Integración con Servicios Web de @firma

31 de marzo de 2009

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

INDICE

1. Introducción
2. El cliente de firma
3. Integración con @firma v5
4. Supuestos prácticos
5. Conclusiones. Ruegos y preguntas

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

1. Introducción

a. Conceptos básicos
b. Tipos de Firma Electrónica
c. Arquitectura @firma

1.a. Conceptos básicos (I)

¿Qué es @firma?

@FIRMA: La plataforma corporativa de autenticación y firma

Última actualización: 25/02/2009

@FIRMA es la plataforma corporativa de la Junta de Andalucía para autenticación y firma electrónica. Gracias a @firma, las aplicaciones de la Junta de Andalucía pueden incorporar procesos de autenticación y firmado digital mediante el uso de certificados digitales, independientemente del entorno de desarrollo en que hayan sido programadas.

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

1.a. Conceptos básicos (II)

Autenticación

- Proceso que permite identificar a las entidades implicadas en una transacción y garantiza que estas entidades son quienes dicen ser.
- Utiliza certificados digitales para su objetivo.
- Aporta mayor información y contenido al proceso de logado a una aplicación.

Firma electrónica

- Una firma electrónica es el resultado de aplicar una serie de operaciones criptográficas a una entidad de información utilizando para ello un certificado electrónico, para obtener dos cosas: la integridad del documento firmado y el no repudio de la firma realizada.

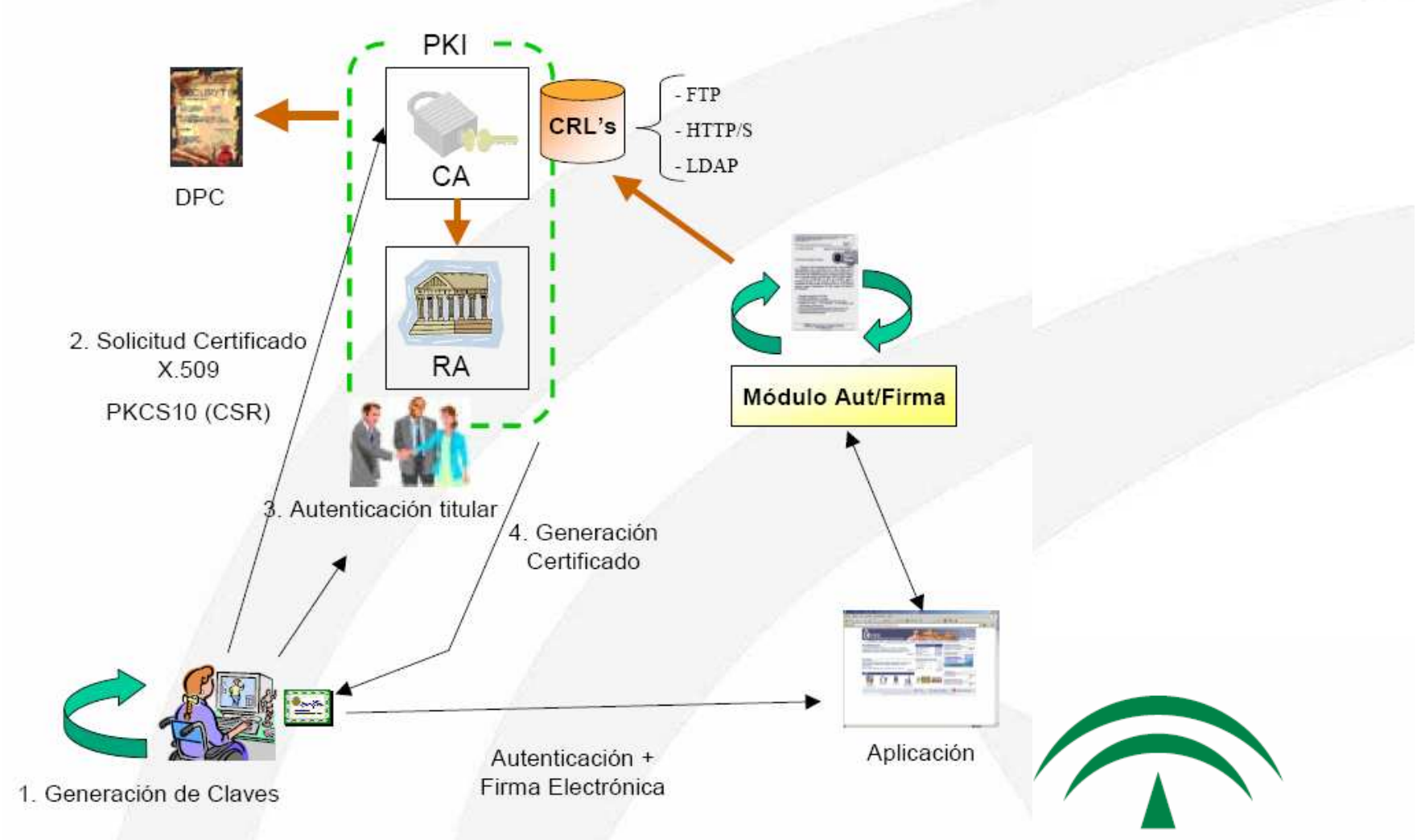
1.a. Conceptos básicos (IV)

Estado de certificado

- Caducado: se ha superado la fecha de vigencia del certificado.
- Revocado: cuando ha sido rechazado, o bien por la Autoridad Certificadora que lo emite o bien el propio titular. Posibles motivos de revocación pueden ser el extravío, robo, copiado por terceros, etcétera.
- Suspendido: el certificado se ve afectado por una investigación o procedimiento judicial o administrativo, por lo que se cancela la validez del certificado durante un cierto período de tiempo, pudiendo volverse a levantar la suspensión dentro del periodo de validez del certificado.
- Válido: el certificado no se encuentra en ninguno de los estados anteriores.
- Un certificado caducado, revocado o suspendido no tiene validez, por lo que las firmas realizadas dejan de tener valor desde el momento de su revocación.

1.a. Conceptos básicos (V)

Infraestructura de Clave pública



1.b. Tipos de Firma Electrónica (I)

Según la ley 59/2003 de firma electrónica

- Reconocidas: Estas firmas electrónicas son las únicas válidas legalmente ante terceros y equivalentes a la firma manuscrita tradicional. Una firma electrónica es reconocida cuando ha sido generada con un medio de creación de firmas seguro y utilizando un certificado electrónico reconocido.
- No reconocidas: No tienen validez legal, aunque técnicamente se pueden probar que son fiables. Son generadas por certificados internos o de PSCs no reconocidos por la Administración Española.

Según el número de firmantes

- Simple: En la estructura de firma electrónica existe un único firmante.
- Multifirma: En la estructura de firma electrónica existen varios firmantes.

1.b. Tipos de Firma Electrónica (II)

Según la jerarquía de la firma electrónica

- Jerárquica (counterSign): Firma de varios firmantes sobre un mismo documento, en un orden determinado de manera que cada uno firma sobre lo firmado anteriormente. Con ello cada firmante manifiesta conformidad con lo firmado por el anterior.
- Paralela (coSign): Cuando en la estructura de firma electrónica no existe ni orden ni jerarquía, lo que realmente importa es que un conjunto de N personas firmen un mismo documento.

Según la ubicación de la información firmada

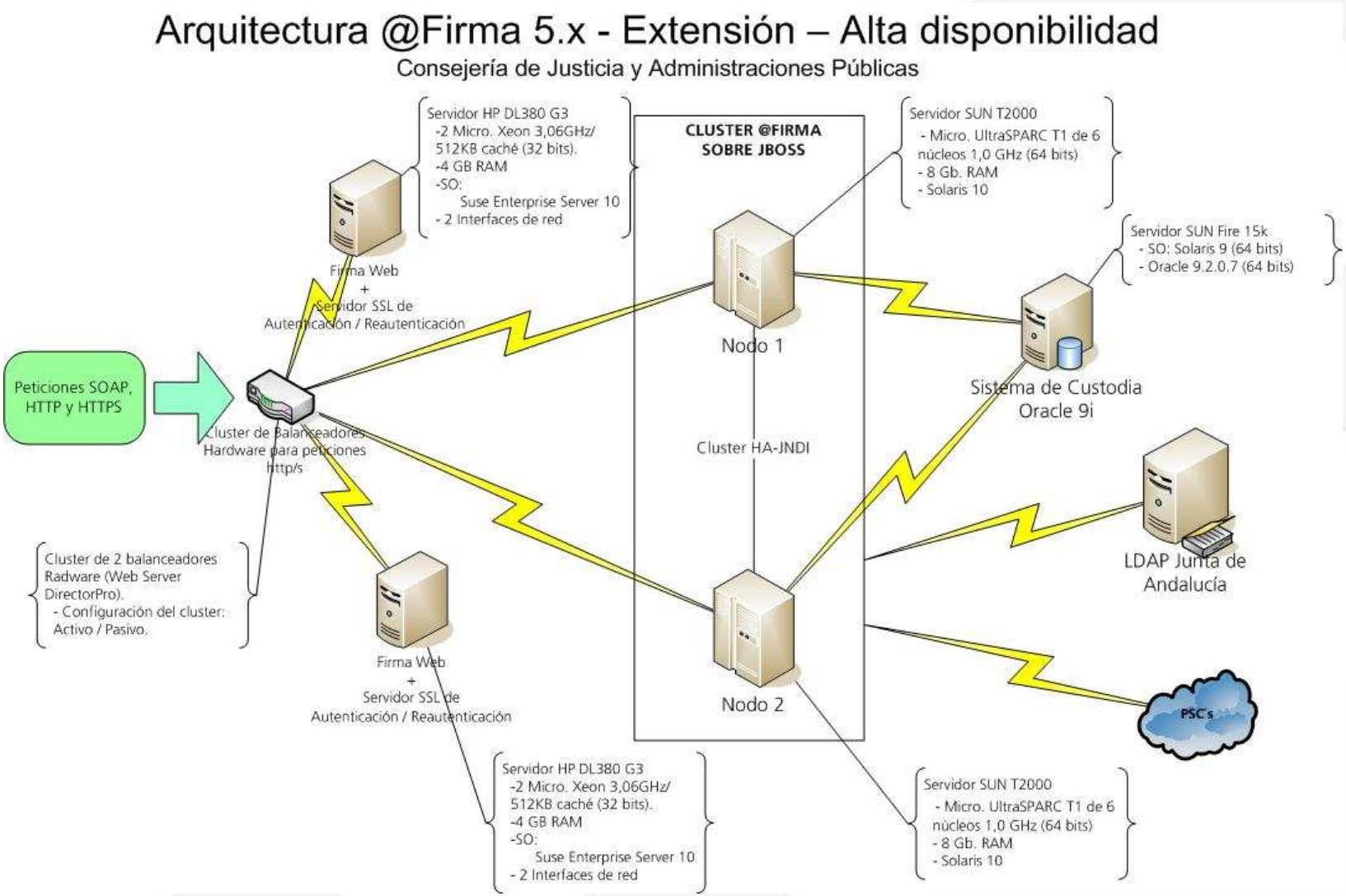
- Explícita: La estructura de firma electrónica es independiente del documento firmado, es decir, se obtienen dos ficheros, uno con la firma y otro con la información original.
- Implícita: La estructura de firma electrónica incorpora el documento firmado. Se suele utilizar cuando los documentos a firmar son pequeños.

1.c. Arquitectura de @firma (I)

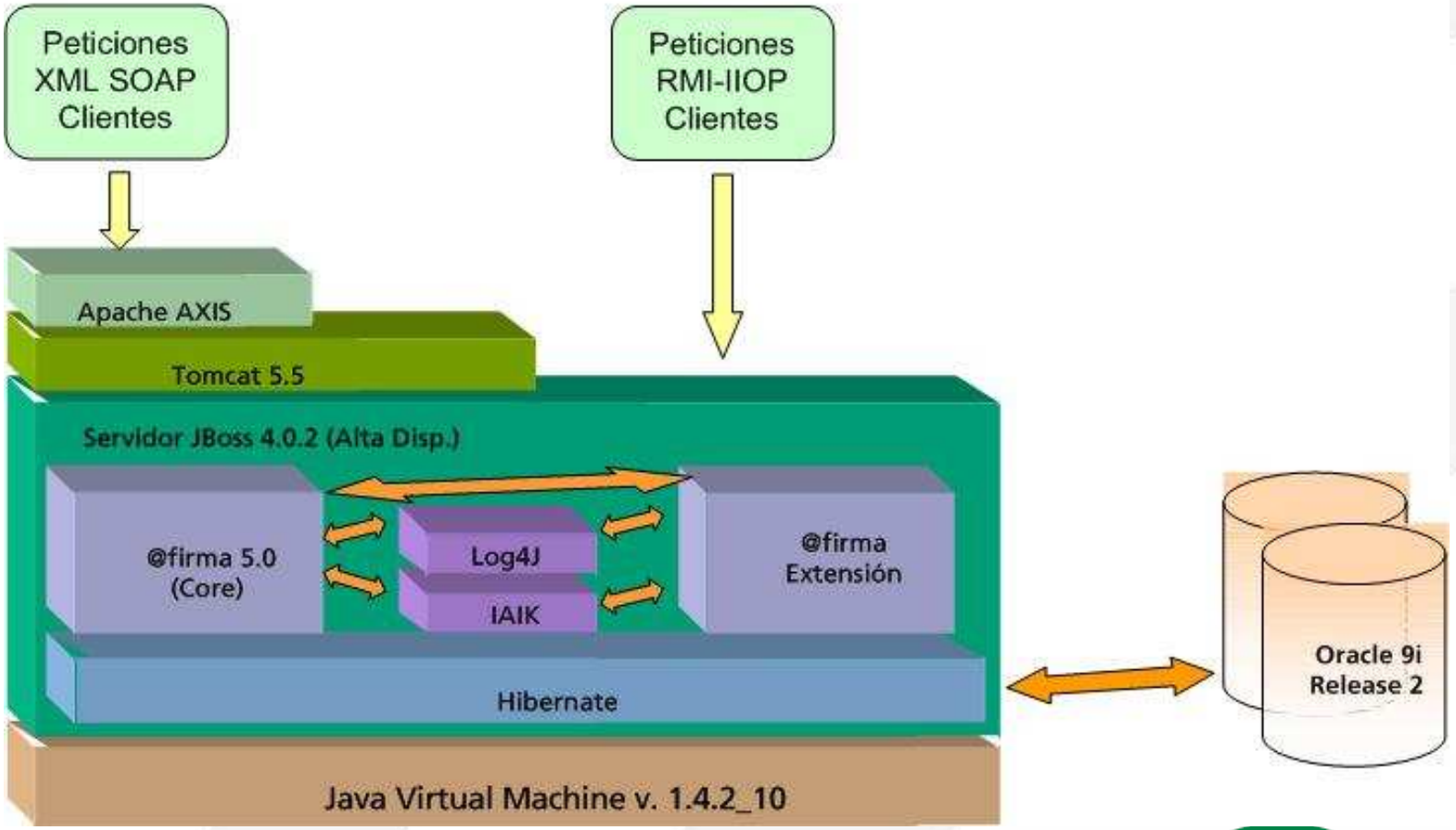
- Arquitectura física
- Arquitectura lógica

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

1.c Arquitectura de @firma – Física (II)



1.c Arquitectura de @firma – Lógica (III)



JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

2. El cliente de firma

a. El instalador: estrategia de despliegue y mecanismo de distribuciones
b. Evolución: la versión 2.3.5
c. Ejemplos del CD de desarrollo de @firma v5

2.a. El instalador: estrategia de despliegue y mecanismo de distribuciones (I)

- Responsable del despliegue de las librerías del cliente de firma.
- Interfaz Javascript disponible en instalador.js.
- Dispone de métodos para instalación, actualización y desinstalación.
- Instalación versiones anteriores 2.3.5.
  - Las librerías Java se copian en una ruta de la carpeta de perfil del usuario
    - Windows XP: C:\Documents and Settings\<usuario>\
    - Linux: /home/<usuario>/
  - Las librerías nativas se copian en carpetas de sistema. Requiere permisos de administrador del equipo.
    - Windows XP: C:\Windows
    - Linux: Seleccionable por el usuario
- Instalación en 2.3.5 y superiores.
  - La instalación completa se realiza en la carpeta de perfil del usuario.
  - No se requieren privilegios de administrador.

2.a. El instalador: estrategia de despliegue y mecanismo de distribuciones (II)

- Si la versión del cliente y la del servidor de aplicaciones difieren se ejecuta el proceso de instalación.
- Dicho comportamiento puede provocar actualizaciones frecuentes del cliente que perjudican la experiencia de usuario.
- A partir de la versión 2.3.5 está disponible el mecanismo de distribuciones, el cual permite alojar varias versiones independientes en la carpeta de perfil del usuario.
- Es necesario configurar la variable distinctDistroDir en scriptfirma.js (aplicación integrada con la extensión) o en el fichero constantes.js (integración nativa).
- Nomenclatura: <Indentificador organismo><X_Y_Z>
- Ejemplo: JA2_3_5

2.b. Evolución: la versión 2.3.5

- Última versión disponible del cliente de firma.
- Si bien la numeración puede sugerir una revisión menor, incorpora importantes mejoras y correcciones de errores.
  - Soporte para Windows Vista.
  - Soporte mejorado para Linux. Guadalinex v3 y v4.
  - Mecanismo de distribuciones.
  - Instalación simplificada y sin privilegios de administrador.
- Soporte revisado para Windows Vista SP1, Windows XP SP2 y SP3, Windows 2000 SP4, Guadalinex v3, v4 y v5 (no soportado), con navegadores Internet Explorer 6, 7, Mozilla Firefox 1.5, 2.0 y 3.0 (no soportado), con Sun JRE 1.5 y 1.6.

2.b. Evolución: la versión 2.3.5

Matriz de compatibilidad

	Sun JRE 1.5				Sun JRE 1.6			
	IE6	IE7	Ff1.5	Ff2.0	IE6	IE7	Ff1.5	Ff2.0
Windows 2000 SP4	OK	N/D	OK	OK	OK	N/D	OK	OK
Windows XP SP2, SP3	OK	OK	OK	OK	OK	OK	OK	OK
Windows Vista, SP1	N/D	OK	OK	OK	N/D	OK	OK	OK
Guadalinex v3	N/D	N/D	OK	OK	N/D	N/D	OK	OK
Guadalinex v4	N/D	N/D	*	*	N/D	N/D	OK	OK
Guadalinex v5	N/D	N/D	x	x	N/D	N/D	x	x

*No soportado JRE 1.5 instalado desde el repositorio

+ Firefox 3 no está soportado en ninguna configuración

x Guadalinex v5 no está soportado en ninguna configuración

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

2.c. Ejemplos del CD de desarrollo de @firma v5

- En el disco de desarrollo de @firma v5 se incluyen ejemplos que permiten familiarizarse con la API del cliente de firma de ficheros y con los conceptos relacionados.
- Los ejemplos se encuentran ubicados en la ruta Cliente\web-instalador
  - demoInstalador.html.
  - demoFirmaWeb-01.htm.
  - demoFirmaMasiva.html.
  - demoMultifirma.html.
  - demoCifrado.html.
  - demoSobreDigital.html.
  - demoVisorNodosMultifirma.html.

3. Integración con @firma v5

a. Mecanismos de seguridad. Acceso seguro y métodos de autorización
b. Módulos. Custodia, firma y validación
c. Mensajes de entrada y respuesta en servicios
   Esquemas de validación

3.a. Mecanismos de seguridad. Acceso seguro y métodos de autorización (I)

- El acceso a los servicios de la plataforma por las aplicaciones está securizado mediante el establecimiento de una conexión segura (SSL) entre el servidor de aplicaciones y el servidor de firma, y su autorización con alguno de los mecanismos configurados para la aplicación.
- Para establecer una conexión segura el cliente Webservice de la aplicación debe estar configurado para tener acceso a la clave pública del servidor de firma.
- La clave pública de cada entorno @firma de la Consejería de Justicia y Administración Pública es proporcionada en el proceso de alta de la aplicación.

3.a. Mecanismos de seguridad. Acceso seguro y métodos de autorización (II)

- En el alta de una aplicación es posible configurar alguno de los siguientes métodos de autorización:
  - Mediante usuario y password. La autorización de uso de un servicio web se encuentra condicionada a la especificación en la llamada al servicio de una pareja usuario-clave dada de alta previamente en la configuración de la aplicación. Es posible especificar en el alta varias parejas usuario-clave. Corresponde al modo de securización UsernameToken del fichero de configuración de los ejemplos del disco de desarrollo de @firma v5.
  - Mediante certificado. Con este método se empleará un certificado digital para la validación de la llamada a un servicio web de la plataforma. Es posible proporcionar en el alta varios certificados digitales para una aplicación. Corresponde al modo de securización BinarySecurityToken del fichero de configuración de los ejemplos del disco de desarrollo de @firma v5.

3.b. Módulos. Custodia, firma y validación

- Los servicios de la plataforma están disponibles en la dirección https://servidor_de_firma/afirmaws/services

- Los servicios se encuentran agrupados funcionalmente en módulos.
  - Módulo de custodia. Incluye los relacionados con el acceso a la custodia de la plataforma.
    - AlmacenarDocumento
    - EliminarContenidoDocumento
    - ObtenerContenidoDocumento
    - ObtenerContenidoDocumentoId
    - ObtenerIdDocumento
    - ActualizarReferencia
    - ObtenerTransaccionesPorFecha
    - ObtenerTransacciones
    - …

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

3.b. Módulos. Custodia, firma y validación (I)

- Módulo de firma. Agrupa los servicios relacionados con las distintas modalidades de firma.
  - ValidarFirma
  - FirmaServidor
  - FirmaServidorCoSign
  - FirmaServidorCounterSign
  - FirmaUsuario3FasesF1
  - FirmaUsuario2FasesF2
  - FirmaUsuarioBloquesF1
  - ValidarFirmaBloquesCompleto
  - …

3.b. Módulos. Custodia, firma y validación (II)

- Módulo de validación. Contiene los servicios relacionados con la validación de certificados.
  - ValidarCertificado
  - ObtenerInfoCertificado

3.c. Mensajes de entrada y respuesta en servicios. Esquemas de validación (I)

- Los parámetros de entrada de los servicios y los resultados de su ejecución se transmiten mediante mensajes XML.
- Ejemplo de mensaje de entrada

```
<?xml version="1.0" encoding="UTF-8"?>
        <mensajeEntrada targetNamespace="https://afirmaws/ws/firma"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:noNamespaceSchemaLocation="https://localhost/afirmaws/xsd/mfirma/ws.xsd">
        <peticion>FirmaServidor</peticion>
        <versionMsg>1.0</versionMsg>
        <parametros>
                    <idAplicacion>appPrueba</idAplicacion>
                    <idDocumento>177</idDocumento>
                    <firmante>RSA.2048</firmante>
                    <idReferencia>idReferencia</idReferencia>
                    <algoritmoHash>SHA1</algoritmoHash>
                    <formatoFirma>CMS</formatoFirma>
        </parametros>
</mensajeEntrada>
```

3.c. Mensajes de entrada y respuesta en servicios. Esquemas de validación (II)

- Ejemplo de mensaje de salida/respuesta

```
<?xml version="1.0"?>
<mensajeSalida xmlns="https://afirmaws/ws/firma"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/ws.xsd ">
       <peticion> FirmaUsuario3FasesF1 </peticion>
       <versionMsg>1.0 </versionMsg>
       <respuesta>
                  <Respuesta>
                             <estado>true</estado>
                             <descripcion>Proceso de fase 1 de firma de usuario en 3
fases realizado correctamente.</descripcion>
                             <idTransaccion>1150302756695137</idTransaccion>
                             <hash>Z3IUyA4ZiemW6cbMlgunG+wPqT8=</hash>
                             <algoritmoHash>SHA1</algoritmoHash>
                  </Respuesta>
       </respuesta>
</mensajeSalida>
```

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

3.c. Mensajes de entrada y respuesta en servicios. Esquemas de validación (III)

- Para cada módulo se encuentra definido un XML-Schema que permite validar los mensajes de entrada y de respuesta de los servicios del módulo.
- En el CD de desarrollo de @firma se encuentran disponibles las definiciones de todos los módulos.
  - KitIntegraciónWS\xsd\mcustodia
  - KitIntegraciónWS\xsd\mfirma
  - KitIntegraciónWS\xsd\mvalidacion

4. Supuesto Práctico

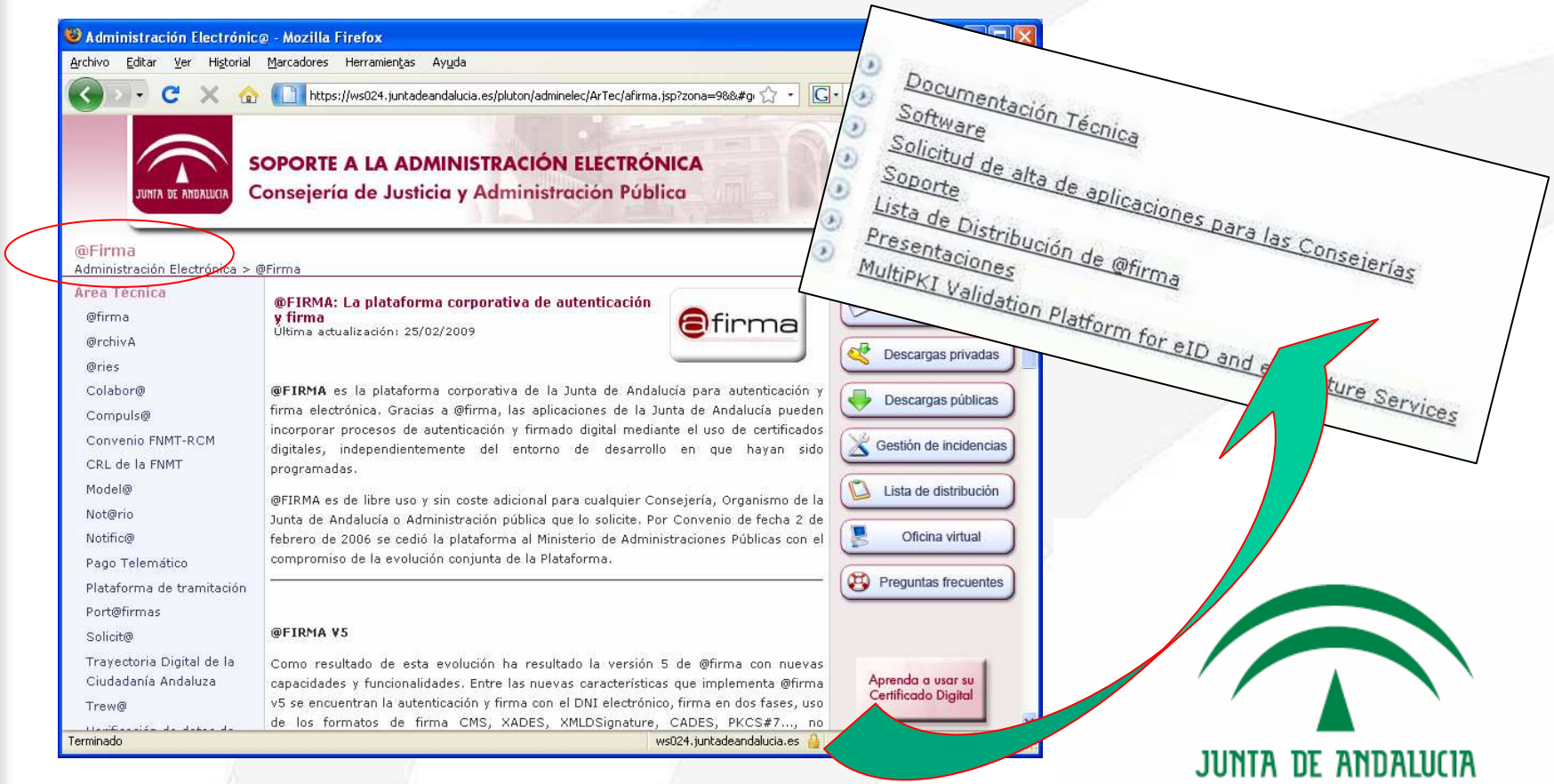
a. Recursos para el desarrollo
b. Proceso de alta
c. CD de desarrollo de @firma
d. Código Fuente. Descripción del Servicio

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

4.a. Recursos para el desarrollo (I)

Web de Plutón - Recursos

https://ws024.juntadeandalucia.es/pluton



JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

4.a. Recursos para el desarrollo (II)

Gestor de Incidencias (iTracker)

https://ws025.juntadeandalucia.es/itracker

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

4.b. Proceso de alta

Datos de configuración

Solicitud de Alta de Aplicaciones en @firma v5

Desde aquí puede acceder al manual para dar de alta una aplicación en @firma, donde se explica detalladamente los requisitos necesarios para solicitar el alta.

Enviar a la cuenta de correo de la Oficina de Administración Electrónica soporte.admonelectronica@juntadeandalucia.es escribiendo en el asunto "SOLICITUD ALTA AI información:

- Datos del solicitante: Nombre, apellidos, teléfono, e-mail.
- Nombre de la empresa.
- Consejería para la que se desarrolla y responsable de la Consejería.
- Nombre de la aplicación.
- Descripción de la aplicación.
- Responsable de la aplicación: Nombre, apellidos, teléfono, e-mail.
- ¿Requiere custodia de documentos? Sí/No (El uso de custodia de documentos limitará el tamaño de los ficheros a firmar a un máximo de 8Mb). En caso de no u: conservar el mismo. Se recomienda no usar custodia de documentos por motivos de rendimiento y al no tener que enviarlo a través de la red para su custodia en
- Tipo de Autorización de acceso:
  - Autorización mediante usuario/clave
  - Autorización basada en certificados digitales (Recomendado)
- Política de TimeStamp:
  - Con TimeStamp
  - Sin TimeStamp
- Plataforma @firma en la que se solicita el alta: Desarrollo / Producción.
- Fecha prevista de puesta en producción.
- Volumen aproximado de accesos/día.
- Tipo de Servicio @firma solicitado:

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

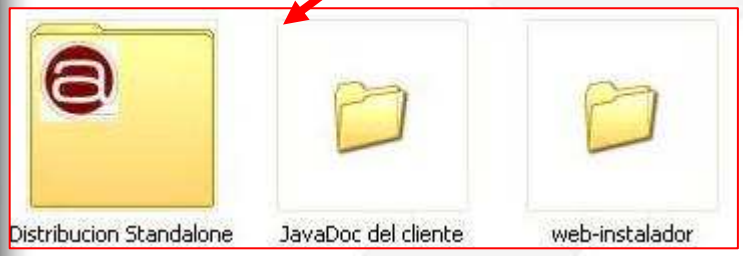
4.c. CD de desarrollo de @firma (I)

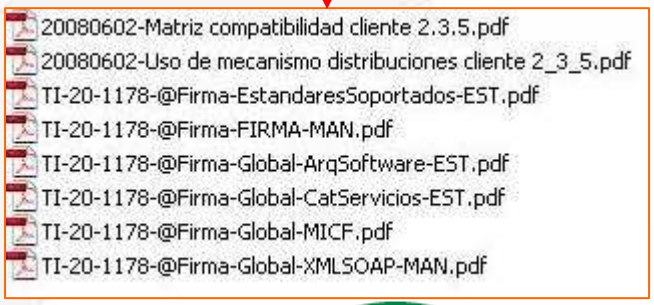
El Cd se obtiene a partir de las descargas privadas de Plutón.

Enviando un email a soporte.admonelectronica@juntadeandalucia.es

Con los siguientes datos: Nombre, apellidos, cargo y DNI de la persona que va a realizar la descarga. Indicando que se desea la descarga del CD de desarrollo

Este CD puede ser solicitado por cuantas personas se desee





JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

4.c. CD de desarrollo de @firma (II)

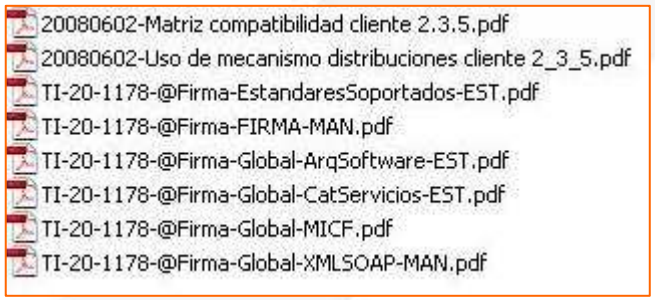
Carpeta Cliente

- Distribución Integrador: Contiene los ficheros a los que se hace referencia en el Manual del Integrador del Cliente de Firma (TI-20-1178-@Firma-Global-MICF) y algunos ejemplos de integración y uso del cliente.
- Distribución Standalone: Contiene una utilidad que instala el cliente de firma en el ordenador sin necesidad de descargarlo desde internet.
- JavaDoc del Cliente: Contiene el api del applet cliente.

4.c. CD de desarrollo de @firma (III)

Carpeta Documentación

- Documentación de la plataforma.



4.c. CD de desarrollo de @firma (IV)

KitIntegracionWS

Contiene la información necesaria para conectarse con los WS de la plataforma. Se incluyen también ejemplos de uso de todos los servicios.

- **Ejemplos** → Ejemplos de uso de todos los WS de la plataforma. Para su uso leer el archivo README.
- **SOAP** → Ejemplos de mensajes SOAP de petición y respuesta.
- **Wsdl** → Ficheros de descripción de cada uno de los servicios web que publica la plataforma.
- **Xml** → Ficheros de ejemplo de xml de entrada para cada servicio web. También incluye el xml de respuesta.
- **Xsd** → XSchema general que han de cumplir los xml de entrada y salida de cada servicio web.

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

4.d. Código Fuente. Descripción del servicio (I)

ObtenerInfoCertificado

- Permite extraer la información de un certificado mediante la aplicación del mapeo definido para su tipo. Este proceso verificará que el tipo de certificado se encuentra definido en la plataforma y que la aplicación que realiza la petición tiene acceso a dicho tipo de certificado.

```
<Campo>
        <idCampo>subject</idCampo>
        <valorCampo>
                EMAIL=test@test.com,CN=FEREN
                TEST,givenName=FEREN,SN=TEST,serialNumber=11111111H,OU=000000000,OU=COLEGIO
                NOTARIAL DE TEST,OU=NOTARIO - PRUEBAS,O=CONSEJO
                GENERAL DEL
                NOTARIADO,L=BARCELONA,ST=BARCELONA,C=ES
        </valorCampo>
</Campo>
<Campo>
        <idCampo>tipoCertificado</idCampo>
        <valorCampo>ANCERT PF FERN</valorCampo>
</Campo>
<Campo>
        <idCampo>versionPolitica</idCampo>
        <valorCampo>31</valorCampo>
        </Campo>
<Campo>
```

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

4.d. Código Fuente. Descripción del servicio (II)

ValidarCertificado

- El servicio ValidarCertificado es el responsable de la validación de certificados X509 y el DNI electrónico.
- Es necesario especificar alguno de los modos de validación siguientes.
  - Validación simple (0). Comprueba la caducidad, integridad y confianza del certificado.
  - Validación intermedia (1). Realiza las comprobaciones de la validación simple y el estado de revocación del certificado.
  - Validación compleja (2). Realiza las comprobaciones de la validación intermedia y valida la cadena de confianza al completo.
- Permite recuperar la información asociada al certificado. El campo TIPOAFIRMA permite identificar el tipo de certificado (Guía de Certificados Reconocidos por @firma).
- Empleado para implementar el proceso de autenticación de las aplicaciones.

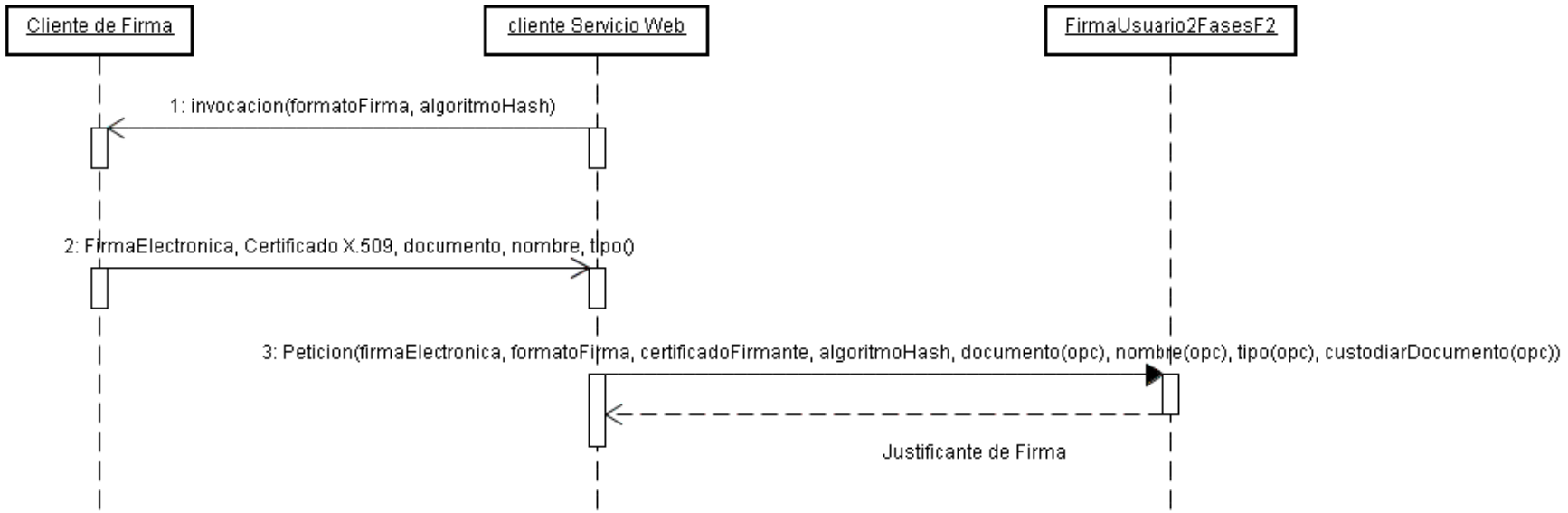
4.d. Código Fuente. Descripción del servicio (III)

Firma electrónica de usuario en 2 fases

- Requiere el uso del cliente de firma de la plataforma.
- Los datos a firmar pueden no ser almacenados en la plataforma.
- Modo de firma introducido en la versión 5 de @firma. Permite la firma de ficheros de gran tamaño.
- Se recomienda el uso de dicho tipo de firma frente a la firma de usuario en 3 fases. Reduce el consumo de recursos de la plataforma.

4.d. Código Fuente. Descripción del servicio (IV)

Firma electrónica de usuario en 2 fases



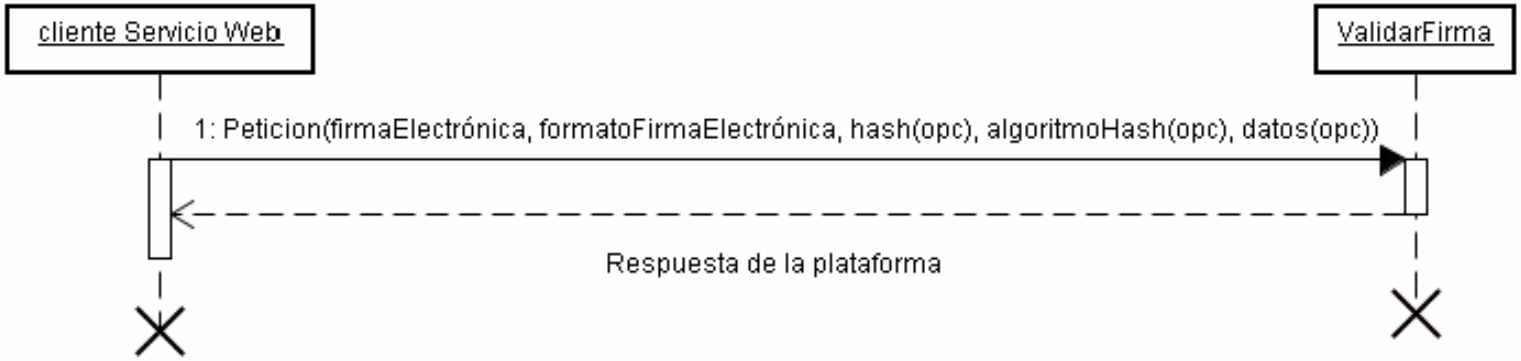
4.d. Código Fuente. Descripción del servicio (V)

Validación de firma electrónica

- Permite realizar una validación completa de la firma electrónica proporcionada al servicio: validación de la firma, validación del certificado X509 y soporte del certificado en la plataforma.
- Puede ser utilizado tanto para validar firmas electrónicas generadas por la plataforma como aquellas ajenas a @firma 5, siempre que su formato sea soportado.

4.d. Código Fuente. Descripción del servicio (VI)

Validación de firma electrónica



4.d. Código Fuente. Descripción del servicio (V)

Obtener Transacción de Firma

- Permite obtener la firma electrónica - codificada en Base64 - asociada a un identificador de transacción
- Con este servicio, se comprueba que la firma realizada está correctamente custodiada en la plataforma, pudiendo además validarla si nuestra aplicación almacena el hash asociado a dicha firma.

5. Conclusiones. Ruegos y Preguntas

JUNTA DE ANDALUCIA
CONSEJERÍA DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA