



## DOP Port@firmas



CONSEJERÍA DE JUSTICIA Y  
ADMINISTRACIÓN PÚBLICA

Documento elaborado por: Francisco José Cantero Villar

Revisado por: Miguel J. Vázquez Rebollo

Versión: 1.0.2

Lugar y fecha: Sevilla, 21 de Octubre de 2005

## Contenido:

1	Requisitos previos de Instalación .....	3
2	Procedimientos de operación de los componentes del sistema.	4
2.1	Creación usuario de base de datos .....	4
2.2	Script's de creación de tablas y objetos .....	4
2.3	Carga de datos .....	5
2.3.1	Carga de constantes binarias mediante TOAD .....	6
2.3.2	Carga de constantes binarias mediante SQLPLUS .....	8
2.4	Carga de procedimientos .....	9
2.4.1	Clase Base64 .....	9
2.4.2	Especificaciones de paquete .....	9
2.4.3	Cuerpos de paquete .....	10
2.5	Tareas programadas en la base de datos .....	11
2.6	Creación de Rol .....	12
3	Procedimientos de operaciones de producción e implantación.	13
3.1	Alta de la aplicación Port@firmas en @firma .....	13
3.2	Despliegue en el servidor de aplicaciones Tomcat .....	16
3.2.1	Detector.js .....	18
3.2.2	Almacén de certificados .....	18
3.2.3	Ampliación del parámetro de memoria de la máquina virtual de Java....	22
3.3	Actualizando Servidores de firma en <a href="#">Port@firmas</a> .....	24
3.4	Actualizando las constantes de la aplicación .....	24
3.4.1	Configuración de los servicios de aviso por correo .....	25
3.5	Permisos Oracle a nuevos usuarios de aplicación .....	26
4	Historia de versiones .....	27

## 1 Requisitos previos de Instalación

Para poder instalar y hacer funcionar correctamente [Port@firmas](#) con el servidor @firma que tengamos instalados debemos cumplir los siguientes requisitos:

- Base de datos Oracle 8i o 9i, y en el caso de 8i con las extensiones Java instaladas en el servidor.
- Servidor con JSDK 1.4.2\_0\_7 o superior, (la versión 1.4.2\_0\_3 tiene un “bug” en el SSL que se corrige de la 4 en adelante). Por reducir posibles “bug’s” de Java se aconseja tener la última versión.
- Librerías JCE de Sun instaladas en el JSDK para la encriptación/descriptación “fuerte” requerida en los WebServices de @firma v4.
- Servidor de aplicaciones Tomcat 4.1.x ó 5.0.x. Se recomienda no usar el Tomcat 5.5.x al hacer uso de las JSE 1.5 de Java y no haberse testado la aplicación bajo la misma.
- (Opcional) Cuenta de Correo para los avisos por correo o bien acceso a @visor.

En cuanto a los requisitos en clientes, hay que cumplir los definidos por la propia plataforma @firma en su versión v4. Para más información acceder a Plutón, Área Técnica de @firma, y el “[Manual de Usuario de @FIRMA](#)” detalla los mismos.

## 2 Procedimientos de operación de los componentes del sistema.

En el presente documento se van a detallar dos procedimientos de operación, la instalación del sistema partiendo desde cero, o bien el cambio de configuración necesario por un cambio de servidor de firma o bien incorporación de uno nuevo al sistema.

### 2.1 Creación usuario de base de datos

1. El primer requisito que debe cumplir es la versión de la base de datos. [Port@firmas](#) es en actualidad compatible con base de datos Oracle 8i y 9i en los que se hayan habilitado clases Java en el servidor (extensión Java en la base de datos).
2. En la instancia de base de datos donde queramos instalar el sistema, tenemos que dar de alta tres “tablespaces”:
  - TS\_PFIRMA\_INDICES
  - TS\_PFIRMA\_DATOS
  - TS\_PFIRMA\_BLOB

Los tamaños de los mismos quedan a elección del administrador, siendo recomendables de partida 16, 64 y 128 respectivamente, con posibilidad de crecimiento automático. Por temas de rendimiento se recomienda además que el fichero de “tablespace” de índices esté en una unidad de disco física distinta de la de datos normales o columnas BLOB’s (documentos binarios).

3. Dar de alta un usuario Oracle, recomendamos “PFIRMAMG” pues será el que empleemos como referencia en el resto del documento, con los roles “CONNECT”, “RESOURCE” y de creación de roles. El “tablespace” por defecto del usuario debe ser “TS\_PFIRMA\_DATOS”, y el temporal el “TEMP”, o el definido en el sistema como temporal. Una vez creado el usuario, con el usuario “SYSTEM”, hay que concederle el permiso adicional, con la instrucción “GRANT CREATE TYPE TO PFIRMAMG”.

### 2.2 Script’s de creación de tablas y objetos

El siguiente paso, una vez creado el usuario y los tablespaces es probar dicho usuario, conectando mediante un SQLPLUS o un cliente oracle tipo TOAD o TORA.

Si la conexión es correcta podemos pasar a crear todas las entidades necesarias para el Port@firmas, en este caso, tablas, índices, constraints, secuencias y tipos en este orden.

Para ello pensemos a partir de ahora que tenemos el CD del kit Port@firmas en la unidad D, y por tanto desde un SQLPLUS debemos poner:

```
SQL>@D:\KitPortafirma\Scripts\tablas\pfirmaGeneral.tab
```

Y pulsamos “intro”, si todo va bien ira apareciendo diálogos indicando “tabla creada”. Puede que al llegar a la tabla PF\_POOL\_PETICIONES, en ocasiones, de un mensaje de error, pero es simplemente que al tratar de crear la tabla temporal parece que tras crearla lo intente de nuevo. Puede ser debido a un error del SQLPLUS.

El administrador de base de datos puede revisar la creación de tablas para ajustar y afinar los parámetros de almacenamiento de columnas BLOB a las características propias de la base de datos sobre la que se vayan a instalar.

Ejecutamos el resto de los scripts en el siguiente orden:

```
SQL>@D:\KitPortafirma\Scripts\tablas\pfirmaGeneral.ind
```

```
SQL>@D:\KitPortafirma\Scripts\tablas\pfirmaGeneral.con
```

```
SQL>@D:\KitPortafirma\Scripts\tablas\pfirmaGeneral.sqs
```

```
SQL>@D:\KitPortafirma\Scripts\tablas\pfirmaGeneral.typ
```

Una vez terminado de ejecutar los scripts el modelo de datos ya está generado en el usuario propietario. Estos mismos scripts se pueden lanzar desde un cliente TOAD o TORA sin problemas, teniendo solo cuidado en ejecutarlo en el mismo orden.

## 2.3 Carga de datos

El siguiente paso es cargar los datos básicos necesarios en las tablas de codificación, el proceso es similar al anterior. Seguimos con el ejemplo en el caso de SQLPLUS. El orden en este caso es el siguiente:

```
SQL> @D:\KitPortafirma\Scripts\datos\PF_SERVIDORES.dat
```

Pulsamos intro y obtendremos el siguiente mensaje:

**1 fila creada.**

**Validación terminada.**

Procedemos con el resto de los scripts:

```
SQL> @D:\KitPortafirma\Scripts\datos\PF_APLICACIONES.DAT
```

```
SQL> @D:\KitPortafirma\Scripts\datos\PF_CONSTANTES.DAT
```

```
SQL> @D:\KitPortafirma\Scripts\datos\PF_ESTADOS.DAT
```

```
SQL> @D:\KitPortafirma\Scripts\datos\PF_EVENTOS.DAT
```

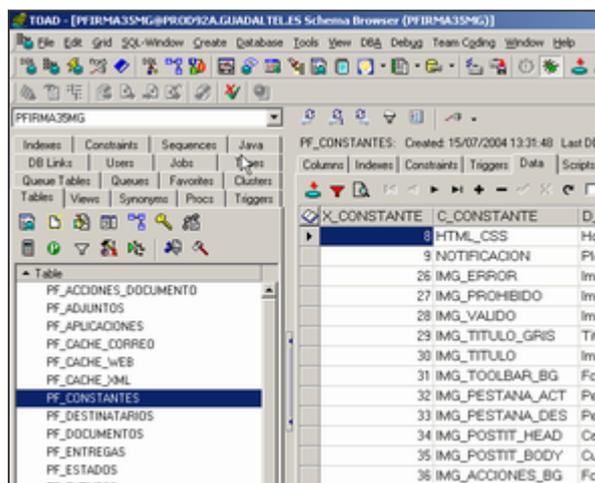
```
SQL> @D:\KitPortafirma\Scripts\datos\PF_TIPOS_DOCUMENTO.dat
```

Al igual que el caso anterior estos scripts se pueden lanzar como tales en el TOAD o similar.

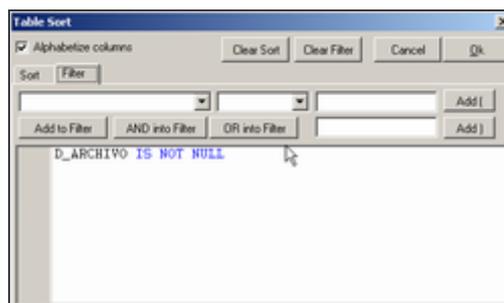
### 2.3.1 Carga de constantes binarias mediante TOAD

Hay una serie de constantes en el Port@firmas que tienen adjunto algo tipo de documento binario, según el caso, imágenes o documentos html como plantillas. Vamos a ver como se cargarían estos documentos mediante un cliente Oracle, en este caso el mas común, el TOAD.

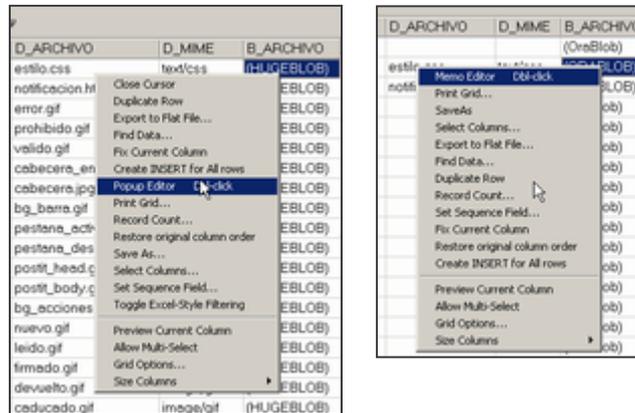
- Abrimos un navegador de objetos de TOAD y nos vamos a la pestaña de tablas, y seleccionamos la tabla constantes.



- Pulsamos el siguiente botón  y introducimos el siguiente criterio de filtrado.



- Pulsamos “OK” y solo nos aparecerán los registros en los que debemos incorporar los archivos. Nos situamos sobre la columna B\_ARCHIVO y pulsamos el botón derecho del ratón, y seleccionaremos la opción



(Ojo, según la versión del TOAD puede que la entrada del menú varíe de nombre)

- Nos aparece la siguiente ventana

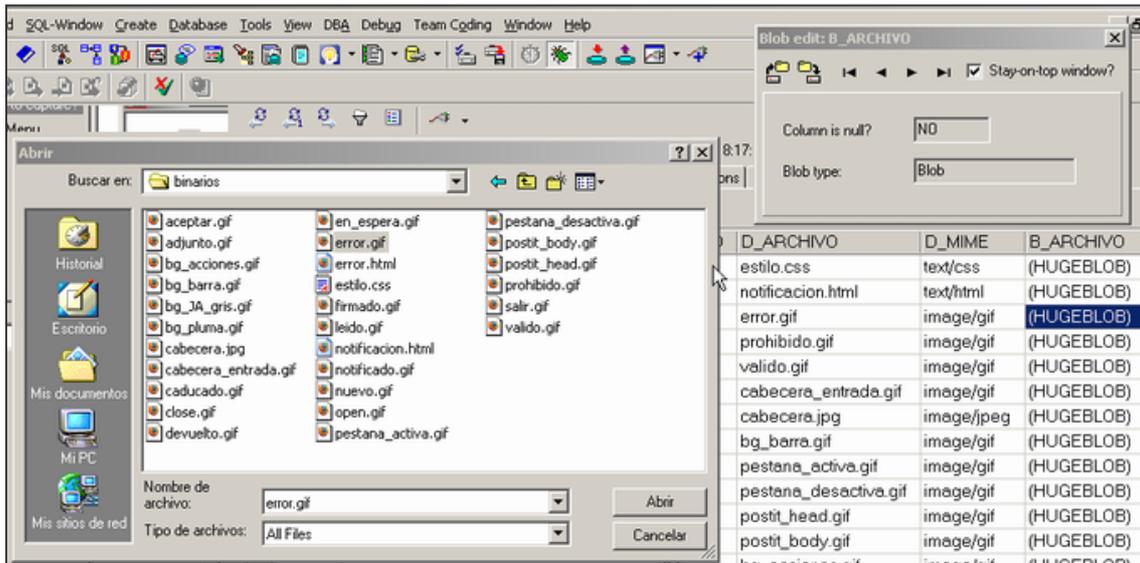


En este menú emergente que nos aparece usaremos los siguientes botones:

-  Para seleccionar un archivo y subirlo a la base de datos.
-  Navegar al primer registro.
-  Navegar al registro anterior.
-  Navegar al registro siguiente.
-  Navegar al último registro.

- Ahora iremos cargando uno a uno las imágenes y documentos existentes en la carpeta:

### D:\KitPortafirma\Scripts\datos\binarios



### 2.3.2 Carga de constantes binarias mediante SQLPLUS

El proceso en este caso es más complejo por eso lo indicamos en el último caso dado que hay que subir a un directorio del servidor de base de datos el contenido de la carpeta **D:\KitPortafirma\Scripts\datos\binarios**, supongamos **/tmp**, y seguir los siguientes pasos.

- Conceder de forma temporal el permiso de creación de directorio al usuario PFIRMAMG con el usuario SYSTEM.

**SQL> grant create any directory to pfirmamg;**

- Tras esto nos conectaremos con el usuario PFIRMAMG, pondremos la siguiente instrucción:

**SQL> create directory READDIR as '/tmp';**

- Crear el siguiente procedimiento

```
CREATE OR REPLACE PROCEDURE CARGA_IMAGENES AS
CURSOR IMAGENES IS
SELECT X_CONSTANTE,D_ARCHIVO
FROM PF_CONSTANTES WHERE D_ARCHIVO IS NOT NULL;
V_IMAGENES IMAGENES%ROWTYPE;
AUX_B_ARCHIVO PF_CONSTANTES.B_ARCHIVO%TYPE;
FILS BFILE;
AMT INTEGER;
BEGIN
UPDATE PF_CONSTANTES SET B_ARCHIVO=EMPTY_BLOB() WHERE D_ARCHIVO IS NOT NULL;
COMMIT;
FOR V_IMAGENES IN IMAGENES LOOP
FILS:= BFILENAME('READDIR',V_IMAGENES.D_ARCHIVO);
DBMS_LOB.FILEOPEN(FILS, DBMS_LOB.FILE_READONLY);
AMT:=DBMS_LOB.GETLENGTH(FILS);
IF AMT>0 THEN
SELECT B_ARCHIVO INTO AUX_B_ARCHIVO FROM PF_CONSTANTES WHERE
X_CONSTANTE=V_IMAGENES.X_CONSTANTE FOR UPDATE;
DBMS_LOB.LOADFROMFILE(AUX_B_ARCHIVO, FILS, AMT);
COMMIT;
END IF;
DBMS_LOB.FILECLOSE(FILS);
END LOOP;
END;
```

- Ejecutar el procedimiento anterior:

```
SQL> exec CARGA_IMAGENES;
```

- Eliminar el procedimiento y quitarle los permisos de creación de directorios al usuario.

## 2.4 Carga de procedimientos

Una vez que hemos cargado todas las tablas de codificación, vamos a proceder a cargar el resto de scripts, en este caso, las clases java y paquetes necesarios.

### 2.4.1 Clase Base64

Esta clase es necesaria para realizar operaciones de codificación y decodificación de BASE64 a binario y viceversa. Hacemos uso de ella debido a que en Oracle 8i no existen clases y paquetes a tal efecto.

Como en los casos anteriores, desde la ventana del SQLPLUS ponemos las siguientes instrucciones:

```
SQL> set scan off;
```

```
SQL> @D:\KitPortafirma\Scripts\base64\Base64plsqlijava.sql
```

### 2.4.2 Especificaciones de paquete

Vamos primero a cargar las especificaciones de los paquetes, para ello en la ventana

del SQLPLUS ejecutamos las siguientes instrucciones:

```
SQL>set scan off;
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_TYPE.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_API.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_TOOL.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_ACCION.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_ADMIN.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_BASE64.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_CORREO.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_DAEMON.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_EVENTO.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_FIRMA.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_LOOKUP.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_NOTIFICA.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_PETICION.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_REDIREC.PKS
```

```
SQL> @D:\KitPortafirma\Scripts\paquetes\PF_PQ_WEB.PKS
```

Si todo va bien irán saliendo diálogos:

**Paquete creado.**

### 2.4.3 Cuerpos de paquete

Al igual que antes, ejecutamos las siguientes líneas en el SQLPLUS.

```
SQL>set scan off;
```

```
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_TYPE.PKB
```

```
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_API.PKB
```

```
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_TOOL.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_ACCION.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_ADMIN.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_BASE64.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_CORREO.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_DAEMON.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_EVENTO.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_FIRMA.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_LOOKUP.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_NOTIFICA.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_PETICION.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_REDIREC.PKB
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_WEB.PKB
```

Si al ver los diálogos de confirmación nos salta al llegar al paquete PF\_PQ\_NOTIFICA el mensaje:

**Advertencia: Cuerpo del paquete creado con errores de compilación.**

Esto quiere indicar que no tenemos acceso al avisador. Si no tenemos o no queremos usar el avisador en [Port@firmas](#) ejecutamos la siguiente línea.

```
SQL>@D:\KitPortafirma\Scripts\paquetes\PF_PQ_NOTIFICA_SIN_AVISADOR.PKB
```

Y con esto hemos terminado de cargar todos los objetos necesarios en la base de datos. Al igual que en los casos anteriores estos script's pueden ser lanzados con el TOAD teniendo cuidado en respetar el orden de ejecución indicado.

Ahora pasaremos a dar de alta la aplicación en @firma y desplegar las aplicaciones en el Tomcat y terminar de configurar las mismas.

## 2.5 Tareas programadas en la base de datos

Hay un par de Job's definidos en el sistema. Uno se encarga de vaciar las tablas temporales periódicas, el otro, solo en el caso de tener activo y configurado el envío de

avisos por o bien a través de la plataforma @visor, del envío de avisos.

Para activar la tarea de borrado de tablas temporales ejecutar desde el SQLPLUS:

```
SQL> @D:\KitPortafirma\Scripts\jobs\SPOOL.sql
```

Si todo va bien debe salir la siguiente línea

**Procedimiento PL/SQL terminado correctamente.:**

Para activar la tarea de envío de avisos ejecutar:

```
SQL> @D:\KitPortafirma\Scripts\jobs\NOTIFICACION.sql
```

Si no se tiene configurado y activo el servicio de envío de correos esta tarea así como el paquete PF\_PQ\_NOTIFICACION puede aparecer como inválido según en cada caso. Por tanto si no se va a usar este servicio es mejor desactivar esta tarea de base de datos o incluso no cargar esta tarea.

Para asegurarnos que se guarden los cambios, hacemos un "commit":

```
SQL> commit;
```

**Validación terminada.**

## 2.6 Creación de Rol

Para controlar y limitar el acceso que puedan hacer terceras aplicaciones sobre las API's se ha definido un rol para adjudicar a los usuarios de base de datos y así tengan acceso únicamente a las API's que les interese.

El script de creación del rol debemos lanzarlo desde el SQLPLUS con la siguiente instrucción:

```
SQL> @"D:\KitPortafirma\Scripts\roles y permisos\CREACION ROL PF_R_PETICIONES.sql"
```

Existen en esta carpeta dos scripts más para ejecutar cuando queramos conceder este rol y el resto de permisos a un usuario de base de datos, así como la generación de sinónimos. En el punto 3.5 del presente documento se detalla más este apartado.



- Dar de alta una página firmable: “pfirma”. Introducir en ella:
  - Identificador de página: pfirma
  - Keystore Certificado: DEFAULT
  - CodeBase: <https://servidorFachada:444/firmadigital>
  - Página firmable:  
<http://<maquina>:<puerto>/pfirma/descarga/>
  - Página Error Certificado: (en blanco)
  - Nombre Formulario: form\_firma
  - Botón Submit: envia\_firma
  - Aplicación: pfirma
  - Página destino: destino\_pfirma.jsp (Hay que colocar este archivo que se encuentra en D:\KitPortafirma\Recibo en el FormbackEnds del servidor de firma y revisar el retorno a nuestro servidor de aplicaciones)
  - Validación de página: Sí
  - Ceremonia de Firmado: (el valor por defecto)
  - Página Destino Multifirma:  
[http://<maquina>:<puerto>/pfirma/pf\\_confirmacion\\_multifirma.jsp](http://<maquina>:<puerto>/pfirma/pf_confirmacion_multifirma.jsp)
  - Clave 3Des Multifirma.



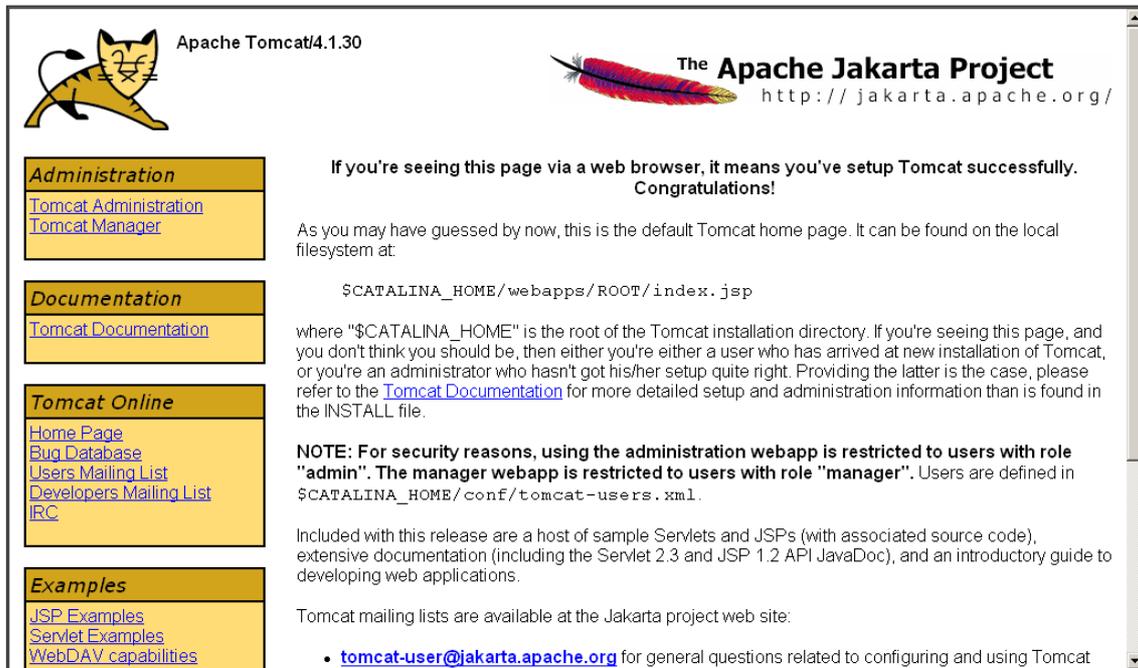
### 3.2 Despliegue en el servidor de aplicaciones Tomcat

Seguidamente vamos a explicar como se despliega la aplicación de [Port@firmas](#) en el Tomcat, así como la herramientas de administración de la misma.

Partimos de la base de que disponemos de un servidor de aplicaciones Tomcat 4.1 o 5.0 y JDK1.4.2.0\_7 o superior en nuestro servidor de aplicaciones (Tomcat 5.5 no es válido al necesitar la JSDK 1.5.0 que no son compatibles con [Port@firmas](#)).

Procedemos a desplegar los wars, para ellos desde una ventana del navegador escribimos la dirección:

<http://servidorAplicaciones:8080/>



Apache Tomcat/4.1.30

The Apache Jakarta Project  
<http://jakarta.apache.org/>

If you're seeing this page via a web browser, it means you've setup Tomcat successfully.  
Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

`$_CATALINA_HOME/webapps/ROOT/index.jsp`

where "\$CATALINA\_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the [Tomcat Documentation](#) for more detailed setup and administration information than is found in the INSTALL file.

**NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager".** Users are defined in `$_CATALINA_HOME/conf/tomcat-users.xml`.

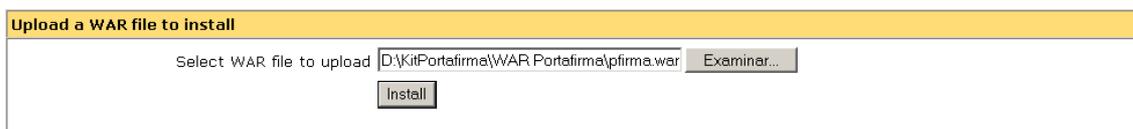
Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.3 and JSP 1.2 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Jakarta project web site:

- [tomcat-user@jakarta.apache.org](mailto:tomcat-user@jakarta.apache.org) for general questions related to configuring and using Tomcat

Con lo que nos saldrá la siguiente ventana:

Entramos en "Tomcat Manager" y tras indicar el usuario y clave administrador del Tomcat con el que dimos de alta el servidor, accederemos al módulo de configuración de aplicaciones. Nos vamos a la parte de Instalación (Install) y pulsamos el botón examinar, escogemos el fichero WAR del Port@firma y pulsamos "instalar" (install)



Upload a WAR file to install

Select WAR file to upload

Hacemos igual con el WAR de la herramienta de administración.

**Upload a WAR file to install**

Select WAR file to upload

Si todo ha ido bien nos saldrá las dos nuevas aplicaciones en la lista de aplicaciones de la parte superior de la pantalla.

Applications					
Path	Display Name	Running	Sessions	Commands	
/	Welcome to Tomcat	true	1	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/TrewaFidea	Escritorio Trewa (Versión para Fidea)	true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/acervobot		true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/acervoweb		true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/admin	Tomcat Administration Application	true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/adminpfirma		true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/avisador		true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/barbecue		true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/demoautenticacion		true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/emuladorAries		true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/eperFirmaPrueba		true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/examples	Tomcat Examples	true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/manager	Tomcat Manager Application	true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/notificador		true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/ord_uni_sub		true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/pdftoimage		true	0	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>
/pfirma		true	2	Start	<a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Remove</a>

Una vez desplegadas las dos aplicaciones, las paramos y accedemos al directorio

**\$ruta\_tomcat\$\webapps\pfirma\WEB-INF\classes**

Y modificamos el archivo de propiedades “conn\_pfirma.properties” con los datos de la conexión:

```
nombreMaquina=maquinaBD
puerto=1521
nombreBD=DESARROLLO
nombreUsuario=pfirmamg
clave=pfirmamg
tituloHTML=Port@firmas - Consejería de XXX - Junta de Andalucía
```

El resto de parámetros del archivo de propiedades solo afectan en caso de emplear avisador o firma mediante RMI.

Para la herramienta de Administración accederemos también al directorio

**\$ruta\_tomcat\$\webapps\adminpfirma\WEB-INF\classes**

Y comprobaremos que los datos de conexión, estén iguales que el caso anterior.

Una vez hecho estos cambios, arrancamos de nuevo las aplicaciones.

### 3.2.1 Detector.js

Dentro del directorio “servicio” de la carpeta creada al desplegar la aplicación en el Tomcat, `$ruta_tomcat$webapps\pfirma\servicio`, se encuentra el fichero “Detector.js” que hay que revisar la variable de retorno en caso de que falten componentes para que apunte al servidor de fachada.

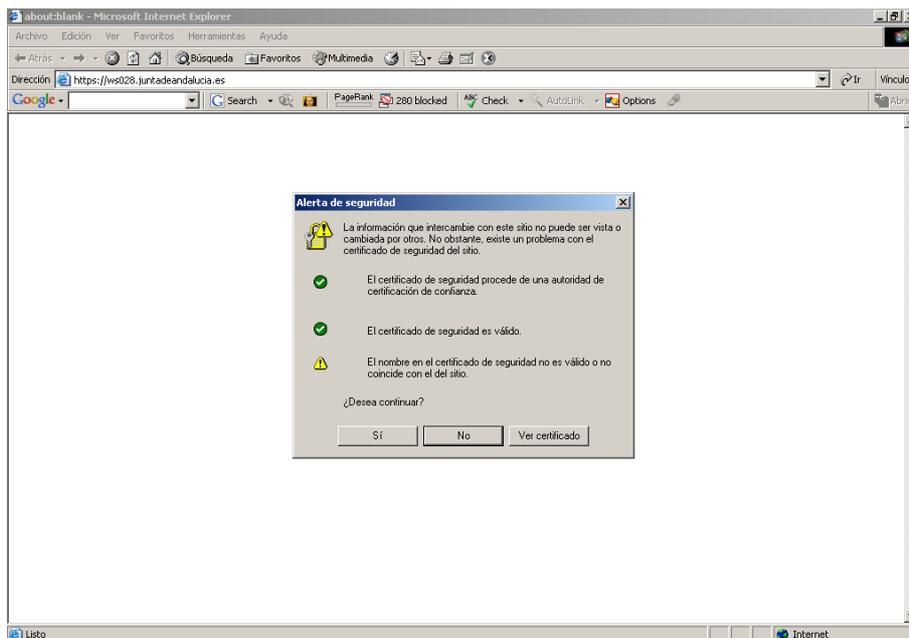
```
// ----- Comienzo Variables a modificar -----  
  
// Url for the next page when all the necessary components are detected  
var nextUrl = "../pf_peticion.jsp";  
  
// Url base of digital sign se  
var url_base = "https://<serviforFachada><puerto>/firmadigital";  
  
// ----- Fin variables a modificar -----
```

Deberemos cambiar el valor marcado en rojo para que apunte al servidor de fachada, por ejemplo:

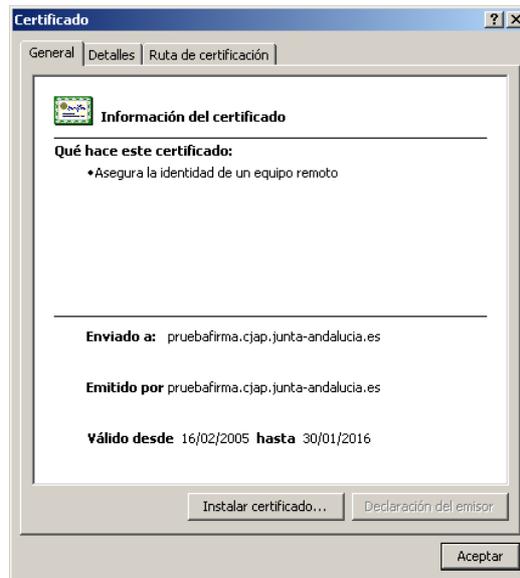
```
var url_base = "https://ws017.juntadeandalucia.es:444/firmadigital";
```

### 3.2.2 Almacén de certificados

Para poder establecer la comunicación SSL entre nuestro servidor de aplicaciones y el servidor de custodia de @firma debemos cargar la clave publica del mismo dentro del almacén de certificados de nuestro servidor de aplicaciones. Para ello, la forma más sencilla es conectarnos con un navegador al servidor de custodia, ejemplo:



Pulsamos “Ver certificado”.



Pulsamos “Instalar certificado”.



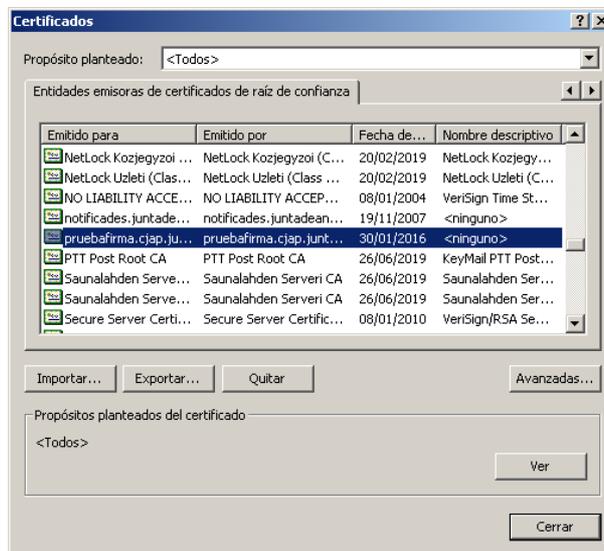
Nos sale un asistente mediante el cual podemos incorporar el certificado del servidor, pulsamos siguiente para continuar, nos preguntará si queremos incorporar a un almacén automáticamente o bien si queremos escogerlo nosotros directamente.

Escogemos esta última tal y como se ve en las siguientes imágenes.



Seguimos hacia delante en el asistente y si todo va bien nos mostrará un diálogo de confirmación de operación realizada con éxito. Tras esto accederemos al menú “Herramientas”, “Opciones de Internet”, “Contenido” pulsamos el botón “Certificados...” de forma que nos saldrá un nuevo asistente.

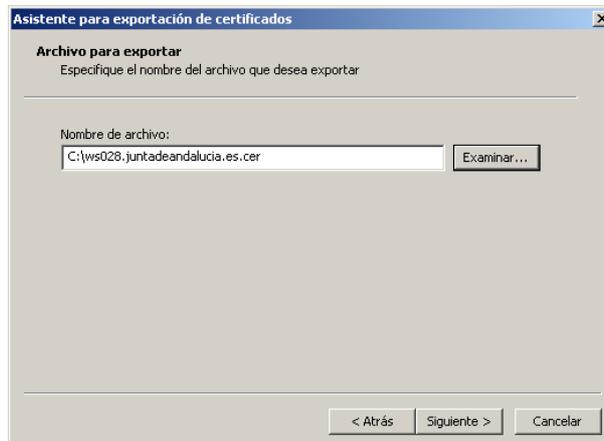
Nos vamos a la última pestaña y buscamos el certificado recién importado.



Seleccionamos el certificado y pulsamos “Exportar...”, nos mostrará un nuevo asistente en donde después de una pantalla de bienvenida, nos preguntará por el formato de exportación.



Escogemos el primero de los formatos, y nos pedirá a continuación también la ruta donde queremos guardarlo.



Tras esto ya tenemos el certificado del servidor, que podremos importar mediante la herramienta “keytool” de java sobre el almacén por defecto, “cacerts” (la clave de este almacén es “changeit”) del runtime de java, que por lo general se encuentra en el directorio:

```
%JAVA_HOME%/jre/lib/security
```

Para incluirlo deberemos importarlo mediante el siguiente comando, que siguiendo con el ejemplo sería:

```
Keytool -import -keystore %JAVA_HOME%/jre/lib/security/cacerts -file C:\ws028.juntadeandalucia.es.cer -alias custodia
```

Tras esto solo debemos recordar la ubicación del almacén de certificados para un paso más adelante.

### 3.2.3 Ampliación del parámetro de memoria de la máquina virtual de Java

Si tenemos una instalación típica de Tomcat, este se estará ejecutando con un límite de memoria RAM de 64 megas, las cuales se quedan cortas para poder funcionar correctamente con [Port@firmas](#) y resto de aplicaciones web desplegadas en el mismo produciendo pasado un tiempo que se den errores “java.lang.OutOfMemoryError”.

Recomendamos añadir por tanto a la variable JAVA\_OPTS el valor máximo de memoria a 256 Megas.

A continuación se explica como modificar este parámetro con lo que conseguimos pasar de 64 megas a un máximo de 256. Si se siguen apreciando caídas por que existan gran número de aplicaciones desplegadas en el mismo servidor de aplicaciones, seguir ampliando dicho parámetro en función a las características del servidor y recursos disponibles.

Para más información es mejor acceder a la FAQ de Apache/Tomcat y buscar en relación a este tema.

#### 3.2.3.1 Servidor de Aplicación Windows

En este caso debemos editar el archivo “catalina.bat” que se encuentra en el directorio “\TomcatX\bin”. Buscamos el siguiente trozo de código e incluimos las partes marcadas en rojo:

```
...
# JAVA_HOME    Must point at your Java Development Kit installation.
#
# JAVA_OPTS    (Optional) Java runtime options used when the "start",
#              "stop", or "run" command is executed.
#
# JPDA_TRANSPORT (Optional) JPDA transport used when the "jpda start"
#              command is executed. The default is "dt_socket".
#
# JPDA_ADDRESS  (Optional) Java runtime options used when the "jpda start"
#              command is executed. The default is 8000.
#
# JSSE_HOME    (Optional) May point at your Java Secure Sockets Extension
#              (JSSE) installation, whose JAR files will be added to the
#              system class path used to start Tomcat.
#
# CATALINA_PID (Optional) Path of the file which should contains the pid
#              of catalina startup java process, when start (fork) is used
#
# $Id: catalina.sh,v 1.13.2.1 2004/08/21 15:49:49 yoavs Exp $
# -----
set JAVA_OPTS="-Xmx256m"

# OS specific support. $var _must_ be set to either true or false.
cygwin=false
os400=false
case "`uname`" in
CYGWIN*) cygwin=true;;
```

```
OS400*) os400=true;;  
...
```

Esto sería para el caso de arrancar el Tomcat con el “startup.bat”.

Para que los cambios se lleven a efecto deberemos reiniciar el Tomcat.

### 3.2.3.2 Servidor de Aplicaciones Linux/Unix

Para el caso de estos servidores hay que editar el archivo “catalina.sh” que se encuentra en el directorio “\TomcatX\bin”. Buscamos el siguiente trozo de código e incluimos las partes marcadas en rojo:

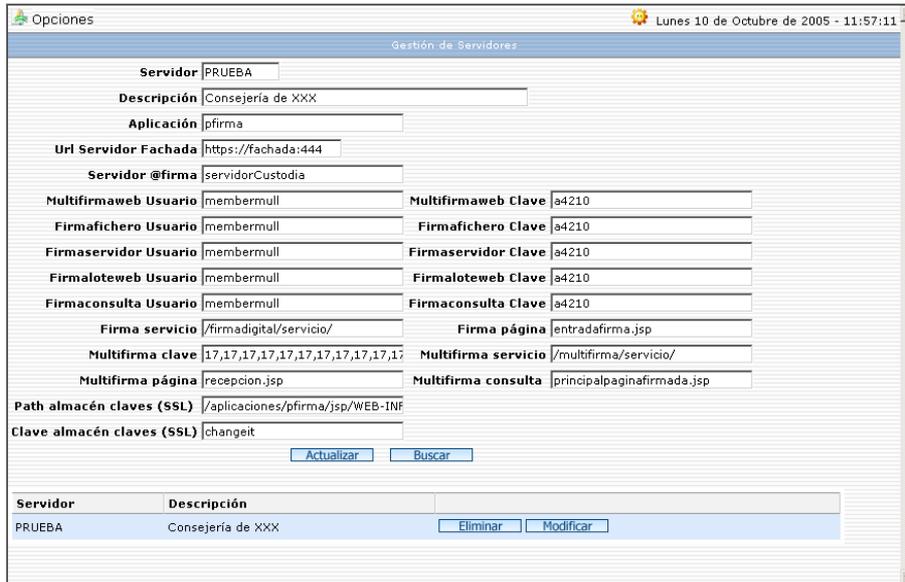
```
...  
# JAVA_HOME    Must point at your Java Development Kit installation.  
#  
# JAVA_OPTS    (Optional) Java runtime options used when the "start",  
#              "stop", or "run" command is executed.  
#  
# JPDA_TRANSPORT (Optional) JPDA transport used when the "jpda start"  
#              command is executed. The default is "dt_socket".  
#  
# JPDA_ADDRESS  (Optional) Java runtime options used when the "jpda start"  
#              command is executed. The default is 8000.  
#  
# JSSE_HOME     (Optional) May point at your Java Secure Sockets Extension  
#              (JSSE) installation, whose JAR files will be added to the  
#              system class path used to start Tomcat.  
#  
# CATALINA_PID  (Optional) Path of the file which should contains the pid  
#              of catalina startup java process, when start (fork) is used  
#  
# $Id: catalina.sh,v 1.13.2.1 2004/08/21 15:49:49 yoavs Exp $  
# -----  
JAVA_OPTS="-Xmx256m"  
  
# OS specific support. $var _must_ be set to either true or false.  
cygwin=false  
os400=false  
case "`uname`" in  
CYGWIN*) cygwin=true;;  
OS400*) os400=true;;  
...  
...
```

Hay que tener cuidado que la forma de definir las variables varía de Windows a este sistema.

Para que los cambios se lleven a efecto deberemos reiniciar el Tomcat.

### 3.3 Actualizando Servidores de firma en [Port@firmas](#)

Una vez desplegadas las aplicaciones, accederemos a la herramienta de administración para volcar la información que habíamos indicado en el servidor de @firma en la configuración del servidor de firma de [Port@firmas](#) así como la ruta al almacén de certificados.



Servidor	Descripción	Eliminar	Modificar
PRUEBA	Consejería de XXX		

### 3.4 Actualizando las constantes de la aplicación

Debido a que las constantes del sistema son muy “sensibles” ante cambios inadecuados, no se ha dejado por ahora que estas se puedan modificar desde la herramienta de administración. Por tanto tendremos que modificarla a mano:

- FIRMA\_AUTEN: Dirección URL de autenticación

<https://servidorFachada/cjap/servlet/com.telventi.autenticacion.ServletAutenticacion>

- FIRMA\_APLIC: Nombre de la aplicación de autenticación pfirma
- FIRMA\_AUTEN\_PASS: Clave de autenticación en decimal.
- SERVIDOR\_PRIMARIO: Servidor primario por defecto.
- SERVER\_WEB: con el servidor de aplicaciones: <http://<maquina>:<puerto>/pfirma/>

### 3.4.1 Configuración de los servicios de aviso por correo

Si queremos habilitar los mecanismo de aviso por correo electrónico a los destinatarios de las petición o bien a los emisores de la misma deberemos disponer de una cuenta de correo y la información de acceso a los servidores POP3 y SMTP de correo. Este servicio está deshabilitado por defecto, para cambiarlo hay que editar la siguiente variable:

- NOTIF\_EMAIL: Valor S o N para habilitarlo o no.

En caso de activarlo tenemos que revisar las siguientes variables:

- EMAIL: Dirección de correo de [Port@firmas](mailto:Port@firmas).
- EMAIL\_HELO: Servidor de correo.
- EMAIL\_NOMBRE: Nombre como remitente.
- EMAIL\_POP3: Servidor POP3.
- EMAIL\_SMTP: Servidor SMTP.
- EMAIL\_USER: Usuario de correo.
- EMAIL\_PASS: Clave de correo.

### 3.5 Permisos Oracle a nuevos usuarios de aplicación

Para permitir el acceso a las API's de [Port@firmas](#), existe un Rol así como una serie de permisos adicionales sobre objetos necesarios para resolver la comunicación vía PLSQL o base de datos de [Port@firmas](#) con el resto de aplicaciones.

Al igual que en pasos anteriores, hay que hacer los siguientes pasos desde un SQLPLUS:

Para la creación del rol es necesario haber lanzado previamente el siguiente script:

```
SQL> @"D:\KitPortafirma\Scripts\roles y permisos\CREACION ROL PF_R_PETICIONES.sql"
```

La creación del rol se realiza una única vez en el sistema. El resto de pasos si hay que repetirlos por cada usuario de aplicación que vaya a emplear las API's.

Para asignarle los permisos a un usuario hay que lanzar el script:

```
SQL>@"D:\KitPortafirma\Scripts\roles y permisos\PERMISOS USUARIO PETICIONES.SQL" USUAPLIC
```

Para crearle los sinónimos, con el usuario final lanzar el siguiente script:

```
SQL>@"D:\KitPortafirma\Scripts\roles y permisos\SINONIMOS USUARIO PETICIONES.SQL" USUAPLIC
```

Tras esto el usuario Oracle tendrá todo lo necesario para probar la demo de integración desde PLSQL o bien atacar directamente las API's.<sup>1</sup>

---

<sup>1</sup> Si se quiere crear nuevos paquetes PLSQL almacenados que ataquen a las API's de [Port@firmas](#), el usuario propietario no le bastará solo el Rol sino necesitará también los permisos específicos de ejecución sobre los mismos.

## 4 Historia de versiones

VERSION	FECHA	AUTOR	DESCRIPCIÓN
1.0.0	27/06/2005	FJCV	Primera versión del documento, Port@firmas v1.0.0
1.0.1	30/09/2005	FJCV	Revisión requisitos, almacén de certificados, gestión de memoria en Linux/Unix y configuración de avisos por correo.
1.0.2	21/10/2005	FJCV	Redirección en detección de componentes a servidor Fachada.