Manual de administración de @firma
Versión 4.0

Documento nº:	TI-20-1074-ADM-001
Revisión:	03
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-ADM-001
Revisión: 4
Fecha: 24/02/05

REALIZADO

26/07/04

Moisés Manuel Infante Gómez
Analista

COMPROBADO

26/07/04

Javier Cerceda García	José Antonio Márquez Contreras
Analista	Director @firma

APROBADO

26/07/04

José Antonio Márquez Contreras
Director @firma

CONTROL DE MODIFICACIONES

Documento nº: TI-20-1074-ADM-001
Revisión: 4
Fecha: 19/08/04

Rev. 1
Fecha 26/07/04
Autor/es MMIG
Descripción Documentación inicial

Rev. 2
Fecha 19/08/04
Autor/es JAMC
Descripción Revisión Final

Rev. 3
Fecha 15/09/04
Autor/es JCG
Descripción Generación dinámica de claves 3DES

Rev. 4
Fecha 24/02/05
Autor/es MMIG
Descripción Se modifica la configuración del componente Servidor Autenticación SSL

CONTROL DE DISTRIBUCIÓN

Documento nº: TI-20-1074-ADM-001
Revisión: 4
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 24/02/2005 13:26

Distribución 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 la administración de la plataforma de Autenticación y Firma Digital de la Junta de Andalucía, @firma.

Los objetivos globales de este proceso son:

- Describir la utilización de la Herramienta de Administración gráfica.
- Describir la configuración de la "Fachada".
- Descripción de los logs del sistema.

2 Alcance

El presente documento recoge la administración de la solución propuesta por Telvent Interactiva ante las necesidades de creación de una herramienta de autenticación y firma digital mediante el uso de certificados digitales para la Junta de Andalucía.

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-INS-001, Manual de Instalación del Servidor @firma.
- Documento TI-20-1074-MPA-001, Manual del Programador del Módulo de Autenticación del Servidor @firma 4.0.
- Documento TI-20-1074-MPF-001, Manual del Programador del Módulo de Firma Web, Multifirma Web y Multifirma masiva del Servidor @firma 4.0.

5 Herramienta de Administración del Servidor @Firma

5.1 Descripción General

La Herramienta de Administración de @firma contempla la administración de todos los componentes que conforman la plataforma de Autenticación y Firma de la Junta de Andalucía.

Entre sus características principales se encuentran:

- Centralización de los parámetros de configuración. Todos los parámetros de configuración de la aplicación @firma han sido agrupados en un solo fichero de configuración, administrado a través de esta Herramienta.

- Distribuida, no necesita estar instalada en el mismo servidor. Permite la administración remota del Sistema @firma.

- Posibilidad de administrar bajo la misma herramienta y sesión, distintos servidores @firma. Un parámetro de arranque de la aplicación define los Servidores @firma que pueden ser administrados por la Herramienta.

- Segura. El sistema de administración se encuentra protegido por un triple sistema de seguridad:

    - Sistema de logado para administradores basado en usuario y contraseña.

    - Securización por SSL de las comunicaciones entre la herramienta y los distintos servidores @firma.

    - Encriptación del fichero de configuración. El fichero de configuración es encriptado a la hora de ser guardado en disco.

- Portable. Al estar escrita en Java, esta puede ser desplegada en cualquier entorno que incluya una máquina virtual de Java 1.4. o superior.

- Posibilidad de publicación de la Herramienta bajo Java WebStart, para facilitar su distribución, acceso y actualización.

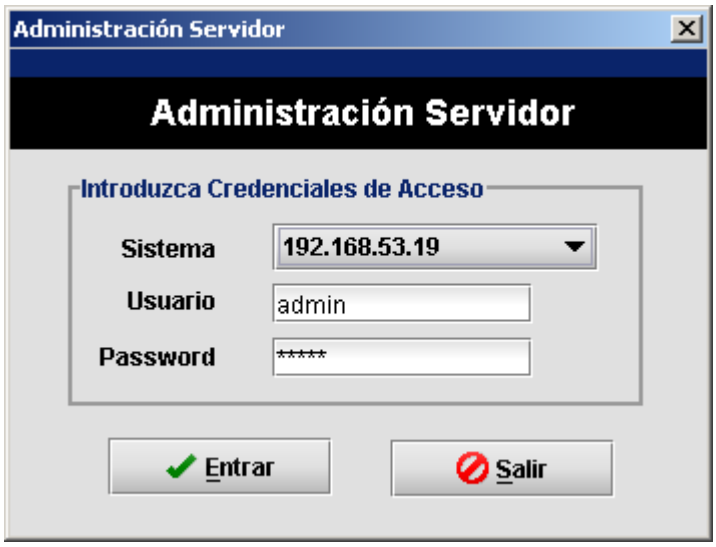
- Detección de colisiones. Se incorpora un mecanismo de detección de errores producidos por el uso concurrente de varias instancias de la Herramienta sobre un mismo servidor.

- Backup automático del fichero de configuración, cada vez que se produce un cambio en la configuración.

La herramienta permite tanto la administración de los parámetros de configuración de las distintas aplicaciones, como la configuración del motor de autenticación y firma.

5.2 Arrancar la Herramienta de Administración.

Para arrancar la Herramienta de Administración nos dirigiremos al directorio donde se instaló y ejecutaremos el script "admin" y nos aparecerá una ventana como la siguiente:



En la lista "Sistema" elegiremos el servidor de @firma que queramos administrar, si no aparece el servidor deseado, deberemos "Salir" y editar el fichero "servidores.properties" que se encuentra en directorio de instalación.

En el archivo "servidores.properties" hay parejas "clave=valor", podemos editar el valor de alguna de las parejas o incluso añadir nuevas parejas, siempre que la clave siga el formato de las existentes: "servidorX" siendo la X el número siguiente al de la última pareja. Ejem:

servidor1=192.168.53.19
servidor2=<servidor2>
servidor3=<servidor3>

Una vez elegido el servidor, deberemos introducir el usuario/password para poder administrar ese servidor. Por defecto aparece uno que se utiliza para poder entrar en la Herramienta de Administración de un servidor recién instalado.

NOTA: se recomienda cambiar el password o incluso el usuario la primera vez que se entre en la Herramienta como se indica más adelante en una sección de los Parámetros Generales.

Si el usuario/password son correctos nos aparecerá la Herramienta de Administración propiamente dicha y en caso contrario nos aparecerá la siguiente ventana:

5.3 Menús

En la Herramienta de Administración podemos distinguir cuatro menús desplegables: Servidor, Utilidades, Look&Feel y Help.

A continuación iremos enumerando el contenido de cada uno de los menús y su utilización.

5.3.1 Menú "Servidor"

Este menú consta de cuatro elementos, como se puede apreciar en la imagen inferior.

- **Nueva Conexión**: Esta opción nos permite cambiar el servidor que estamos administrando, para ello nos sale la misma ventana que nos salió para entrar en la herramienta.

- **Enviar Configuración Servidor**: Esta opción nos permite enviar la configuración local al servidor. Al seleccionarla nos pedirá la confirmación de que realmente queremos enviar la información al servidor y si todo es correcto nos lo indicará con la siguiente ventana:

- **Obtener Configuración Servidor:** Esta opción nos permite actualizar la información mostrada por la herramienta con la configuración que se encuentra actualmente en el servidor.

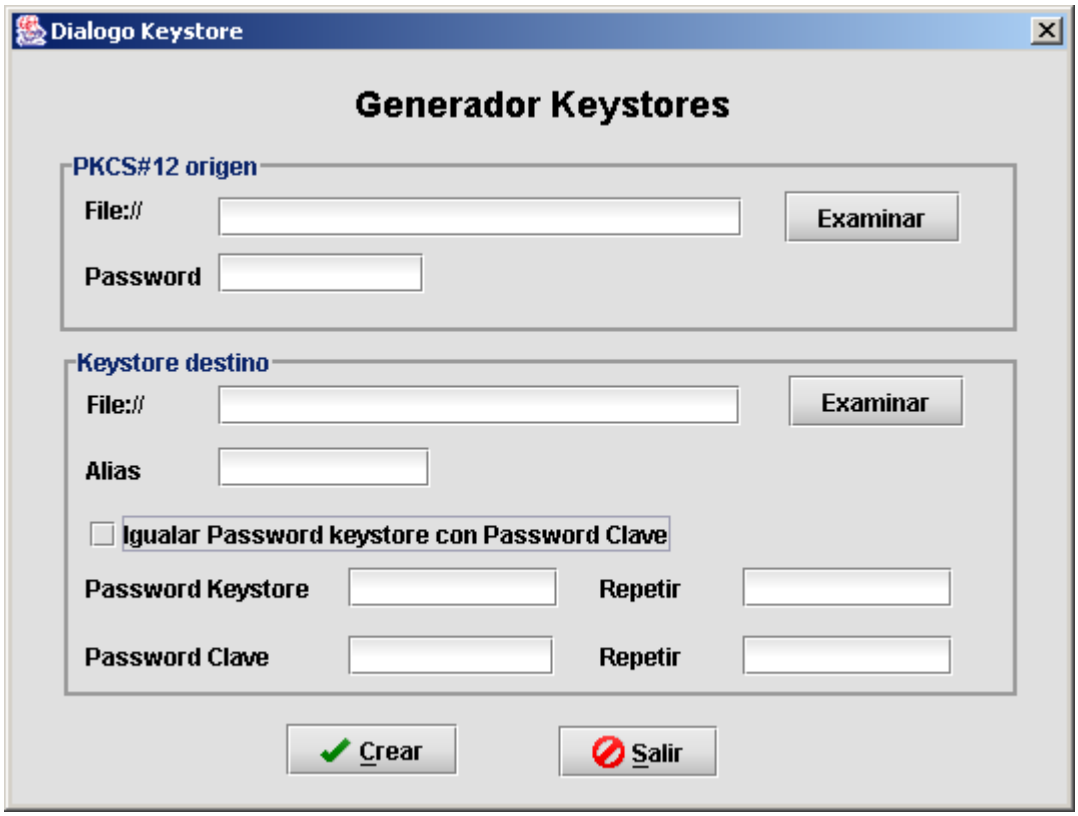
- **Exit:** Sirve para cerrar la Herramienta de Administración.

Justo debajo de los menús se encuentra una barra de herramientas con botones que corresponden a cada una de las opciones enumeradas anteriormente.

5.3.2 Menú Utilidades

Este menú consta de cuatro elementos, como se puede apreciar en la imagen inferior.

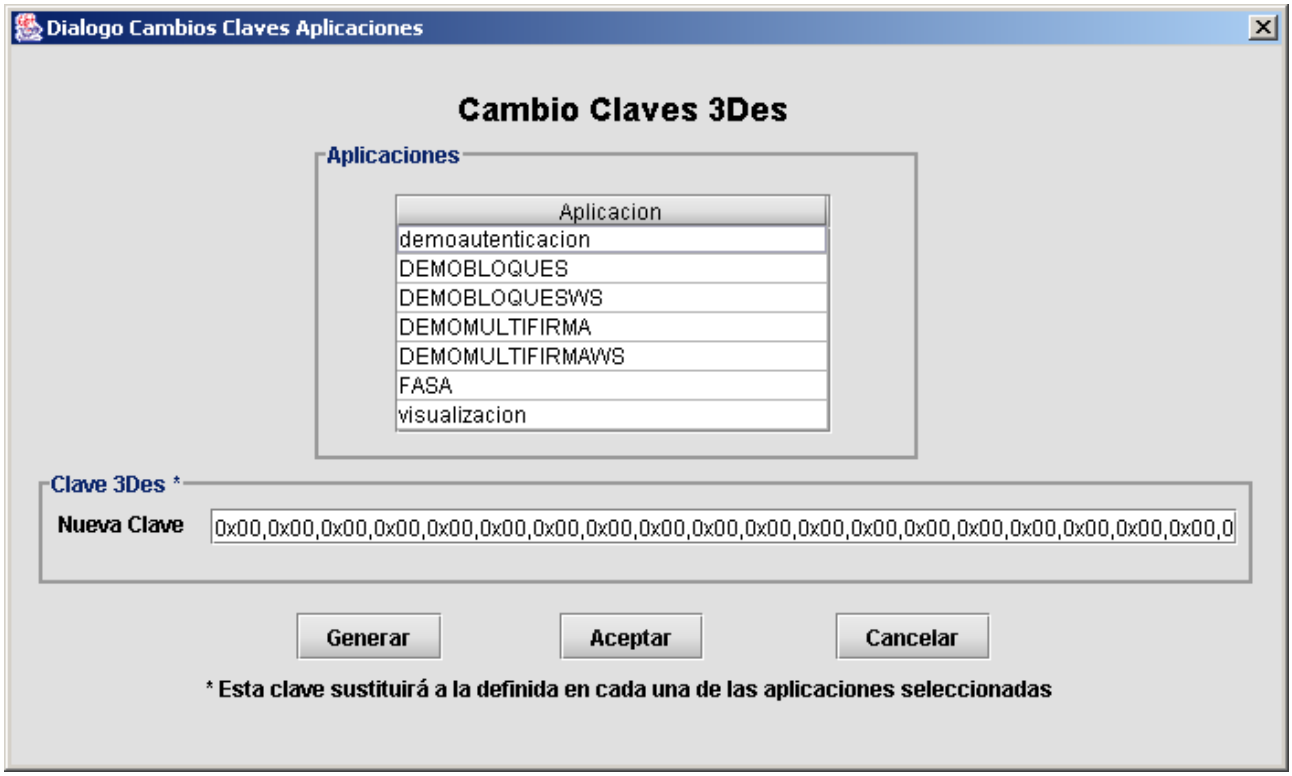
- **Generar Keystore HTTPS:** Esta opción nos mostrará una ventana con la que podremos convertir archivos en formato".p12" en archivos de keystore utilizados en el servidor para configurar las conexiones HTTPS (Ver Manual de Instalación TI-20-1074-INS-001). La utilización de esta utilidad simplemente consiste en rellenar los campos de la ventana con el contenido indicado en sus nombres y pulsar el botón "Crear".



- Cambiar Claves 3Des Aplicaciones: Pulsando en esta opción nos saldrá una ventana que nos facilitará el cambio de las Claves 3Des utilizadas por las "Aplicaciones" dadas de alta en la Herramienta de Administración. En esta ventana se muestra una lista con todas las aplicaciones, un campo de texto para introducir la nueva clave y tres botones "Generar", "Aceptar" y "Cancelar". El botón "Aceptar" cambia la clave de la aplicación/es seleccionada/s en la lista por la nueva clave introducida en el campo de texto. El botón "Generar" permite generar dinámicamente una nueva clave 3Des en el campo de texto. El botón "Cancelar" cancelará el proceso cerrando la ventana.

- Cambiar Claves 3Des Páginas Web Firmables: Pulsando en esta opción nos saldrá una ventana que nos facilitara el cambio de las Claves 3Des utilizadas por las "Paginas Web Firmables" dadas de alta en la Herramienta de Administración. En esta ventana se muestra una lista con todas las paginas, un campo de texto para introducir la nueva clave y tres botones "Generar","Aceptar" y "Cancelar". El botón "Aceptar" cambia la clave de la pagina/s seleccionada/s en la lista por la nueva clave introducida en el campo de texto. El botón "Generar" permite generar dinámicamente una nueva clave 3Des en el campo de texto. El botón "Cancelar" cancelará el proceso cerrando la ventana.

El aspecto de la ventana mostrada por las dos opciones anteriores es el siguiente:



- Generar Listado PDF: Esta opción nos permite generar un fichero.pdf con toda la información de las aplicaciones, páginas web firmables y páginas multifirma masiva registradas. Al pulsarla nos saldrá un dialogo de elección de archivo donde deberemos introducir el nombre del fichero que vamos a generar. Si todo es correcto nos lo indicará con una ventana como la siguiente:

5.3.3 Menú Look&Fell.

Este menú consta de 4 elementos que indican la apariencia de la Herramienta de Administración. Pulsando sobre cada uno de los estilos cambia la apariencia. Los estilos disponibles son:

- Metal: Estilo propio de las aplicaciones Java.
- CDE/Motif: Estilo de las aplicaciones Unix/Linux.
- Windows: Estilo de las aplicaciones Windows.

- Kunstostoff: Estilo utilizado por defecto por la Herramienta de Administración.

5.3.4 Menú Help

Este menú tiene la opción "About" que al pulsarla muestra la ventana siguiente:

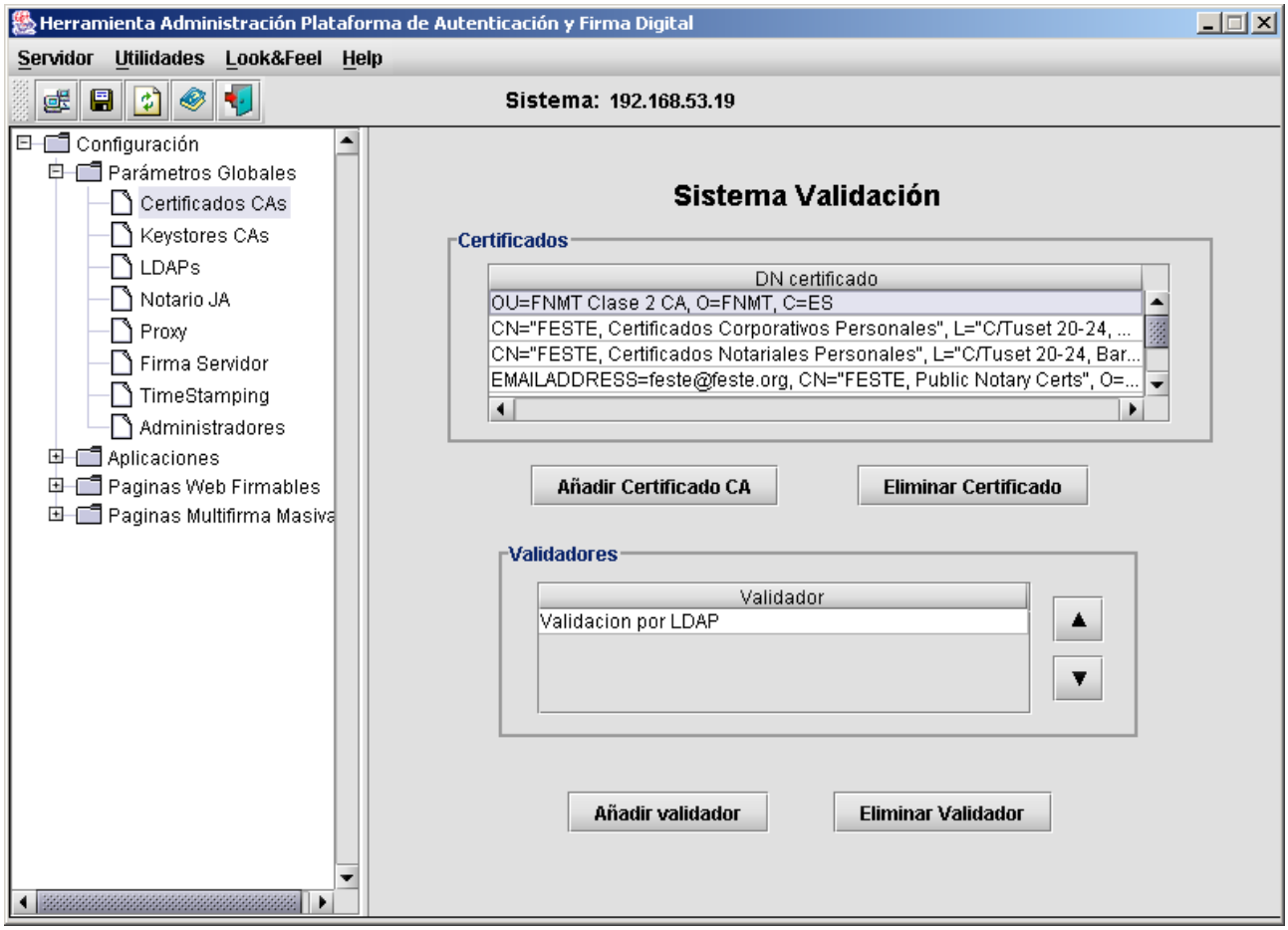
5.4 Parámetros Globales

Los parámetros globales sirven para configurar el motor de autenticación y firma. Dentro de la Herramienta de Administración se encuentran en el primer lugar del árbol que se encuentra en la parte izquierda de la herramienta.

Seleccionando cada una de las hojas del árbol cambiará el panel de la derecha y mostrará la información relacionada con cada parámetro, a continuación iremos explicando cada uno de los parámetros de forma individualizada.

5.4.1 Certificados CAs

Dentro del panel que aparece al seleccionar esta hoja dentro del árbol podemos administrar los certificados de las CAs aceptadas de forma global por el sistema de autenticación y firma, así como los mecanismos de validación asociados a cada uno de los certificados. Estos mecanismos permiten la validación de certificados basados en CRLs publicadas bajo http, https, ftp y LDAPs.

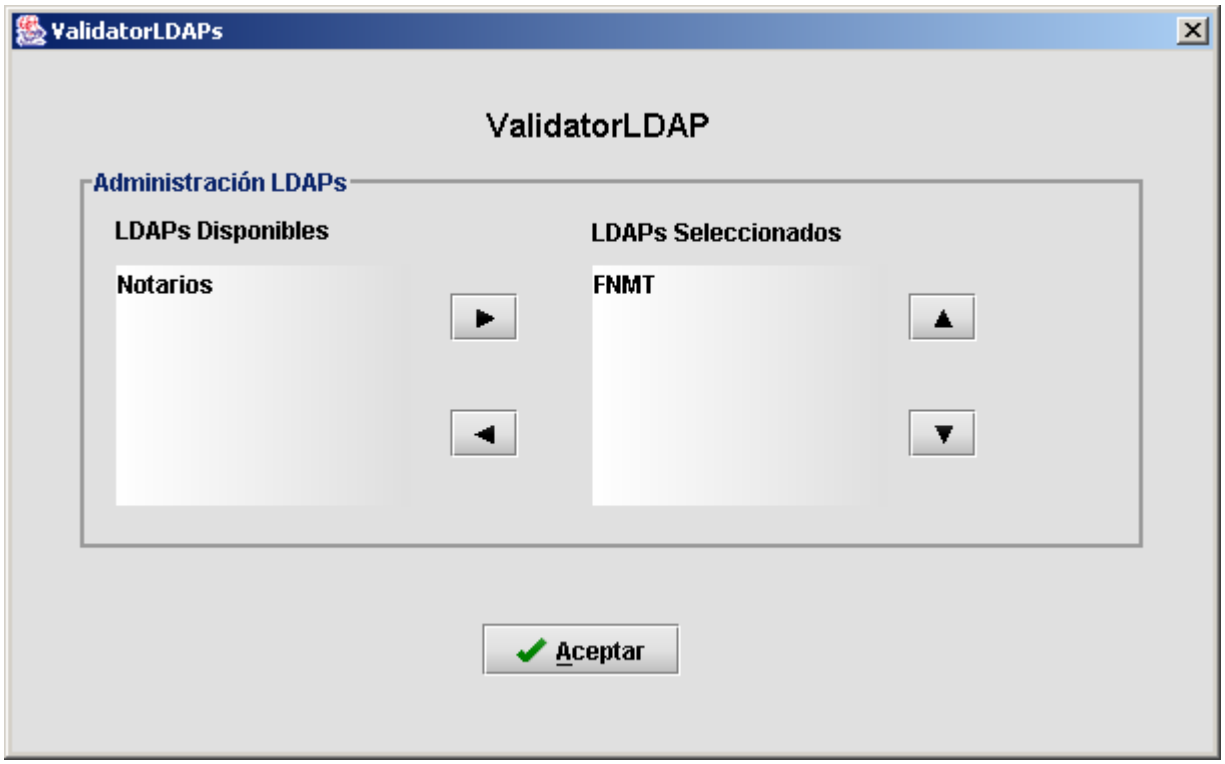


Seleccionando algún certificado de la lista nos aparecerán los validadores asociados a dicho certificado dentro del cuadro "Validadores". Podemos añadir nuevos validadores o eliminar alguno de los existentes así como modificar el orden en el que usarán los validadores.

Si pulsamos el botón "Añadir validador" nos aparecerá la siguiente ventana, donde podremos elegir el tipo de validador que queremos añadir, sólo se podrá añadir un validador de cada tipo.

El tipo básico corresponde a validación por http/ftp. La opción de validador mediante OCSP todavía no se encuentra operativa por lo cual no se puede usar.

Si para el certificado seleccionado hemos añadido la "Validación por LDAP" haciendo doble click sobre ella nos aparecerá una ventana donde podremos elegir los directorios LDAPs que vamos a utilizar para validar los certificados emitidos por esta CA así como el orden en el que se van a consultar dichos directorios.



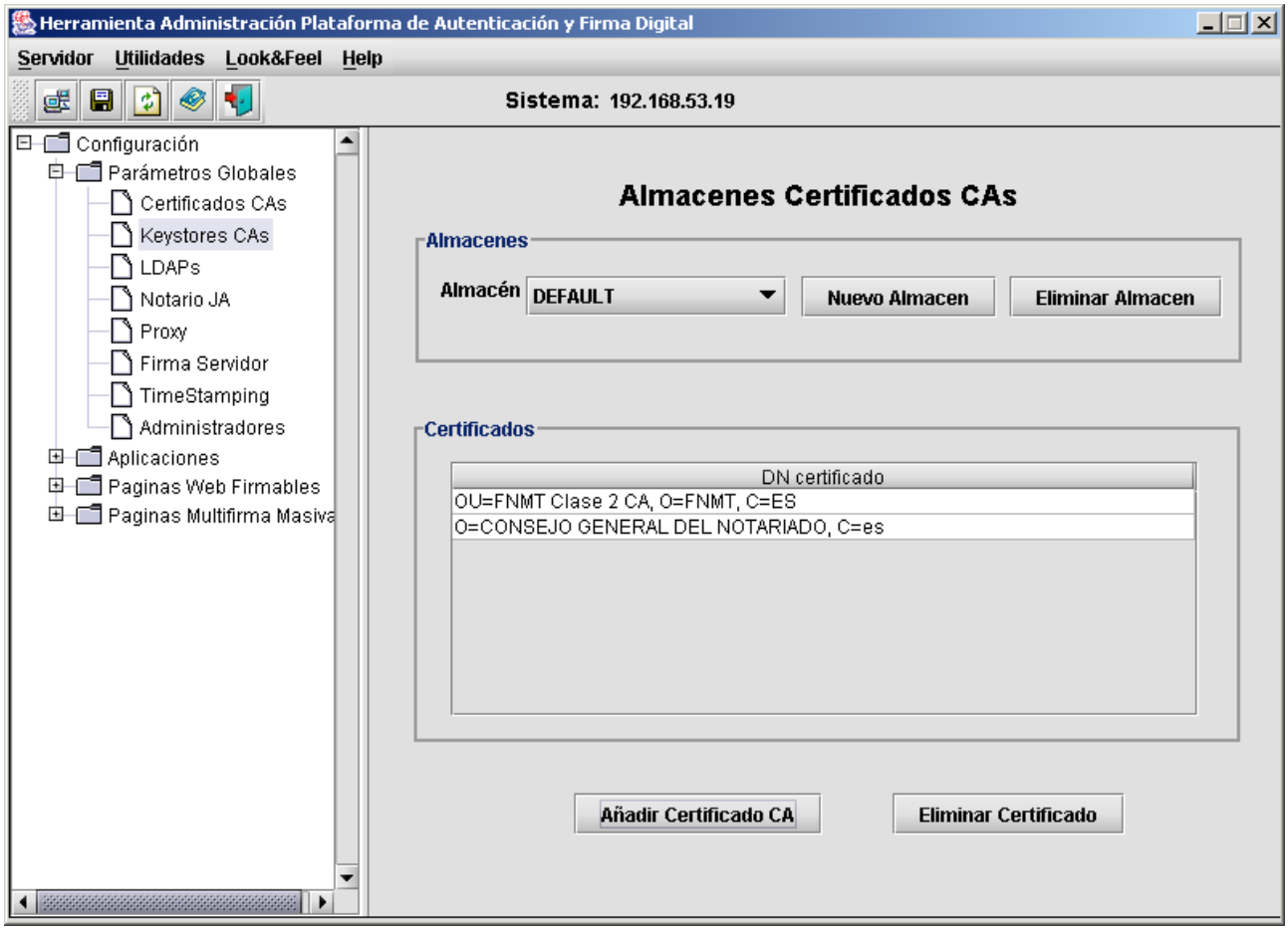
En esta ventana aparecen todos los LDAPs dados de alta, en otro de los parámetros globales: "LDAPs".

Si hacemos doble click sobre alguno de los certificados se nos mostrará una ventana con información sobre dicho certificado.

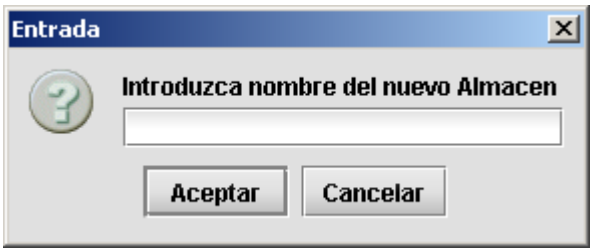
5.4.2 Keystores CAs

Con este parámetro incluimos la noción de Almacenes de Certificados (Keystore CA), los cuales son asociados a las aplicaciones concretas. De esta forma se define más cómodamente el conjunto de CAs válidas por aplicación.

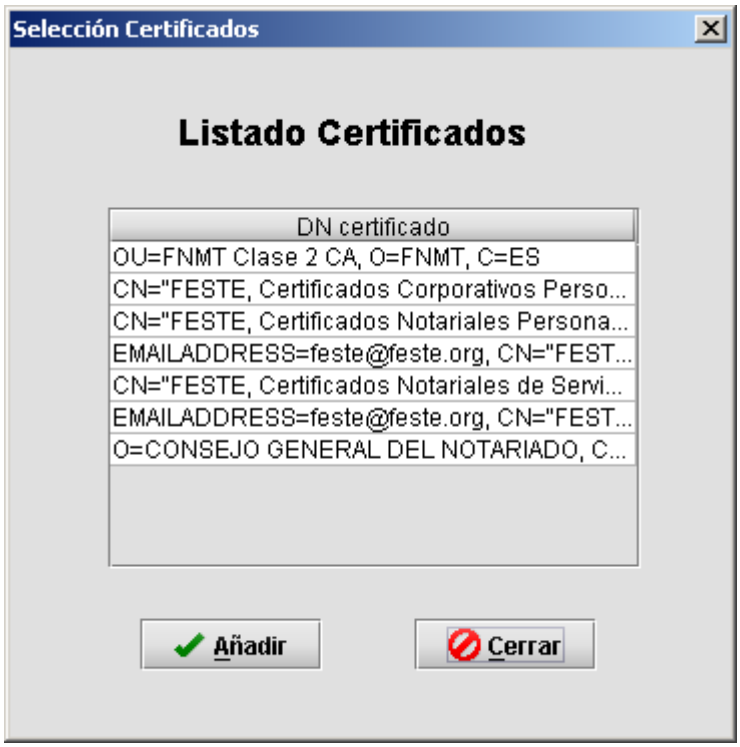
En este panel podemos crear y eliminar almacenes así como asociar a cada almacén los certificados de las CAs válidas para las aplicaciones que usen dichos almacén.



Cuando pulsamos el botón "Nuevo Almacén" nos aparecerá una ventana para introducir el nombre del nuevo almacén.



Una vez introducido el nombre este se incluirá en la lista de almacenes y aparecerá seleccionado, mostrándose la lista de certificados, en la parte inferior, vacía como era de esperar. Ahora procederemos a introducir los certificados de las CAs, para introducirlos pulsaremos el botón "Añadir Certificado CA" con lo que se nos mostrará una ventana con todos los certificados introducidos en el panel del parámetro global "Certificados CAs".



También podemos introducir o eliminar certificados en los almacenes ya existentes. Para eliminar un certificado lo seleccionamos en la lista "Certificados" y pulsamos sobre el botón "Eliminar Certificado".

5.4.3 LDAPs

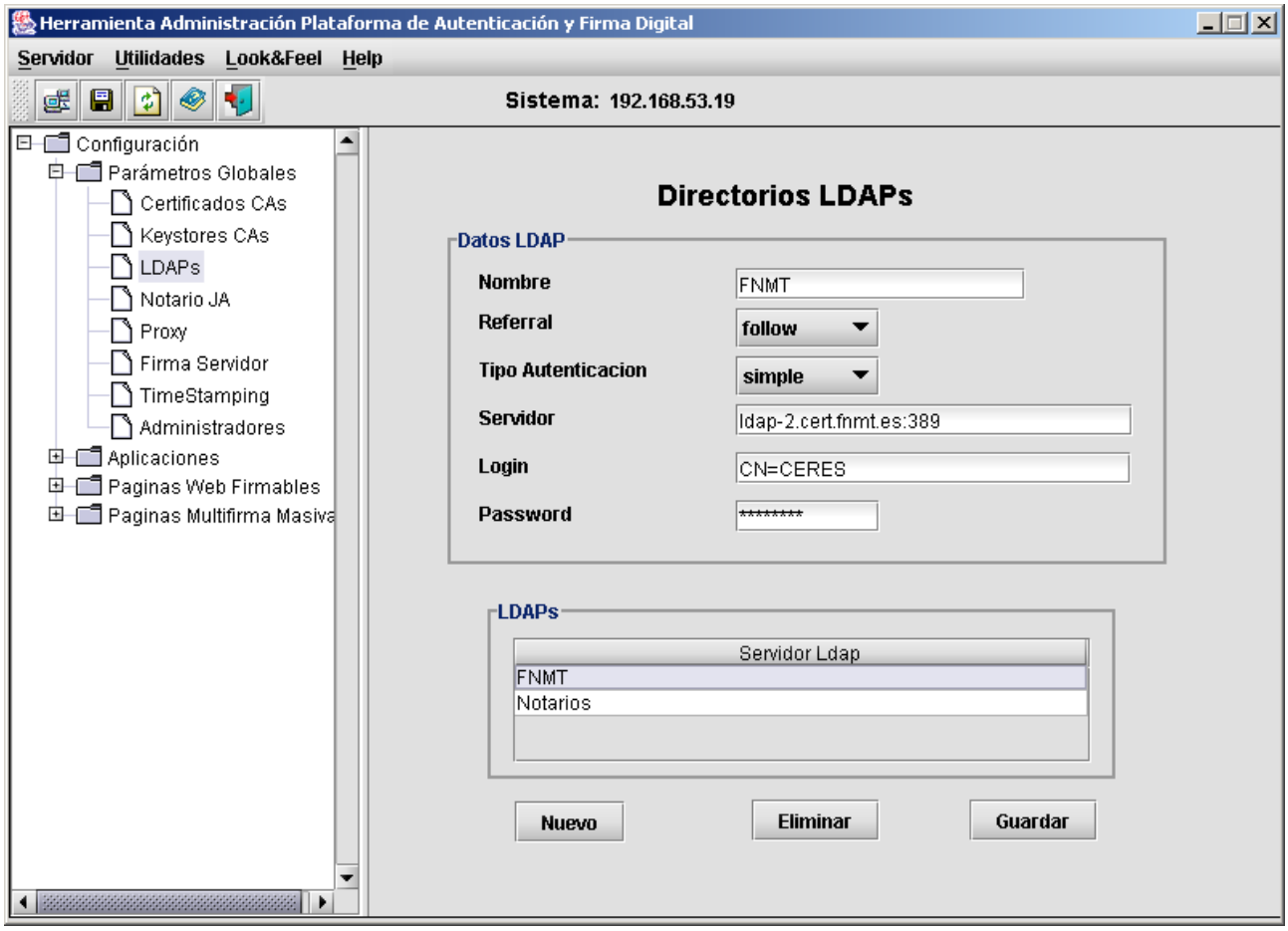
Seleccionando este parámetro podemos administrar las configuraciones de los directorios LDAPs usados anteriormente en la "Validación por LDAP". Como se recordará estas validaciones pertenecen a los certificados existentes definidos en "Certificados CAs".

En esta ventana podemos crear nuevas configuraciones o modificar algunas de las existentes para luego asociarlas a los certificados de CAs como se vio anteriormente.

Cada servidor LDAP tiene la siguiente información:

- Nombre: nombre del servidor.
- Referral: Para la FNMT siempre poner el siguiente valor "follow".
- Tipo Autenticación: Indica si el servidor necesita autenticación. Puede tomar los valores:
  - None: Cuando no necesita autenticación de directorio.
  - Simple: Cuando necesita autenticación, se toman los valores de login y password.

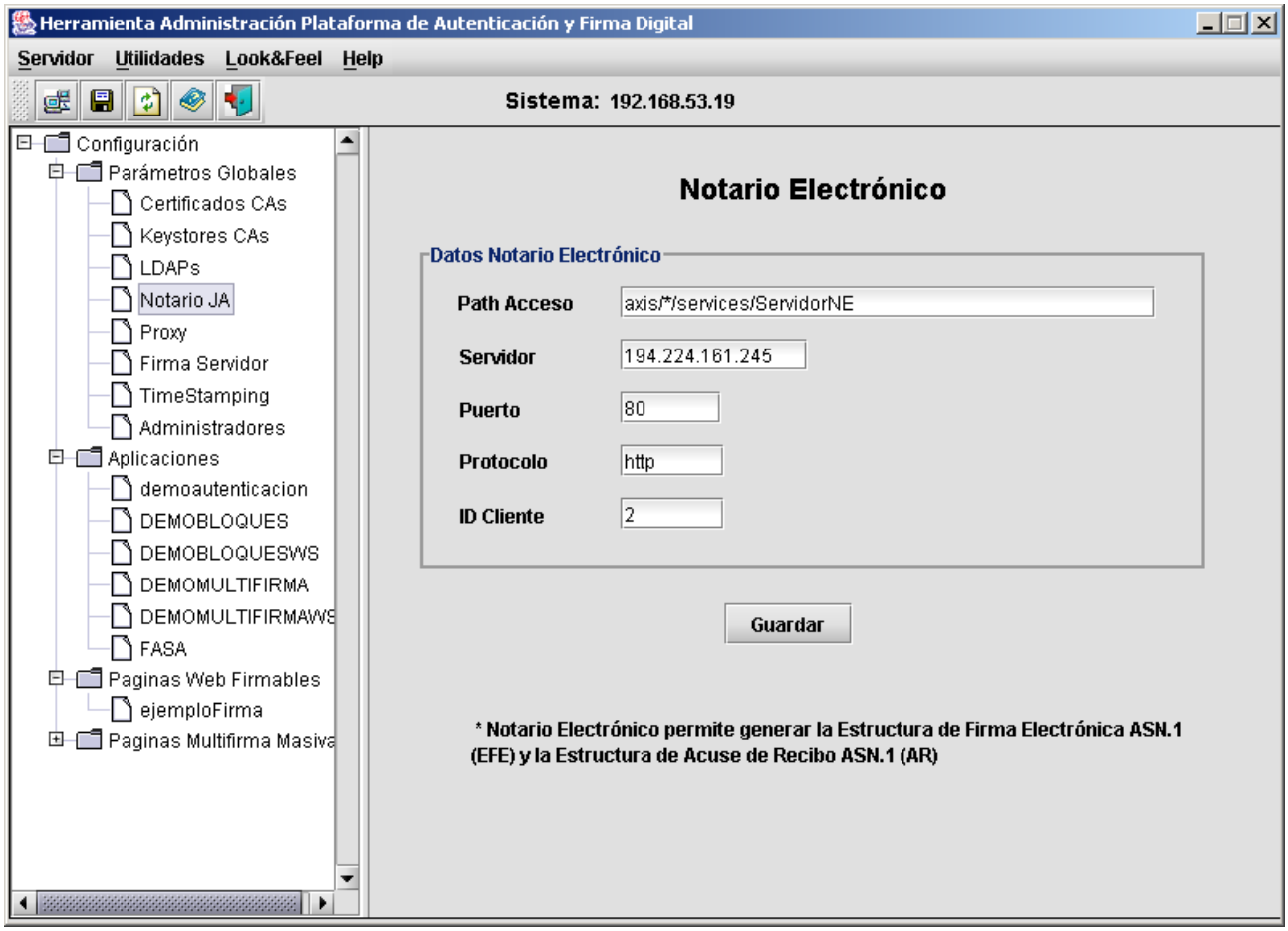
- Servidor: Dirección del servidor de LDAP incluido el puerto de conexión(separado por ":"). Ejem: "ldap.cert.fnmt.es:389".
- Login: Nombre del usuario cuando se necesita autenticación.
- Password: password del usuario.



En la lista inferior nos aparecen todos los LDAPs existentes y seleccionando alguno se nos mostrarán los datos correspondientes a dicho LDAP.

5.4.4 Notario JA

Este parámetro nos permite configurar el acceso al Notario Electrónico, el cual permite a las aplicaciones, paginas web y paginas multifirma masiva poder utilizar las Estructura de Firma Electrónica ASN.1 (EFE) y la Estructura de Acuse de Recibo ASN.1 (AR). Ver los documentos relacionados para comprender que son dichas estructuras.

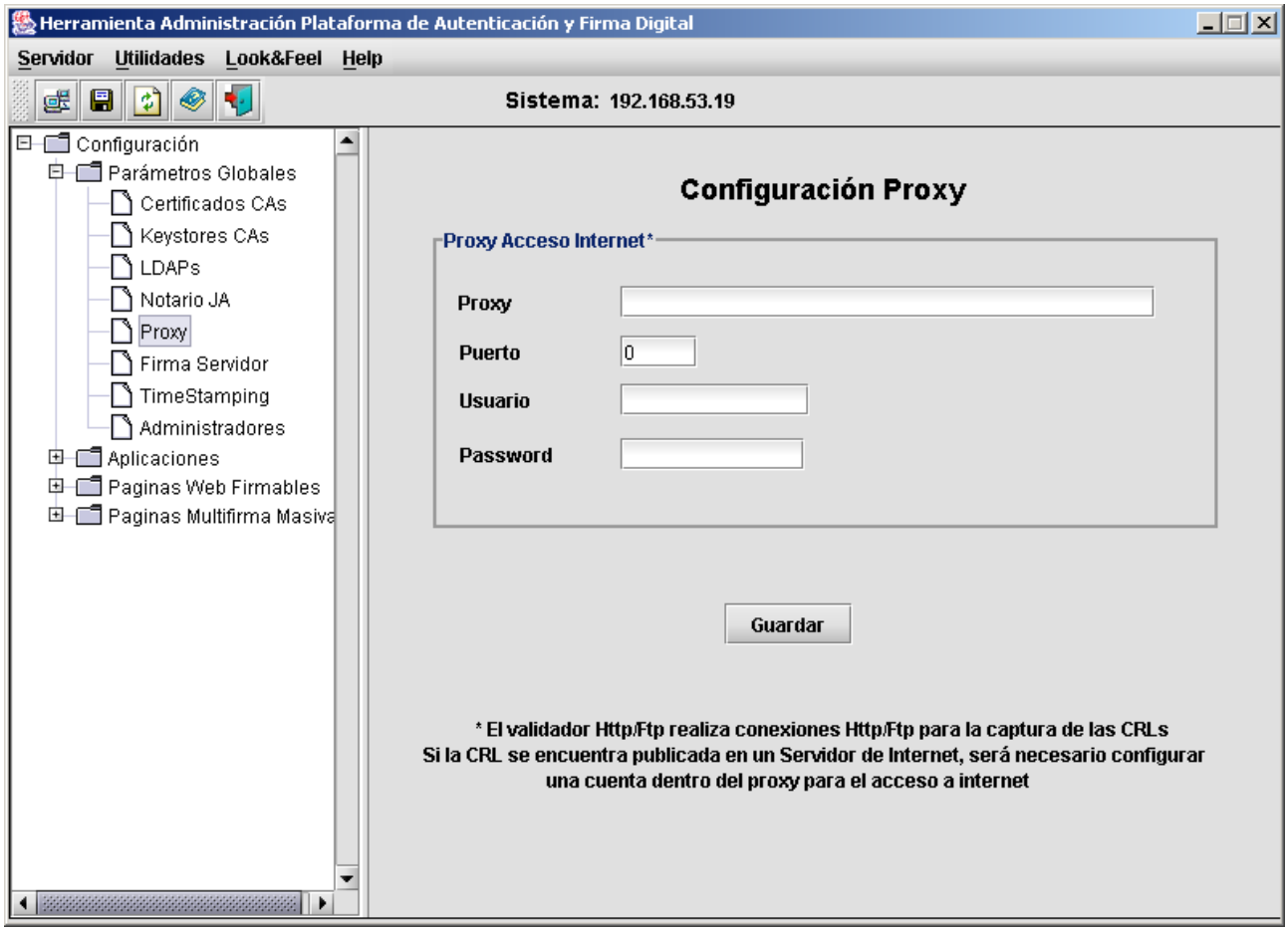


Los parámetros necesarios son:

- Path acceso. Path de acceso al webservice de notario. (Por defecto viene configurada la del Notario de la Junta).
- Servidor. Indica la dirección IP o nombre del Servidor de Notario Electrónico.
- Puerto. Indica el puerto para el protocolo de comunicación con el Servidor de Notario Electrónico. Será *80* para *http* y *443* para *https*.
- Protocolo. Indica el protocolo de comunicación con el Servidor de Notario Electrónico *http* o *https*.
- ID Cliente. Identificador utilizado por el notario para saber que cliente está haciendo la petición. Cada Consejería de la Junta de Andalucía tendrá un identificador único proporcionado por la Consejería de Justicia y Administración Pública que serán el que deban utilizar.

5.4.5 Proxy

En este parámetro global se incluye la información necesaria para la configuración del servidor proxy de acceso a Internet, empleado en los mecanismos de "Validación por http/ftp".

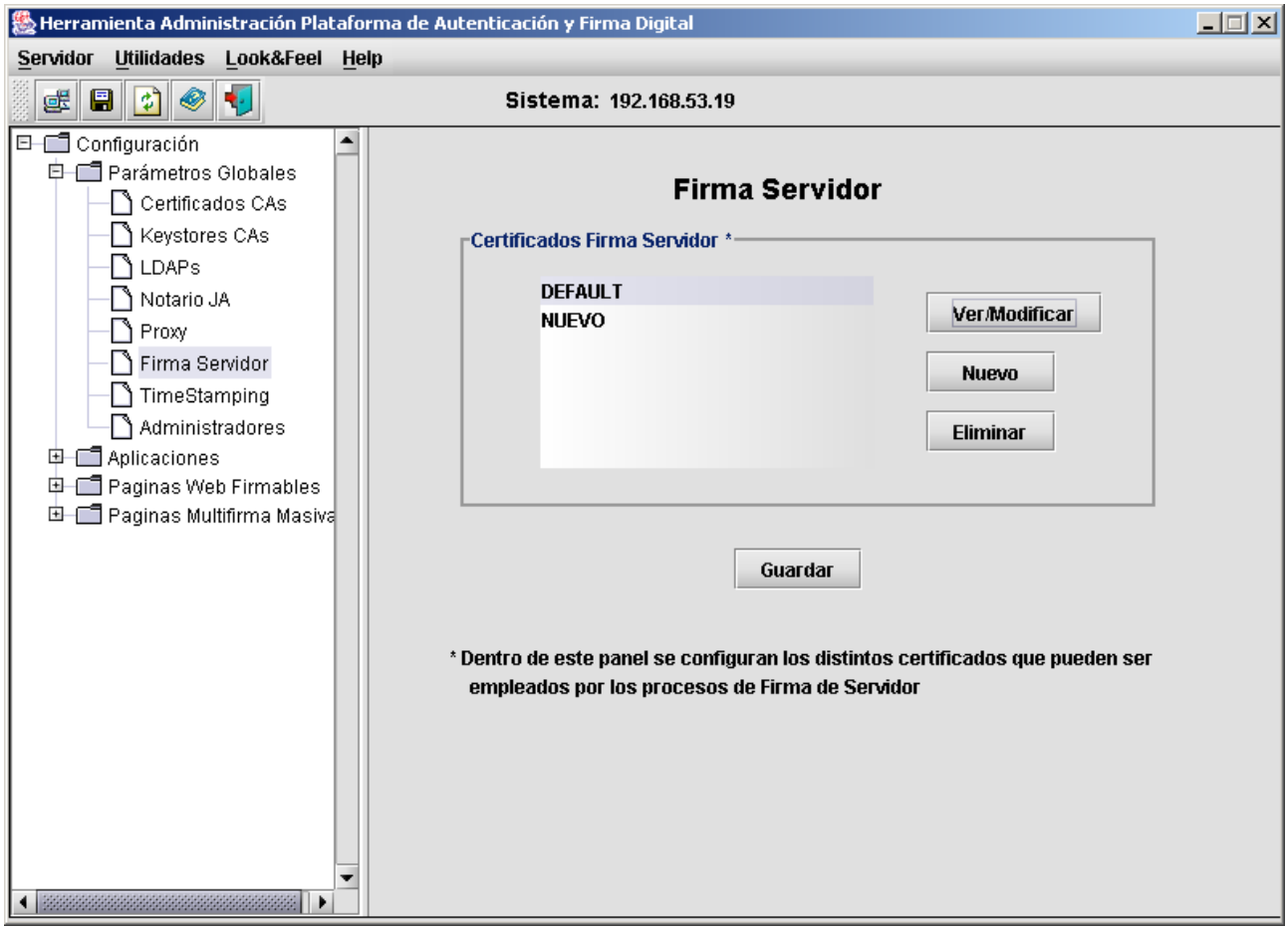


Los datos necesarios son:

- Proxy. Dirección IP o nombre del Proxy.
- Puerto. Indica el puerto para el acceso al Proxy.
- Usuario. Usuario autorizado para utilizar el Proxy.
- Password. Contraseña del usuario.

5.4.6 Firma Servidor

En el panel de este parámetro global podemos configurar los distintos certificados que pueden ser utilizados en los procesos de Firma de Servidor, tanto de las "Aplicaciones" como de las "Paginas de Multifirma Masiva".



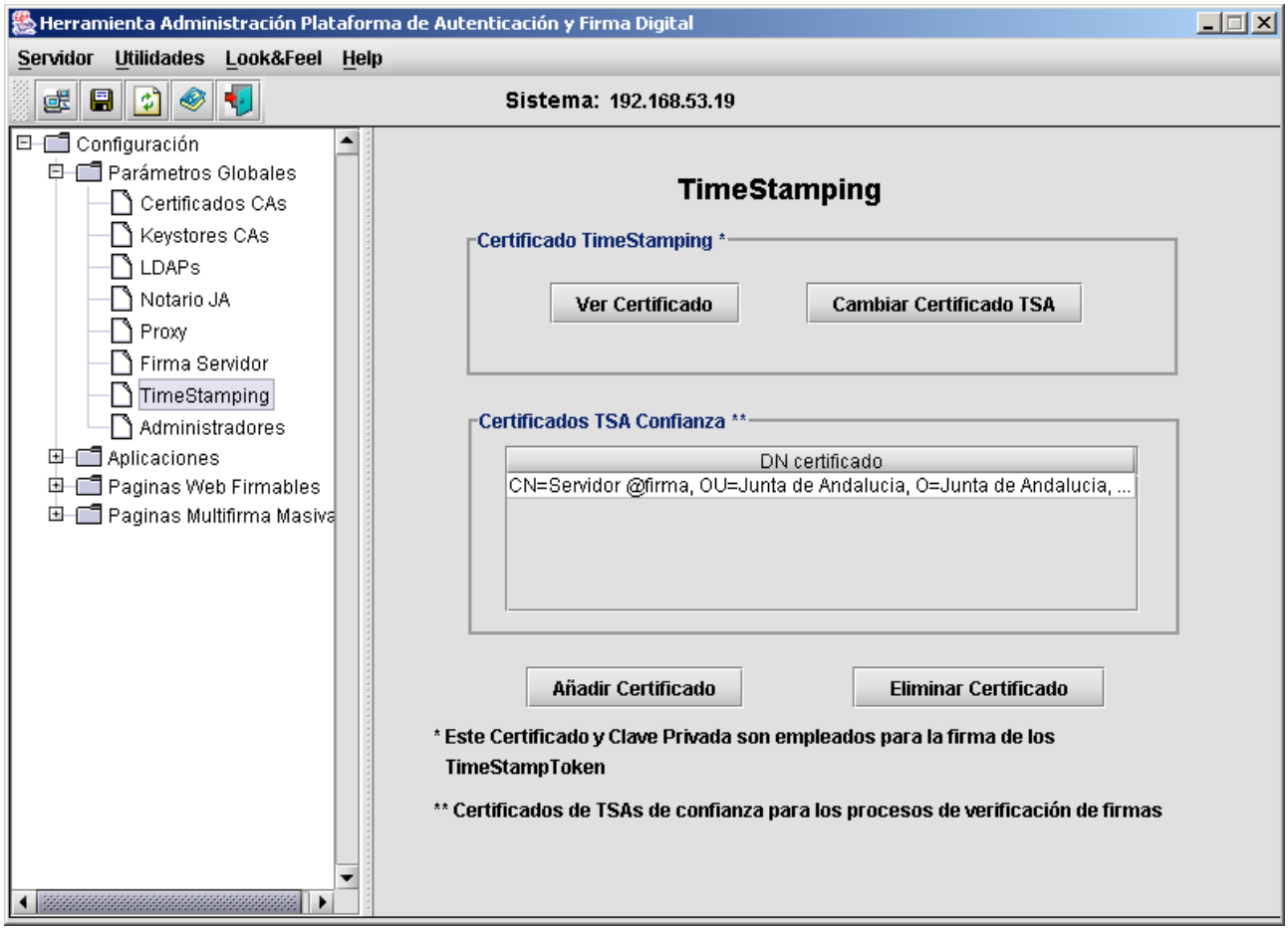
En el panel vemos una lista con los identificadores asociados a los certificados para realizar Firmas de Servidor. Estos identificadores serán los utilizados por las "Aplicaciones" y "Paginas Multifirma Masiva".

Si seleccionamos un identificador y pulsamos el botón "Ver/Modificar" se nos mostrará la siguiente ventana, donde podremos cambiar el identificador, establecer un nuevo certificado o ver la información del certificado asociado.

NOTA: Los certificados deberán venir en archivos con el formato .p12 .

5.4.7 TimeStamping

En el panel de este parámetro global podemos configurar el certificado utilizado por la TSA local para firmar los token de TimeStamping, así como un keystore con los certificados de confianza para verificar firmas con TimeStampings externos.



Certificado TimeStamping

Es el certificado, con clave privada, que se emplea para firma los token de TimeStamp generados por la TSA interna integrada en el servidor de @firma.

- **Ver Certificado:** Pulsando este botón podemos ver información sobre el certificado utilizado actualmente.
- **Cambiar Certificado TSA:** Pulsando este botón podemos cambiar el certificado. Nos mostrará un navegador donde deberemos seleccionar un archivo en formato.p12.

Certificados TSA Confianza

Es un almacén de certificados donde deberán estar los certificados de las TSA externas en las que confiamos, estos certificados se utilizarán para verificar firmas que contengan TimeStamp. Un TimeStamp no deja de ser otra firma y debemos de comprobar que se ha realizado por una TSA en la que confiamos.

- **Añadir Certificado:** Pulsando este botón nos saldrá un navegador donde elegir un archivo que contenga un certificado.

- **Eliminar Certificado:** Eliminara del almacén todos los certificados seleccionados en la lista. Debe de haber algún certificado seleccionado.

5.4.8 Administradores

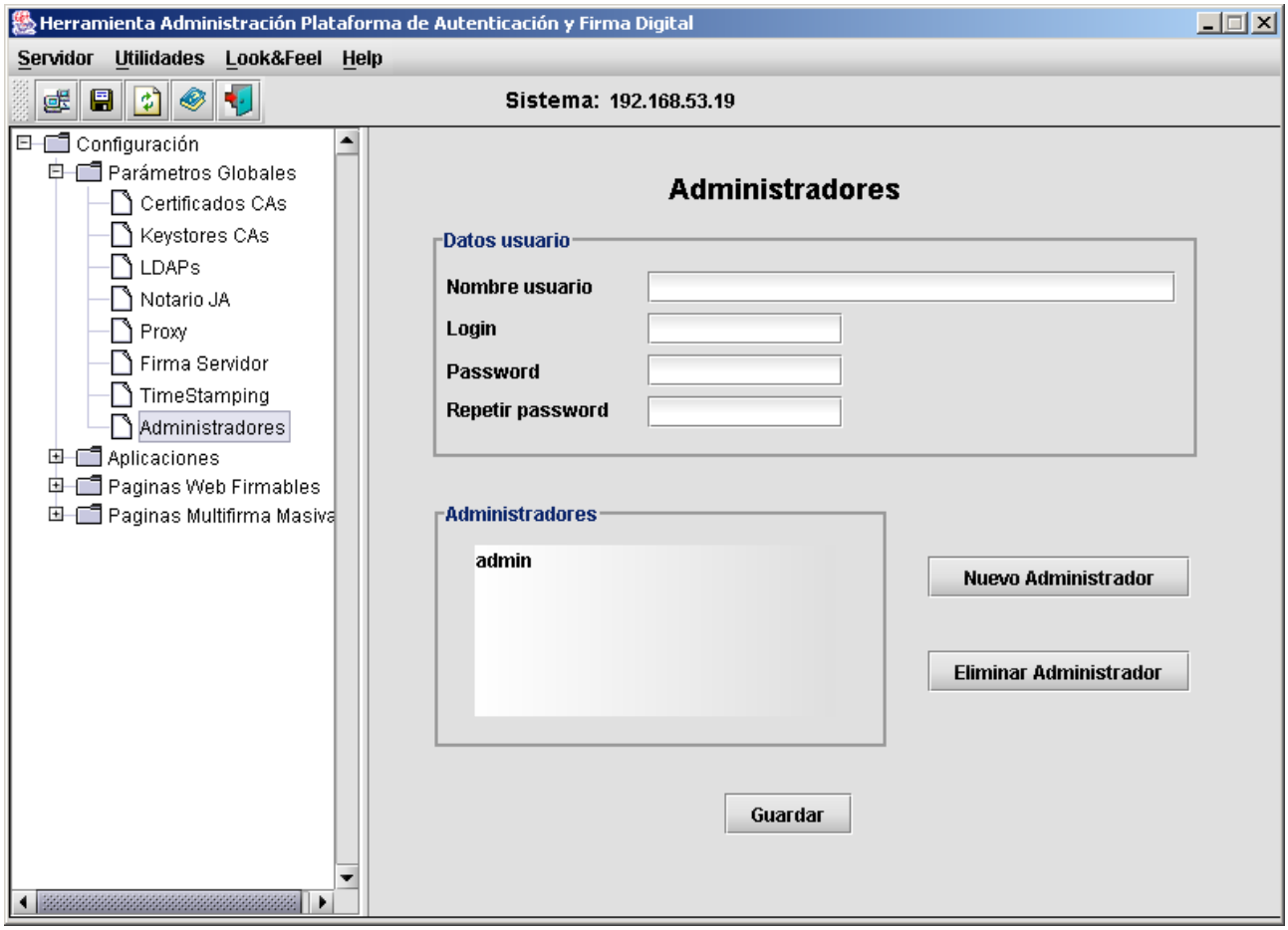
Seleccionando esta opción podemos administrar a los usuarios que tienen permiso para poder entrar en la Herramienta de Administración y administrar el Servidor de @firma al que estamos actualmente conectado.

Los datos de un usuario administrador son:

- **Nombre usuario:** Nombre descriptivo para información únicamente.
- **Login:** Nombre del usuario utilizado para la autenticación.
- **Password:** clave del usuario.
- **Repetir Password:** repetición de la clave para comprobar que es correcta.

NOTA: Es importante cambiar la clave del usuario "admin" o incluso crearse otro usuario la primera vez que se entre a administrar un nuevo servidor de @firma.

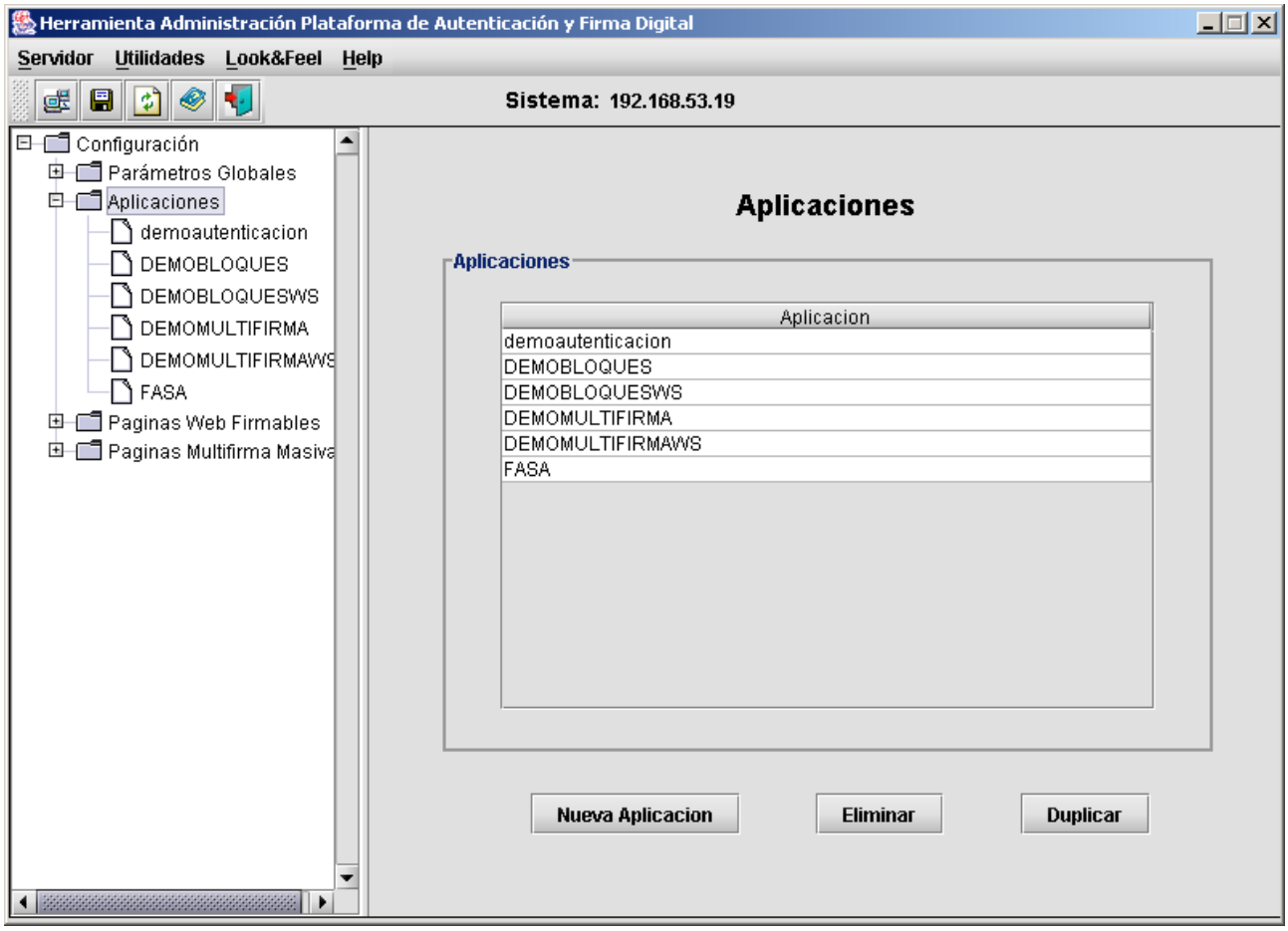
NOTA: Es importante que exista al menos un usuario administrador o no se podrá entrar en la Herramienta de Administración.


Herramienta Administración Plataforma de Autenticación y Firma Digital
Servidor
Utilidades
Look&Feel
Help
Sistema: 192.168.53.19
Configuración
Parámetros Globales
Certificados CAs
Keystores CAs
LDAPs
Notario JA
Proxy
Firma Servidor
TimeStamping
Administradores
Aplicaciones
Paginas Web Firmables
Paginas Multifirma Masiva
Administradores
Datos usuario
Nombre usuario
Login
Password
Repetir password
Administradores
admin
Nuevo Administrador
Eliminar Administrador
Guardar

5.5 Aplicaciones

En esta rama del árbol se encuentra la configuración de todas las aplicaciones de Autenticación y de Firma de Ficheros, en todas sus modalidades (Ver Manual de Programador del módulo Firma de Ficheros TI-20-1074-PFF-001).

Si seleccionamos la carpeta "Aplicaciones" veremos una ventana como la siguiente:



En esta ventana vemos en el centro una lista con los identificadores de todas las "aplicaciones" existentes en le sistema. Vemos que coinciden con las hojas que hay debajo de la carpeta "Aplicaciones" en el árbol de la izquierda. Si hacemos doble click sobre algún elemento de la lista o seleccionamos una de las hojas del árbol se nos mostrará un panel con la configuración de la "aplicación" seleccionada (Ver: 5.5.3 Configuración de una Aplicación).

Esta ventana mediante los botones inferiores nos permite administrar de forma general las "aplicaciones".

5.5.1 Crear una Aplicación.

Hay dos formas de crear una nueva aplicación:

1.- Mediante el botón "Nueva Aplicación", crea una aplicación con los valores por defecto.

2.- Mediante el botón "Duplicar", siempre y cuando haya alguna aplicación seleccionada en la lista, crea una nueva aplicación con los mismos valores que la seleccionada excepto el nombre.

En cualquiera de los dos casos se mostrará un panel con la configuración de la aplicación (se explican más abajo) y el botón "Guardar", para que la creación tenga efecto habrá que pulsar este botón. Si todo es correcto aparecerá una nueva hoja debajo de la carpeta "Aplicaciones" con el nombre de la nueva aplicación.

NOTA: Tener en cuenta que los cambios se realizan siempre en local, para que tengan efecto en el servidor hay que mandarle la información, ya sea con le menú "Servidor\Mandar Configuracion Servidor" o con el botón correspondiente de la barra de herramientas.

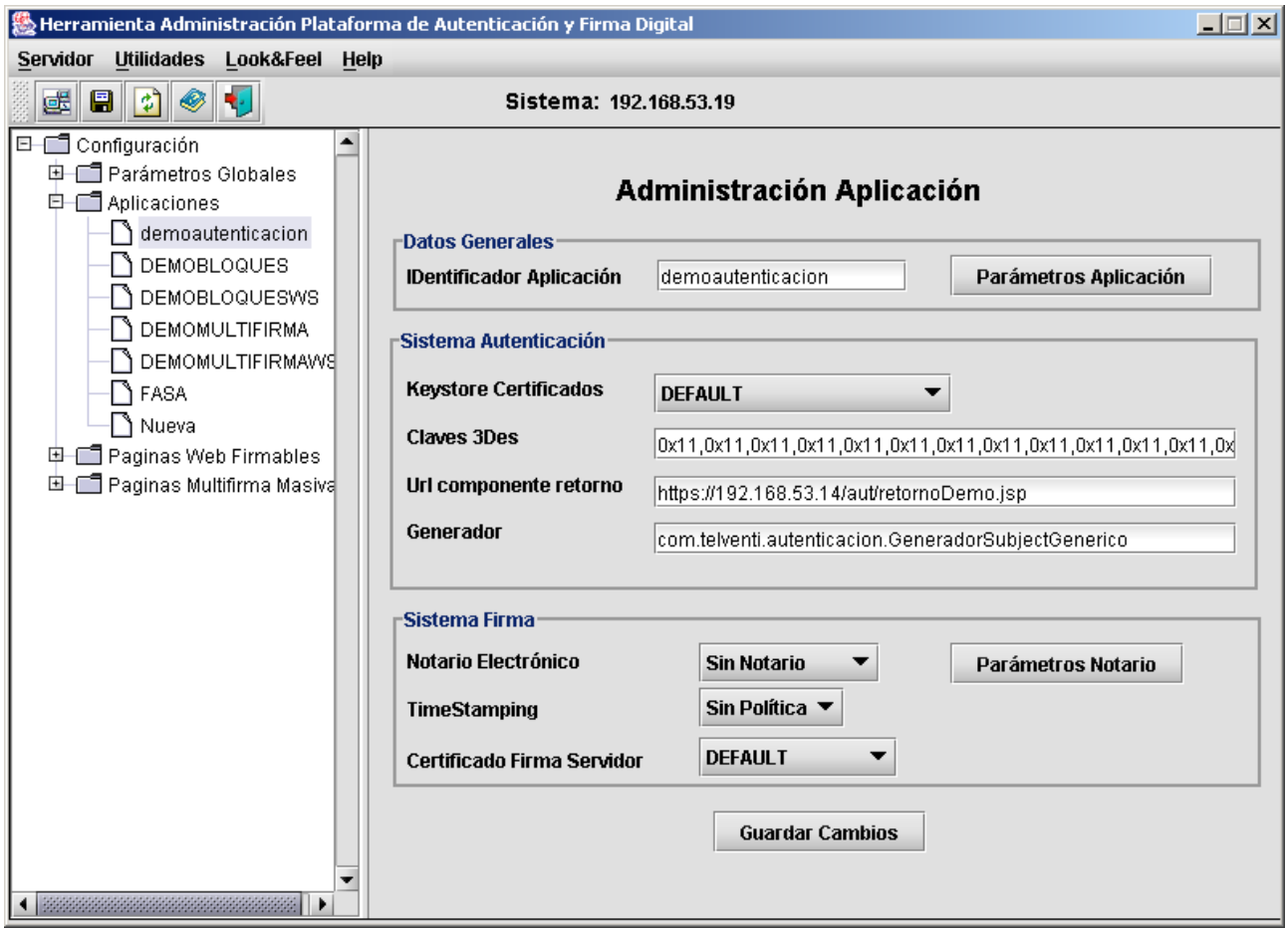
5.5.2 Eliminar una Aplicación.

Para eliminar una aplicación lo único que hay que hacer es seleccionarla en la lista que aparece cuando seleccionamos la carpeta "Aplicaciones" en el árbol de configuración y pulsar el botón "Eliminar". Tener cuidado no pide confirmación de la eliminación.

NOTA: Tener en cuenta que los cambios se realizan siempre en local, para que tengan efecto en el servidor hay que mandarle la información, ya sea con le menú "Servidor\Mandar Configuracion Servidor" o con el botón correspondiente de la barra de herramientas.

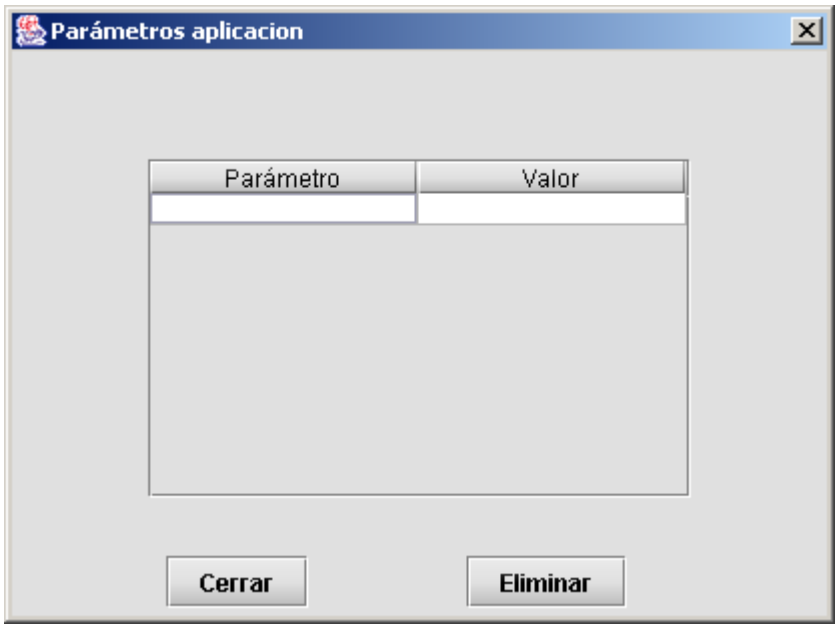
5.5.3 Configuración de una Aplicación.

Cuando seleccionamos una "aplicación" nos aparece el panel "Administración Aplicación" con la configuración de dicha aplicación.



Datos Generales:

- **Identificador Aplicación:** Identificador de la aplicación.
- **Parámetros Aplicación:** parámetros específicos para cada aplicación. Es decir, las aplicaciones concretas pueden definir sus propios parámetros de configuración bajo la forma de parejas nombre/valor. Estos parámetros son empleados por los generadores de Subjects programados para cada aplicación en concreto. El generador de Subject Genérico utilizado por la mayoría de aplicaciones no tiene definidos ningún par de valores. Pulsando en el botón se muestra la ventana siguiente:



Sistema Autenticación

- **Keystore Certificados:** Indica el keystore utilizado para verificar los certificados digitales de usuario utilizados en la autenticación y/o firma. (Ver Keystores CAs en Parámetros Globales).

- **Clave 3Des:** Es la clave DES necesaria para encriptar los datos de vuelta en las aplicaciones de autenticación web. Es importante anotar esta clave para distribuirla posteriormente a los desarrolladores que utilicen esta aplicación. La clave puede y ha de ser cambiada con "sensata" frecuencia poniendo especial cuidado es distribuirla a todas aquellas personas que trabajen con la aplicación configurada.

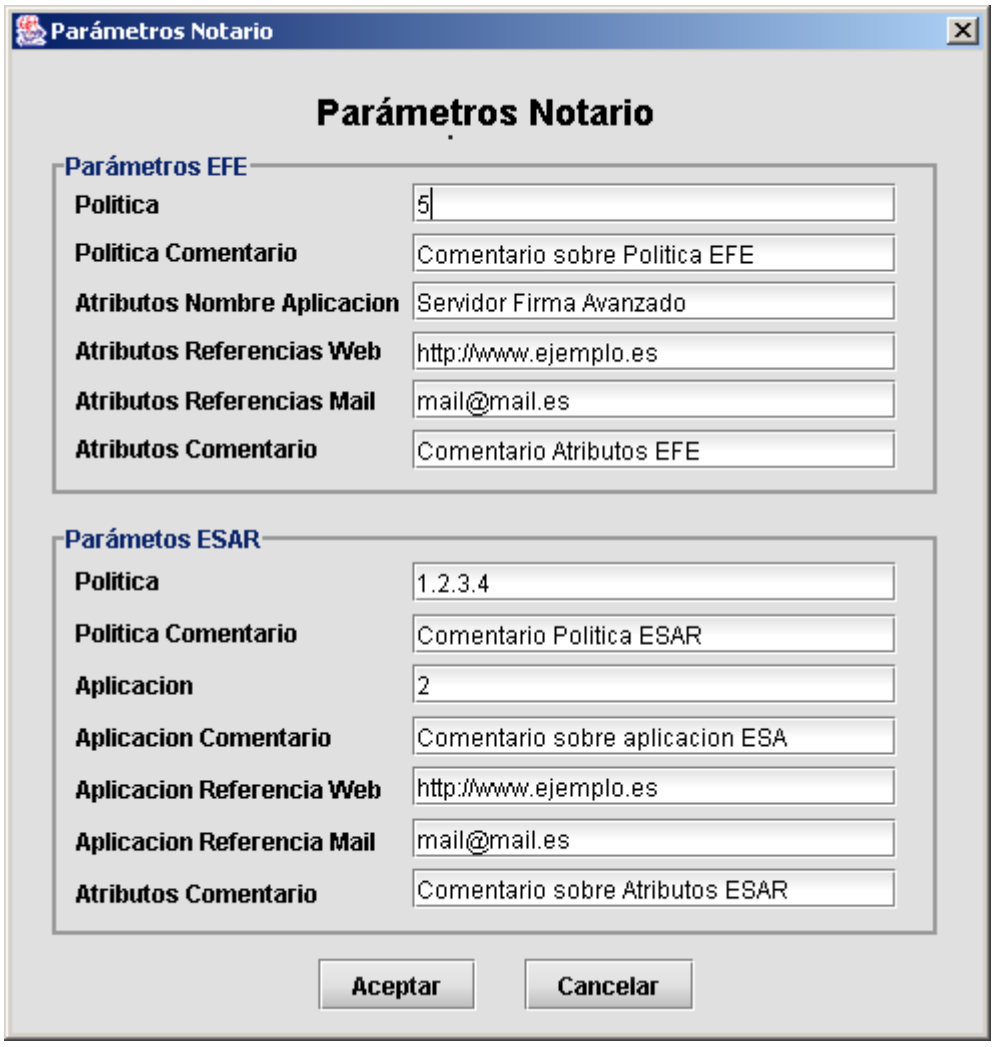
- **URL componente retorno**. Indica la URL del componente que trata los datos de vuelta, y que está ubicado en el servidor de aplicaciones donde se necesite autenticación.

- **Generador**. Es el componente de lógica de negocio desarrollado en Java que ofrece la funcionalidad requerida para una aplicación en concreto, y que ha sido desarrollado según las especificaciones del manual del programador del Módulo de Autenticación. Por defecto, se utiliza el componente"com.telventi.autenticacion.GeneradorSubjectGenerico"

NOTA: Si se quiere configurar una página de error especifica para la aplicación ver el Manual del Programador del Modulo de Autenticacion (TI-20-1074-MPA-001)

Sistema Firma

- Notario Electrónico: Indica si queremos utilizar o no Firma Avanzada y el tipo de Firma.
  - Sin Notario: Servidor Básico. Generación PKCS#7.
  - EFE: Servidor Avanzado. Genera la estructura PKCS#7, y la Estructura de Firma Electrónica ASN.1 con TimeStamp de Servidor de Notario Electrónico.
  - EFE+AR: Servidor Avanzado. Genera la estructura PKCS#7, la Estructura de Firma Electrónica ASN.1 con TimeStamp de Servidor de Notario Electrónico y la Estructura de Acuse de Recibo ASN.1 de Servidor de Notario Electrónico.
  - EFE(Hora local): Servidor Avanzado. Genera la estructura PKCS#7 y la Estructura de Firma Electrónica ASN.1 con TimeStamp local del Servidor de Firma.
- Parámetros Notario: En caso de utilizar Firma Avanzada deberemos configurar los parámetros del Notario Electrónico (Ver anexo). La siguiente figura muestra dichos parámetros:



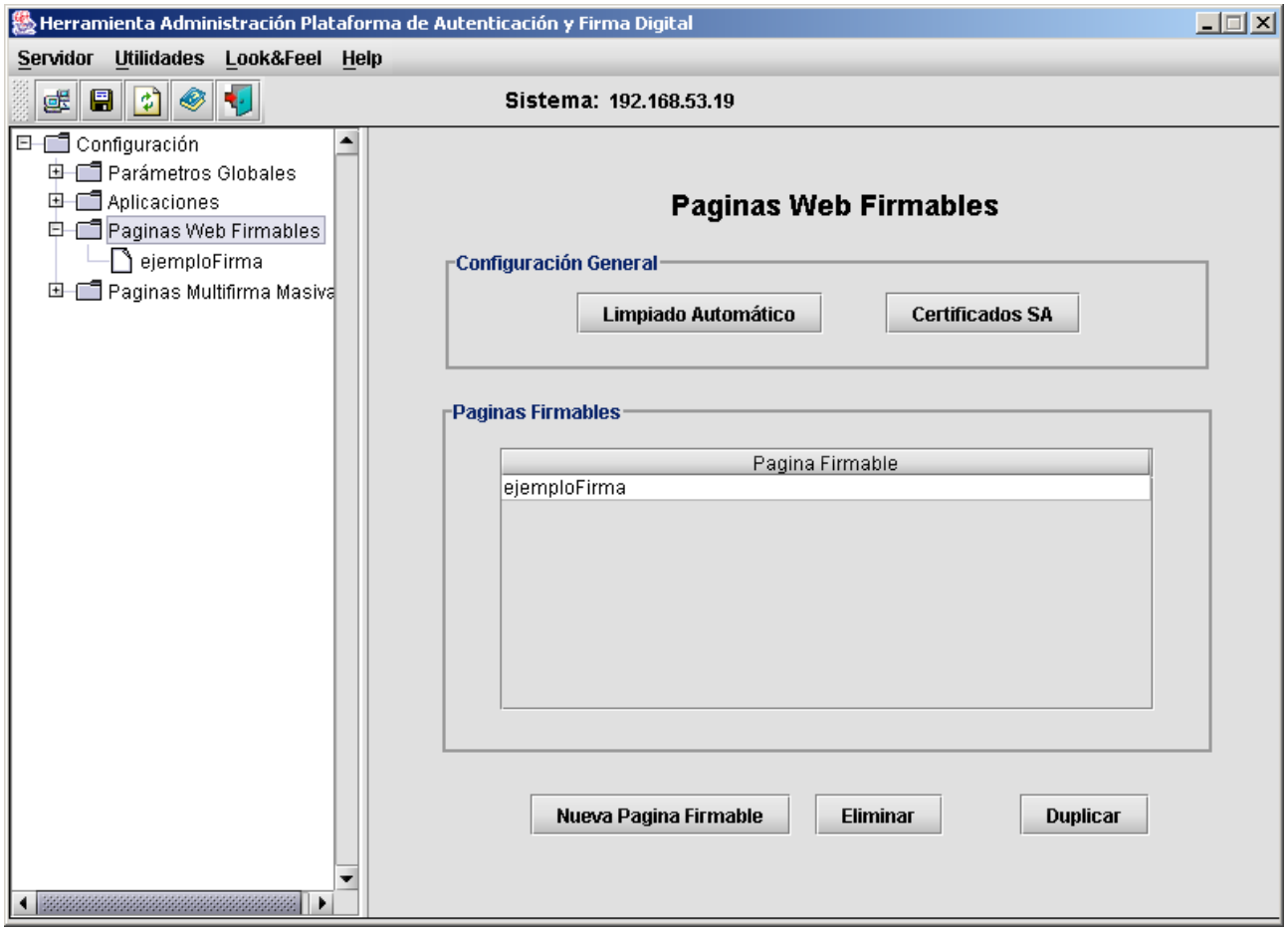
- **TimeStamping:** En el caso de no poder utilizar el Notario de la Junta y querer utilizar la TSA local de @firma, se configura a la aplicación con la "Política 1". **En el caso de utilizar el Notario electrónico de la Junta se debe desactivar este parámetro con la opción "Sin Política".**

- **Certificado Firma Servidor**: Indica el Certificado Digital que se utilizará para firmar los documentos cuando se solicite una Firma de Servidor. (ver apartado 5.4.6 Firma de Servidor).

5.6 Páginas Web Firmables

En esta rama del árbol se encuentra la configuración de todas las aplicaciones de Firma y Multifirma Web. (Ver Manual de Programador del módulo Firma de Web TI-20-1074-MPF-001).

Si seleccionamos la carpeta "Paginas Web Firmables" veremos una ventana como la siguiente:

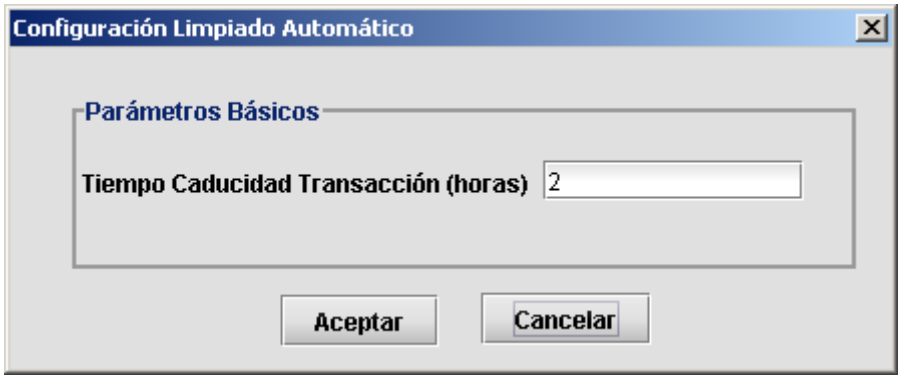


En esta ventana vemos en el centro una lista con los identificadores de todas las "paginas firmables" existentes en le sistema. Vemos que coinciden con las hojas que hay debajo de la carpeta "Paginas Web Firmables" en el árbol de la izquierda. Si hacemos doble click sobre algún elemento de la lista o seleccionamos una de las hojas del árbol se nos mostrará un panel con la configuración de la "pagina web" seleccionada (Ver: Configuración de una Pagina Web Firmable).

Esta ventana mediante los botones inferiores nos permite administrar de forma general las "paginas web firmables".

5.6.1 Limpiado Automático

Cuando se realizan transacciones de firma web incompletas o erróneas, estas deben ser eliminadas de la plataforma, para ello existe un proceso automático que se encarga de limpiarlas. Este proceso se configura mediante el botón "Limpiado Automático":



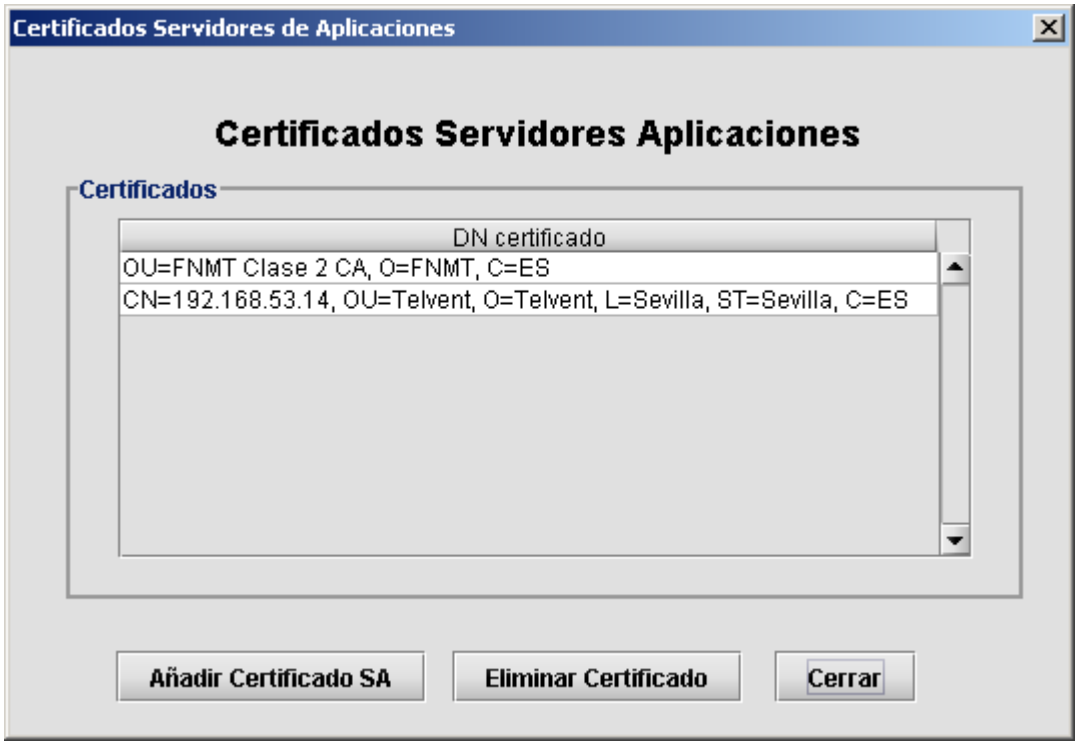
El "Tiempo Caducidad Transacción (horas)" indica el tiempo de permanencia máximo de transacciones incompletas o erróneas en la Base de Datos.

5.6.2 Certificados SA

Para que la plataforma @firma pueda comunicarse con los servidores de aplicaciones, que contienen las paginas que se van ha firmar, mediante https, @firma debe de tener los certificados con la clave pública de dichos servidores de aplicaciones.

Esta utilidad se utiliza para facilitar la gestión de los certificados de los servidores de aplicaciones.

Pulsando en el botón "Certificados SA" aparece la siguiente ventana:



En la ventana se muestra una lista con los certificados de los servidores de aplicaciones existentes en @firma y unos botones para añadir nuevos certificados y eliminar certificados existentes.

Al pulsar sobre el botón "*Añadir Certificado SA*" te muestra un navegador para que elijas el archivo que contiene el certificado. NOTA: el certificado debe de venir en formato DER X.509, y sólo ha de contener la clave pública para establecer conexiones SSL. La clave privada del servidor de aplicaciones no es necesaria.

Para eliminar uno o varios certificados hay que seleccionarlos en la lista y pulsar el botón "*Eliminar Certificado*".

NOTA: Para que los cambios realizados en esta ventana tengan efecto hay que parar y arrancar de nuevo el servidor de @firma.

5.6.3 Crear una Pagina Web Firmable.

Hay dos formas de crear una nueva pagina firmable:

1.- Mediante el botón "Nueva Pagina Firmable", crea una pagina firmable con los valores por defecto.

2.- Mediante el botón "Duplicar", siempre y cuando haya alguna pagina firmable seleccionada en la lista, crea una nueva pagina firmable con los mismos valores que la seleccionada excepto el nombre.

En cualquiera de los dos casos se mostrará un panel con la configuración de la pagina firmable (apartado 5.6.5 Configuración de una página firmable) y el botón "Guardar", para que la creación tenga efecto habrá que pulsar este botón. Si todo es correcto aparecerá una nueva hoja debajo de la carpeta "Paginas Web Firmables" con el nombre de la nueva pagina firmable.

NOTA: Tener en cuenta que los cambios se realizan siempre en local, para que tengan efecto en el servidor hay que mandarle la información, ya sea con le menú "Servidor\Mandar Configuración Servidor" o con el botón correspondiente de la barra de herramientas.

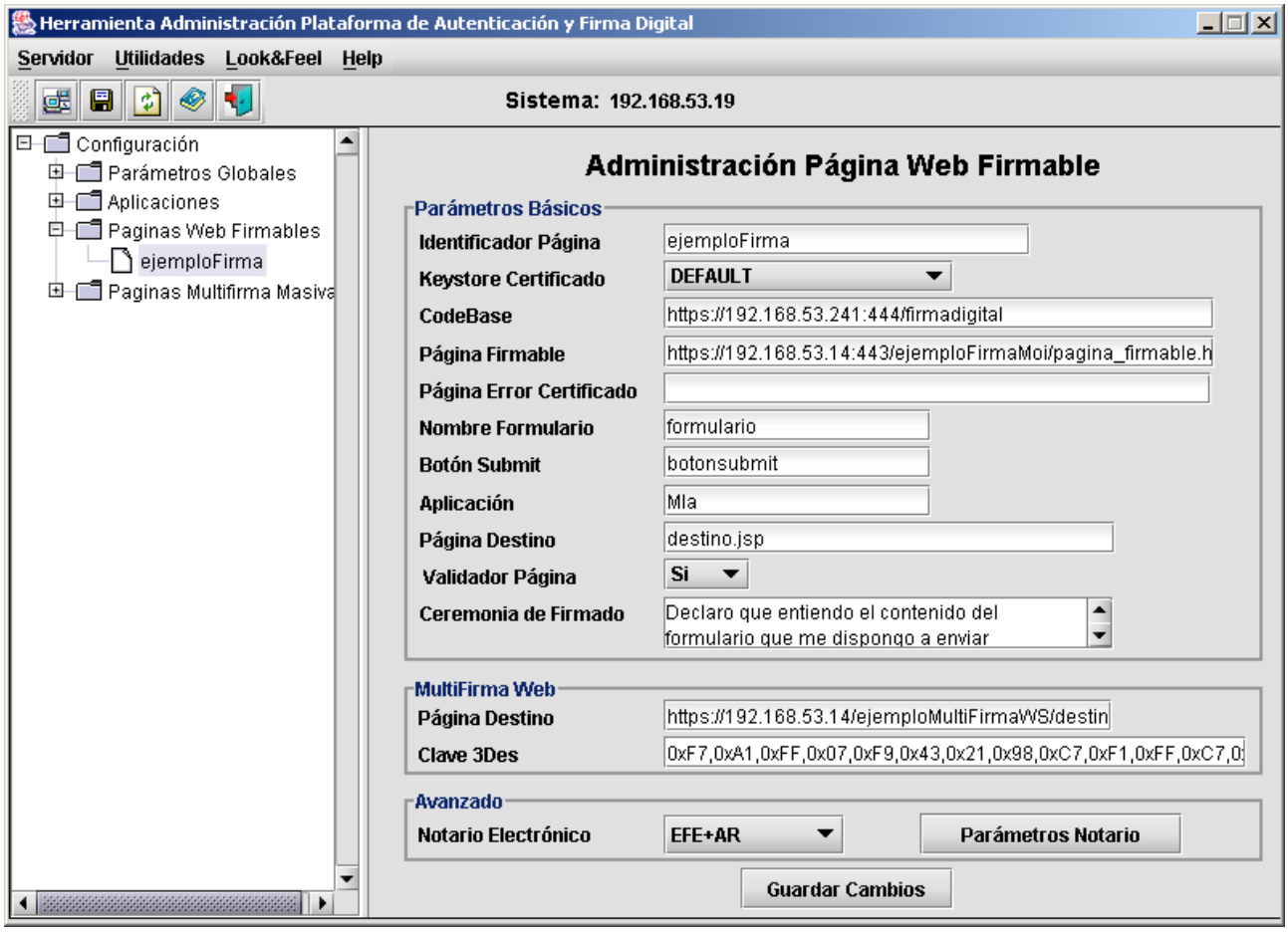
5.6.4 Eliminar una Pagina Web Firmable.

Para eliminar una pagina firmable lo único que hay que hacer es seleccionarla en la lista que aparece cuando seleccionamos la carpeta "Paginas Web Firmables" en el árbol de configuración y pulsar el botón "Eliminar". Tener cuidado no pide confirmación de la eliminación.

NOTA: Tener en cuenta que los cambios se realizan siempre en local, para que tengan efecto en el servidor hay que mandarle la información, ya sea con le menú "Servidor\Mandar Configuración Servidor" o con el botón correspondiente de la barra de herramientas.

5.6.5 Configuración de una Pagina Web Firmable.

Cuando seleccionamos una "pagina firmable" nos aparece el panel "Administración Página Web Firmable" con la configuración de dicha aplicación.



Parámetros Básicos:

- **Identificador Página:** Identificador de la aplicación de firma y/o multifirma web.
- **Keystore Certificado:** Indica el keystore utilizado para verificar los certificados digitales de usuario utilizados en la firma. (Apartado 5.4.2 Keystores CAs en Parámetros Globales).
- **CodeBase:** https://*hostname:port*/firmadigital. Indica la url lógica base del módulo de firma, que será la url de la **Fachada**. Será necesario establecer el nombre de la **Fachada** (hostname) y puerto (port). No debe colocarse la "/" del final. NOTA: mantener */firmadigital* como nombre lógico.
- **Pagina Firmable**: Nombre de página web que deseamos hacer firmable incluida su ruta lógica completa http. Ej.: http://<hostname>:<port>/ruta…./página.html

- **Pagina Error Certificado:** URL completa de la página de error que toma el control cuando el usuario presenta un certificado no valido.

- **Nombre Formulario:** Nombre del formulario de la página que deseamos hacer firmable.

- **Botón Submit:** Nombre del botón de SUBMIT sobre el que opera el proceso de firmado.

- **Aplicación:** Nombre de la aplicación a la cual pertenece la página firmable actual.

- **Pagina Destino:** Nombre de "página destino firmado" de la página firmable.

- **Validador Página:** Indica si se usa un validador para comprobar que la página es correcta, cumple las especificaciones para ser firmable, antes de iniciar el proceso de firma.

- **Ceremonia de Firmado:** . Indica el texto que se muestra al cliente cuando se dispone a firmar.

Multifirma Web:

- **Pagina Destino:** URL completa de la página de retorno de una aplicación de multifirma. Este atributo solo es necesario si se va a realizar multifirma.

- **Clave 3Des:** Es la clave DES necesaria para encriptar el identificador de transacción para poder llamar al componente web que devuelve la página original con los datos y adjuntos firmados. Es importante anotar esta clave para distribuirla posteriormente a los desarrolladores que utilicen esta aplicación. La clave puede y ha de ser cambiada con "sensata" frecuencia poniendo especial cuidado es distribuirla a todas aquellas personas que trabajen con la aplicación configurada.

Avanzado

- **Notario Electrónico**: Indica si queremos utilizar o no Firma Avanzada y el tipo de Firma .

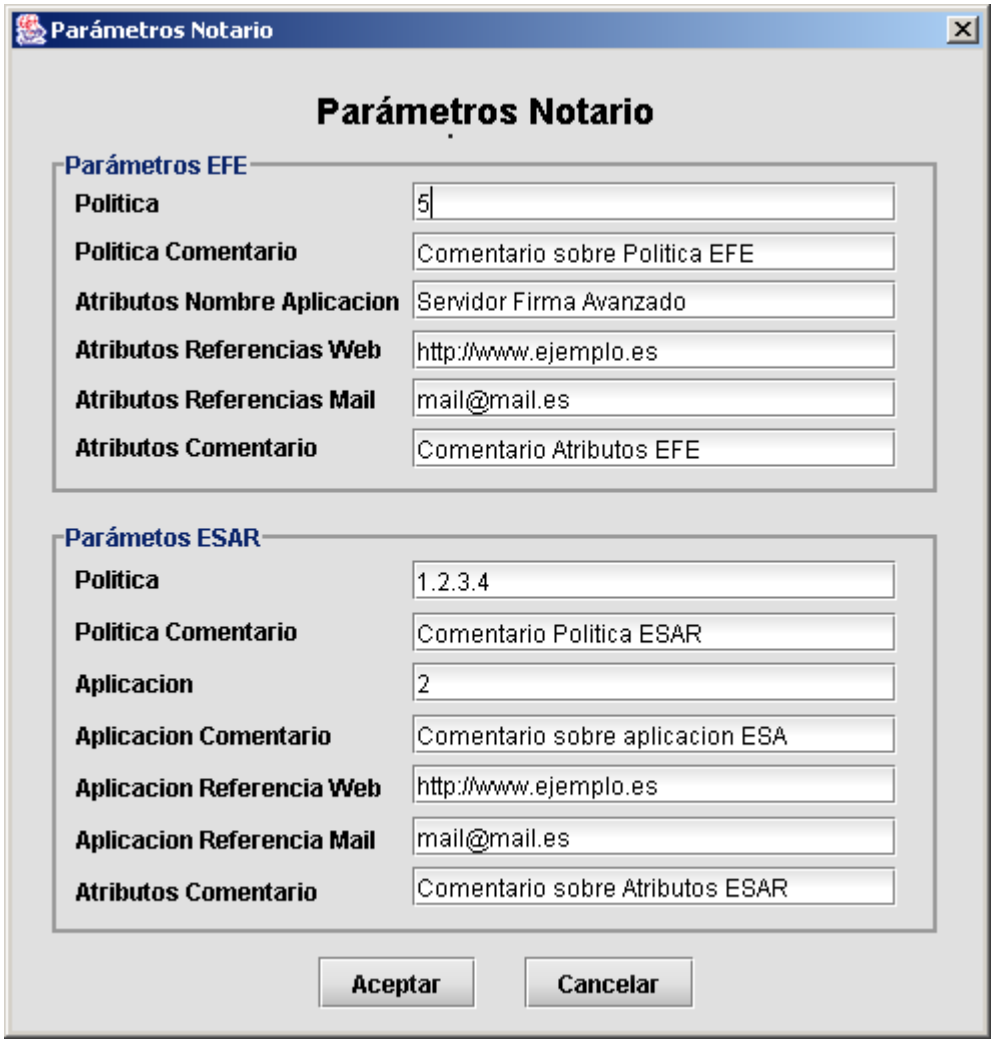
  - **Sin Notario**: Servidor Básico. Generación PKCS#7.

  - **EFE**: Servidor Avanzado. Genera la estructura PKCS#7, y la Estructura de Firma Electrónica ASN.1 con TimeStamp de Servidor de Notario Electrónico.

  - **EFE+AR**: Servidor Avanzado. Genera la estructura PKCS#7, la Estructura de Firma Electrónica ASN.1 con TimeStamp de Servidor de Notario Electrónico y la Estructura de Acuse de Recibo ASN.1 de Servidor de Notario Electrónico.

  - **EFE(Hora local)**: Servidor Avanzado. Genera la estructura PKCS#7 y la Estructura de Firma Electrónica ASN.1 con TimeStamp local del Servidor de Firma.

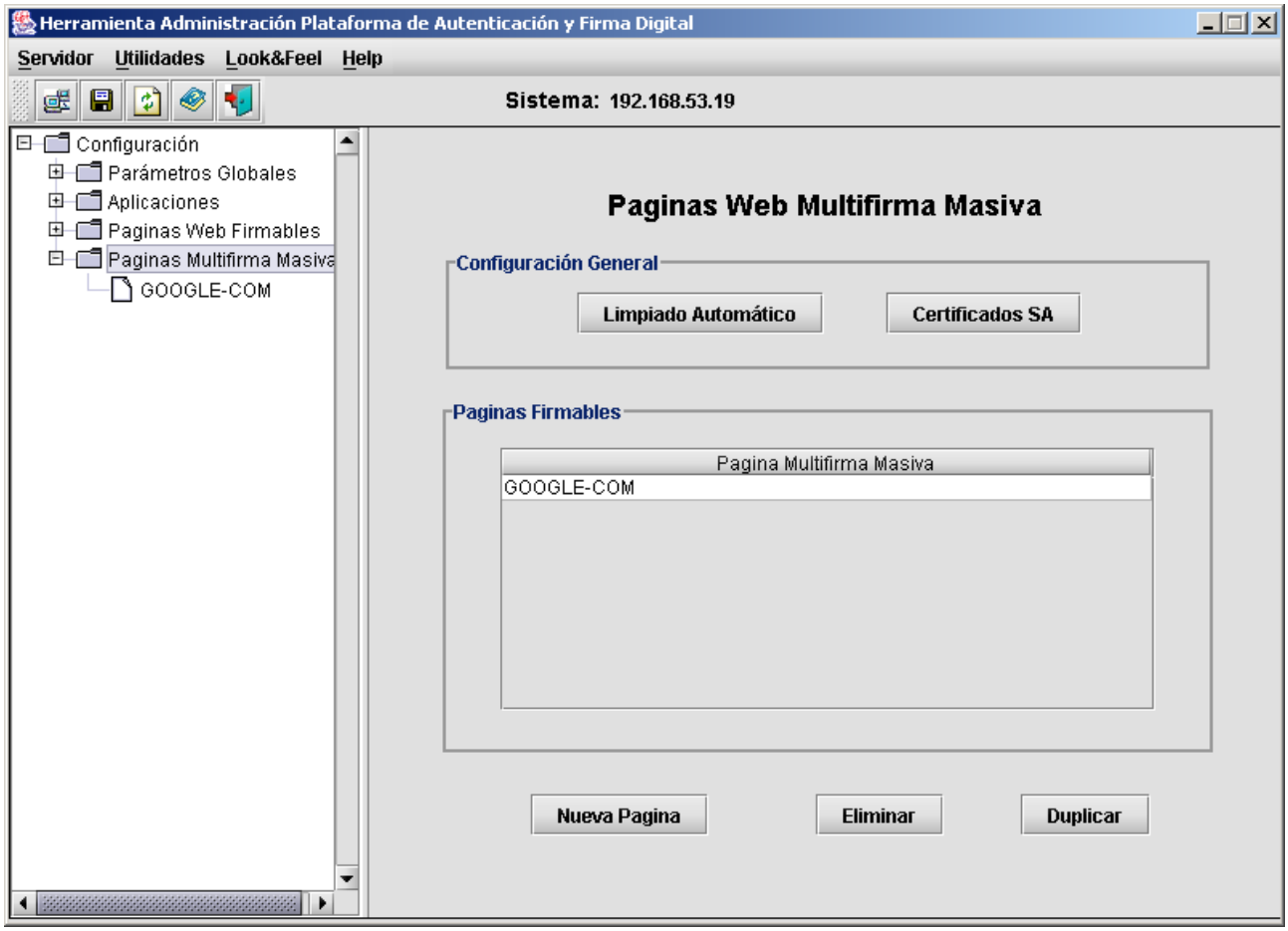
- Parámetros Notario: En caso de utilizar Firma Avanzada deberemos configurar los parámetros del Notario Electrónico (Ver anexo). La siguiente figura muestra dichos parámetros:



5.7 Páginas Multifirma Masiva

En esta rama del árbol se encuentra la configuración de todas las aplicaciones de Multifirma Masiva. (Ver Manual de Programador del módulo Firma de Web TI-20-1074-MPF-001).

Si seleccionamos la carpeta "Paginas Multifirma Masiva" veremos una ventana como la siguiente:

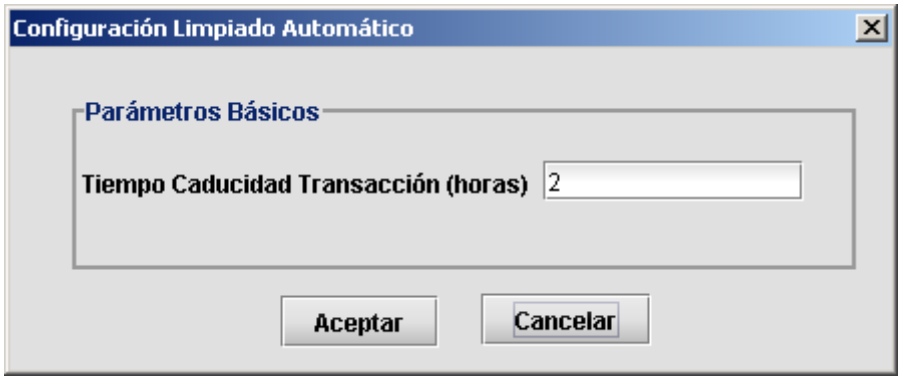


En esta ventana vemos en el centro una lista con los identificadores de todas las "paginas multifirma masiva" existentes en le sistema. Vemos que coinciden con las hojas que hay debajo de la carpeta "Paginas Multifirma Masiva" en el árbol de la izquierda. Si hacemos doble click sobre algún elemento de la lista o seleccionamos una de las hojas del árbol se nos mostrará un panel con la configuración de la "pagina multifirma masiva" seleccionada (Apartado 5.7.5 Configuración de una Pagina Multifirma Masiva).

Esta ventana mediante los botones inferiores nos permite administrar de forma general las "paginas multifirma masiva".

5.7.1 Limpiado Automático

Cuando se realizan transacciones de firma web incompletas o erróneas, estas deben ser eliminadas de la plataforma, para ello existe un emonio automático que se encarga de limpiarlas. Mediante el botón "Limpiado Automático" aparece la siguiente ventana:



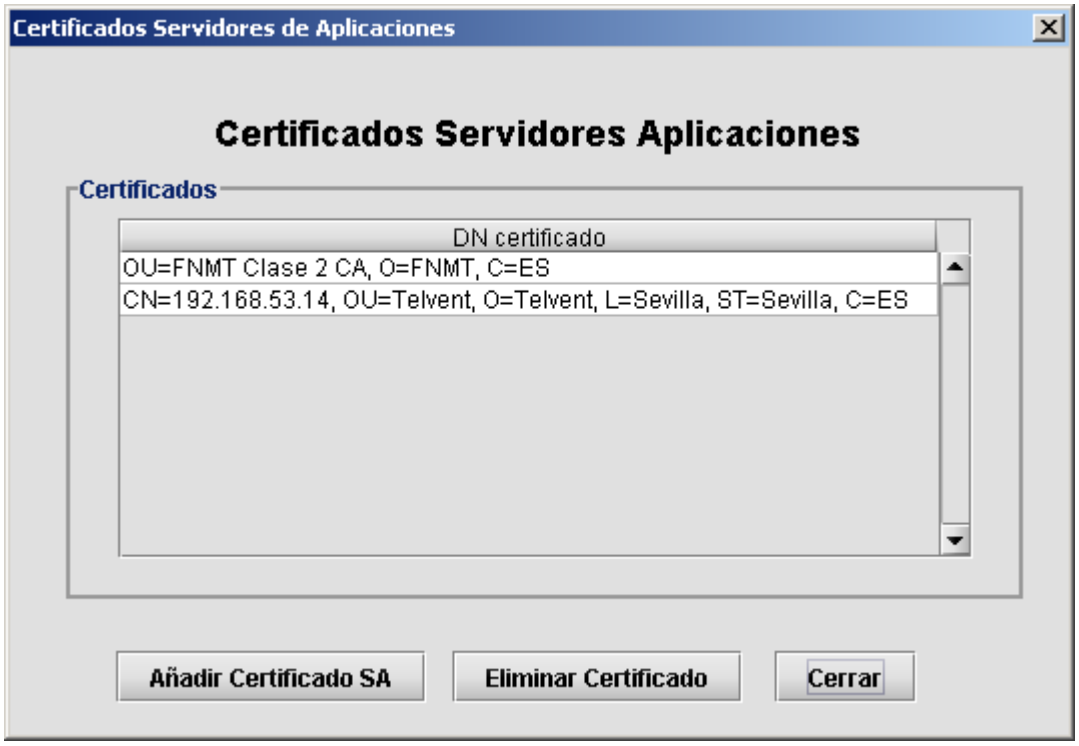
El "Tiempo Caducidad Transacción (horas)" indica el tiempo de permanencia máximo de transacciones incompletas o erróneas en la Base de Datos.

5.7.2 Certificados SA

Para que la plataforma @firma pueda comunicarse con los servidores de aplicaciones que contienen las paginas que se van ha firmar mediante https, @firma debe de tener los certificados de dichos servidores de aplicaciones.

Esta utilidad se utiliza para facilitar la gestión de los certificados de los servidores de aplicaciones.

Pulsando en el botón "Certificados SA" aparece la siguiente ventana:



En la ventana se muestra una lista con los certificados de los servidores de aplicaciones existentes en @firma y unos botones para añadir nuevos certificados y eliminar certificados existentes.

Al pulsar sobre el botón "*Añadir Certificado SA*" te muestra un navegador para que elijas el archivo que contiene el certificado. NOTA: el certificado debe de venir en formato DER X.509, y sólo ha de contener la clave pública para establecer conexiones SSL. La clave privada del servidor de aplicaciones no es necesaria.

Para eliminar uno o varios certificados hay que seleccionarlos en la lista y pulsar el botón "*Eliminar Certificado*".

NOTA: Para que los cambios realizados en esta ventana tengan efecto hay que parar y arrancar de nuevo el servidor de @firma.

5.7.3 Crear una Pagina Multifirma Masiva.

Hay dos formas de crear una nueva pagina multifirma masiva:

1.- Mediante el botón "Nueva Pagina", crea una pagina multifirma masiva con los valores por defecto.

2.- Mediante el botón "Duplicar", siempre y cuando haya alguna pagina multifirma masiva seleccionada en la lista, crea una nueva pagina multifirma masiva con los mismos valores que la seleccionada excepto el nombre.

En cualquiera de los dos casos se mostrará un panel con la configuración de la pagina multifirma masiva (Apartado 5.7.5) y el botón "Guardar", para que la creación tenga efecto habrá que pulsar este botón. Si todo es correcto aparecerá una nueva hoja debajo de la carpeta "Paginas Multifirma Masiva" con el nombre de la nueva pagina firmable.

NOTA: Tener en cuenta que los cambios se realizan siempre en local, para que tengan efecto en el servidor hay que mandarle la información, ya sea con le menú "Servidor\Mandar Configuración Servidor" o con el botón correspondiente de la barra de herramientas.

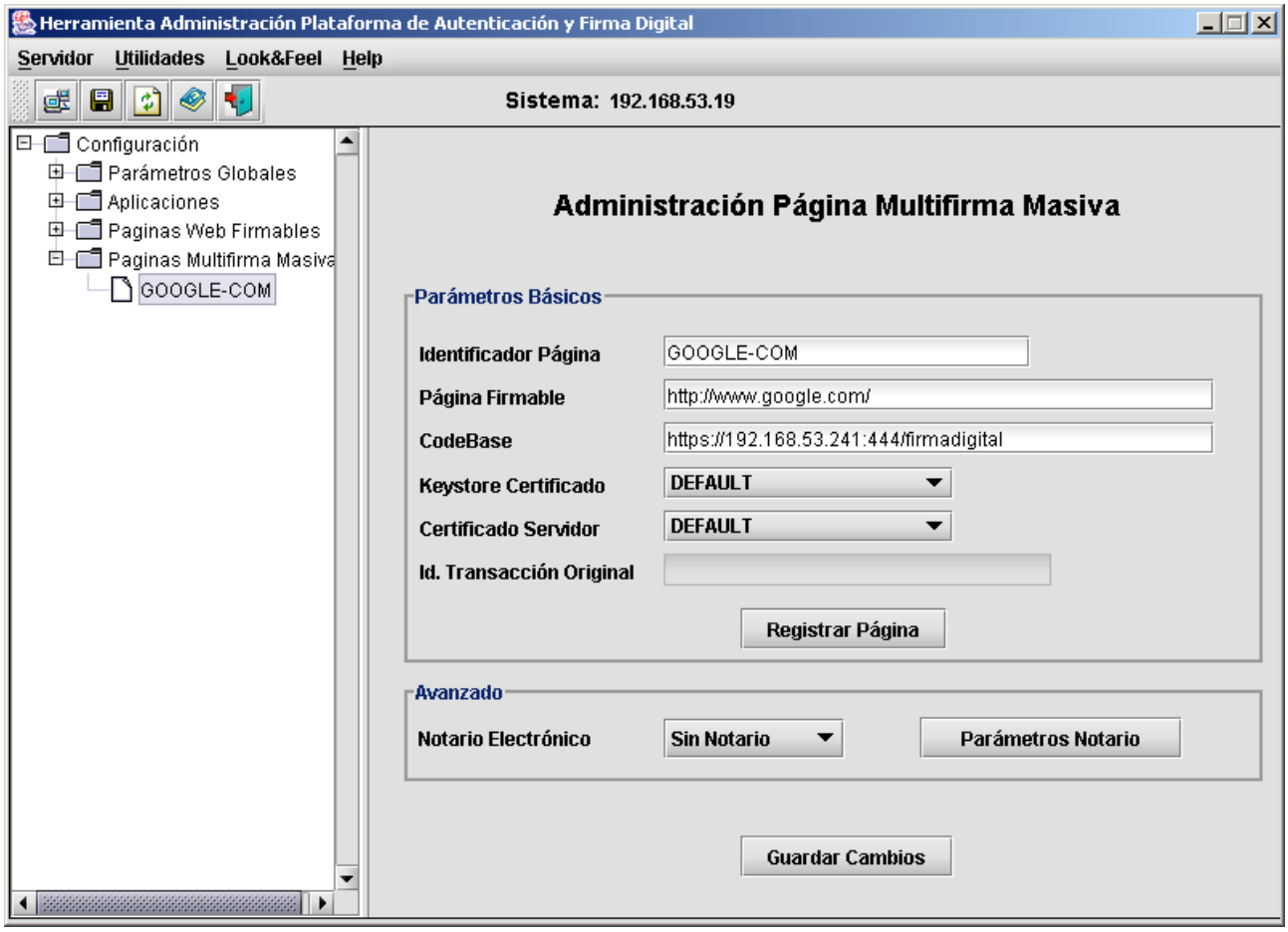
5.7.4 Eliminar una Pagina Multifirma Masiva.

Para eliminar una pagina multifirma masiva lo único que hay que hacer es seleccionarla en la lista que aparece cuando seleccionamos la carpeta "Paginas Web Firmables" en el árbol de configuración y pulsar el botón "Eliminar". Tener cuidado no pide confirmación de la eliminación.

NOTA: Tener en cuenta que los cambios se realizan siempre en local, para que tengan efecto en el servidor hay que mandarle la información, ya sea con le menú "Servidor\Mandar Configuración Servidor" o con el botón correspondiente de la barra de herramientas.

5.7.5 Configuración de una Pagina Multifirma Masiva.

Cuando seleccionamos una "pagina multifirma masiva" nos aparece el panel "Administración Página Multifirma Masiva" con la configuración de dicha aplicación.



Parámetros Básicos:

- **Identificador Página:** Identificador de la aplicación de firma y/o multifirma web.
- **Pagina Firmable**: Nombre de página web que deseamos hacer firmable incluida su ruta lógica completa http. Ej. http://<hostname>:<port>/ruta…./página.html
- **CodeBase:** https://*hostname:port*/firmadigital. Indica la url lógica base del módulo de firma, que será la url de la **Fachada**. Será necesario establecer el nombre de la **Fachada** (hostname) y puerto (port). No debe colocarse la "/" del final. NOTA: mantener */firmadigital* como nombre lógico.
- **Keystore Certificado:** Indica el keystore utilizado para verificar los certificados digitales de usuario utilizados en la firma. (Apartado 5.4.2 Keystores CAs en Parámetros Globales).

- **Certificado Servidor:** Certificado de Servidor utilizado para realizar la primera firma en una multifirma masiva.

- **Id. Transacción Original:** Identificador de la primera transacción de una multifirma masiva, lo genera la aplicación automáticamente cuando se pulsa le botón "**Registrar Página**" y no se puede modificar. Este identificador hay que pasárselo a los creadores de aplicaciones de Multifirma Masiva para que lo usen en las llamadas a los métodos de la interfaz proporcionada.

NOTA: No se puede registrar dos veces la misma Pagina Firmable.

Avanzado

- **Notario Electrónico**: Indica si queremos utilizar o no Firma Avanzada y el tipo de Firma.

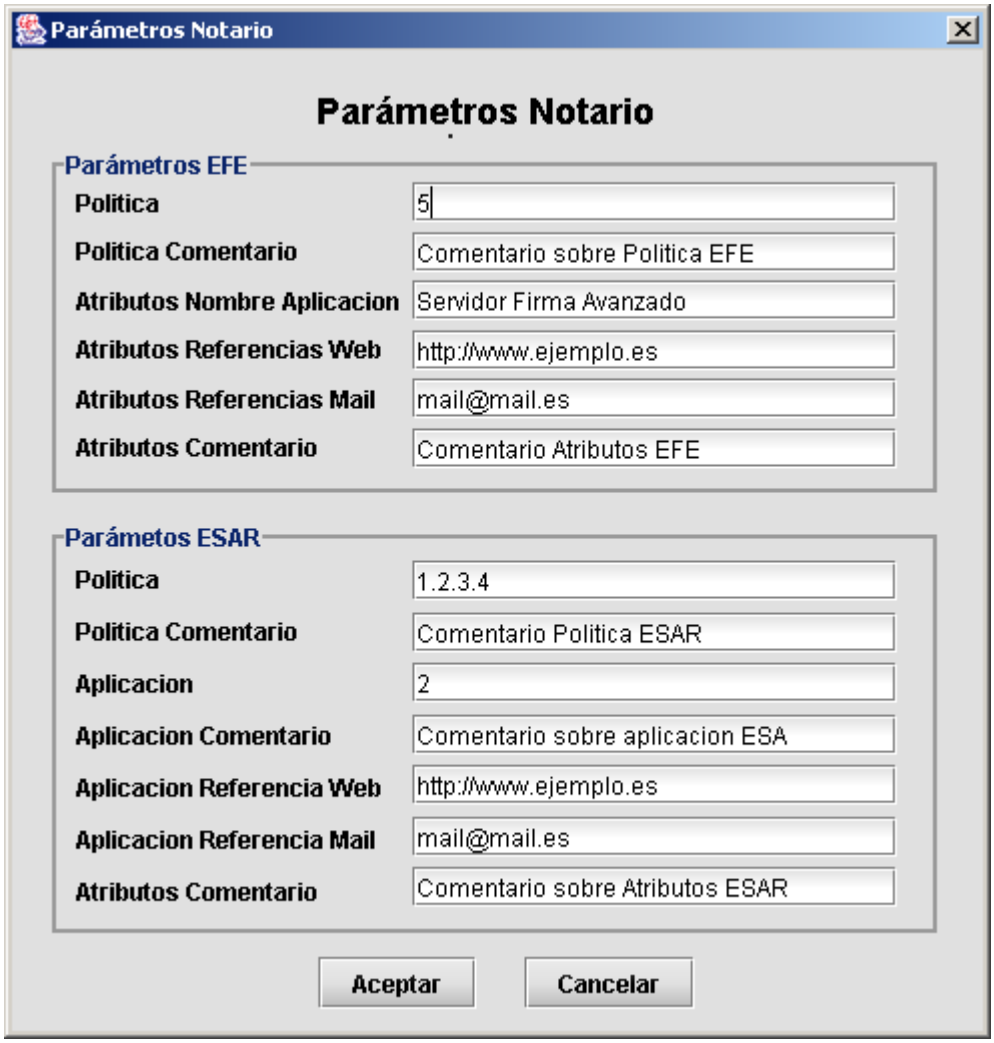
  - **Sin Notario**: Servidor Básico. Generación PKCS#7.

  - **EFE**: Servidor Avanzado. Genera la estructura PKCS#7, y la Estructura de Firma Electrónica ASN.1 con TimeStamp de Servidor de Notario Electrónico.

  - **EFE+AR**: Servidor Avanzado. Genera la estructura PKCS#7, la Estructura de Firma Electrónica ASN.1 con TimeStamp de Servidor de Notario Electrónico y la Estructura de Acuse de Recibo ASN.1 de Servidor de Notario Electrónico.

  - **EFE(Hora local)**: Servidor Avanzado. Genera la estructura PKCS#7 y la Estructura de Firma Electrónica ASN.1 con TimeStamp local del Servidor de Firma.

- Parámetros Notario: En caso de utilizar Firma Avanzada deberemos configurar los parámetros del Notario Electrónico (Ver anexo). La siguiente figura muestra dichos parámetros:



6 Administración de la Fachada

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.

La fachada consta de dos componentes diferenciados cuya administración es extremadamente simple.

6.1 Administración del componente Servidor de Aplicaciones

Este componente es un Jboss con varias aplicaciones web instaladas, la única configuración que necesita es la necesaria para conectarse con el servidor de @firma, aparte de la necesaria por el Jboss propiamente dicho.

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.
- afirma.clave: clave del usuario anterior.

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

6.2 Administración del componente Servidor Autenticación SSL

Este componente es un Servidor de SSL que se arranca desde un main, la configuración necesaria para su funcionamiento 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="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.

- 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. Este certificado tiene que estar en formato PKCS#12.

- 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.

- 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.

- 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. Camino absoluto 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. No cambiar el que viene por defecto.

- flog4j. Camino absoluto 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.

7 Gestión de Aplicaciones: Tareas y funciones del administrador de @firma

En este apartado se introduce a modo de guía las tareas y obligaciones que ha de seguir el administrador de @firma. Entre las principales tareas del administrador se pueden destacar:

- Alta / Modificación / Baja de aplicaciones. El administrador es el encargado de dar de alta las nuevas aplicaciones tanto de autenticación como de firma, en @firma. Para ello, los desarrolladores de aplicaciones han de suministrar al administrador los datos de las aplicaciones necesarios para su registro o modificación. Así mismo el administrador es el encargado de eliminar las aplicaciones que hayan sido dadas de baja y que no se utilizan. Es aconsejable dejar un margen de tiempo de seguridad antes de eliminar una aplicación definitivamente y evitar interrumpir el servicio de forma inmediata.

- Mantenimiento claves DES. El administrador es el responsable de asignar una clave DES a una nueva aplicación de autenticación o multifirma web registrada en @firma, y de suministrar esta clave a los desarrolladores de la aplicación correspondiente. Adicionalmente se recomienda que el administrador cambie las claves DES de cada aplicación cada cierto período de tiempo (varios meses) por motivos de seguridad. El cambio de claves ha de realizarse prudentemente, avisando con varios días de antelación a los desarrolladores de las aplicaciones del cambio y de la nueva clave DES, y realizándolo en horario no laboral para reducir al mínimo la interrupción del servicio.

- Mantenimiento de la comunicaciones. El administrador es el encargado de velar por el buen estado de las comunicaciones de @firma: con el Notario, con la fachada, con las CAs, con el sistema de custodia y con los servidores de aplicaciones. Adicionalmente se debe configurar el demonio de limpiado de transacciones fallidas.

    - El servidor @firma tiene que tener conexión directa a través del puerto 389 (LDAP) con la FNMT para descargarse la lista de CRL's, o en su defecto con la réplica del directorio LDAP disponible.

    - El servidor @firma tiene que tener conexión por el puerto 80 con el servidor de Notario Electrónico.

    - La Fachada ha de tener conexión http/https/RMI-IIOP con el Servidor de @firma.

    - El servidor @firma ha de tener conexión con el Servidor de Base de Datos de custodia.

    - El servidor @firma ha de tener conexión http/https/RMI-IIOP con los servidores de aplicaciones que utilizan los servicios de autenticación y firma digital.

- Mantenimiento del Sistema de Custodia. Esta tarea es exclusiva de un Administrador de Bases de Datos (DBA) con experiencia en Oracle.

8 Logs del Servidor

8.1 Descripción

Para registrar todos los logs del Servidor se utiliza una herramienta que trae el Servidor de aplicaciones JBoss, denominada "Log4j". Log4j posee 4 tipos de objetos: categories, priorities, appenders y layouts, que permiten a los desarrolladores registrar mensajes conforme al tipo y a la prioridad, y controlar en tiempo de ejecución el formato y la información de estos mensajes.

Clase org.apache.log4j.Category

Una categoría es un nombre de entidad que se organiza de forma jerárquica, y que es sensible a mayúsculas (de forma parecida a como se organizan los paquetes Java). De todos los métodos de esta clase sólo tiene interés destacar la fábrica y los métodos logging y tipo de prioridad.

Clase org.apache.log4j.Priority

Esta clase representa la importancia o el nivel de un determinado mensaje. Siempre que se loga un mensaje, éste lleva asociado una prioridad a él. Existen un conjunto de prioridades definidas por defecto y que se pueden utilizar en el logado de mensajes: FATAL, ERROR, WARN, INFO, TRACE y DEBUG. No obstante, siempre es posible extender el conjunto de prioridades predefinidas heredando de la clase Priority.

- TRACE, es un nivel de prioridad para logar mensajes que están directamente asociados con una actividad originada por un request. Cada request generaría un mensaje, con lo que el número de mensajes originados es N, siendo N el número de request. Se utiliza para depurar a fondo el servidor de aplicaciones.

- DEBUG, es un nivel de prioridad para logar un mensaje que muestra información extra sobre los eventos del ciclo de vida del servicio.

- INFO, es un nivel de prioridad para los eventos del ciclo de vida del servicio. Los mensajes INFO para un servicio con una categoría determinada, indicarían de esta forma en qué estado del servicio se encuentran.

- WARN, es un nivel de prioridad para eventos que indican errores no críticos de servicio.

- ERROR, es un nivel de prioridad para eventos que indican una disfunción en un request, o la incapacidad para dar servicio a un request. El servicio debería ser capaz de continuar después de informar del error.

- FATAL, es un nivel de prioridad para eventos que indican un fallo crítico de servicio. Una vez que se produce un evento de esta prioridad en un servicio es imposible continuar aceptando requests.

El objetivo de asociar una prioridad a un mensaje es la posibilidad de poder filtrar mensajes en función de su importancia o prioridad.

Clase Org.apache.log4j.Logger

La clase Category ha sido sustituida en la última versión de Log4j (versión 1.2) por la clase org.apache.log4j.Logger, para dar mas consistencia a la compatibilidad con el JDK 1.4, en especial con el paquete java.util.logging. La clase Logger es una subclase de Category y únicamente añade los métodos fábrica para obtener una instancia de org.apacher.log4j.Logger.

Interfaz org.apache.log4j.Appender

Los appenders son elementos que se asocian a una categoría que recibe un mensaje de log, y que gestionan la serialización del mensaje. Es decir, que un appender no es más que un destino lógico del mensaje. Pueden existir múltiples appenders asociados a una categoría, lo cual hace posible que un mismo mensaje posea varios destinos. Existen appenders para Consolas, ficheros, componentes Gráficos, sockets, Java Messaging Service, Windows event loggers, y demonios syslog de UNIX.

Clase org.apache.log4j.Layout

La renderización (serialización) de un mensaje de log hacia un "string" se delega a las instancias de la clase Layout. Por lo tanto, un Layout es un formateador que transforma un objeto LoggingEvent en un String.

Patrones de uso en Log4j

A veces se nos presenta la duda sobre qué nombre de categorías usar y que prioridades deberían tener asignada. En JBoss se suele utilizar el nombre de la clase del componente que realiza el logging. En el módulo de autenticación de @firma cada componente desarrollado tiene asignado una categoría con el nombre de la clase a la que pertenece el componente. Por ejemplo,

```
<category name="com.telventi.autenticacion">
   <priority value="INFO" />
</category>
```

8.2 Configuración

En este apartado se van a describir las distintas partes y mejoras realizadas en el fichero de configuración xml "log4j.xml".

El fichero log4j.xml posee dos secciones. En la primera de ellas se definen los appenders y las propiedades asociadas a los mismos y en la segunda sección se definen las categorías y los appenders que llevan asociadas cada una de ellas. Existen varios tipos de Appenders: File (por fecha o por tamaño), Console, Mail, etc…

Para una mejor comprensión de los appenders se muestra un ejemplo:

```
<appender name="FILE" class="org.JBoss.logging.appender.DailyRollingFileAppender">
   <param name="File" value="${JBoss.server.home.dir}/log/server.log"/>
   <param name="Append" value="false"/>
   <param name="Threshold" value="INFO"/>
   <!-- Rollover at midnight each day -->
   <param name="DatePattern" value="'.'yyyy-MM-dd"/>

   <!-- Rollover at the top of each hour
   <param name="DatePattern" value="'.'yyyy-MM-dd-HH"/>
   -->
   <layout class="org.apache.log4j.PatternLayout">
     <!-- The default pattern: Date Priority [Category] Message\n -->
     <param name="ConversionPattern" value="%d %-5p [%c] %m%n"/>

     <!-- The full pattern: Date MS Priority [Category] (Thread:NDC) Message\n
     <param name="ConversionPattern" value="%d %-5r %-5p [%c] (%t:%x) %m%n"/>
      -->
   </layout>
 </appender>
```

Este appender es de tipo DailyRollingFile (genera un nuevo fichero por cada día transcurrido), y lleva asociadas las siguientes propiedades:

- La propiedad File le indica la ruta donde se genera el fichero de log.

- La propiedad Append si se concatena o si se escribe un fichero nuevo cada vez que exista un rollover. Un rollover es un finalización de un período para empezar otro nuevo. El período de finalización es la medianoche "00:00" de un día a otro.

- La propiedad threshold indica la prioridad a partir de la que se registran los mensajes.

- La propiedad DatePattern indica el formato de la fecha y hora, y si se genera un registro cada hora o cada día (en función del formato elegido).

- En ultimo lugar se define el Layout que no es mas que el formato en que se muestran los mensajes de logs. Para mayor información acerca de la sintaxis de formatos de mensajes consultar el Javadoc de log4j.

El resto de los appenders es prácticamente igual (cada uno con sus propiedades) y no tienen complicación.

En la segunda parte del fichero se definen las categorías con las prioridades, y los appenders asociadas a ellas. Por ejemplo:

```
<category name= "telvent.ejemplos ">
   <priority value= "INFO "/>
 <appender-ref= "FILE ">
 </category>
```

De esta forma todos los ejemplos de Telvent quedarían registrados en el fichero de log especificado en el appender FILE con el nivel de prioridad INFO.

9 Códigos de error de autenticación

A continuación se incluyen una lista con los códigos de error en autenticación para su identificación:

00 -> Certificado 0K
11 -> Algoritmo de firma en certificado de cliente invalido
12 -> Clave en certificado cliente no valida
13 -> Proveedor de certificado cliente no encontrado
14 -> Error al comprobar la firma del certificado de cliente
15 -> Error al obtener los campos obligatorios del certificado
16 -> No se ha encontrado el certificado de la CA de este certificado.
NO ES CONFIABLE PARA LA APLICACION
17 -> No se ha construido el objeto de forma correcta
18 -> Error al chequear la fecha del certificado, no válido o expirado.
19 -> No se ha encontrado la CRL
20 -> Error al descargar la CRL
21 -> Error al verificar la crl con el certificado de su CA
22 -> No se ha encontrado el certificado de la CA de esta CRL
23 -> Error al crear el objeto X09CRL
24 -> Certificado revocado
25 -> Certificado revocado, clave comprometida
26 -> Certificado revocado, clave CA comprometida
27 -> Certificado revocado, cambio información
28 -> Certificado revocado, certificado reemplazado
29 -> Certificado revocado, propósito original del certificado ya no valido
30 -> Certificado revocado, certificado suspendido temporalmente
31 -> Certificado revocado, el certificado debe ser removido de una CRL anterior
32 -> Certificado revocado, un privilegio del certificado ha sido retirado
33 -> Certificado sin puntos de distribución de CRL
34 -> Imposible validar el certificado con sus DP

Anexos

A.1 Parametros notario

Para una mejor comprensión de la funcionalidad de los parámetros véase documentación sobre ASN.1 Estructura de Firma Electrónica y ASN.1 Estructura de Acuse de Recibo.

A continuación se describen los parámetros necesarios para Estructura de Firma Electrónica ASN.1:

EFE_Politica_ID	Identificador de Politica de Estructura de Firma Electrónica ASN.1. Debe ser un ENTERO. OBLIGATORIO
EFE_Politica_Comentario	Comentario sobre Identificador de Política de Estructura de Firma Electrónica ASN.1. OPCIONAL
EFE_Atributos_NombreAplicacion	Nombre de Aplicación en la Estructura de Firma Electrónica ASN.1 OPCIONAL. Si no está presente se considera que no habrá estructura *Atributos*.
EFE_Atributos_Referencias_Web	Referencia web de la aplicación en la Estructura de Firma Electrónica ASN.1 OPCIONAL
EFE_Atributos_Referencias_Mail	Dirección de correo de la aplicación en la Estructura de Firma Electrónica ASN.1 OPCIONAL. Si no está presente se considera que no hay estructura *Referencias*.
EFE_Atributos_Comentario	Cualquier información de aplicación en la Estructrua de Firma Electrónica ASN.1 OPCIONAL

A continuación se describen los parámetros necesarios para Estructura de Solicitud de Acuse de Recibo ASN.1:

ESAR_Politica_ID	Identificador de Politica de Estructrua de Solicutd de Acuse de Recibo ASN.1. Es una CADENA con la forma 1.2.3.4. OBLIGATORIO
ESAR_Politica_Comentario	Comentario sobre Política de Estructura de Solicitud de Acuse de Recibo ASN.1. OPCIONAL
ESAR_Aplicacion_ID	Identificador de Aplicación en Estructura de Solicitud de Acuse de Recibo ASN.1. Debe ser un ENTERO. Debe coincidir con el puesto en ID Cliente de la ventana NOTARIO JA. OBLIGATORIO
ESAR_Aplicacion_Comentario	Comentario sobre Aplicación en Estructura de Solicitud de Acuse de Recibo ASN.1. OPCIONAL
ESAR_Aplicacion_Referencia_Web	Referencia Web sobre Aplicación en Estructura de Solicitud de Acuse de Recibo ASN.1 OPCIONAL
ESAR_Aplicacion_Referencia_Mail	Referencia Mail sobre Aplicación en Estructura de Solicitud de Acuse de Recibo ASN.1 OBLIGATORIO
ESAR_Atributos_Comentario	Comentario sobre Atributos en Estructura de Solicitud de Acuse de Recibo ASN.1. OPCIONAL