

Seminario de integración y despliegue del módulo @Firma v5 de Autenticación web mediante tickets

Febrero 2009



JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

➔ Índice

1. Introducción

2. Requisitos previos

3. CD Entregable de instalación del módulo de autenticación med. tickets.

4. Procedimiento de instalación en el núcleo de @firma v5

5. Procedimiento de instalación en la fachada de @firma v5

6. Turno de ruegos y preguntas.

➔ 1. Introducción

- **Funcionalidades principales.**
- **Versiones instaladas.**
- **Arquitectura física y lógica en CJAP.**

- **Funcionalidades principales**

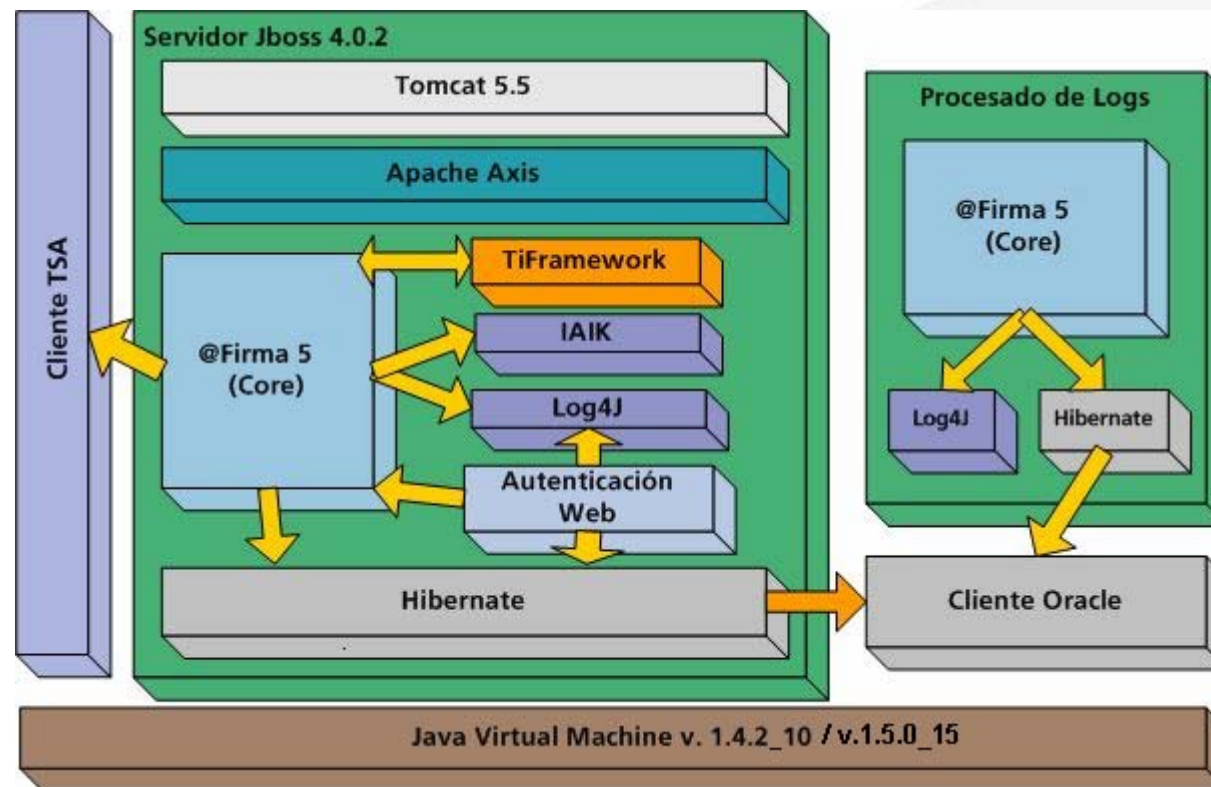
- El módulo de Autenticación Web es un sistema genérico y centralizado basado en certificados digitales, que permite a cualquier aplicación Web ya desarrollada o por desarrollar delegar el proceso de autenticación Web en este sistema.
- Para ello utiliza un componente cliente de llamada y otro de retorno, ambos componentes proporcionados en la tecnología de la aplicación a integrar para que sea más fácil su manipulación y adaptación para cada aplicación en concreto.

- **Versiones**

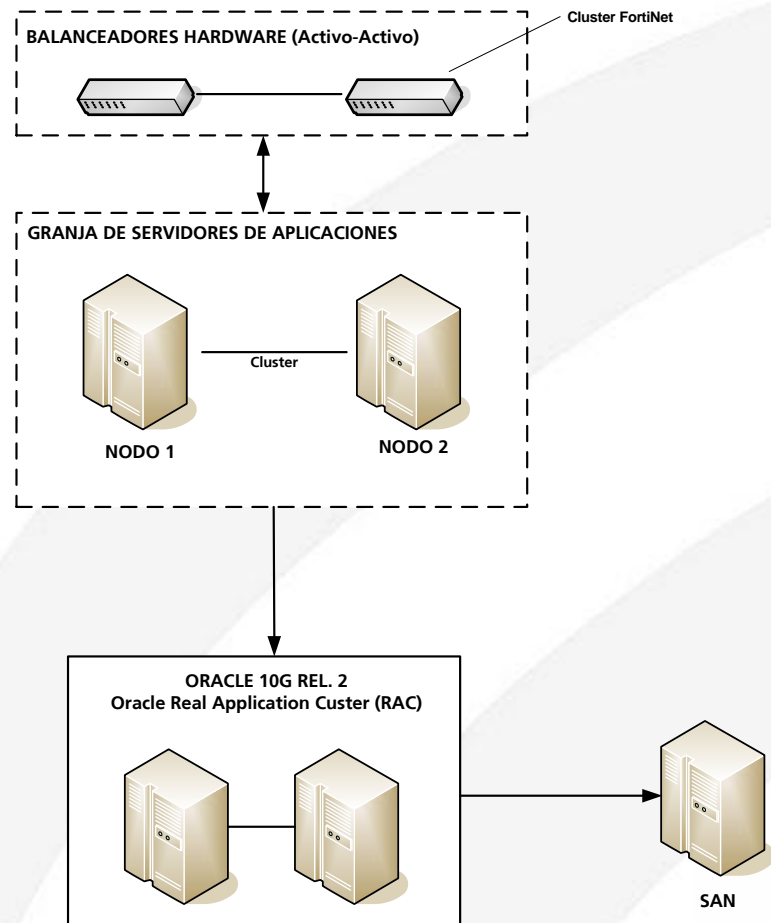
- Diciembre 2008: v1.1.2 (C. Justicia y Administración Pública)

- **Arquitectura física y lógica de @firma v5 en CJAP.**

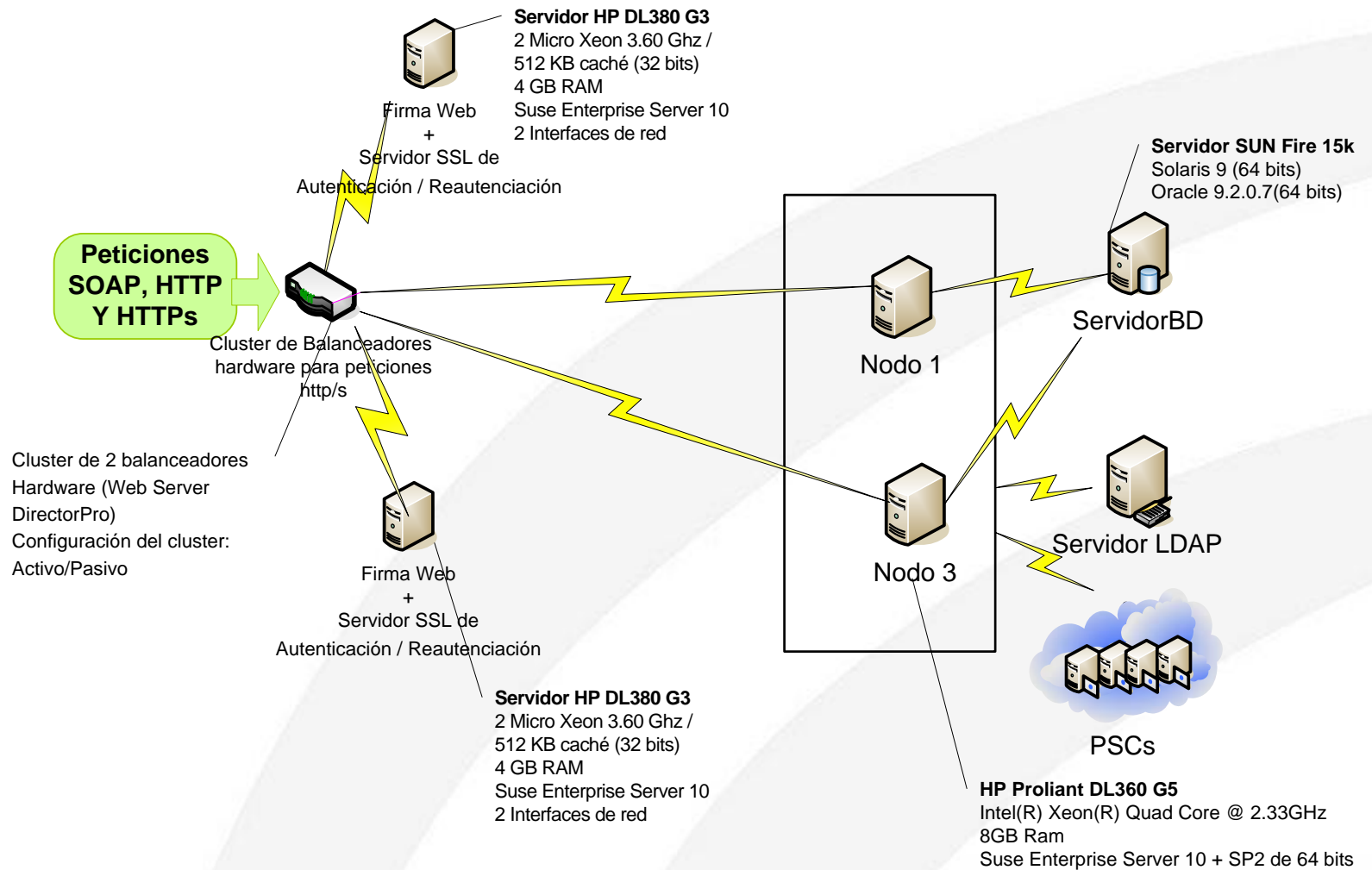
- **Arquitectura Software.**



➤ **Arquitectura Hardware.**



➤ Arquitectura Hardware en la Junta de Andalucía.



➔ Índice

1. Introducción

2. Requisitos previos

3. CD Entregable de instalación del módulo de autenticación med. tickets.

4. Procedimiento de instalación en el núcleo de @firma v5

5. Procedimiento de instalación en la fachada de @firma v5

6. Turno de ruegos y preguntas.

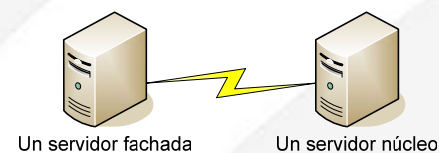
➔ Requisitos previos

- **Requisitos hardware: configuración y versiones utilizadas.**

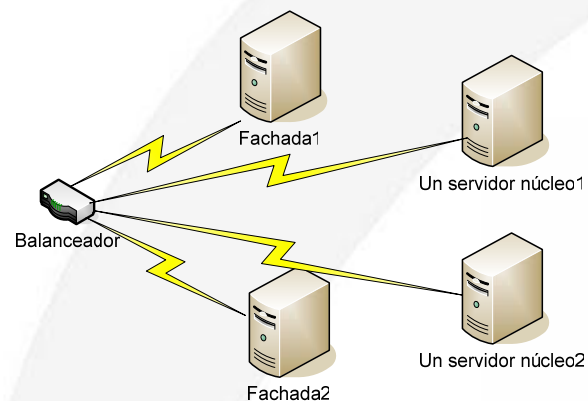
- Arquitecturas recomendadas: *(Se recomiendan ambas a 64 bits)*
 - *Intel (Xeon Dual Core o Quad Core)*
 - *Sparc (no recomendable ultraSparc T1)*
- Tarjeta/s de red adicional/es (Módulo Fachada)
- Servidores necesarios

❖ Plataforma @Firma v5.0.1 ya instalada:

Entorno Desarrollo:



Entorno Producción



➔ Requisitos previos

- **Requisitos software:**

- SSOO compatibles:

Suse Enterprise Server 9 o 10 (recomendado de 64 bits)
Red Hat Enterprise Linux 4 o 5 (recomendado de 64 bits)
Solaris 9 o 10 (recomendado de 64 bits)

- Java:

Módulo Fachada y Módulo núcleo

Versiones `jdk1.5.0_15` recomendado de 64 bits.

- @Firma v5:

Plataforma @Firma v5.0.1 revisión 05, con o sin extensiones de compatibilidad, correctamente instalada.

➔ Requisitos previos

- **Requisitos de configuración:**

- Es necesario para el entorno de producción, un balanceador que distribuya las peticiones entre los nodos que componen la plataforma, para asegurar el rendimiento, la escalabilidad, y el servicio continuado de la plataforma.
 - La publicación de la plataforma en RCJA (caso de organismos que estén dentro de RCJA), se hará siguiendo el estándar https con autenticación cliente (<https://wsXYZ.juntadeandalucia.es>)

- Certificados de servidor:
Es necesario un certificado de servidor:

- a) Con el fin de asegurar por https la plataforma, se dispone de un certificado wildcard para el dominio juntadeandalucia.es que protege a todos sus subdominios, de gran utilidad por ejemplo para todos los servidores publicados bajo el estándar wsXYZ.juntadeandalucia.es.

Aquellas Consejerías y Organismos de la Junta de Andalucía que deseen utilizarlo pueden contactar con: soporte.admonelectronica@juntadeandalucia.es.

Solicitud de certificados de servidor FNTM-RCM

<https://ws024.juntadeandalucia.es/pluton/ofivirtual/guias/componentes.jsp>

• Reautenticación web. ¿Qué es?

Módulo de Reautenticación

- En una misma sesión web, el protocolo SSL sólo realiza el intercambio de certificados una sola vez, con lo cual en el caso anterior el navegador sólo pide el certificado anterior una única vez y no “n veces” como sería aconsejable. Las aplicaciones suelen comprobar que un usuario no accede más de una vez al servidor de @firma en una misma sesión web, para evitar que si un usuario deja abierta la ventana del navegador, otra persona pueda utilizar “fraudulentamente” el certificado del usuario.
- Para solucionar este inconveniente una solución podría ser la existencia de varios Servidores SSL para autenticación y que la aplicación llamara a uno distinto cada vez que necesitara la autenticación. Esta solución ha sido adoptada por la AEAT (Agencia Tributaria).
- La solución aportada en la nueva versión de @firma es la instalación de un nuevo componente de reautenticación, que permite simular la existencia de varios “servidores SSL virtuales” configurados a través de un certificado wildcard.

CERTIFICADOS WILDCARD (comodín)



Un certificado Wildcard Digital permite ser utilizado conjuntamente con cualquier URL en el formato https://*.dominio.es sin generar una alerta de incompatibilidad con el nombre de dominio.

• Reautenticación web. Solicitud y configuración

Solicitud a RCJA

- 1) Solicitud alias necesarios para el correcto funcionamiento de la fachada de reautenticación web.
- 2) Serán necesarios 3 alias apuntando a la ip de la fachada de reautenticación (10.A.B.C - wsXYZ.juntadeandalucia.es) siguiendo el estándar de https con autenticación cliente consecutivas (*wsXYZ-1.juntadeandalucia.es*, *wsXYZ-2.juntadeandalucia.es* y *wsXYZ-3.juntadeandalucia.es*) para el módulo de reautenticación de la Plataforma @Firma v5 del organismo X.

Es decir, la petición quedaría de la siguiente manera siguiendo el ejemplo, contando la Plataforma con un total de 4 reautenticaciones en todas sus aplicaciones integradas con dicho módulo:

10.A.B.C - wsXYZ.juntadeandalucia.es

Alias

10.A.B.C – wsXYZ-1.juntadeandalucia.es

10.A.B.C – wsXYZ-2.juntadeandalucia.es

10.A.B.C – wsXYZ-3.juntadeandalucia.es

Configuración

La configuración de este servicio, se detalla en el manual de instalación y despliegue del módulo fachada de tickets "*TI-@Firma-SSLServer-Tickets-Despliegue-MAN.pdf*".

➔ Requisitos previos

- **Requisitos de instalación.**

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

1) Instalar el jdk1.5.0_15 proporcionado en la siguiente url (página oficial de SUN):

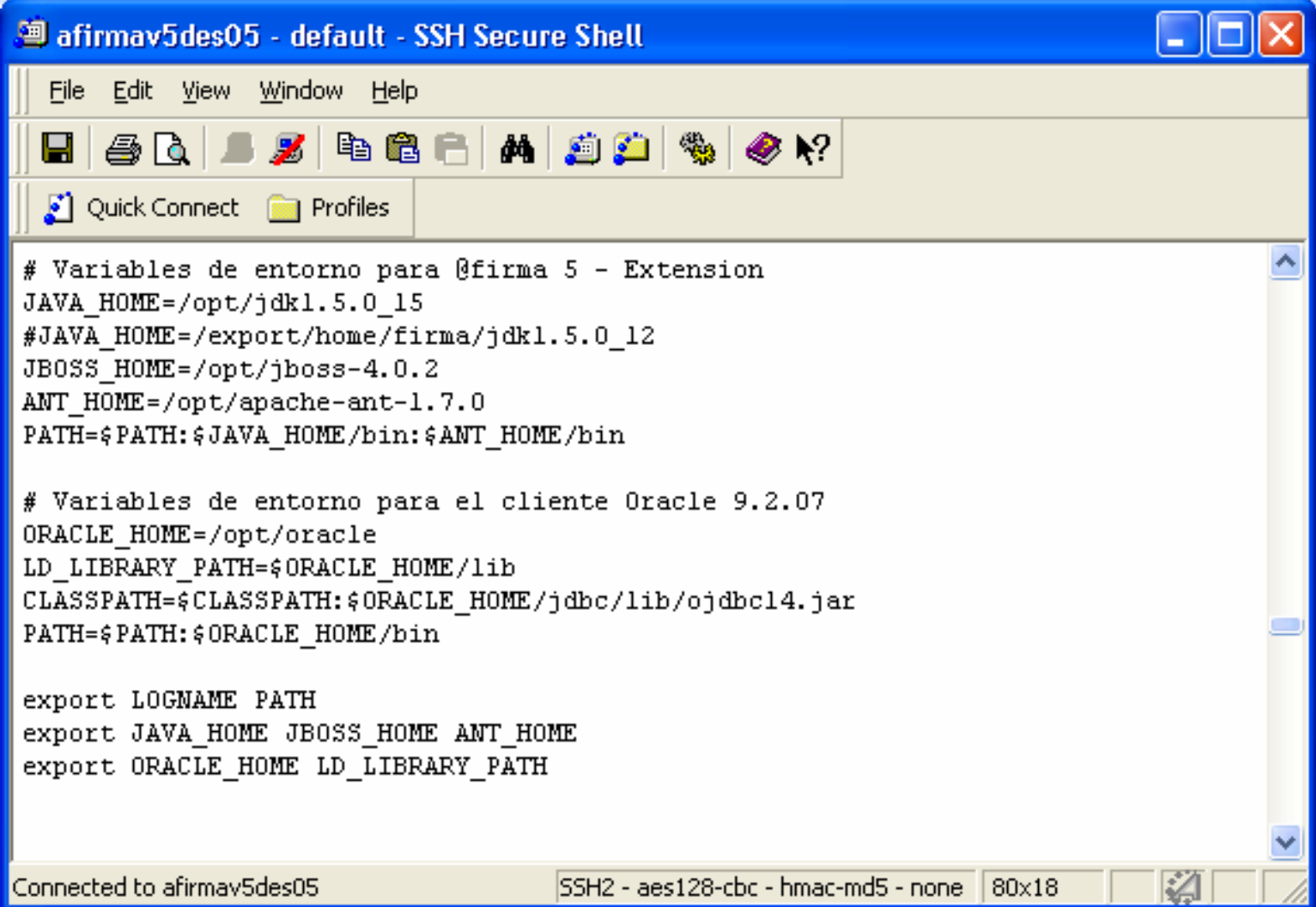
<http://java.sun.com/products/archive/>

2) El sistema operativo debe tener instalado el **paquete de utilidad “dos2unix”**.

3) Tener instalada la **herramienta gratuita Ant** (<http://ant.apache.org/>) e incluida en el classpath el directorio de ejecutables de dicha herramienta.

➔ Requisitos previos

4) Definir las variables de entorno apropiadas



```
afirmav5des05 - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles

# Variables de entorno para @firma 5 - Extension
JAVA_HOME=/opt/jdk1.5.0_15
#JAVA_HOME=/export/home/firma/jdk1.5.0_12
JBOSS_HOME=/opt/jboss-4.0.2
ANT_HOME=/opt/apache-ant-1.7.0
PATH=$PATH:$JAVA_HOME/bin:$ANT_HOME/bin

# Variables de entorno para el cliente Oracle 9.2.07
ORACLE_HOME=/opt/oracle
LD_LIBRARY_PATH=$ORACLE_HOME/lib
CLASSPATH=$CLASSPATH:$ORACLE_HOME/jdbc/lib/ojdbc14.jar
PATH=$PATH:$ORACLE_HOME/bin

export LOGNAME PATH
export JAVA_HOME JBOSS_HOME ANT_HOME
export ORACLE_HOME LD_LIBRARY_PATH

Connected to afirmav5des05  SSH2 - aes128-cbc - hmac-md5 - none  80x18
```

➔ Requisitos previos

5) **IMPORTANTE.** Librerías del proveedor criptográfico IAIK. Es necesario obtener los siguientes componentes de IAIK:

- JCE v3.1.4
- ISASILK v4.0

Para los organismos pertenecientes a la Junta de Andalucía, se da la opción de descargar estas librerías mediante correo solicitandolo al área de descargas privadas de la web técnica Plutón.

Para los organismos no pertenecientes a la Junta de Andalucía:

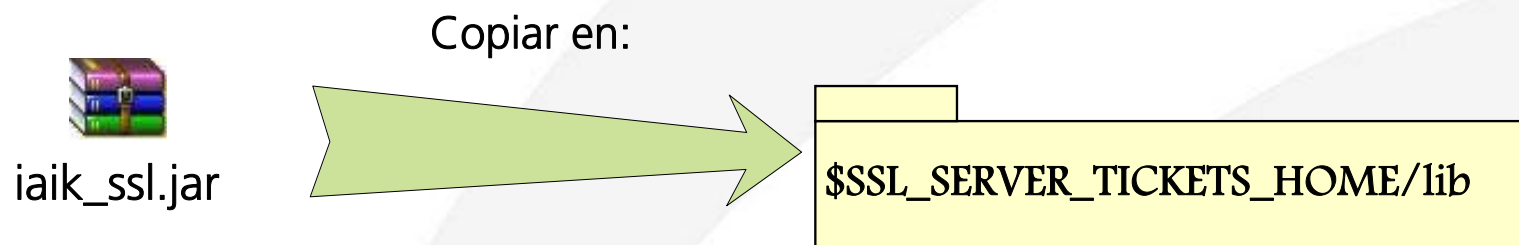
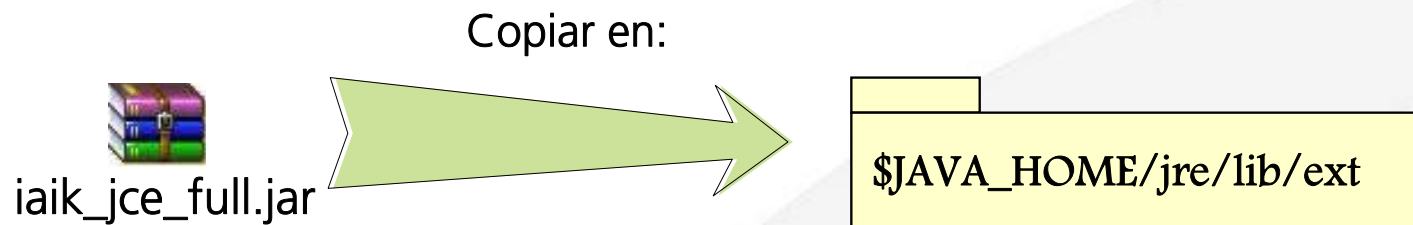
<http://jce.iaik.tugraz.at/>

A continuación se detalla la estructura del software obtenido y los directorios en los que habrá que copiar dicho software.



➔ Requisitos previos

- Requisitos de instalación



➔ Requisitos previos

- **Requisitos de instalación.**

6) **Modo de funcionamiento.** El módulo de autenticación Web mediante tickets presenta dos modos de funcionamiento:

a. **Modo simple:** permite efectuar una única autenticación de usuario por sesión web. Este modo no requiere una configuración adicional, ni el uso de ningún elemento adicional.

b. **Modo múltiple (Reautenticación):** permite llevar a cabo varias autenticaciones independientes de usuario por sesión Web. Para que el módulo funcione correctamente en este modo se requiere registrar en un servidor de DNS inverso tantos alias para la IP / DNS del componente fachada como autenticaciones deseen realizarse por sesión y hacer uso de un certificado wildcard, o de dominio, en el componente de fachada del módulo.

➔ Índice

1. Introducción

2. Requisitos previos

3. CD Entregable de instalación del módulo de autenticación med. tickets.

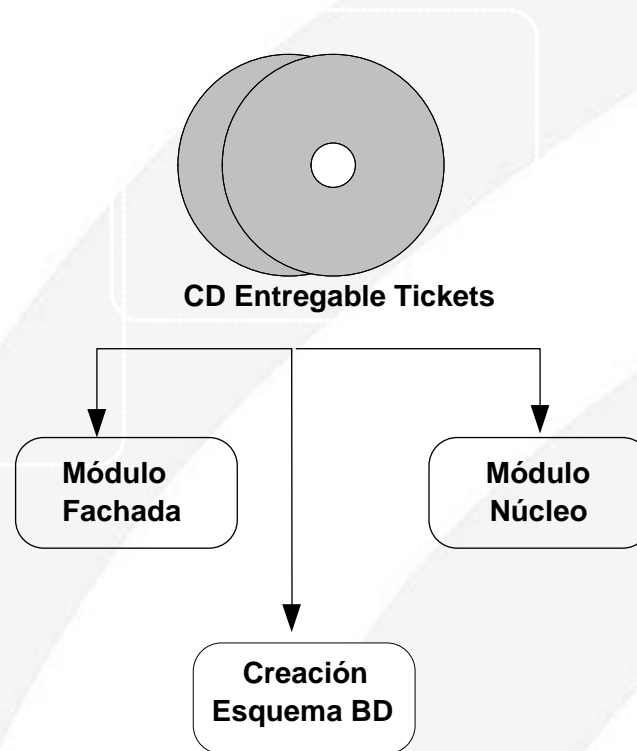
4. Procedimiento de instalación en el núcleo de @firma v5

5. Procedimiento de instalación en la fachada de @firma v5

6. Turno de ruegos y preguntas.

➔ CD Entregable del módulo de tickets

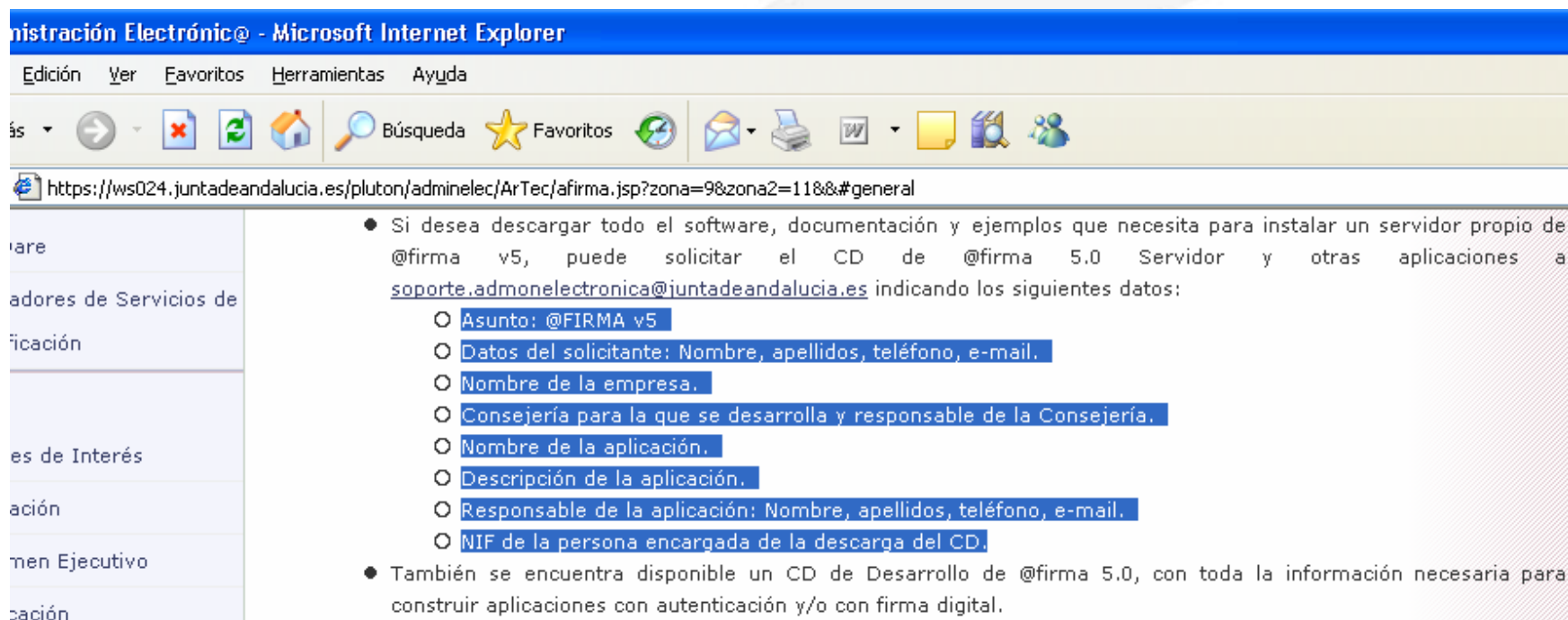
- **Componentes:**
 - a. **Modulo fachada de autenticación web med. tickets,**
 - b. **Módulo núcleo de autenticación web med. tickets.**
 - c. **Creación Esquema Base de datos.**



• Solicitud del cd de instalación y despliegue

Pueden solicitar el software de @firma5 todas aquellos Organismos que han firmado el Convenio para la Cesión de Software.

- <https://ws024.juntadeandalucia.es/pluton/adminelec/ArTec/afirma.jsp?zona=9&zona2=11&&#general>



Administración Electrónica - Microsoft Internet Explorer

Edición Ver Favoritos Herramientas Ayuda

https://ws024.juntadeandalucia.es/pluton/adminelec/ArTec/afirma.jsp?zona=9&zona2=11&&#general

Si desea descargar todo el software, documentación y ejemplos que necesita para instalar un servidor propio de @firma v5, puede solicitar el CD de @firma 5.0 Servidor y otras aplicaciones a soporte.admonelectronica@juntadeandalucia.es indicando los siguientes datos:

- Asunto: @FIRMA v5
- Datos del solicitante: Nombre, apellidos, teléfono, e-mail.
- Nombre de la empresa.
- Consejería para la que se desarrolla y responsable de la Consejería.
- Nombre de la aplicación.
- Descripción de la aplicación.
- Responsable de la aplicación: Nombre, apellidos, teléfono, e-mail.
- NIF de la persona encargada de la descarga del CD.

También se encuentra disponible un CD de Desarrollo de @firma 5.0, con toda la información necesaria para construir aplicaciones con autenticación y/o con firma digital.

- Solicitud mediante correo electrónico al área técnica de soporte de Administración electrónica:



soporte.admonelectronica@juntadeandalucia.es

Indicándose los siguientes datos:

Asunto: @FIRMA v5 – CD Instalación Autenticación Web med. tickets

Datos del solicitante: Nombre, apellidos, teléfono, e-mail.

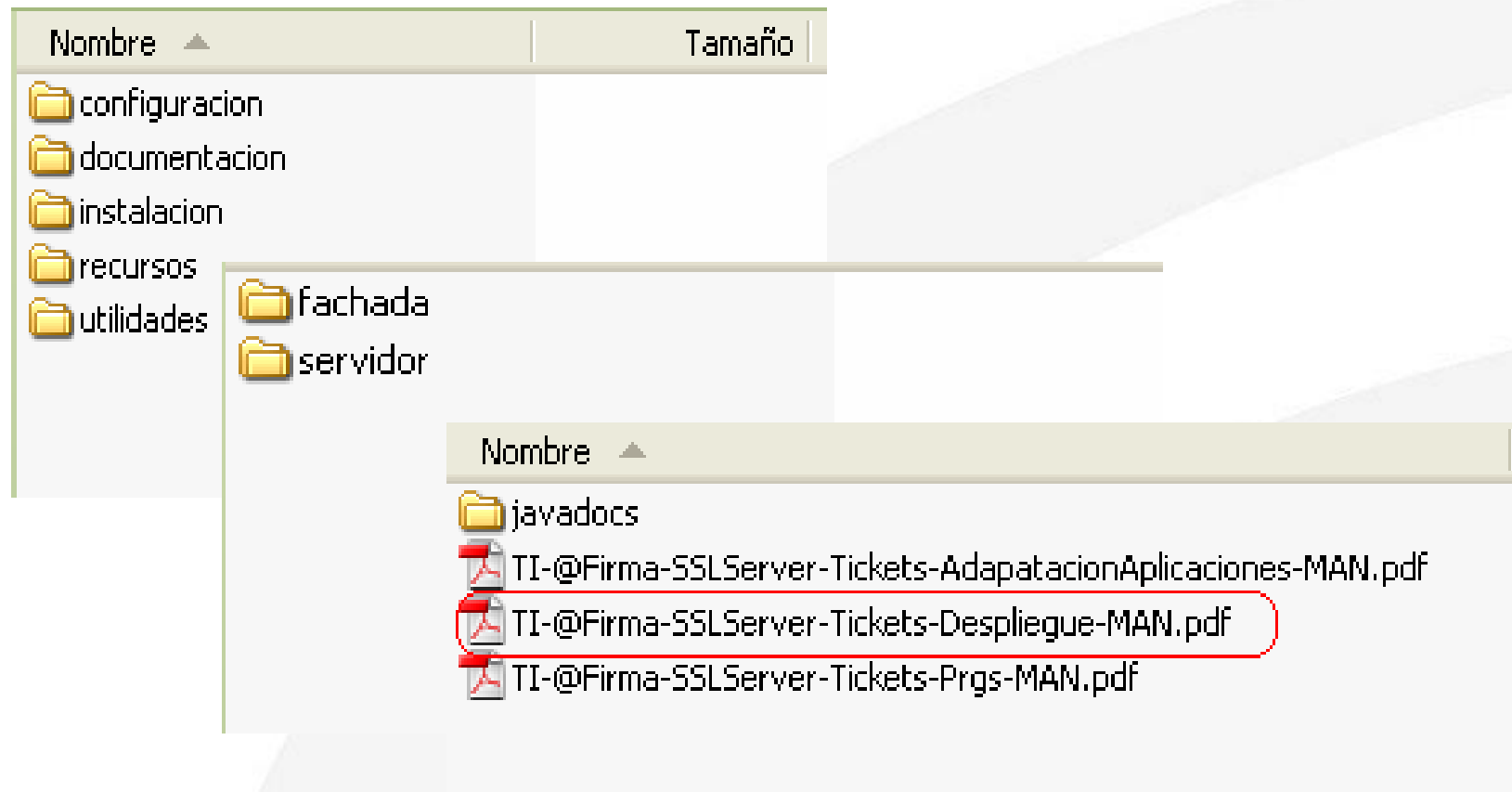
Organismo en el que se va a realizar el despliegue.

Responsable de la aplicación: Nombre, apellidos, teléfono, e-mail.

Empresa encargada.

NIF de la persona encargada de la descarga del CD.

- Examinando el cd entregable del módulo de tickets



➔ Índice

1. Introducción

2. Requisitos previos

3. Entregable de instalación del módulo de autenticación med. tickets.

4. Procedimiento de instalación en el núcleo de @firma v5

5. Procedimiento de instalación en la fachada de @firma v5

6. Turno de ruegos y preguntas.

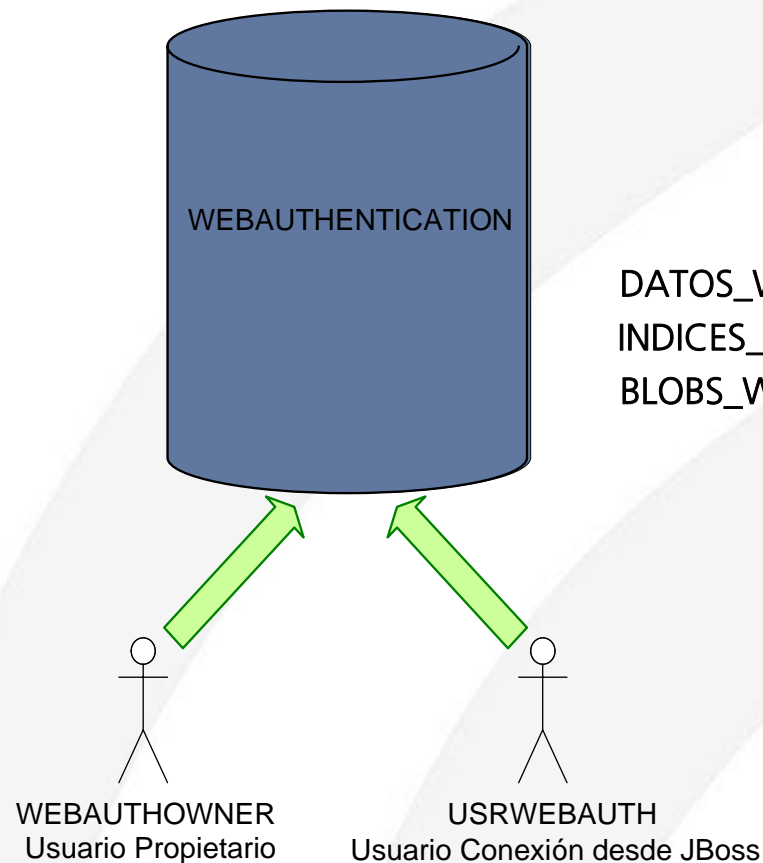
➔ Procedimiento de instalación en el núcleo de @firma5

1. Creación del esquema de base de datos.
2. Despliegue del módulo servidor en el núcleo.
3. Configuración del módulo servidor en el núcleo.
4. Comprobación de la instalación.
5. Dónde ver la versión instalada.

➔ Procedimiento de instalación en el núcleo de @firma5

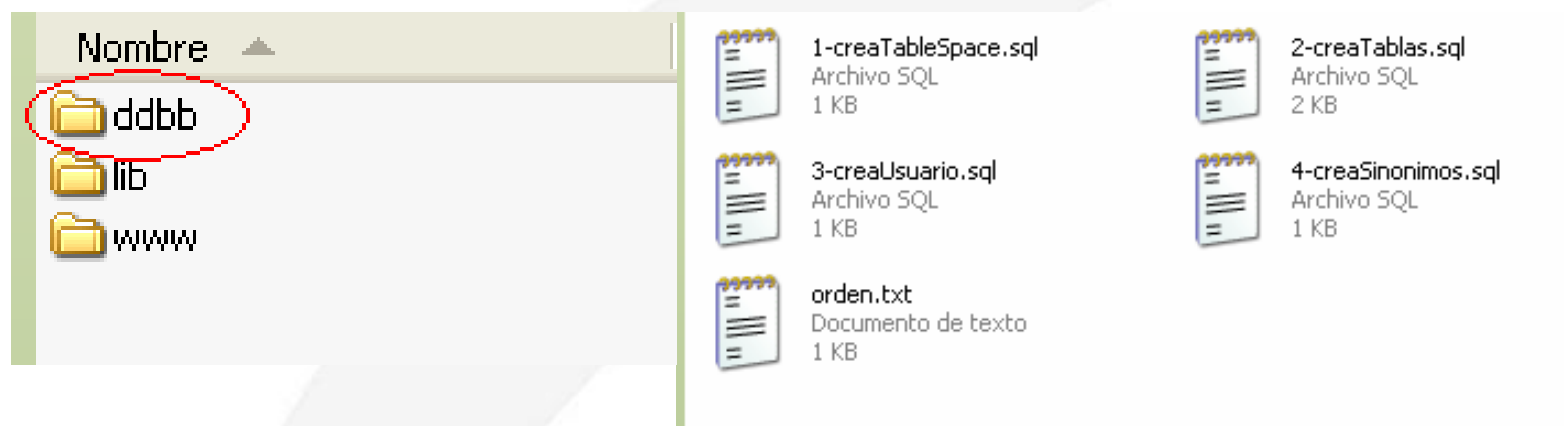
1. Creación del esquema de base de datos.

- Existe un esquema de Base de Datos, con dos usuarios, y tres tablespaces
 - ❖ Esquema WEBAUTHENTICATION



1. Creación del esquema de base de datos.

- El proceso de creación de estos esquemas consiste únicamente en ejecutar los script, en el Sistema de Gestión de Base de Datos en el orden establecido en el fichero orden.txt y con el usuario indicado en dicho fichero.



- Se recomienda que la ejecución de estos scripts la realice personal técnico cualificado en Base de Datos, preferiblemente un DBA.

➔ Procedimiento de instalación en el núcleo de @firma5

1. Creación del esquema de base de datos.
2. Despliegue del módulo servidor en el núcleo.
3. Configuración del módulo servidor en el núcleo.
4. Comprobación de la instalación.
5. Dónde ver la versión instalada.

2. Despliegue del módulo servidor en el núcleo.

1) Copiar el contenido del CD de Instalación en el servidor.

2) Configuración Servicios Web. Modificar el fichero "recursos/www/servidor /WEB-INF/server-config.wsdd".



server-config.wsdd

a. IP JNDI.

b. URL pública del servidor @Firma.

3) Modificación de la ip de los ficheros xml y descriptores wsdl.

4) Diseño y configuración de la página de error por defecto.

IMPORTANTE: Diseñar e incluir, antes de realizar el despliegue.



2. Despliegue del módulo servidor en el núcleo.

5) Configuración de las propiedades del script de despliegue

- *core.home*: ruta al directorio del servidor de aplicaciones JBOSS.
Ej: */export/home/firmaAdmin/*
- *appServer.rootDir*: nombre del directorio JBOSS. Ej: *JBoss-4.0.2*
- *webAuthMod.deploy.soapContext.lib.mode*: (unificado o no).
- *webAuthMod.deploy.date*: Fecha de despliegue del módulo.

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

```
> dos2unix instalacion_servidor.sh instalacion_servidor.sh
```

7) Ejecutar el script de instalación:

```
> sh instalacion_servidor.sh
```

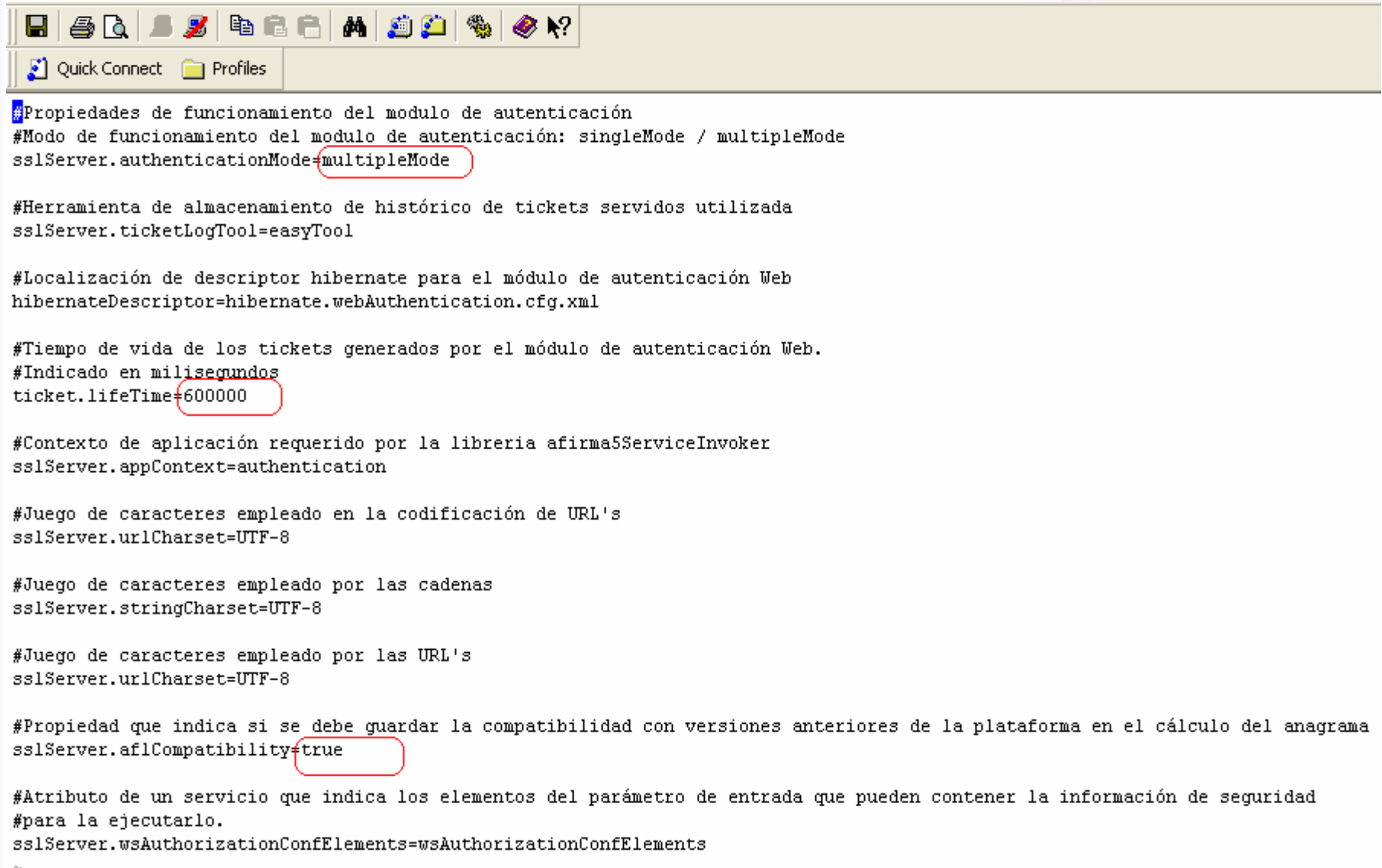
➔ Procedimiento de instalación en el núcleo de @firma5

1. Creación del esquema de base de datos.
2. Despliegue del módulo servidor en el núcleo.
3. Configuración del módulo servidor en el núcleo.
4. Comprobación de la instalación.
5. Dónde ver la versión instalada.

3. Configuración del módulo servidor en el núcleo.

\$JBOSS_HOME/server/all/conf/afirma_webAuthentication.properties

- Fichero donde se especifican propiedades genéricas del módulo de autenticación mediante tickets.



```
#Propiedades de funcionamiento del modulo de autenticación
#Modo de funcionamiento del modulo de autenticación: singleMode / multipleMode
sslServer.authenticationMode=multipleMode

#Herramienta de almacenamiento de histórico de tickets servidos utilizada
sslServer.ticketLogTool=easyTool

#Localización de descriptor hibernate para el módulo de autenticación Web
hibernateDescriptor=hibernate.webAuthentication.cfg.xml

#Tiempo de vida de los tickets generados por el módulo de autenticación Web.
#Indicado en milisegundos
ticket.lifeTime=600000

#Contexto de aplicación requerido por la librería afirma5ServiceInvoker
sslServer.appContext=authentication

#Juego de caracteres empleado en la codificación de URL's
sslServer.urlCharset=UTF-8

#Juego de caracteres empleado por las cadenas
sslServer.stringCharset=UTF-8

#Juego de caracteres empleado por las URL's
sslServer.urlCharset=UTF-8

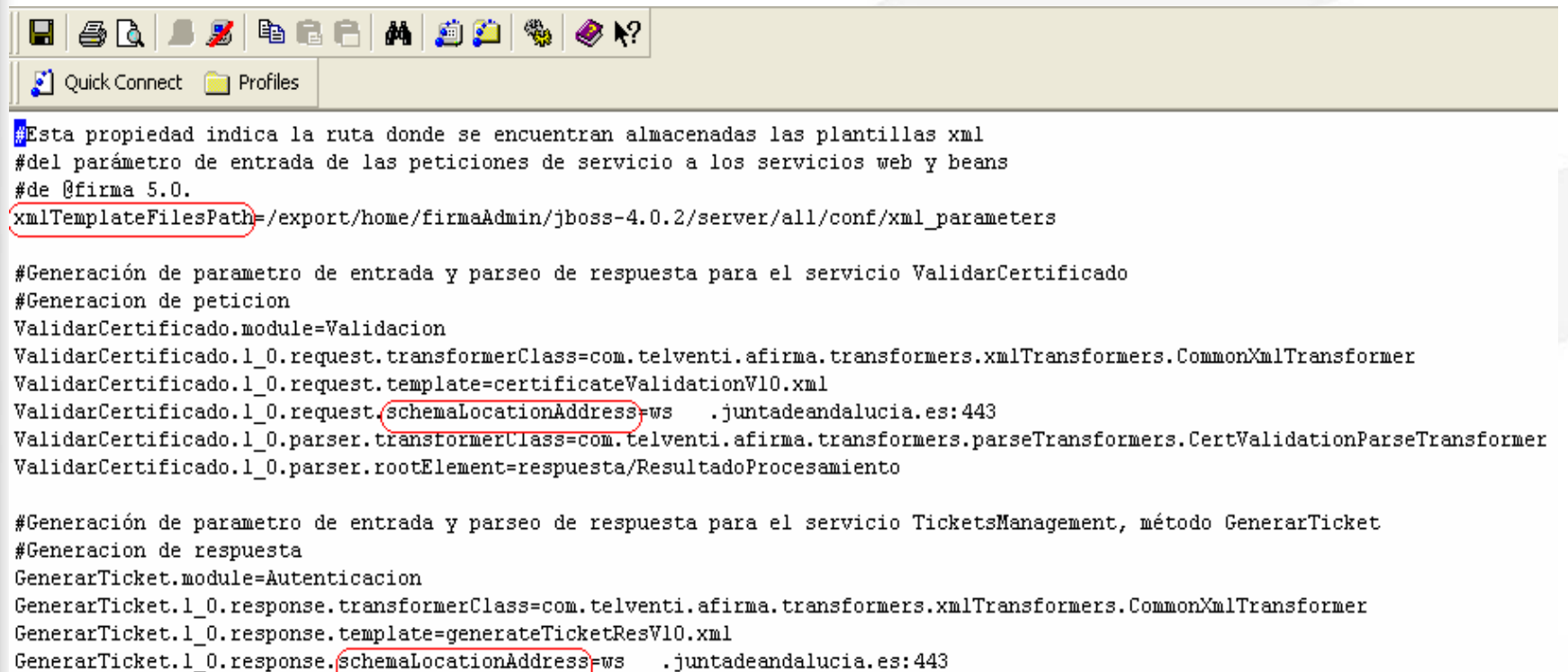
#Propiedad que indica si se debe guardar la compatibilidad con versiones anteriores de la plataforma en el cálculo del anagrama
sslServer.aflCompatibility=true

#Atributo de un servicio que indica los elementos del parámetro de entrada que pueden contener la información de seguridad
#para la ejecutarlo.
sslServer.wsAuthorizationConfElements=wsAuthorizationConfElements
~
```


3. Configuración del módulo servidor en el núcleo.

\$JBOSS_HOME/server/all/conf/transformers.properties

-Fichero de configuración del componente de generación y parseo de parámetros de entrada y salida de los servicios publicados



```
#Esta propiedad indica la ruta donde se encuentran almacenadas las plantillas xml
#del parámetro de entrada de las peticiones de servicio a los servicios web y beans
#de @firma 5.0.
xmlTemplateFilesPath=/export/home/firmaAdmin/jboss-4.0.2/server/all/conf/xml_parameters

#Generación de parametro de entrada y parseo de respuesta para el servicio ValidarCertificado
#Generacion de peticion
ValidarCertificado.module=Validacion
ValidarCertificado.1_0.request.transformerClass=com.telventi.afirma.transformers.xmlTransformers.CommonXmlTransformer
ValidarCertificado.1_0.request.template=certificateValidationV10.xml
ValidarCertificado.1_0.request.schemaLocationAddress=ws .juntadeandalucia.es:443
ValidarCertificado.1_0.parser.transformerClass=com.telventi.afirma.transformers.parseTransformers.CertValidationParseTransformer
ValidarCertificado.1_0.parser.rootElement=respuesta/ResultadoProcesamiento

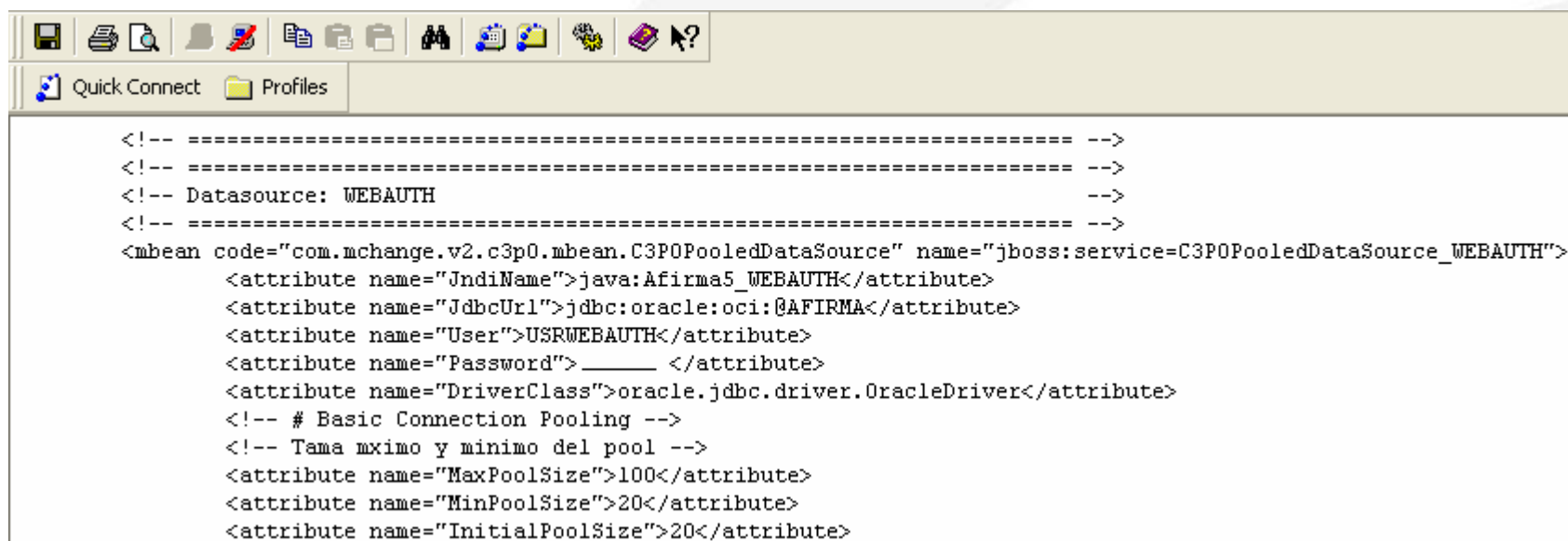
#Generación de parametro de entrada y parseo de respuesta para el servicio TicketsManagement, método GenerarTicket
#Generacion de respuesta
GenerarTicket.module=Autenticacion
GenerarTicket.1_0.response.transformerClass=com.telventi.afirma.transformers.xmlTransformers.CommonXmlTransformer
GenerarTicket.1_0.response.template=generateTicketResV10.xml
GenerarTicket.1_0.response.schemaLocationAddress=ws .juntadeandalucia.es:443
```

3. Configuración del módulo servidor en el núcleo.

\$JBOSS_HOME/server/all/deploy/cluster-service.xml

- Fichero de definición de las particiones del servidor de aplicaciones así como los servicios o MBEANS que deben ser instanciados. Tienen ya definidos al menos 3 diferentes Datasources y sus pool de conexiones.

IMPORTANTE: Mantener los datasources anteriores y añadir el de tickets.



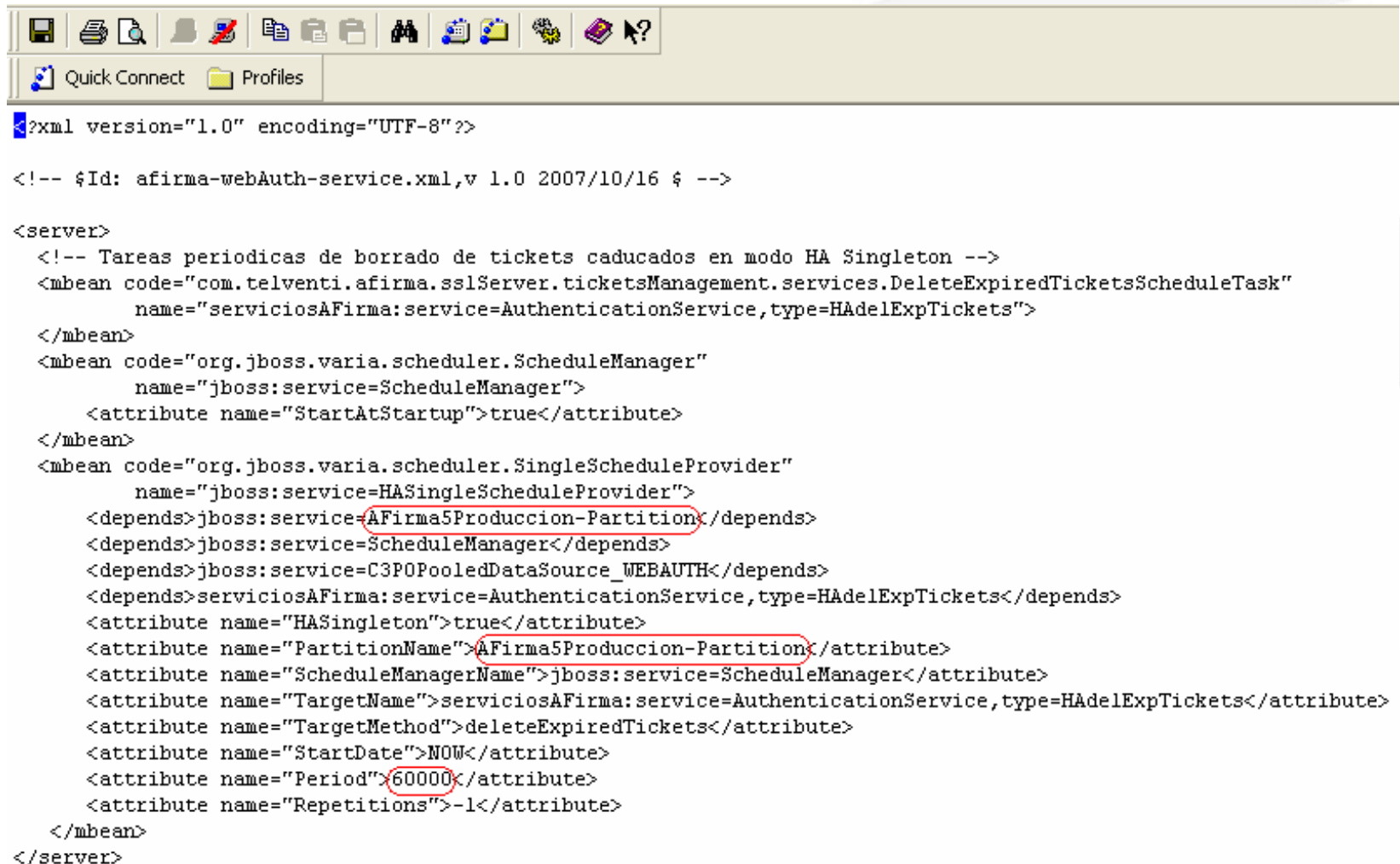
```
<!-- ===== -->
<!-- ===== -->
<!-- Datasource: WEBAUTH -->
<!-- ===== -->
<mbean code="com.mchange.v2.c3p0.mbean.C3P0PooledDataSource" name="jboss:service=C3P0PooledDataSource_WEBAUTH">
  <attribute name="JndiName">java:Afirma5_WEBAUTH</attribute>
  <attribute name="JdbcUrl">jdbc:oracle:oci:@AFIRMA</attribute>
  <attribute name="User">USRWEBAUTH</attribute>
  <attribute name="Password">_____ </attribute>
  <attribute name="DriverClass">oracle.jdbc.driver.OracleDriver</attribute>
  <!-- # Basic Connection Pooling -->
  <!-- Tama mximo y minimo del pool -->
  <attribute name="MaxPoolSize">100</attribute>
  <attribute name="MinPoolSize">20</attribute>
  <attribute name="InitialPoolSize">20</attribute>
</mbean>
```

3. Configuración del módulo servidor en el núcleo.

\$JBOSS_HOME/server/all/deploy/afirma-webAuth-service.xml

- Fichero donde se define la tarea de borrado de los tickets.

IMPORTANTE: Establecer correctamente el nombre de Partición de Jboss.



```
?xml version="1.0" encoding="UTF-8"?>

<!-- $Id: afirma-webAuth-service.xml,v 1.0 2007/10/16 $ -->

<server>
  <!-- Tareas periodicas de borrado de tickets caducados en modo HA Singleton -->
  <mbean code="com.telventi.afirma.sslServer.ticketsManagement.services.DeleteExpiredTicketsScheduleTask"
    name="serviciosAFirma:service=AuthenticationService,type=HAdeleExpTickets">
  </mbean>
  <mbean code="org.jboss.varia.scheduler.ScheduleManager"
    name="jboss:service=ScheduleManager">
    <attribute name="StartAtStartup">true</attribute>
  </mbean>
  <mbean code="org.jboss.varia.scheduler.SingleScheduleProvider"
    name="jboss:service=HASingleScheduleProvider">
    <depends>jboss:service=AFirma5Produccion-Partition</depends>
    <depends>jboss:service=ScheduleManager</depends>
    <depends>jboss:service=C3POpooledDataSource_WEBAUTH</depends>
    <depends>serviciosAFirma:service=AuthenticationService,type=HAdeleExpTickets</depends>
    <attribute name="HASingleton">true</attribute>
    <attribute name="PartitionName">AFirma5Produccion-Partition</attribute>
    <attribute name="ScheduleManagerName">jboss:service=ScheduleManager</attribute>
    <attribute name="TargetName">serviciosAFirma:service=AuthenticationService,type=HAdeleExpTickets</attribute>
    <attribute name="TargetMethod">deleteExpiredTickets</attribute>
    <attribute name="StartDate">NOW</attribute>
    <attribute name="Period">60000</attribute>
    <attribute name="Repetitions">-1</attribute>
  </mbean>
</server>
```

➔ Procedimiento de instalación en el núcleo de @firma5

1. Creación del esquema de base de datos.
2. Despliegue del módulo servidor en el núcleo.
3. Configuración del módulo servidor en el núcleo.
4. **Comprobación de la instalación.**
5. Dónde ver la versión instalada.

4. Comprobación de la instalación

- Arranque del servidor JBoss del núcleo y comprobación de los logs.

```
INFO [com.telventi.afirma.sslServer.ticketsManagement.services.DeleteExpiredTicketsScheduleTask] Inicio de la tarea periodica de borrado de tickets expi
```

```
INFO [com.telventi.afirma.sslServer.ticketsManagement.services.DeleteExpiredTicketsScheduleTask] N mero de tickets expirados: 1
```

```
INFO [com.telventi.afirma.sslServer.ticketsManagement.services.DeleteExpiredTicketsScheduleTask] Fin de la tarea periodica de borrado de tickets expirad
```

- Acceso a la p gina de error personalizada.



 Junta de Andalucía

Ocurri  un error en el M dulo de Autenticaci n de Tickets de la plataforma @Firma v5

C digo de Error: Ticket Inv lido

 CONSEJER A DE JUSTICIA Y ADMINISTRACI N P BLICA

➔ Procedimiento de instalación en el núcleo de @firma5

1. Creación del esquema de base de datos.
2. Despliegue del módulo servidor en el núcleo.
3. Configuración del módulo servidor en el núcleo.
4. Comprobación de la instalación.
5. Dónde ver la versión instalada.

5. Dónde ver la versión instalada.

Para ver la versión instalada del módulo servidor de tickets, se incorpora el siguiente archivo en la ruta del servidor:

\$JBOSS_HOME/server/all/conf/@firma-WA.version



```
File Edit View Window Help
[Icons: Save, Print, Find, Undo, Redo, Copy, Paste, Undo, Redo, Home, End, Stop, Run, Help]
Quick Connect Profiles

# Despliegue del modulo de autenticación Web de la plataforma @firma v5 / Core
@firma-WA.version=1.1.2
@firma-WA.fecha_liberacion=05-11-2008

component.core.version=1.2.4
component.afirmaV5ServiceInvoker.version=2.1.0
component.transformers.version=2.3.1
component.afirma.utils.version=1.1.1
~
~
```

➔ Índice

1. Introducción

2. Requisitos previos

3. Entregable de instalación del módulo de autenticación med. tickets.

4. Procedimiento de instalación en el núcleo de @firma v5

5. Procedimiento de instalación en la fachada de @firma v5

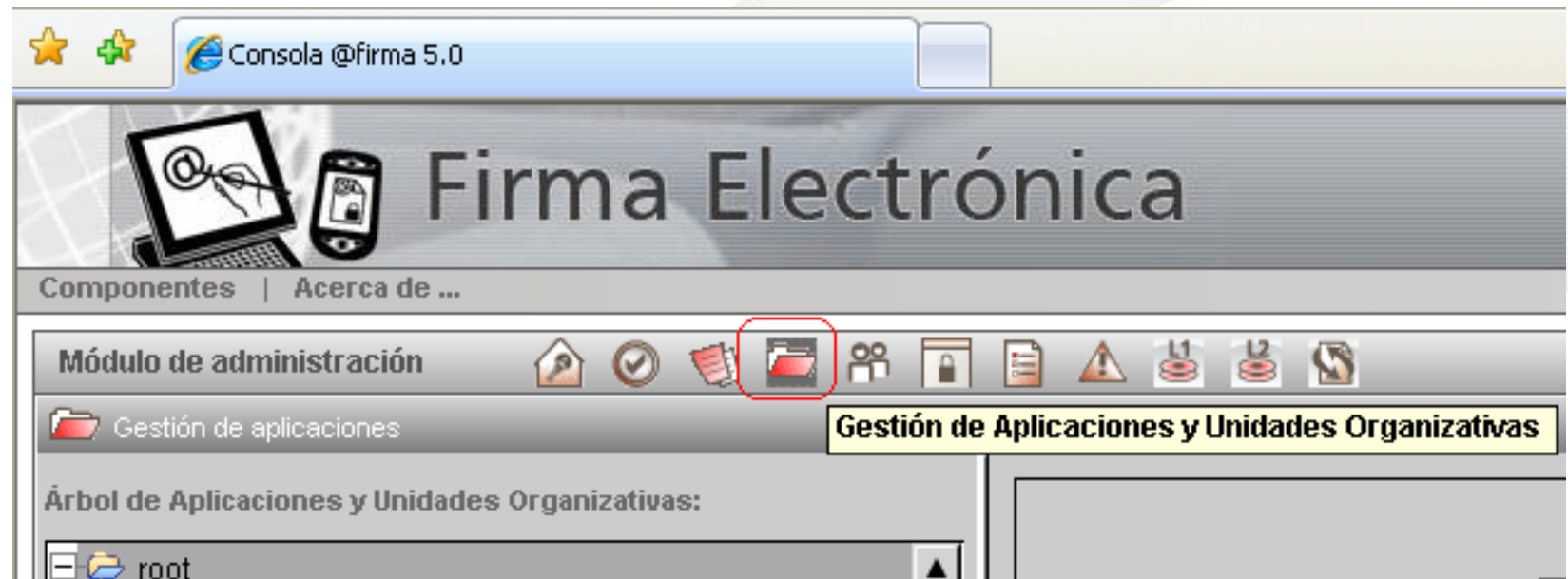
6. Turno de ruegos y preguntas.

➔ Procedimiento de instalación en la fachada de @firma5

1. Alta de aplicación para el módulo fachada.
2. Despliegue del módulo fachada en el servidor.
3. Configuración del módulo fachada en el servidor.
4. Comprobación de la instalación.
5. Dónde ver la versión instalada.

1. Alta de aplicación para el módulo fachada.

- El identificador de esta aplicación es utilizado por este componente para hacer más segura la invocación del servicio ValidarCertificadoTicket publicado por el núcleo del módulo de Autenticación Web.



➔ Procedimiento de instalación en la fachada de @firma5

1. Alta de aplicación para el módulo fachada.
2. Despliegue del módulo fachada en el servidor.
3. Configuración del módulo fachada en el servidor.
4. Comprobación de la instalación.
5. Dónde ver la versión instalada.

2. Despliegue del módulo fachada en el servidor

- 1) Copiar el contenido del CD de Instalación al disco duro del sistema.
- 2) Modificar el siguiente fichero, indicando la ruta del despliegue (P. ej: /opt/sslServer_tickets)
 - a. *instalacion/fachada/build-despliegue.properties*
- 3) Establecer los valores adecuados de los parámetros de configuración para los siguientes archivos:
configuracion/fachada/afirma5_webAuthentication.properties
configuracion/fachada/afirma5ServiceInvoker.properties
configuracion/fachada/transformers.properties
- 4) Pasar el comando "dos2unix" al fichero instalacion.sh.
> *dos2unix instalacion_fachada.sh instalacion_fachada.sh*
- 5) Ejecutar el *script instalacion_extension.sh*

2. Despliegue del módulo fachada en el servidor

- Ejemplo de salida del script de instalación del módulo fachada.

```
=====
Despliegue del Modulo de Autenticacion Web de la plataforma @Firma 5
                                Fachada

JAVA_HOME: /opt/jdk1.5.0_14/
=====

Construyendo ficheros de despliegue...
Buildfile: build-despliegue-fachada.xml

init:
[echo] +-----+
[echo] |                                     |
[echo] |                               BORRANDO DIRECTORIOS |
[echo] |                                     |
[echo] +-----+

build-folders:
[echo] +-----+
[echo] |                                     |
[echo] |                               CREANDO DIRECTORIOS |
[echo] |                                     |
[echo] +-----+
[mkdir] Created dir: /opt/sslServer_tickets/bin
[mkdir] Created dir: /opt/sslServer_tickets/conf
[mkdir] Created dir: /opt/sslServer_tickets/lib
[mkdir] Created dir: /opt/sslServer_tickets/logs

copy-facade-components:
[echo] +-----+
[echo] |                                     |
[echo] |                               Despliegue parte frontal |
[echo] |                               Modulo de Autenticacion Web |
[echo] |                               Plataforma @Firma5 |
[echo] |                                     |
[echo] +-----+
[copy] Copying 20 files to /opt/sslServer_tickets/lib
[copy] Copying 8 files to /opt/sslServer_tickets/conf
[copy] Copying 2 files to /opt/sslServer_tickets/bin
[copy] Copying 1 file to /opt/sslServer_tickets

main:

BUILD SUCCESSFUL
Total time: 0 seconds

- Instalacion finalizada -
```

➔ Procedimiento de instalación en la fachada de @firma5

1. Alta de aplicación para el módulo fachada.
2. Despliegue del módulo fachada en el servidor.
3. Configuración del módulo fachada en el servidor.
4. Comprobación de la instalación.
5. Dónde ver la versión instalada.

3. Configuración del módulo fachada en el servidor

\$SSL_TICKETS_HOME/conf/afirma5_webAuthentication.properties

Fichero donde se configuran los parámetros generales del módulo fachada.

```
#Propiedades de funcionamiento del modulo de autenticación
#Modo de funcionamiento del modulo de autenticación: singleMode / multipleMode
sslServer.authenticationMode=multipleMode

#Propiedades del proceso servidor standalone
sslServer.host=
sslServer.port=443
#Fichero P12, PFX
sslServer.keystoreFile=/opt/sslServer_tickets/conf/WildcardJuntadeandaluciaes.p12
sslServer.keystorePass=
sslServer.timeout=30000

#Juego de caracteres empleado en la codificación de URL's
sslServer.urlCharset=UTF-8

#Juego de caracteres empleado por las cadenas
sslServer.stringCharset=UTF-8

#Configuración de logging
sslServer.log4jFile=/opt/sslServer_tickets/conf/log4j.xml

#Identificador de aplicación @Firma requerido para la invocación del servicio Web de validación
#de certificado asociado a ticket
sslServer.afirmaAppId= Id aplicación dada de alta en @Firma

#Contexto de aplicación requerido por la librería afirma5ServiceInvoker
sslServer.appContext=authFacade

#Página de error para el módulo de autenticación
sslServer.defaultErrorPage=https://ws__.juntadeandalucia.es/authentication/defaultErrorPage.jsp

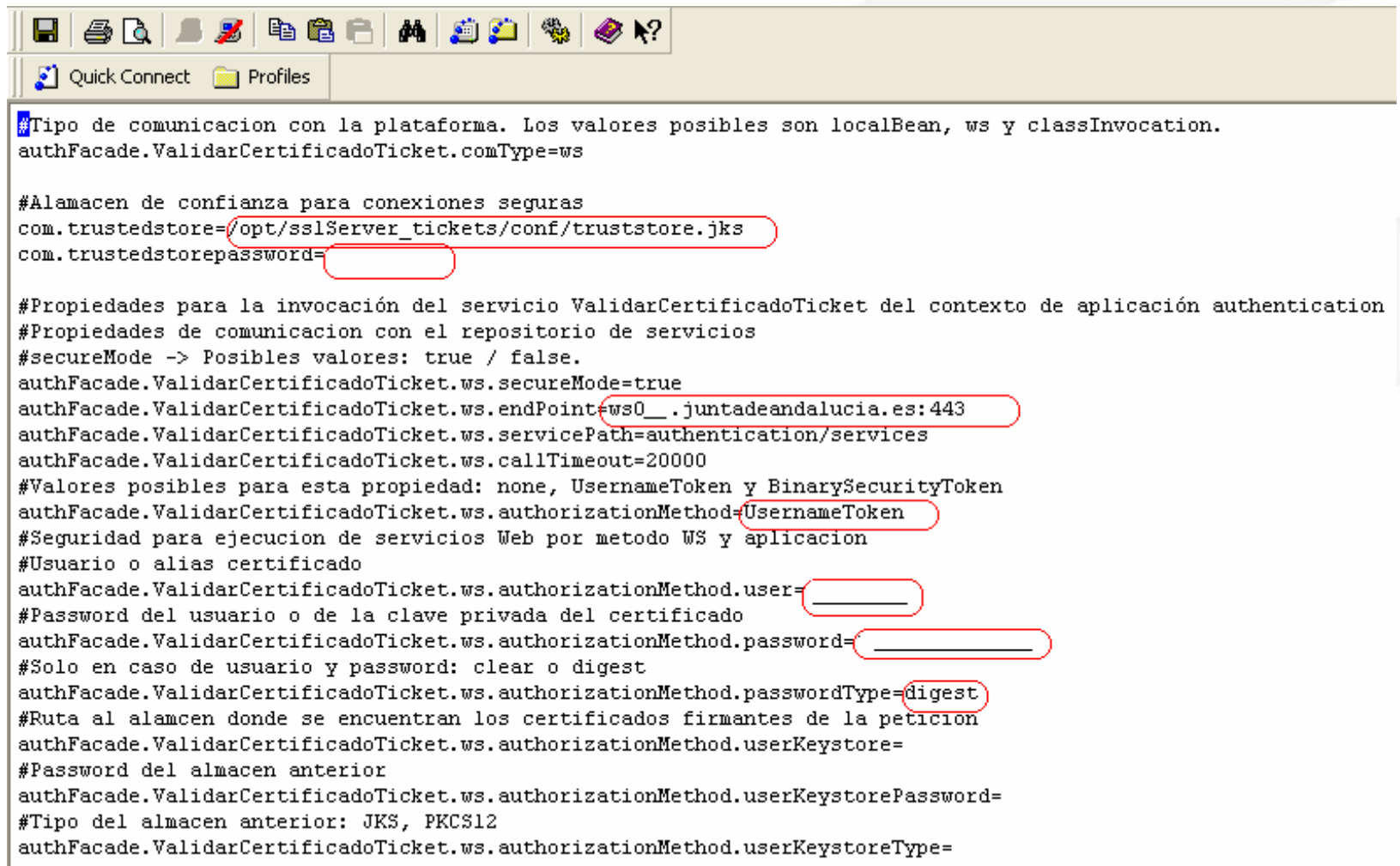
#Parametro de reautenticación
#Dominio de reautenticación
sslServer.multipleMode.domain=juntadeandalucia.es
#URL (sin dominio) donde se encuentran localizados las fachadas virtuales de autenticación
sslServer.multipleMode.url.1=ws -1
sslServer.multipleMode.url.2=ws -2
sslServer.multipleMode.url.3=ws -3
sslServer.multipleMode.url.4=ws -4
sslServer.multipleMode.url.5=ws -5
sslServer.multipleMode.url.6=ws -6

#Puerto seguro de redirección utilizado por la fachada en autenticación múltiple. Es obligatorio establecer
#un valor para este parámetro si el puerto configurado es distinto del puerto por defecto para HTTPS (443).
sslServer.multipleMode.port=
#Primera url de reautenticación
sslServer.multipleMode.firstVirtualSSLFacadeNumber=1
#Última url de reautenticación
sslServer.multipleMode.lastVirtualSSLFacadeNumber=6
```

3. Configuración del módulo fachada en el servidor

`$SSL_TICKETS_HOME/conf/afirma5ServiceInvoker.properties`

Fichero donde se configuran los parámetros necesarios para establecer la comunicación con el núcleo del módulo.



```
#Tipo de comunicacion con la plataforma. Los valores posibles son localBean, ws y classInvocation.
authFacade.ValidarCertificadoTicket.comType=ws

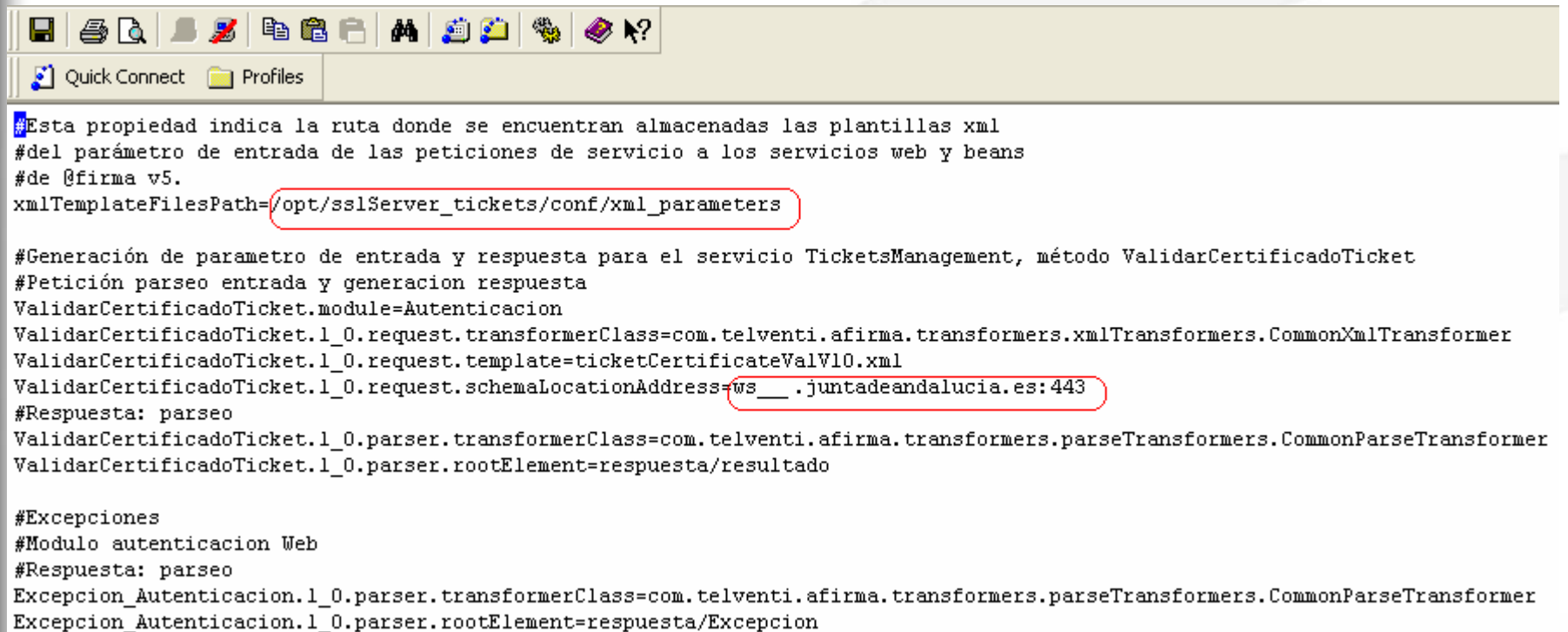
#Almacen de confianza para conexiones seguras
com.trustedstore=/opt/sslServer_tickets/conf/truststore.jks
com.trustedstorepassword=

#Propiedades para la invocación del servicio ValidarCertificadoTicket del contexto de aplicación authentication
#Propiedades de comunicacion con el repositorio de servicios
#secureMode -> Posibles valores: true / false.
authFacade.ValidarCertificadoTicket.ws.secureMode=true
authFacade.ValidarCertificadoTicket.ws.endpoint=ws0__.juntadeandalucia.es:443
authFacade.ValidarCertificadoTicket.ws.servicePath=authentication/services
authFacade.ValidarCertificadoTicket.ws.callTimeout=20000
#Valores posibles para esta propiedad: none, UsernameToken y BinarySecurityToken
authFacade.ValidarCertificadoTicket.ws.authorizationMethod=UsernameToken
#Seguridad para ejecucion de servicios Web por metodo WS y aplicacion
#Usuario o alias certificado
authFacade.ValidarCertificadoTicket.ws.authorizationMethod.user=
#Password del usuario o de la clave privada del certificado
authFacade.ValidarCertificadoTicket.ws.authorizationMethod.password=
#Solo en caso de usuario y password: clear o digest
authFacade.ValidarCertificadoTicket.ws.authorizationMethod.passwordType=digest
#Ruta al almacen donde se encuentran los certificados firmantes de la petición
authFacade.ValidarCertificadoTicket.ws.authorizationMethod.userKeystore=
#Password del almacen anterior
authFacade.ValidarCertificadoTicket.ws.authorizationMethod.userKeystorePassword=
#Tipo del almacen anterior: JKS, PKCS12
authFacade.ValidarCertificadoTicket.ws.authorizationMethod.userKeystoreType=
```


3. Configuración del módulo fachada en el servidor

`$SSL_TICKETS_HOME/conf/transformers.properties`

Fichero donde se configuran los parámetros necesarios para establecer la comunicación con el núcleo del módulo.



```
#Esta propiedad indica la ruta donde se encuentran almacenadas las plantillas xml
#del parámetro de entrada de las peticiones de servicio a los servicios web y beans
#de @firma v5.
xmlTemplateFilePath=/opt/sslServer_tickets/conf/xml_parameters

#Generación de parametro de entrada y respuesta para el servicio TicketsManagement, método ValidarCertificadoTicket
#Petición parseo entrada y generacion respuesta
ValidarCertificadoTicket.module=Autenticacion
ValidarCertificadoTicket.l_0.request.transformerClass=com.telventi.afirma.transformers.xmlTransformers.CommonXmlTransformer
ValidarCertificadoTicket.l_0.request.template=ticketCertificateValV10.xml
ValidarCertificadoTicket.l_0.request.schemaLocationAddress=ws__ .juntadeandalucia.es:443
#Respuesta: parseo
ValidarCertificadoTicket.l_0.parser.transformerClass=com.telventi.afirma.transformers.parseTransformers.CommonParseTransformer
ValidarCertificadoTicket.l_0.parser.rootElement=respuesta/resultado

#Excepciones
#Modulo autenticacion Web
#Respuesta: parseo
Excepcion_Autenticacion.l_0.parser.transformerClass=com.telventi.afirma.transformers.parseTransformers.CommonParseTransformer
Excepcion_Autenticacion.l_0.parser.rootElement=respuesta/Excepcion
```

➔ Procedimiento de instalación en la fachada de @firma5

1. Alta de aplicación para el módulo fachada.
2. Despliegue del módulo fachada en el servidor.
3. Configuración del módulo fachada en el servidor.
4. Comprobación de la instalación.
5. Dónde ver la versión instalada.

4. Comprobación de la instalación.

- Arranque del nuevo servidor fachada, y comprobación de los logs.

```
2009-02-05 10:02:03,671 INFO [com.telventi.afirma.transformers.TransformersUtils] Leyendo plantilla xml, peticiÃ³n:ValidarCertificadoTicket, tipo: request, version: 1_0
2009-02-05 10:02:03,672 INFO [com.telventi.afirma.transformers.TransformersUtils] Fichero que contiene la platilla: ticketCertificateValV10.xml
2009-02-05 10:02:03,673 INFO [com.telventi.afirma.transformers.TransformersUtils] Documento parseado correctamente: mensajeEntrada
2009-02-05 10:08:58,041 INFO [com.telventi.afirma.transformers.TransformersUtils] Leyendo plantilla xml, peticiÃ³n:ValidarCertificadoTicket, tipo: request, version: 1_0
2009-02-05 10:08:58,041 INFO [com.telventi.afirma.transformers.TransformersUtils] Fichero que contiene la platilla: ticketCertificateValV10.xml
2009-02-05 10:08:58,043 INFO [com.telventi.afirma.transformers.TransformersUtils] Documento parseado correctamente: mensajeEntrada
```

- Realización de una prueba desplegando el ejemplo disponible en el cd de instalación y despliegue.

Modulo de Autenticación Web @Firma 5 - Component...

Información de validación asociada al ticket aTJynvDAkqqk4U:

ResultadoValidacion

- o ValidacionSimple
 - excepcion: java.security.cert.CertificateExpiredException
 - codigoResultado: 1
 - descResultado: Certificado caducado
- o descripcion: El certificado no paso la validacion
- o resultado: 1

InfoCertificado

- o usoCertificado: digitalSignature | keyEncipherment
- o FECHACREACION: 2004-03-02 mar 09:45:40 +0100
- o ApellidosResponsable: ESPAÑOL ESPAÑOL
- o validoHasta: 2006-03-02 jue 09:45:40 +0100
- o politica: 1.3.6.1.4.1.5734.3.5
- o subject: CN=NOMBRE ESPAÑOL ESPAÑOL JUAN - NIF 00000000T,OU=500070015,OU=FNMT Clase 2 CA,O=FNMT,C=ES
- o tipoCertificado: FNMT PF
- o versionPolitica: 31
- o OrganizacionEmisora: FNMT
- o idPolitica: DEFAULT
- o NIFResponsable: 00000000T
- o FECHACADUCIDAD: 2006-03-02 jue 09:45:40 +0100
- o numeroSerie: 1014531857
- o ANAGRAMA: 00000000TESPAESPJ
- o nombreResponsable: JUAN
- o idEmisor: OU=FNMT Clase 2 CA,O=FNMT,C=ES
- o email:
- o clasificacion: FNMT
- o validoDesde: 2004-03-02 mar 09:45:40 +0100
- o TIPOAFIRMA: 0
- o NombreApellidosResponsable: JUAN ESPAÑOL ESPAÑOL
- o segundoApellidoResponsable: ESPAÑOL
- o primerApellidoResponsable: ESPAÑOL

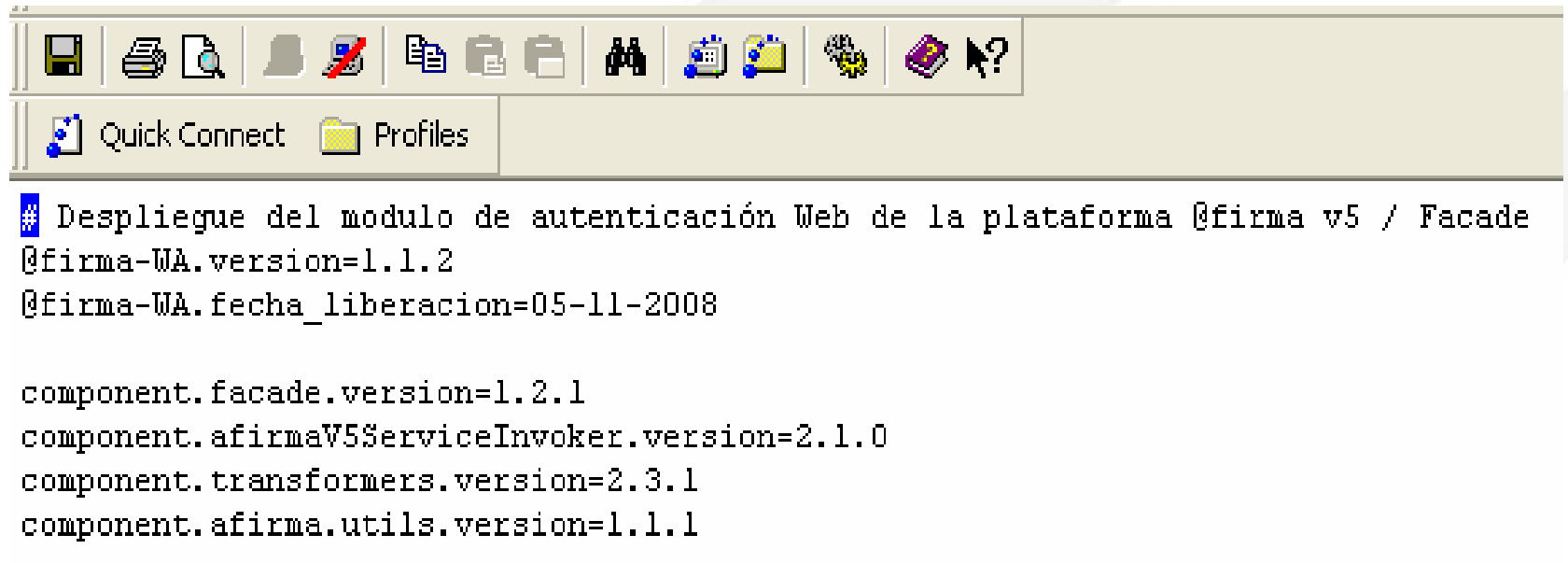
➔ Procedimiento de instalación en la fachada de @firma5

1. Alta de aplicación para el módulo fachada.
2. Despliegue del módulo fachada en el servidor.
3. Configuración del módulo fachada en el servidor.
4. Comprobación de la instalación.
5. Dónde ver la versión instalada.

5. Dónde ver la versión instalada.

Para ver la versión instalada del módulo fachada de tickets, se incorpora el siguiente archivo en la ruta del servidor:

`$$$SSL_TICKETS_HOME/@firma-WA.version`



```
# Despliegue del modulo de autenticación Web de la plataforma @firma v5 / Facade
@firma-WA.version=1.1.2
@firma-WA.fecha_liberacion=05-11-2008

component.facade.version=1.2.1
component.afirmaV5ServiceInvoker.version=2.1.0
component.transformers.version=2.3.1
component.afirma.utils.version=1.1.1
```

➔ Índice

1. Introducción

2. Requisitos previos

3. Entregable de instalación del módulo de autenticación med. tickets.

4. Procedimiento de instalación en el núcleo de @firma v5

5. Procedimiento de instalación en la fachada de @firma v5

6. Turno de ruegos y preguntas.

Conclusiones.

Ruegos y Preguntas.

Muchas gracias

Cristóbal Fernández Ramírez



JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA