemente un DBA) que esté familiarizado con Oracle.

Partimos de que la máquina tiene correctamente instalado un Servidor de Base de Datos Oracle 8i / Oracle 9i y las herramientas administrativas básicas, entre ellas "sqlplus".

Partimos de que se ha creado un SID BD nuevo o existente que albergará el sistema de custodia.

El sistema de custodia de la plataforma de firma se instala automáticamente ejecutando una serie de scripts de creación, que deben ser configurados previamente para ello, adaptándolos a las necesidades de cada caso concreto.

Si la máquina desde la que se ejecuta el script no es el mismo servidor de BD, se debe instalar el sqlplus en esa máquina y configurar correctamente el fichero tnsnames.ora.

A continuación se describen los parámetros a configurar en el script de creación en las diferentes plataformas y como realizar la ejecución del mismo.

6.1.2 Desde Sistema Operativo Windows

El proceso se compone de los siguientes archivos:

- creacion.bat
- 001-crea_tablespaces-system.sql
- 002-crea_tablas-cuowner.sql
- 003-crea_rol-system.sql
- 004-crea_usuario-system.sql
- 005-crea_sinonimos-cuusr01.sql

En primer lugar se debe editar el fichero creación.bat y definir tres parámetros al comienzo del mismo (No ejecutar aún):

set CUSTODIA=<nombre sid de BD donde se creará el sistema de custodia. Ejem: FIRMA4>

set SYSTEM_USER=<Usuario system o con permisos DBA del SID anterior. Ejem: system>

set SYSTEM_PASS=<password del usuario anterior. Ejem: manager>

A continuación editar el fichero 001-crea_tablespaces-system.sql y colocar correctamente los directorios donde residirán físicamente los tablespaces, es decir, los atributos DATAFILE de las sentencias CREATE TABLESPACE. En este fichero se puede definir también el password del usuario CUOWNER modificando el atributo IDENTIFIED BY de la sentencia CREATE USER "CUOWNER". **IMPORTANTE:** Si cambiamos este password, no olvidar modificar la línea 6 del fichero "creación.bat" indicando el nuevo password en la cadena de conexión a sqlplus.

Si se desea cambiar el password del usuario de conexión CUUSR01, editar el fichero 004-crea_usuario-system.sql y modificar el atributo IDENTIFIED BY de la sentencia CREATE USER "CUUSR01". **IMPORTANTE:** Si cambiamos este password, no olvidar modificar la línea 9 del fichero "creación.bat" indicando el nuevo password en la cadena de conexión a sqlplus.

Seguidamente, editar el fichero 002-crea_tablas-cuowner.sql para indicar el valor inicial para los SIDs del sistema de custodia, es decir, los identificadores de clave primaria. Para ello cambiar las etiquetas <valor_inicial> de la sentencia CREATE SEQUENCE SEQ_SID ubicada en la línea 4 del fichero. En el caso de tratarse de una instalación desde cero y no una migración, se puede colocar el valor que se considere oportuno. Ejemplo:

```
CREATE SEQUENCE SEQ_SID
 START WITH 100000
 NOMAXVALUE
 MINVALUE 100000
 NOCYCLE
 NOCACHE
 NOORDER;
```

Finalmente, desde una consola MSDOS ejecutar el archivo creación.bat. Si ocurre algún problema, consultar con el administrador de Base de Datos.

NOTA: la máquina desde la que se ejecute el archivo creación.bat debe tener instalada correctamente la herramienta "sqlplus" y configurado el fichero "tnsnames.ora".

6.1.3 Desde Sistema Operativo Linux

El proceso se compone únicamente del fichero:

- creacion.sh

En primer lugar se debe editar el fichero creacion.sh y definir los parámetros presentes al comienzo del mismo:

SQLPLUS=<ruta completa del comando sqlplus. Ej:/firma/oracle/OraHome1/bin/sqlplus>

SYSTEM_USER==<Usuario system o con permisos DBA del SID Base de Datos. Ej:system>

SYSTEM_PASS=<passord del usuario anterior. Ej:manager>

CUSTODIA=<nombre sid de BD donde se creará el sistema de custodia. Ej:FIRMA4>

OWNER_PASS=<password que tendrá el usuario CUOWNER>

CONNECT_USER=<nombre del usuario de conexión para la instalación del servidor de firma. Se recomienda dejar CUUSR01>

CONNECT_PASS=<password del usuario anterior>

NORMAL_DATAFILE=<ruta completa donde se creará el DATAFILE para tipos de datos normales. Ej: "C:\ORACLE\ORADATA\AFIRMA\CUSTODIA_NORMAL_TEST_00001.ora"

DATA_DATAFILE=<ruta completa donde se creará el DATAFILE para blobs pequeños. Ej: "C:\ORACLE\ORADATA\AFIRMA\CUSTODIA_TEST_DATA00001.ora"

LOB_DATAFILE=<ruta completa donde se creará el DATAFILE para blobs grandes. Ej: "C:\ORACLE\ORADATA\AFIRMA\CUSTODIA_TEST_LOG00001.ora"

A continuación, indicar el valor inicial para los SIDs del sistema de custodia, es decir, los identificadores de clave primaria. Para ello cambiar las etiquetas <valor_inicial> de la sentencia CREATE SEQUENCE SEQ_SID ubicada en la línea 56 del fichero *creación.sh*. Ejemplo:

```
CREATE SEQUENCE SEQ_SID
  START WITH 100000
  NOMAXVALUE
  MINVALUE 100000
  NOCYCLE
  NOCACHE
  NOORDER;
```

Finalmente, desde una consola de sistema ejecutar el archivo creación.sh. Si ocurre algún problema, consultar con el administrador de Base de Datos.

NOTA: la máquina desde la que se ejecute el archivo creación.sh debe tener instalada correctamente la herramienta "sqlplus" y configurado el fichero "tnsnames.ora".

6.2 Instalación del Servidor de Firma

El Servidor de Firma representa el núcleo de la plataforma y publica las interfaces necesarias para la comunicación con el mismo (RMI-IIOP, WEBSERVICES). Este elemento debe colocarse en la red interna del organismo, sin visibilidad desde Internet.

Para que la instalación del Servidor de Firma sea satisfactoria es importante que el usuario sea administrador de la máquina donde se lleve a cabo la instalación.

IMPORTANTE: Si instala varios Servidores de Firma en una misma red se pondrán automaticamente en cluster, compartiendo la información de configuración. Si desea tener un servidor en "*producción*" y otro para desarrollo se deben instalar en subredes distintas sin visibilidad entre ellos.

6.2.1 Consideraciones previas

Previo a la instalación del Servidor de Firma es necesario realizar los siguientes pasos:

1) Instalar el JDK 1.4.1 proporcionado en el CD Servidor de la plataforma y definir la variable de entorno JAVA_HOME. Para información detallada sobre este paso ver apartado 7.1 del presente manual.

2) Instalar el Cliente Oracle en la máquina Servidor de Firma. Este elemento es necesario para que el Servidor de Firma pueda establecer conexión con el sistema de Custodia. Para más información sobre este paso ver apartado 7.2 del presente manual.

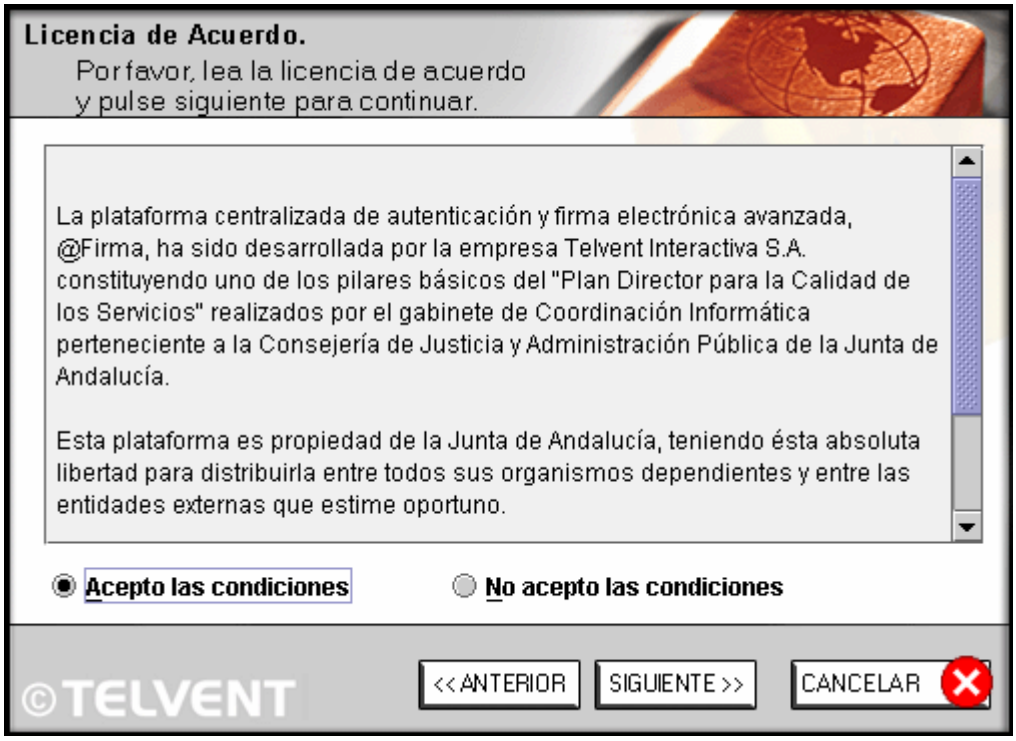
6.2.2 Instalación del componente Servidor de Aplicaciones

Este elemento representa el núcleo del Servidor de Firma. A continuación se describe su instalación en las diferentes plataformas.

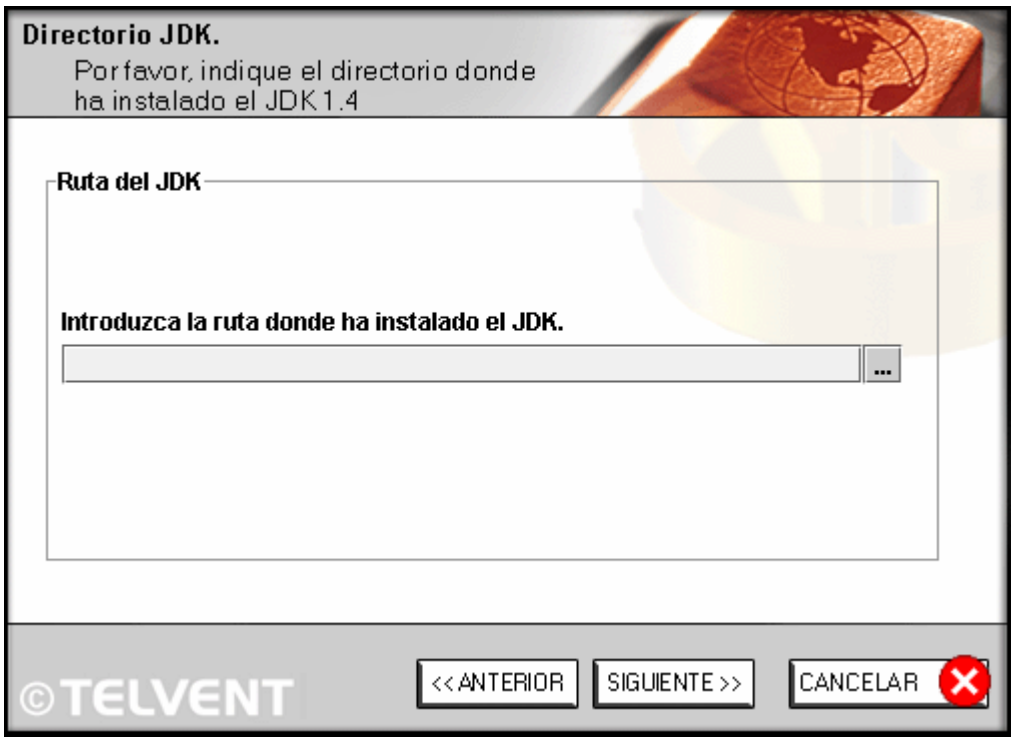
6.2.2.1 Sistema Operativo Windows

El proceso de instalación se realiza ejecutando el fichero "instalar.bat" disponible en el directorio "Instalación @firma / servidorfirma / win" del CD Servidor. Esto desplegará un interfaz gráfico que nos guiará a través del proceso de instalación.

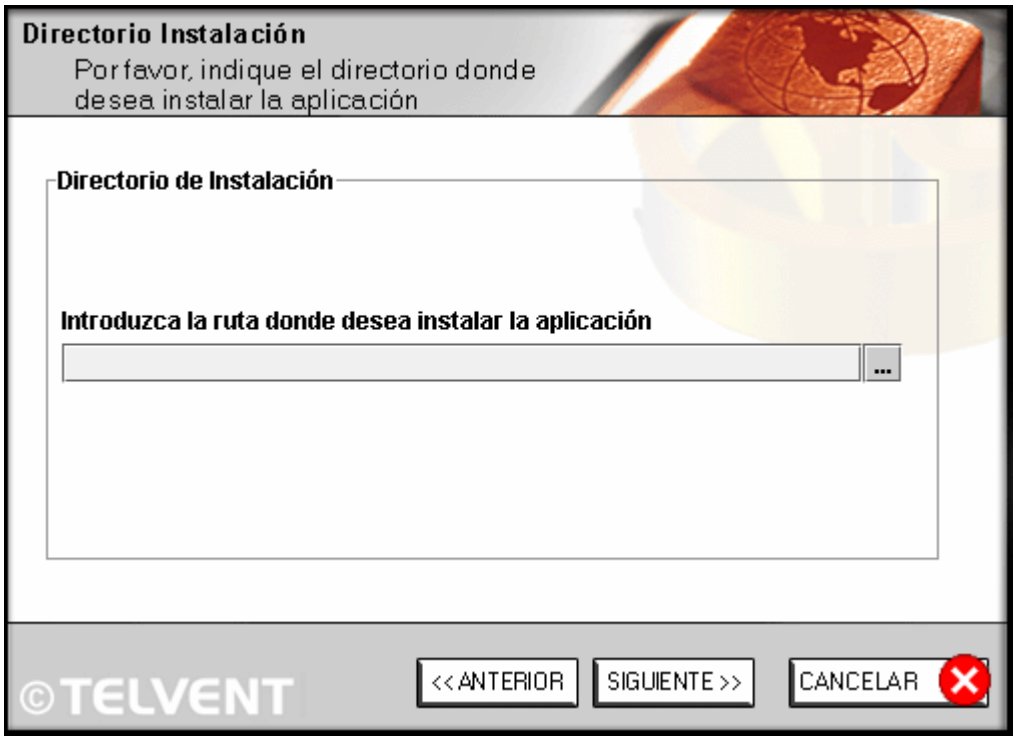
Pulsando el botón "Siguiente" iniciamos el proceso de instalación....



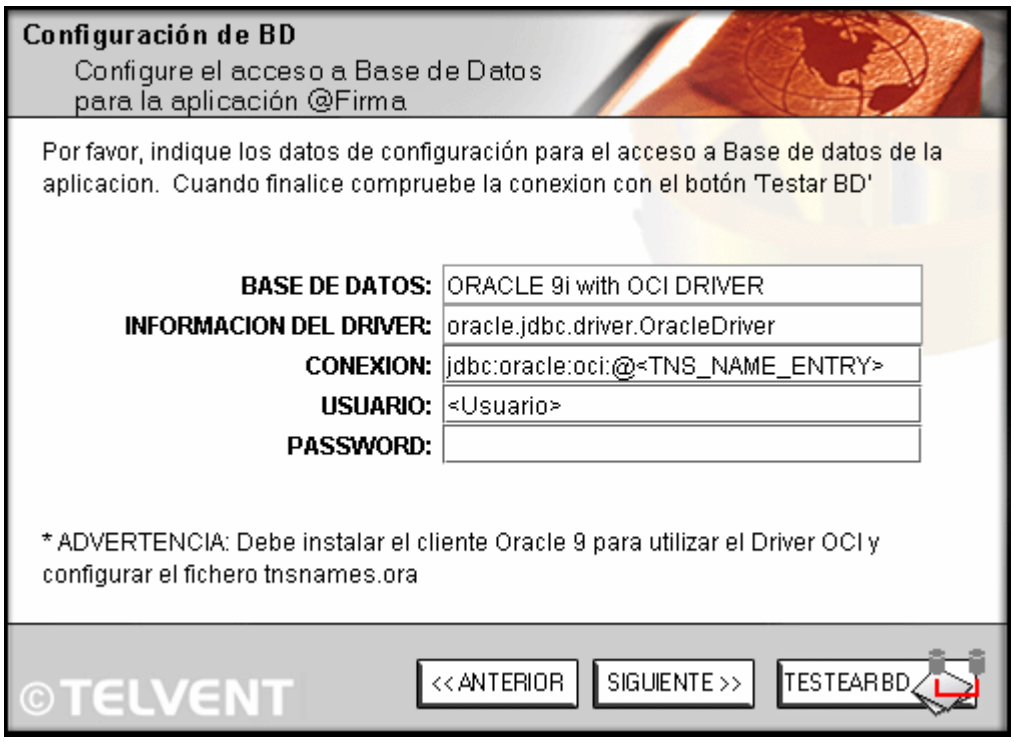
Aceptamos las condiciones y pulsamos el botón "Siguiente" para continuar con el proceso...



A continuación nos solicita el directorio donde se encuentra instalado el JDK 1.4.1 del CD Servidor de la plataforma. Una vez indicado, pulsar el botón "Siguiente" para continuar con el proceso...



En este momento nos solicita el directorio donde se instalará el Servidor de Aplicaciones de la plataforma de firma. Una vez introducido un directorio pulsar el botón "Siguiente" para continuar con el proceso de instalación ...



A continuación nos solicita la información de conexión a Base de Datos. Se utiliza el driver OCI de Oracle obligatoriamente, para ello se requiere el Cliente Oracle correctamente instalado y el fichero tnsnames.ora correctamente configurado.

El campo CONEXIÓN se debe completar con el nombre que se dio a la conexión contra el SID del Sistema de Custodia en el fichero tnsnames.ora. En concreto, cambiar <TNS_NAME_ENTRY> por el valor adecuado.

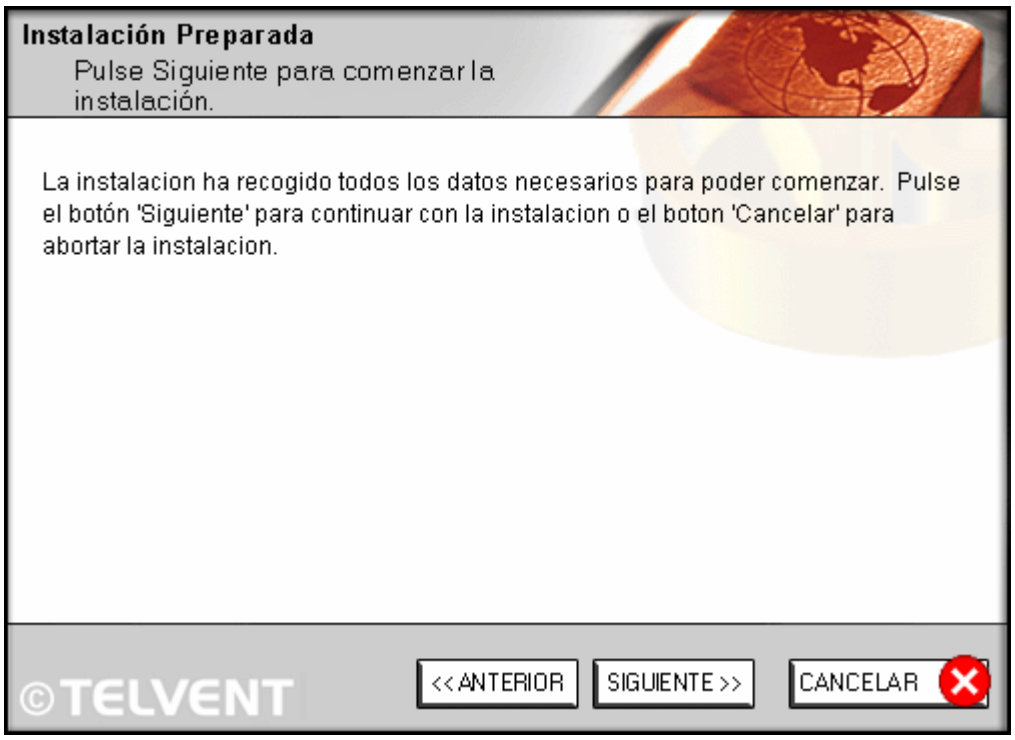
El campo USUARIO contendrá el valor CUUSR01, es decir, el usuario de conexión que se creó en el apartado 6.1. Si el nombre de este usuario se modificó en el script de creación del sistema de custodia se debe indicar aquí el nuevo nombre.

El campo PASSWORD contendrá el password del usuario anterior. Este password se asignó en el proceso del apartado 6.1.

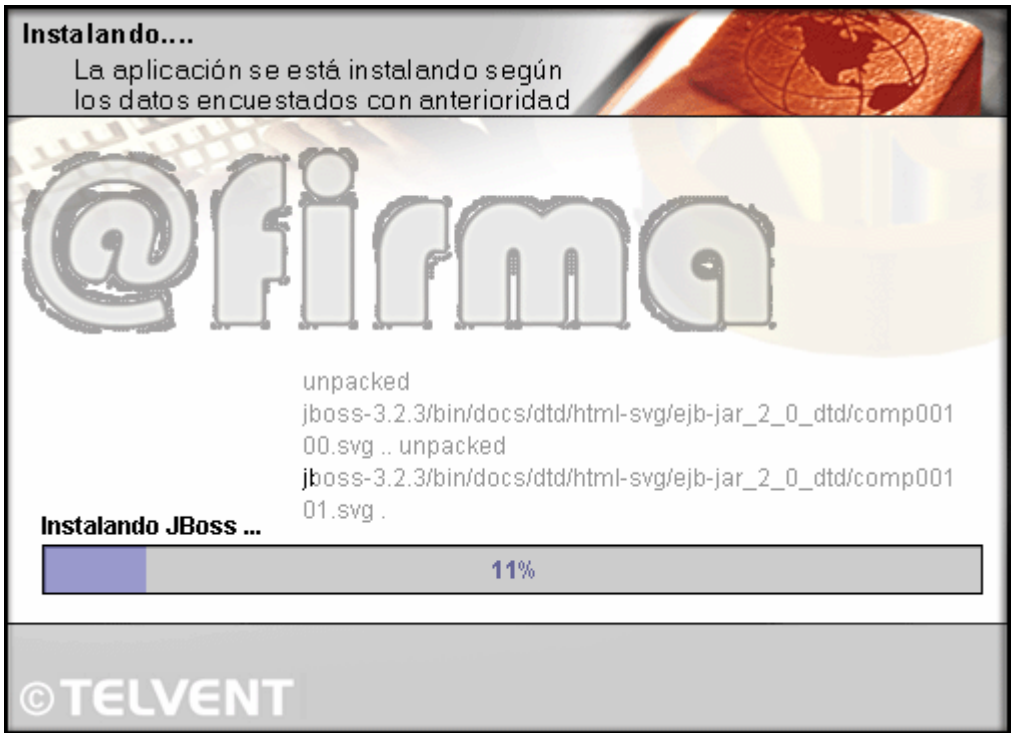
Mientras no se introduzcan los datos correctos el proceso de instalación no permitirá continuar. El botón "TestearBD" nos permitirá testear si los datos introducidos son correctos o no.

NOTA: Si hay problemas para configurar estos datos, revisar la instalación del Cliente Oracle y la configuración del fichero "tnsnames.ora".

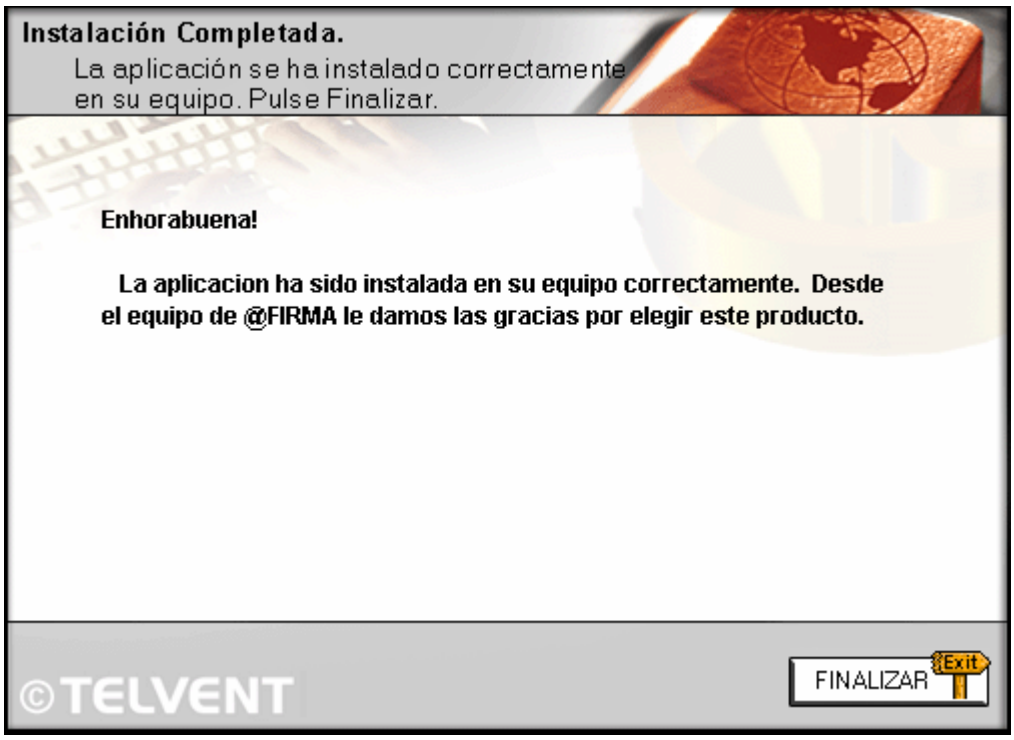
El botón "Siguiente" continuará con el proceso de instalación siempre y cuando los datos de conexión a Base de Datos sean los adecuados....



El proceso de recogida de datos ha finalizado correctamente, pulsando el botón "Siguiente" se procederá a instalar en el sistema el Servidor....



La siguiente ventana instala los componentes necesarios mostrando el progreso de los mismos...



La ventana final nos muestra que el proceso ha finalizado correctamente. Pulsando el botón "Finalizar" daremos por concluida la instalación.

6.2.2.2 Sistema Operativo Linux

El proceso de instalación ha sido testeado en la distribución de guadalinex v1.0, en la cual es necesario disponer de la librería "*libstdc++-libc6.1-1.so.2*". Así pues, se recomienda instalar esta librería mediante el comando "dpkg –i".

El proceso de instalación se realiza a partir del directorio "Instalación @firma / servidorfirma / linux" del CD Servidor mediante los siguientes pasos:

1) Copiar el contenido del directorio de instalación anterior al disco duro del sistema.

2) Asegurarse de haber definido la variable JAVA_HOME al instalar el JDK 1.4.1 del CD Servidor.

3) Pasar el comando "dos2unix" al fichero instalacion.sh presente en el directorio de instalación: dos2unix instalación.sh.

   NOTA: Si no se dispone de dicha utilidad, en el directorio del CD de instalación "*utilidades/herramientas_linux*" se proporcionan los fuentes de la misma. Para compilar la utilidad dos2unix, seguir los siguientes pasos:

   - gunzip hd2u-0.8.1.tar.gz
   - tar xvf hd2u-0.8.1.tar
   - cd hd2u-0.8.1

- ./configure
- make
- make install

4) Ejecutar la instrucción "chmod +x instalacion.sh", de esa forma le damos permiso de ejecución.

5) Ejecutar el script "instalacion.sh" presente en el directorio de instalación. Esto actualizará el JDK 1.4.1 con los ficheros adecuados.

6) Descomprimir el fichero "jboss.zip" presente en el directorio de instalación mediante el comando "unzip".

7) Definir la variable de sistema JBOSS_HOME apuntando al directorio raíz del jboss.

export JBOSS_HOME = dir_instalacion_JBOSS

EJEMPLO: *export JBOSS_HOME = /usr/local/jboss*

8) A continuación editar el fichero run.sh del directorio JBOSS_HOME/bin y establecer los parámetros adecuados del jboss, editando la línea 187 del fichero:

org.jboss.Main -c all --host=<server_name> "$@"

donde <server_name> es el nombre o ip del servidor de firma

9) Configurar en el fichero JBOSS_HOME/server/all/deploy/oracle-ds.xml los parámetros de conexión al sistema de custodia.

```
<datasources>
  <local-tx-datasource>
    <jndi-name>DefaultDS</jndi-name>
    <connection-url>jdbc:oracle:oci:@<TNS_NAME_ENTRY></connection-url>
    <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
    <user-name><USUARIO></user-name>
    <password><PASSWORD></password>
    .....
  </local-tx-datasource>
</datasources>
```

Los parámetros que se deben indicar son los siguientes :

connection-url: completar con el nombre que se dio a la conexión contra el SID del Sistema de Custodia en el fichero tnsnames.ora. En concreto, cambiar <TNS_NAME_ENTRY> por el valor adecuado.

user-name: contendrá el valor CUUSR01, es decir, el usuario de conexión que se creó en el apartado 6.1. Si el nombre de este usuario se modificó en el script de creación del sistema de custodia se debe indicar aquí el nuevo nombre

password: contendrá el password del usuario anterior. Este password se asignó en el proceso del apartado 6.1.

10) Arrancar el Servidor Jboss mediante el comando "sh run.sh", observando que no aparezcan errores en la consola del mismo.

11) Si ocurre algún problema, revisar detenidamente los parámetros de conexión a Base de Datos en el fichero oracle-ds.xml, la instalación del cliente oracle y el fichero de oracle tnsnames.ora.

12) Crear un usuario llamado "firma" y hacer que sea el dueño del directorio JBOSS_HOME y todo su contenido. Utilizar este usuario para ejecutar el Servidor de Aplicaciones.

6.2.3 Configuración del Servidor de Firma

6.2.3.1 Configuración HTTPS del puerto 443

Para un correcto funcionamiento del Servidor de Firma en conexión HTTPS es necesario configurar un certificado de servidor para el puerto de conexión 443. Para ello se debe editar el fichero jboss-service.xml ubicado en el directorio "JBOSS_HOME/server/all/deploy/jbossweb-tomcat41.sar//META-INF", donde JBOSS_HOME es el directorio raiz del servidor de firma jboss.

Localizar la clase Connector del puerto 443 y cambiar el valor de los atributos keystoreFile y keystorePass por los que se consideren adecuados.

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
    port="443" minProcessors="5" maxProcessors="75" enableLookups="false"
    acceptCount="100" debug="0" scheme="https" secure="true"
    useURIValidationHack="false" disableUploadTimeout="true">

     <Factory
    className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
    keystoreFile="${jboss.server.home.dir}/conf/keystoreCajaNegra4"
    keystorePass="changeit" clientAuth="false" protocol="TLS" />

</Connector>
```

El atributo keystoreFile contendrá el fichero keystore con el nuevo certificado servidor y el atributo keystorePass contendrá el password del keystore anterior.

NOTA: Si estamos en Linux en lugar de utilizar el puerto 443 utilizaremos el 4430, ya que en Linux solo el usuario root puede abrir puertos por debajo del 1024, y haremos una redirección de puertos como se esplica en el punto 7.4 Redirección de Puertos en Linux.

6.2.3.2 Configuración SSL Jaas Security Domain

Las interfaces RMI-IIOP y los WebServices publicados en el Servidor de Firma se encuentran protegidos por JAAS + SSL, así pues, es necesario configurar el Certificado de Servidor que se utilizará para la encriptación SSL.

Para ello se debe editar el fichero jboss-service.xml ubicado en el directorio "JBOSS_HOME/server/all/conf", donde JBOSS_HOME es el directorio raiz del servidor de firma jboss.

Localizar el siguiente mbean y cambiar el valor de los atributos keyStoreURL y KesyStorePass por los que se consideren adecuados.

```
<mbean code="org.jboss.security.plugins.JaasSecurityDomain"
name="Security:service=JaasSecurityDomain,domain=TomcatSSL">
  <depends>jboss.security:service=JaasSecurityManager</depends>
```

```
<constructor><arg type="java.lang.String" value="TomcatSSL" />
</constructor>
 <attribute name="KeyStoreURL"> file://${jboss.server.home.dir}/conf/keystore
</attribute>
<attribute name="KeyStorePass">changeit</attribute>
</mbean>
```

El atributo keyStoreURL contendrá el fichero keystore con el certificado servidor y el atributo KesyStorePass contendrá el password del keystore anterior.

Una vez finalizada la instalación y la configuración del servidor se debe realizar un arranque manual del mismo ejecutando el script "run.bat" / "run.sh" según S.O. del directorio JBOSS_HOME/bin.

Para testear el funcionamiento del servidor conectarse a la siguiente url desde un navegador IE:

https://<servidor_firma>/axis/servlet/AxisServlet

Nos solicitará introducir el usuario/password JAAS para WebServices (por defecto membermull/a4210). Esto nos permitirá ver la lista de interfaces WebServices publicadas.

6.2.3.3 Configuración Usuario/Password JAAS RMI-IIOP/WebServices

Mediante los ficheros *roles.properties* y *users.properties* se configura el usuario/password para autenticación JAAS de acceso a las interfaces RMI-IIOP y webservices publicadas en el Servidor de Firma.

Estos ficheros se encuentran ubicados el directorio JBOSS_HOME/server/all/conf del Servidor de Firma.

El fichero *roles.properties* contiene líneas del tipo:

usuario=role1,role2,...

usuario.CallerPrincipal=*usuario*

El fichero users.properties contiene líneas del tipo

usuario=password

6.2.3.3.1 Usuario / password para interfaces RMI-IIOP

- roles.properties:

member=custodia,firmaweb,administracion,verificarfirmas,autenticacionaplicaciones,firmaenbloque,primitivas,visualizacion,firmawebMCA,FirmaApiFacadeRole,FirmaPaginaWebRole,MultiFirmaMasivaRole,MultiFirmaRole

member.CallerPrincipal=member

- users.properties:

member=tummel

6.2.3.3.2 Usuario / password para interfaces WebServices

- roles.properties:

membermull=roleWebServices

membermull.CallerPrincipal=membermull

- users.properties:

membermull=a4210

6.2.3.4 Configuración de la memoria de la JVM

Para configurar la memoria que va a utilizar la JVM debemos de usar las siguientes opciones de la JVM:

-Xms*n*

Specify the initial size, in bytes, of the memory allocation pool. This value must be a multiple of 1024 greater than 1MB. Append the letter `k` or `K` to indicate kilobytes, or `m` or `M` to indicate megabytes. The default value is 2MB. Examples:

```
-Xms6291456
-Xms6144k
-Xms6m
```

-Xmx*n*

Specify the maximum size, in bytes, of the memory allocation pool. This value must a multiple of 1024 greater than 2MB. Append the letter `k` or `K` to indicate kilobytes, or `m` or `M` to indicate megabytes. The default value is 64MB. Examples:

```
-Xmx83886080
```

```
-Xmx81920k
-Xmx80m
```

Dependiendo de la memoria física de la máquina y de la utilización de la misma el administrador del sistema debe de asignarle valores a dichos parámetros.

6.2.3.4.1 Windows

Editar el fichero run.bat y buscar la linea:

rem set JAVA_OPTS=%JAVA_OPTS% -server -Xms256m -Xmx896m

Descomentar dicha linea, eliminando el "rem", y asignarle unos valores adecuados.

6.2.3.4.2 Linux

Editar el fichero run.conf y buscar la linea:

#JAVA_OPTS="-server -Xms256m -Xmx896m"

Descomentar dicha linea, eliminando el "#", y asignarle unos valores adecuados.

6.2.3.5 Configuración para maquinas con varias interfaces de red

Si la máquina donde se va ha instalar el Servidor de Firma tiene varias interfaces de red, cada una con un nombre distinto hay que añadir una configuración adicional.

Editar el fichero JBOSS_HOME\server\all\deploy\cluster-service.xml y buscar todas las apariciones de la linea:

<UDP mcast_addr="228.1.2.3" mcast_port="45566"

y añadir el atributo **bind_addr** indicando la IP donde se ha lanzado el Servidor de Firma.

Ej.- <UDP mcast_addr="228.1.2.3" mcast_port="45566" bind_addr="172.19.1.23"

6.2.3.5.1 Windows

Editar el fichero run.bat y buscar la linea:

rem set JAVA_OPTS=%JAVA_OPTS% -Djava.rmi.server.hostname=<server_name> -Djava.rmi.server.useLocalHostname=false

donde <server_name> es el nombre o ip del servidor de firma

Descomentar dicha linea, eliminando el "rem", y sustituir <server_name>.

6.2.3.5.2 Linux

Editar el fichero run.conf y buscar la linea:

> #JAVA_OPTS="$JAVA_OPTS -Djava.rmi.server.hostname=<server_name> -Djava.rmi.server.useLocalHostname=false"
>
> donde <server_name> es el nombre o ip del servidor de firma

Descomentar dicha linea, eliminando el "#", y sustituir <server_name>

6.2.3.6 Configuración de los clusters

Una vez alcanzado éste punto del manual tenemos nuestro servidor de Firma instalado y configurado. Pero si queremos instalar varios servidores de Firma para que funcionen en Cluster, debemos primero realizar una instalación idéntica en el otro nodo del cluster. Después de lo cual tendríamos nuestro cluster de Firma configurado. Ahora el problema surge cuando queremos instalar el sistema de Firma en diferentes entornos, por ejemplo Producción y Desarrollo, en ése caso debemos realizar la configuración que se explica más adelante, ya que por defecto, la instalación de Firma viene configurada para funcionar todos los nodos del cluster en la misma partición. Se selecciona un nombre diferente para cada entorno de trabajo. Los pasos a seguir son: Se edita el fichero %JBOSS_HOME%\server\all\deploy\cluster-service.xml y el fichero %JBOSS_HOME%\server\all\deploy\jbossha-httpsession.sar\ClusteredHttpSessionEB.jar\META-INF\jboss.xml, en estos ficheros se deben de sustituir todas las apariciones de FirmaPartition y DefaultPartition por lo aquí indicado: ENTORNO DE DESARROLLO FirmaPartition □ DesarrolloPartition DefaultPartition □ DefaultPartitionDesarrollo ENTORNO DE PRODUCCION FirmaPartition □ ProduccionPartition DefaultPartition □ DefaultPartitionProduccion

6.3 Instalación Fachada de Comunicación

La fachada de comunicaciones representa la parte de la plataforma encargada de atender las peticiones de Autenticación y Firma Web externas / internas y redirigirlas al Servidor de Firma. También publica los applets necesarios y componentes descargables. Este elemento debe colocarse en la DMZ del organismo, con visibilidad desde Internet / Intranet.

6.3.1 Consideraciones previas

Previo a la instalación del componente Fachada es necesario realizar los siguientes pasos:

1) Instalar el JDK 1.4.1 proporcionado en el CD Servidor de la plataforma y definir la variable de entorno JAVA_HOME. Para información detallada sobre este paso ver apartado 7.1 del presente manual.

6.3.2 Instalación del componente Servidor de Aplicaciones

Este elemento representa el punto de entrada al sistema para las aplicaciones de firma y multifirma web. A continuación se describe su instalación en las diferentes plataformas.

6.3.2.1 Sistema Operativo Windows

El proceso de instalación se realiza a partir del directorio "Instalación @firma / fachada / win" del CD Servidor mediante los siguientes pasos:

1) Copiar el contenido del directorio de instalación anterior al disco duro del sistema.

2) Asegurarse de haber definido la variable JAVA_HOME al instalar el JDK 1.4.1 del CD Servidor.

3) Ejecutar el script "instalacion.bat" presente en el directorio de instalación. Esto actualizará el JDK 1.4.1 con los ficheros adecuados.

4) Descomprimir el fichero "jboss.zip" presente en el directorio "file" dentro del directorio de instalación.

5) A continuación editar el fichero run.bat del directorio JBOSS_HOME/bin y establecer los parámetros adecuados del jboss, editando la línea 21 del fichero:

org.jboss.Main -c all --host=<server_name> "$@"

donde <server_name> es el nombre o ip del servidor de la fachada de @Firma

6) Arrancar el Servidor Jboss desde una ventana de comando ejecutando el script "run.bat", observando que no aparezcan errores en la consola del mismo.

6.3.2.2 Sistema Operativo Linux

El proceso de instalación ha sido testeado en la distribución de guadalinex v1.0, en la cual es necesario disponer de la librería "*libstdc++-libc6.1-1.so.2*". Así pues, se recomienda instalar esta librería mediante el comando "dpkg –i".

El proceso de instalación se realiza a partir del directorio "Instalación @firma / fachada / linux" del CD Servidor mediante los siguientes pasos:

1) Copiar el contenido del directorio de instalación anterior al disco duro del sistema.

2) Asegurarse de haber definido la variable JAVA_HOME al instalar el JDK 1.4.1 del CD Servidor.

3) Pasar el comando "dos2unix" al fichero instalación.sh presente en el directorio de instalación: dos2unix instalación.sh.

4) NOTA: Si no se dispone de dicha utilidad, en el directorio del CD de instalación "*utilidades/herramientas_linux*" se proporcionan los fuentes de la misma. Para compilar la utilidad dos2unix, seguir los siguientes pasos:

   - gunzip hd2u-0.8.1.tar.gz
   - tar xvf hd2u-0.8.1.tar
   - cd hd2u-0.8.1
   - ./configure
   - make
   - make install

5) Ejecutar el script "instalacion.sh" presente en el directorio de instalación. Esto actualizará el JDK 1.4.1 con los ficheros adecuados.

6) Descomprimir el fichero "jboss.zip" presente en el directorio "file" dentro del directorio de instalación mediante el comando "unzip".

7) Definir la variable de sistema JBOSS_HOME apuntando al directorio raíz del jboss.

   export JBOSS_HOME = dir_instalacion_JBOSS

EJEMPLO: *export JBOSS_HOME = /usr/local/jboss*

8) A continuación editar el fichero run.sh del directorio JBOSS_HOME/bin y establecer los parámetros adecuados del jboss, editando la línea 187 del fichero:

   org.jboss.Main -c all --host=<server_name> "$@"

   donde <server_name> es el nombre o ip del servidor de firma

9) Pasar el comando "dos2unix" al fichero run.sh presente en el directorio JBOSS_HOME/bin: dos2unix run.sh.

10) Arrancar el Servidor Jboss mediante el comando "sh run.sh", observando que no aparezcan errores en la consola del mismo.

11) Crear un usuario llamado "firma" y hacer que sea el dueño del directorio JBOSS_HOME y todo su contenido. Utilizar este usuario para ejecutar el Servidor de Aplicaciones.

6.3.3 Instalación del componente Servidor Autenticación SSL

Este elemento representa el punto de entrada al sistema para las aplicaciones de autenticación web y es el encargado de capturar los certificados de usuario. A continuación se describe su instalación en las diferentes plataformas.

Para instalar este componente lo único que hay que hacer es copiar el contendido del directorio "Instalación @firma / fachada / SSLServer / Autenticacion" o del directorio "Instalación @firma / fachada / SSLServer / Reautenticacion" al disco duro.

Después de esto ejecutar el script "ejecutar" que corresponda al sistema operativo utilizado, recordar que si es linux pasar primero el comando "dos2unix" al fichero "ejecutar.sh". Observar que no aparezca ningún mensaje de error en la consola. Comentar que en el caso de Linux, debemos tener definidas las variables de entorno JAVA_HOME e incluir en la variable de entorno PATH, el camino JAVA_HOME/bin. Ya que el script supone que dichas variables están correctamente definidas.

Si se instala el SSLServer de Reautenticación hay que tener en cuenta que el certificado utilizado para la maquina debe ser un certificado "wildcard" o de dominio (*.URLBase) y hay que introducir una entrada en el DNS de la red para que cualquier url del tipo "*.URLBase" (aut1.URLBase, aut2.URLBase, …) apunte a la máquina donde se instale la Fachada @Firma.

NOTA: Si estamos en linux crear un usuario llamado firma y hacer que sea el dueño del directorio donde hemos instalado este componente y todo su contenido. Utilizar este usuario para ejecutar el Servidor Autenticacion SSL.

6.3.4 Configuración Fachada

6.3.4.1 Configuración del componente Servidor de Aplicaciones

6.3.4.1.1 Configuración HTTPS del puerto 444

Para un correcto funcionamiento del componente Servidor de Aplicaciones en conexión HTTPS es necesario configurar un certificado de servidor para el puerto de conexión 444. Para ello se debe editar el fichero jboss-service.xml ubicado en el directorio "JBOSS_HOME/server/all/deploy/jbossweb-tomcat41.sar/META-INF", donde JBOSS_HOME es el directorio raíz del componente Servidor de Aplicaciones JBoss.

Localizar la clase Connector del puerto 444 y cambiar el valor de los atributos keystoreFile y keystorePass por los que se consideren adecuados.

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
    port="444" minProcessors="5" maxProcessors="75" enableLookups="false"
    acceptCount="100" debug="0" scheme="https" secure="true"
    useURIValidationHack="false" disableUploadTimeout="true">

     <Factory
    className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
    keystoreFile="${jboss.server.home.dir}/conf/keystoreCajaNegra4"
    keystorePass="changeit" clientAuth="false" protocol="TLS" />

</Connector>
```

El atributo keystoreFile contendrá el fichero keystore con el nuevo certificado servidor y el atributo keystorePass contendrá el password del keystore anterior.

NOTA: Si estamos en Linux en lugar de utilizar el puerto 444 utilizaremos el 4440, ya que en Linux solo el usuario root puede abrir puertos por debajo del 1024, y haremos una redirección de puertos como se esplica en el punto 7.4 Redirección de Puertos en Linux.

6.3.4.1.2 Configuración de la comunicación con el Servidor de Firma

Para que el componente Servidor de Aplicaciones pueda comunicarse con el Servidor de Firma hay que configurar unos parámetros de conexión.

La configuración para comunicarse con el Servidor de Firma se encuentra en el fichero: "JBOSS_HOME\server\all\deploy\properties-service.xml" y solo consta de tres parámetros:

- afirma.servidor: nombre o dirección IP del Servidor de Firma.

- **afirma.usuario:** nombre del usuario para poder utilizar las interfaces RMI-IIOP del Servidor de Firma, ya que están protegidas por JAAS. (Ver el punto 6.2.3.3)

- **afirma.clave:** clave del usuario anterior.

Localizar los parámetros indicados anteriormente y cambiar los valores por los correctos.

6.3.4.2 Configuración del componente Servidor Autenticación SSL

La configuración necesaria para el funcionamiento del componente Servidor Autenticación SSL se encuentra en un fichero llamado constantes.xml que se encuentra en el directorio de instalación del componente.

La estructura del fichero xml es la siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>
<ti>
  <seccion nombre="entorno_E">
            <token nombre="port" valor="443"/>
            <token nombre="ip" valor="10.244.2.54"/>
            <token nombre="servidorfirma" valor="192.168.53.19"/>
            <token nombre="p12" valor="certificado.p12"/>
            <token nombre="passP12" valor="changeit"/>
            <token nombre="pgerrores" valor="http://[dir pagina errores]"/>
            <token nombre="loginrmi" valor="rueda"/>
            <token nombre="passrmi" valor="9876543210"/>
            <token nombre="fauthconf" valor="auth.conf"/>
            <token nombre="flog4j" valor="log4j.xml"/>
            <token nombre="timeout" valor="30000"/>
</seccion>
</ti>
```

A continuación se detallan cada uno de los parámetros:

- port. Puerto por el que la aplicación de captura de certificados de cliente abrirá las conexiones https. Normalmente el 443.

- ip: Es la IP en la cual va a escuchar el servidor de autenticación.

- servidorfirma. Nombre DNS o dirección IP donde se encuentra el servidor de Firma y Autenticación.

- p12. Fichero que contiene el certificado digital de servidor que se utilizará en las conexiones SSL con el cliente para garantizarle la identidad y seguridad de la comunicación que está realizando. Cambiarlo por el apropiado.

- passp12. Password asociado al certificado digital de servidor que se utilizará en las conexiones SSL con el cliente para garantizarle la identidad y seguridad de la comunicación que está realizando. En caso de reautenticación debe se ser un certificado "wildcard" o de dominio (*.DNSBase).

- pgerrores. URL a la que se redireccionará el navegador del usuario cuando se produzca un error de tipo 1, 2 o 6 en el proceso de autenticación. Por defecto será la siguiente:

  "https://<fachada_firma>/firmadigital/servicio/formsBackEnd/errorCertificadoAut.jsp"

- loginrmi. Login de la aplicación de captura de certificados para poder realizar llamadas por RMI/SSL a los compontes de autenticación y validación de certificados del servidor de Firma y Autenticación. (Ver el punto 6.2.3.3)

- passrmi. Password de la aplicación de captura de certificados para poder realizar llamadas por RMI/SSL a los compontes de autenticación y validación de certificados del servidor de Firma y Autenticación.

- fauthconf. ruta absoluta de la localización del fichero que almacena las políticas de autenticación de las llamadas desde la aplicación de captura de certificados al servidor de firma y autenticación. NOTA: No cambiar el que viene por defecto.

- flog4j. ruta absoluta de la localización del fichero que almacena la configuración del Log4j.

- timeout. Timeout para que la aplicación de captura de certificados considere que una conexión https abierta está inactiva, expresado en milisegundos.

NOTA: Si estamos en Linux en lugar de utilizar el puerto 443 utilizaremos el 4430, ya que en Linux solo el usuario root puede abrir puertos por debajo del 1024, y haremos una redirección de puertos como se esplica en el punto 7.4 Redirección de Puertos en Linux.

6.4 Instalación Herramienta de Administración Servidor de Firma

La herramienta de Administración permite administrar remotamente el Servidor de Firma desde cualquier máquina de la Intranet.

Para su funcionamiento requiere una máquina virtual JDK1.4.1 o superior con el parche de seguridad instalado.

El propio Servidor de Firma o la Fachada ya poseen este requisito, así pues, en caso de instalar en ellas la herramienta de administración no es necesario hacer nada previamente.

El caso normal es utilizar cualquier máquina que no sea ninguna de las dos anteriores, así pues, se deben seguir los siguientes pasos:

1) Instalar el JDK 1.4.1 proporcionado en el CD Servidor de la plataforma y definir la variable de entorno JAVA_HOME. Para información detallada sobre este paso ver apartado 7.1 del presente manual.

2) Pasar el parche de seguridad al JDK instalado en el paso anterior, para ello copiar todos los ficheros del directorio "Instalación @firma / utilidades / update JDK1.4.1_02 / security" al directorio "JAVA_HOME / jre / lib / security ".

Terminados los pasos anteriores procedemos a instalar la herramienta de administración propiamente dicha. Para ello, simplemente hay que copiar el contenido del directorio "Administración @firma" del CD Servidor en el disco duro de la máquina.

La herramienta dispone de un fichero de configuración denominado "servidores.properties" en el cual se indican los servidor de Firma que se desean administrar.

servidor1=192.168.53.19

servidor2=<servidor2>

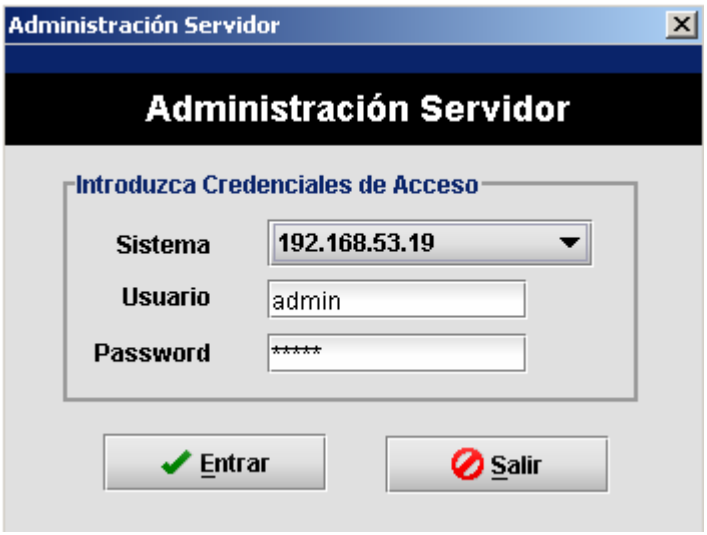
servidor3=<servidor3>

servidor4=<servidor4>

servidor5=<servidor5>

Cada línea contendrá el nombre o ip de un servidor. Así pues, debemos indicar aquí el servidor de Firma de la plataforma que acabamos de instalar.

Finalmente, para arrancar la herramienta se utilizarán los scripts "admin.bat" y "admin.sh" según el sistema operativo windows o linux. Seguidamente se mostrará una ventana que nos permitirá escoger el servidor de Firma que deseamos administrar:



NOTA LINUX: En caso de utilizar una distribución de guadalinex, será necesario disponer de la librería linux "*libstdc++-libc6.1-1.so.2*". Así pues, se recomienda instalar esta librería mediante el comando "dpkg –i".

7 Información adicional

7.1 Instalación del JDK 1.4.1 proporcionado en el CD Servidor

En el directorio "Instalación Jdk1.4" del CD Servidor se proporciona el JDK versión 1.4.1_02. Se recomienda instalar esta versión pues el parche de seguridad de Java de la instalación de la plataforma corresponde a esta versión.

Los pasos necesarios para su instalación son los siguientes:

7.1.1 Sistema Operativo Windows

1. Ejecutar el fichero "j2sdk-1_4_1_02-windows-i586.exe" disponible en el directorio del CD Servidor *"Instalacion Jdk1.4/windows"* y seguir los pasos del asistente hasta completar la instalación. Elegir como tipo de instalación: la instalación por defecto o completa. Es importante tener en cuenta el directorio donde se va a instalar el JDK ya que va a servir de referencia en futuras configuraciones y conviene que no sea muy complejo, ni contenga espacios en blanco en su nombre. (Por ejemplo: c:\jdk1.4)

2. A continuación es necesario crear la variable de entorno de sistema JAVA_HOME y modificar la variable PATH. Para establecer una variable de entorno en Windows 2000, Ir a "panel de control\Sistema\Pestaña Avanzado\Variables de entorno". Establecer la variable JAVA_HOME al directorio donde se instaló el JDK:

   JAVA_HOME = dir_instalación_JDK .....(ejem. JAVA_HOME = c:\jdk1.4)

   Actualizar la variable de sistema PATH añadiendo al contenido existente el directorio *"bin"* del JDK:

   PATH=c:\jdk1.4\bin;%PATH%

A partir de este momento y en el resto del documento, el directorio de instalación del JDK se referenciará como JAVA_HOME.

7.1.2 Sistema Operativo Linux

1. Ejecutar el fichero "j2sdk-1_4_1_02-linux-i586.bin" (es necesario copiarlo al disco duro y darle permiso de ejecución chmod +x) disponible en el directorio del CD *"Instalacion Jdk1.4/linux"* y seguir los pasos del asistente hasta completar la instalación. Es importante tener en cuenta el directorio donde se va a instalar el JDK ya que va a servir de referencia en futuras configuraciones y conviene que no sea muy complejo, ni contenga espacios en blanco en su nombre. (Por ejemplo: /usr/local/jdk1.4)

2. A continuación es necesario crear la variable de entorno de sistema JAVA_HOME y modificar la variable PATH:

   export JAVA_HOME = dir_instalacion_JDK

EJEMPLO: *export JAVA_HOME = /usr/local/jdk1.4*

Actualizar la variable de sistema PATH añadiendo al contenido existente el directorio *"bin"* del JDK:

PATH=$PATH:/usr/local/jdk1.4/bin

A partir de este momento y en el resto del documento, el directorio de instalación del JDK se referenciará como JAVA_HOME.

7.2 Consideraciones sobre instalación Cliente Oracle

El Servidor de Firma necesita para su funcionamento tener instalado el Cliente Oracle para disponer del driver OCI. Solamente se permite este driver por la necesidad de transferir ficheros de tamaño del orden de Mbytes en el módulo de Firma de Documentos.

Para instalar el Cliente Oracle utilizar el manual y software apropiados de Oracle. No obstante, a continuación se comentan unas consideraciones adicionales para poder utilizar dicho driver desde JAVA.

7.2.1 Sistema Operativo Windows

Una vez instalado el Cliente Oracle Windows, se deben considerar los siguientes pasos:

1) Configurar el fichero "*tnsnames.ora"*.

2) Copiar los ficheros *"heteroxa9.dll"* y *"ocijdbc9.dll"* ubicados en el directorio de instalación del cliente oracle al directorio %JAVA_HOME%\bin

7.2.2 Sistema Operativo Linux

Una vez instalado el Cliente Oracle Linux.

1) Configurar el fichero "*tnsnames.ora"*.

2) Copiar los ficheros *"ocrs12.zip"* y *"ojdbc14_g.jar"* disponibles en la instalación del cliente oracle en el directorio $JAVA_HOME/jre/lib/ext.

3) Definir las siguientes variables de entorno:

ORACLE_HOME = <directorio_oracle>/OraHome1

LD_LIBRARY_PAH = $ORACLE_HOME/lib

CLASSPATH = $ORACLE_HOME/jlib

TNS_ADMIN = $ORACLE_HOME/network/admin/tnsnames.ora

PATH=$PATH:<dir_jdk>/bin:$ORACLE_HOME/bin

export ORACLE_HOME LD_LIBRARY_PATH CLASSPATH TNS_ADMIN PATH

NOTA: Esta información PUEDE que sea diferente en función de la versión de Oracle, Linux, drivers, etc… Así pues, solo debe tomarse como una ayuda complementaria en caso de encontrar problemas en la instalación del Cliente Oracle Linux del manual Oracle.

7.3 Poner componentes plataforma como Servicio del Sistema Operativo

7.3.1 Servidor de Aplicaciones JBOSS

Después de tener instalado el sistema y correctamente funcionando se indican los pasos necesarios para instalar el servidor como servicio del sistema operativo

7.3.1.1 Sistema Operativo Windows

1. Copiar los scritpts "InstallJBossService.bat", "UninstallJBossService.bat" y el fichero JavaService.exe situados dentro del directorio "Instalacion @firma\utilidades\Jboss Service\ windows" del CD Servidor en el directorio "JBOSS_HOME\bin".

2. Para instalar el servicio desplazarse al directorio "JBOSS_HOME\bin" y ejecutar desde línea de comandos el script "InstallJBossService.bat" con la siguiente sintaxis:

   InstallJBossService <nombre_servicio> <nombre_hosh>

   Donde <nombre_servicio> ha de substituirse por el nombre que le queremos dar al servicio que lanza JBoss y <nombre_hosh> por el nombre o la IP de la máquina donde se lanza. Por ejemplo:

   InstallJBossService JBoss 172.19.132.110

3. Comprobar que el servicio se ha instalado correctamente mirando la lista de servicios del sistema y una vez localizado proceder a iniciarlo. Es necesario esperar un minuto aprox. hasta que el servidor se haya levantado por completo. Se puede consultar la gestión de recursos del Administrador de tareas del sistema operativo para ver cuando la CPU vuelve a funcionar a los niveles normales.

4. Para desinstalar el servicio ejecutar desde línea de comandos el script "UninstallJBossService.bat" con la siguiente sintaxis:

   UninstallJBossService <nombre_servicio>

   Donde <nombre_Servicio> ha de substituirse por el nombre del servicio que lanza JBoss. Por ejemplo:

UninstallJBossService JBoss

7.3.1.2 Sistema Operativo Linux

Para una mejor compresión de este apartado se presupone que JBoss está instalado en /usr/local/JBoss.

1. Copiar el fichero "jboss" incluido en el CD de instalación en la ruta "Instalacion @firma/utilidades/Jboss Service/unix", en el directorio "/etc/init.d". Dar permisos de ejecución al fichero jboss:

> chmod u+x /etc/init.d/jboss

2. Modificar la variable de entorno PATH para incluir el camino JAVA_HOME/bin.

3. Editar el fichero "/etc/init.d/jboss", para indicar correctamente la localización del jboss y del JDK instalado.

JBOSS_HOME=${JBOSS_HOME:-"<directiorio_jboss> "}

JAVA_HOME=<directorio_jdk>

Donde <directorio_jboss> es el directorio donde se ha instalado el JBOSS y <directorio_jdk> es el directorio donde se ha instalado el jdk. Por ejemplo:

JBOSS_HOME=${JBOSS_HOME:-"/usr/local/jboss-3.2.3/"}

JAVA_HOME=/usr/local/j2sdk1.4.1_02

4. Usar lo siguiente para crear un link simbólico con los niveles de ejecución apropiados. JBoss se reiniciará cada vez que lo haga el servidor.

RedHat y derivados:

> chkconfig --set jboss 345

Resto de sabores linux:

> cd /etc/rc2.d/

> ln -s /etc/init.d/jboss S99jboss

> cd /etc/rc6.d/

> ln -s /etc/init.d/jboss K01jboss

5. Si queremos eliminar el servicio, sólo tendremos que borrar los enlaces creados anteriormente con los siguientes comandos:

> rm /etc/init.d/S99jboss

> rm /etc/init.d/K01jboss

6. Cambiar la codificación del fichero de dos a unix mediante el comando dos2unix:

   > dos2unix jboss

   NOTA: Si no se dispone de dicha utilidad, en el directorio del CD de instalación "*utilidades/herramientas_linux*" se proporcionan los fuentes de la misma. Para compilar la utilidad dos2unix, seguir los siguientes pasos:

   - gunzip hd2u-0.8.1.tar.gz
   - tar xvf hd2u-0.8.1.tar
   - cd hd2u-0.8.1
   - ./configure
   - make
   - make install

7. Iniciar el servicio:

   > /etc/init.d/jboss start

8. Parar el servicio

   > /etc/init.d/jboss stop

7.3.2 Servidor Autenticación SSL

Después de tener instalado el sistema y correctamente funcionando se indican los pasos necesarios para instalar el servidor como servicio del sistema operativo.

7.3.2.1 Sistema Operativo Windows

1. Copiar los scritpts "InstallSSLServerService.bat", "UninstallSSLServerService.bat" y el fichero JavaService.exe situados dentro del directorio "Instalacion @firma\utilidades\SSLServer Service\ windows" del CD Servidor en el directorio de instalación de este componente.

2. Editar el fichero "InstallSSLServerService.bat" para indicar la localización del Servidor de Autenticacion SSL.

   set SSLSERVER_HOME=<dir_servidor_autenticacion>

Donde <dir_servidor_autenticacion> es el directorio donde se ha instalado el Servidor de Autenticacion. Por ejemplo:

set SSLSERVER_HOME=c:\Autenticacion

3. Para instalar el servicio desplazarse al directorio anterior y ejecutar desde línea de comandos el script "InstallSSLServerService.bat" con la siguiente sintaxis:

   InstallSSLServerService <nombre_servicio>

   Donde <nombre_Servicio> ha de substituirse por el nombre que le queremos dar al servicio que lanza Servidor de Autenticación. Por ejemplo:

   InstallSSLServerService SSLServer

4. Comprobar que el servicio se ha instalado correctamente mirando la lista de servicios del sistema y una vez localizado proceder a iniciarlo.

5. Para desinstalar el servicio ejecutar desde línea de comandos el script "UninstallSSLServerService.bat" con la siguiente sintaxis:

   UninstallSSLServerService <nombre_servicio>

   Donde <nombre_Servicio> ha de substituirse por el nombre del servicio que lanza el Servidor de Autenticación. Por ejemplo:

   UninstallSSLServerService SSLServer

7.3.2.2 Sistema Operativo Linux

1. Copiar el scritpt "sslserver" situado dentro del directorio "Instalacion @firma\utilidades\SSLServer Service\ unix" del CD Servidor en el directorio "/etc / init.d".

2. Definir la variable de entorno JAVA_HOME e incluir el path JAVA_HOME/bin en la variable de entorno PATH.

3. Cambiar la codificación del fichero de dos a unix mediante el comando dos2unix:

   > dos2unix sslserver

   NOTA: Si no se dispone de dicha utilidad, en el directorio del CD de instalación "*utilidades/herramientas_linux*" se proporcionan los fuentes de la misma. Para compilar la utilidad dos2unix, seguir los siguientes pasos:

   - gunzip hd2u-0.8.1.tar.gz
   - tar xvf hd2u-0.8.1.tar
   - cd hd2u-0.8.1
   - ./configure
   - make
   - make install

4. Editar el fichero y modificar la siguientes variable, que se encuentran al principio del fichero:

- SSLSERVER_HOME : Directorio donde se encuentra instalado el Servidor de Autenticación SSL.

5. Cambiar los permisos del fichero con los siguientes comandos:

   > chmod u+x /etc/init.d/sslserver

6. Usar lo siguiente para crear un link simbólico con los niveles de ejecución apropiados. JBoss se reiniciará cada vez que lo haga el servidor.

   RedHat y derivados:

   > chkconfig --set jboss 345

   Resto de sabores linux:

   > cd /etc/rc2.d/

   > ln-s /etc/init.d/sslserver.sh S99sslserver

   > cd /etc/rc6.d/

   > ln –s /etc/init.d/sslserver.sh K01sslserver

7. Si queremos eliminar el servicio, sólo tendremos que borrar los enlaces creados anteriormente con los siguientes comandos:

   > rm /etc/init.d/S99sslserver

   > rm /etc/init.d/K01sslserver

7.4 Redirección de Puertos en Linux.

En Linux solo el usuario root puede abrir puertos por debajo del 1024 y como hemos visto al configurar tanto el servidor como la fachada se utilizan los puertos 443 (https) y 444, para poder utilizar dichos puertos sin tener que ejecutarlos con el usuario root, lo cual seria un agujero de seguridad, sino con el usuario "firma" que nos hemos creado a tal efecto configuraremos el servidor y la fachada con puertos por encima del 1024 como el 4430 y 4440 y realizaremos una redirección de puertos utilizando iptables.

Debemos crear una regla de iptables de la siguiente forma:

iptables -t nat -A PREROUTING -p tcp -m tcp --dport <puerto_origen> -d <ip_maquina> -j REDIRECT --to-port <puerto_destino>

Donde <puerto_origen> es el puerto por donde vienen las peticiones (443 o 444), la <ip_maquina> es la dirección IP de la máquina y <puerto_destino> es el puerto que hemos utilizado en la configuración (4430 o 4440). Por ejemplo:

iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -d 192.168.53.58 -j REDIRECT --to-port 4430

La codificación de dicha regla se da a modo orientativo y puede variar según la versión concreta de iptables que tenga instalado el linux. Esta regla está probada en SuSE Server 8.

Para hacer la redirección de puertos en SuSE Server 8 hemos utilizado el firewall que viene por defecto, "SuSEfirewall2":

1. Sustituir los ficheros "SuSEfirewall2" y "SuSEfirewall2_custom" por los situados dentro del directorio "Instalacion @firma\utilidades\redireccion de puertos" del CD Servidor.

2. Cambiar la codificación de los ficheros de dos a unix mediante el comando dos2unix:

   > dos2unix SuSEfirewall2

   NOTA: Si no se dispone de dicha utilidad, en el directorio del CD de instalación "*utilidades/herramientas_linux*" se proporcionan los fuentes de la misma. Para compilar la utilidad dos2unix, seguir los siguientes pasos:

   - gunzip hd2u-0.8.1.tar.gz
   - tar xvf hd2u-0.8.1.tar
   - cd hd2u-0.8.1
   - ./configure
   - make
   - make install

3. Editar el fichero "SuSEfirewall2" y configurar las siguientes variables:

   - FW_DEV_EXT="<interfaz_red>"

   - FW_SERVICES_EXT_TCP="<puertos>"

Donde <interfaz_red> es nombre de la interfaz de red que está utilizando la máquina y <puertos> es la lista de puertos que estan abiertos en firewall. Por ejemplo:

- *FW_DEV_EXT="eth0"*

- *FW_SERVICES_EXT_TCP="22 443 4430"*

4. Editar el fichero "SuSEfirewall2_custom" y buscar y configurar la regla de iptables como explicamos más arriba.

5. Poner el firewall como servicio de linux ejecutando los siguientes comandos en la carpeta /etc/init.d/:

   - chkconfig SuSEfirewall2_init

   - chkconfig SuSEfirewall2_setup

   - chkconfig SuSEfirewall2_final

7.5 Arranque y parada manual del Servidor de Aplicaciones JBOSS

El arranque y parada manual del servidor Jboss se realiza desde una ventana shell del sistema operativo.

Para el arranque sólo es necesario ejecutar el fichero "run" situado en el directorio JBOSS_HOME\bin. El arranque total del servidor tiene una duración variable que va desde los 20 segundos a los 2 minutos aproximadamente y que depende de los recursos del sistema. NOTA: JBOSS_HOME es el directorio donde se ha instalado el servidor Jboss.

En Sistema Operativo Linux es necesario cambiar la codificación del fichero de dos a unix, para ello se utiliza el comando dos2unix:

dos2unix run.sh

NOTA: Si no se dispone de dicha utilidad, en el directorio del CD de instalación "*utilidades/herramientas_linux*" se proporcionan los fuentes de la misma. Para compilar la utilidad dos2unix, seguir los siguientes pasos:

- gunzip hd2u-0.8.1.tar.gz
- tar xvf hd2u-0.8.1.tar
- cd hd2u-0.8.1
- ./configure
- make
- make install

Para la parada del servidor sólo es necesario ejecutar el fichero "shutdown" situado en el directorio JBOSS_HOME\bin.

En Sistema Operativo Linux es necesario cambiar la codificación del fichero de dos a unix, para ello se utiliza el comando dos2unix:

dos2unix shutdown.sh

7.6 Requisitos Clientes plataforma de Firma

Entre los requerimientos mínimos del Cliente de la plataforma destacan:

- Sistema Operativo: Windows (9x, NT, 2000) y Linux.

- *Máquina virtual de Java: Java Development Kit 1.4.x, de Sun Microsystems. Este requisito sólo es necesario para las aplicaciones Java que hagan uso de las interfaces RMI-IIOP de @firma.

- Clientes Firma web:

    - El navegador tiene que estar configurado con encriptación alta (128 bits).

    - Los navegadores han de tener instalado el certificado de la FNMT-RCM como entidad certificadora en la que se confía y tener instalados los certificados digitales expedidos por la FNMT-RCM de los usuarios que vayan a utilizarlo. Los certificados pueden residir en fichero o en soporte seguro, por ejemplo, tarjeta criptográfica.

    - Para Windows: El navegador web de los clientes que accedan a la aplicación ha ser Internet Explorer 5.0 o superior, ó Netscape 6 o superior, con una máquina virtual de Java (JVM 1.1.4 de Microsoft ó JRE 1.4.x de Sun) correctamente instalada y activada.

    - Para Linux: El navegador web de los clientes que accedan a la aplicación ha ser Mozilla 1.3 o superior con JRE 1.4.1 o superior de Sun y librería JSS33.

    La siguiente figura representa las pruebas realizadas en navegadores clientes con diferentes máquinas virtuales de java.

Sistema Operativo Linux						
	Navegador / JRE	Mozila 1.3				
	JRE 1.4.1+					
Sistema Operativo Windows (9x/NT/2000)						
	Navegador / JRE	IE 5.0	IE 5.5	IE 6.0	NS 4.7	NS 7
	JVM 1.1.4				No aplica	No aplica
	JRE 1.4.0					No aplica
	JRE 1.4.1+					
Sistema Operativo Win XP						
	Navegador / JRE	IE 6.0				
	JVM 1.1.4					
	JRE 1.4.0					
	JRE 1.4.1+					

- Clientes Firma Ficheros:

  - El navegador tiene que estar configurado con encriptación alta (128 bits).

  - Los navegadores han de tener instalado el certificado de la FNMT-RCM como entidad certificadora en la que se confía y tener instalados los certificados digitales expedidos por la FNMT-RCM de los usuarios que vayan a utilizarlo. Los certificados pueden residir en fichero o en soporte seguro, por ejemplo, tarjeta criptográfica.

  - Para Windows: El navegador web de los clientes que accedan a la aplicación ha ser Internet Explorer 5.0 o superior, Mozilla 1.3 o superior y sus derivados, es decir Netscape, Firebird, etc.. (con una máquina virtual de Java JRE 1.4.x de Sun correctamente instalada y activada). NOTA: JRE solamente necesario para Mozilla y derivados, no para Internet Explorer.

  - Para Linux: El navegador web de los clientes que accedan a la aplicación ha ser Mozilla 1.3 o superior con JRE 1.4.1 o superior de Sun y librería JSS33.