



Consejería de Hacienda y Administración Pública

Plataforma @firma

Integración con servicios de validación OCSP

Versión: v01r01

Fecha: 20/04/2011

Queda prohibido cualquier tipo de explotación y, en particular, la reproducción, distribución, comunicación pública y/o transformación, total o parcial, por cualquier medio, de este documento sin el previo consentimiento expreso y por escrito de la Junta de Andalucía.



HOJA DE CONTROL

Título	Integración con servicios de validación OCSP		
Entregable			
Nombre del Fichero	Integración OCSP v01r01.doc		
Autor	SCAE		
Versión/Edición	v01r01	Fecha Versión	20/04/2011
Aprobado por		Fecha Aprobación	20/04/2011
		Nº Total Páginas	14

REGISTRO DE CAMBIOS

Versión	Causa	Responsable	Área	Fecha
v01r00	Primera versión del documento	JJLP		18/04/2011
v01r01	Revisión del documento	MPD		20/04/2011

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área
Manuel Perera Domínguez	Jefe de Servicio	Servicio de Coordinación de Admón. Electrónica
José Ignacio Cortés Santos	Gabinete Admón. Electrónica	Servicio de Coordinación de Admón. Electrónica
Cristina Romero Bedoya		Soporte técnico de administración electrónica
Juan José López Portillo		Soporte técnico de plataforma @firma



ÍNDICE

1	Introducción	4
2	Gestión de keystores y contraseñas	5
3	Gestión de métodos de validación	10
4	Gestión de políticas	13



1 Introducción

En este documento se detalla el proceso de configuración de la plataforma, de forma que pueda integrarse con un servicio de validación de certificados electrónicos OCSP (Online Certificate Status Protocol) implantado por un Prestador de Servicios de Certificación. Este protocolo establece que las peticiones deben estar firmadas según la política que imponga este servicio. Este documento se centra en la configuración del método de validación OCSP de forma que siempre envíe las peticiones firmadas, pero al estar relacionada con otras propiedades se explicarán estas para evitar confusiones.

La primera versión de @firma5 compatible con firma de peticiones OCSP es @firma5.2.1 y posteriores, de forma que de tratarse de una versión anterior (ej. @firma5.0.1) no podrá efectuarse esta configuración.

En cuanto se refiere a la política del servidor OCSP, éste puede establecer restricciones en el tipo de certificado que debe usarse para la firma de las peticiones, de forma que solo confiará en aquellas que sean firmadas por certificados de este tipo. Por ejemplo, para hacer uso del servicio OCSP implantado por la FNMT-RCM deben firmarse electrónicamente las peticiones con un “certificado de servicios avanzados” emitido por dicha entidad.

Por parte de @firma, una propiedad importante en el certificado usado para la firma de peticiones es que contenga la extensión OCSPSigning, ya que solo de esta forma se estará cumpliendo con la norma del protocolo OCSP. Además, durante el proceso de petición de alta en el servicio OCSP también se precisa obtener la parte pública del certificado con el cual el servicio OCSP firmará las respuestas y así poder confiar en él. Este certificado deberá incluirse en el AlmacenConfianzaOCSP para que @firma pueda confiar en las respuestas obtenidas.

La configuración final en la plataforma una vez obtenido el certificado necesario es muy sencilla y se lleva a cabo haciendo uso de la gestión de keystores, la gestión de métodos de validación y la gestión de políticas. En la primera parte se incluirá el par de claves del certificado obtenido y el certificado de confianza del OCSP, en la segunda parte se configurará el método de validación de forma que use este certificado para firmar cada petición OCSP enviada y finalmente en la tercera parte se incluirá el método de validación configurado para que sea usado al validar los certificados emitidos por el PSC correspondiente.

Para todo el proceso de configuración se debe acceder a la herramienta de Administración de la plataforma usando la siguiente URL, donde <AFIRMA> debe ser sustituido por la URL real de acceso a la plataforma.

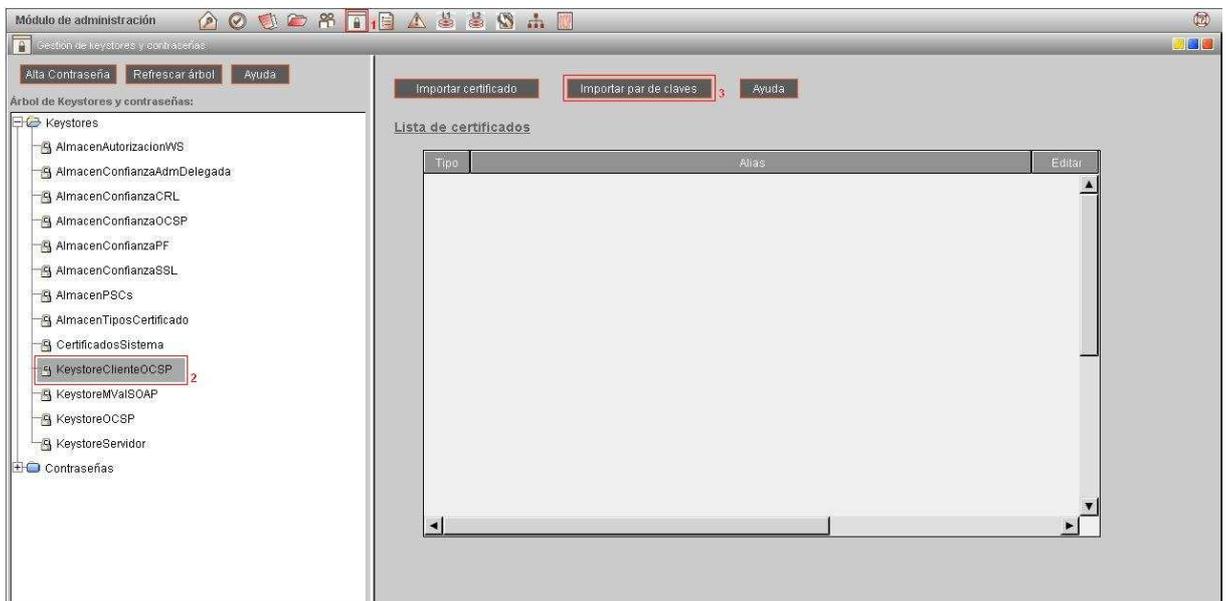
<https://<AFIRMA>/Administracion/index.html>

Las pantallas que se muestran en los siguientes apartados han sido tomadas de la versión 5.3.1 y puede existir alguna diferencia con las otras versiones compatibles, pero los botones básicos de configuración son los mismos. Se resalta en cuadros rojos la selección que debe realizarse en cada caso.

2 Gestión de keystores y contraseñas

La primera parte de la configuración se realiza mediante la gestión de keystores y contraseñas, concretamente en el KeystoreClienteOCSP y el AlmacenConfianzaOCSP. El proceso de configuración es el siguiente:

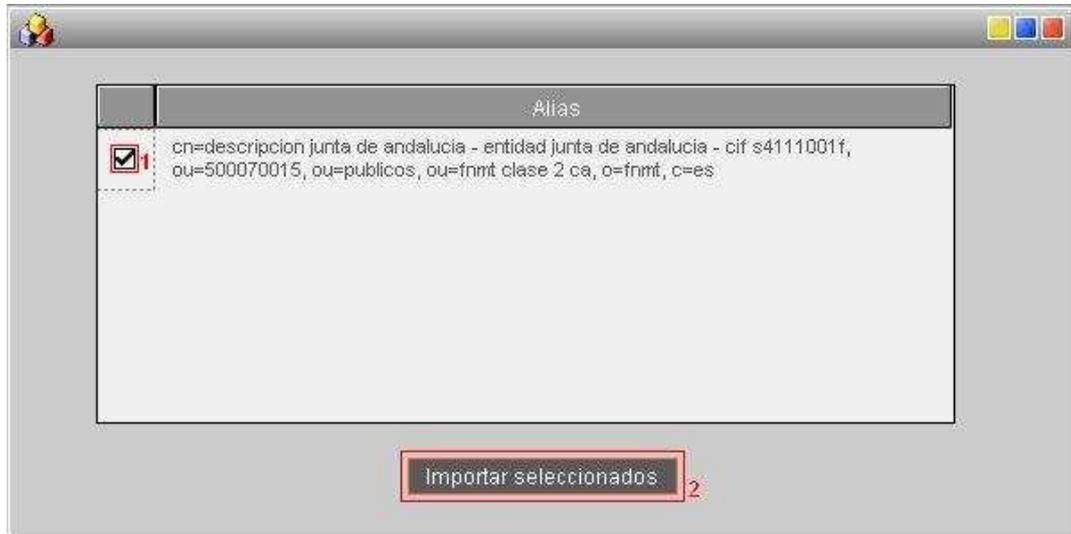
1. Se procede a Incluir el par de claves obtenido dentro del KeystoreClienteOCSP. (A partir de @firma5.3.1 se pide al usuario la contraseña usada para logarse para poder realizar la operación).



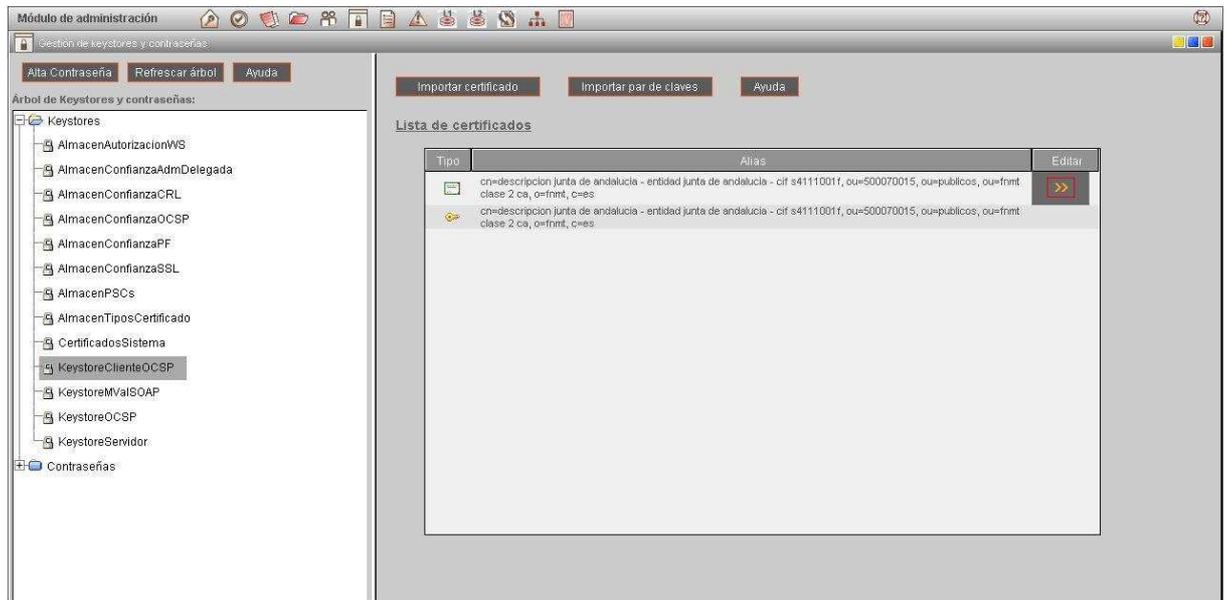
2. Se selecciona el archivo que contiene el par de claves e introducimos su clave



3. Se selecciona el certificado correspondiente. En caso de haber varios debemos saber cual usar.



4. Se selecciona el par de claves importado para modificar su alias.



- Se modifica el alias con el nombre deseado, ya que posteriormente se deberá utilizarlo. (A partir de @firma5.3.1 se pide al usuario la contraseña usada para logarse para poder realizar la operación).



Datos del certificado

Alias: *

Versión:

Subject:

Emisor:

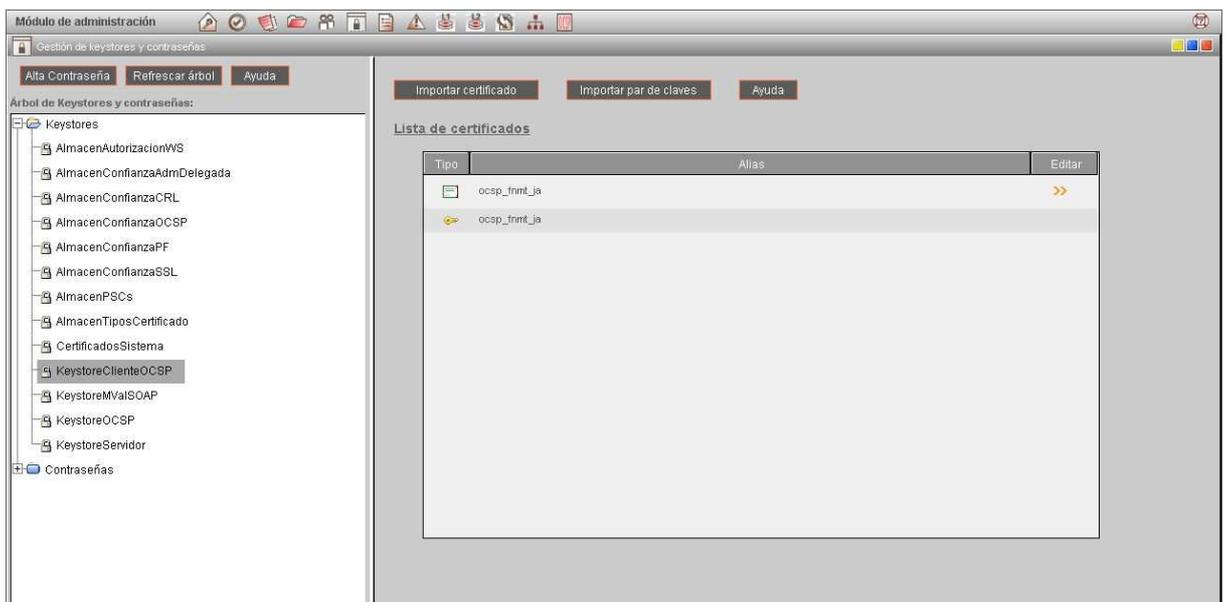
Número de serie:

Válido desde:

Válido hasta:

Clave pública:

- Ya se tiene configurado el keystore con el par de claves necesario.



Módulo de administración

Gestión de keystores y contraseñas

Alta Contraseña Refrescar árbol Ayuda

Importar certificado Importar par de claves Ayuda

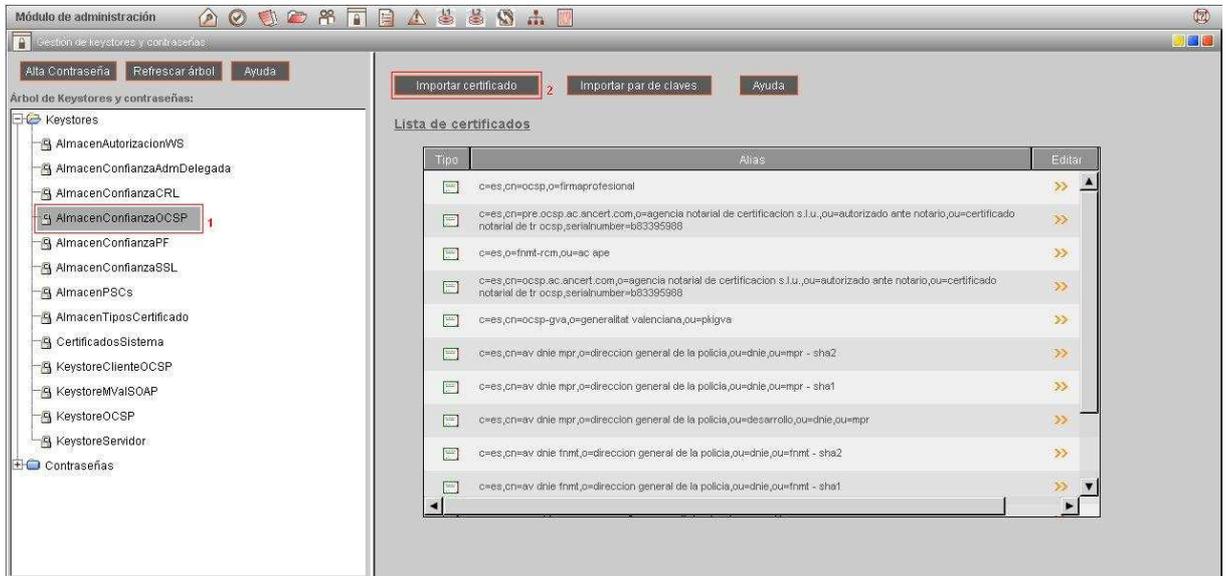
Árbol de Keystores y contraseñas:

- Keystores
 - AlmacenAutorizacionWS
 - AlmacenConfianzaAdmDelegada
 - AlmacenConfianzaCRL
 - AlmacenConfianzaOCSP
 - AlmacenConfianzaPF
 - AlmacenConfianzaSSL
 - AlmacenPSCs
 - AlmacenTiposCertificado
 - CertificadosSistema
 - KeystoreClienteOCSP
 - KeystoreMValSOAP
 - KeystoreOCSP
 - KeystoreServidor
- Contraseñas

Lista de certificados

Tipo	Alias	Editar
	ocsp_fnmt_ja	
	ocsp_fnmt_ja	

7. Se incluye el certificado de confianza del servicio OCSP en el AlmacenConfianzaOCSP, seleccionando esta vez Importar Certificado.



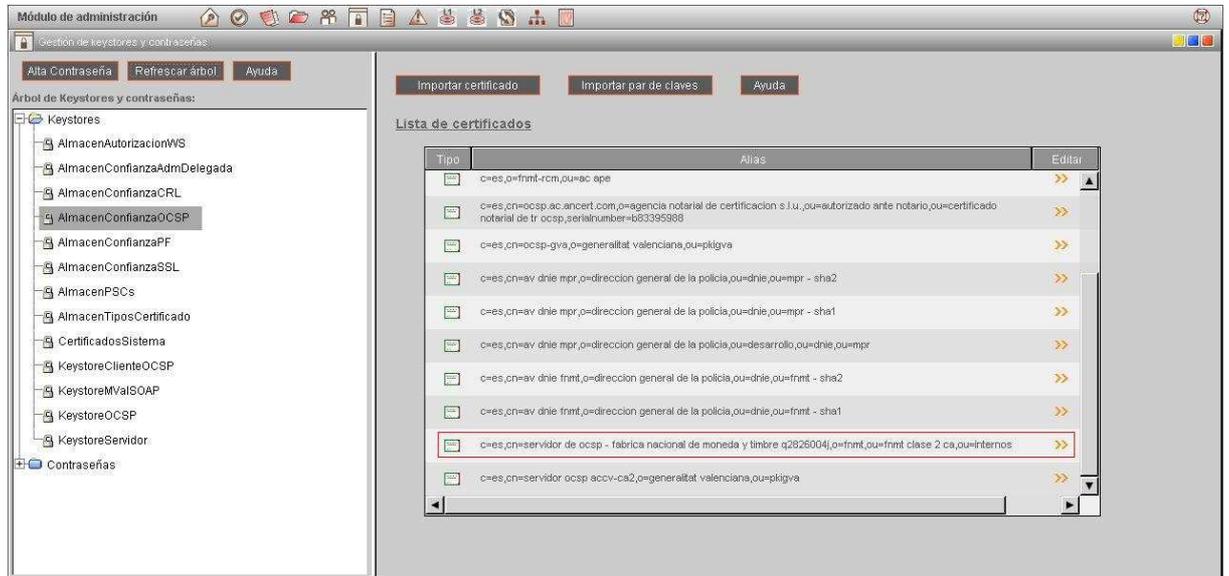
8. Se selecciona el certificado obtenido en el alta para confiar en el servicio OCSP.



9. Se acepta el alias que ya tiene el certificado o se modifica si se cree conveniente. Este alias solo es indicativo y no se usa en otras configuraciones.



10. Se puede comprobar que efectivamente ya se tiene el certificado de confianza incluido y así @firma podrá confiar en las respuestas del servicio OCSP.



Módulo de administración

Gestión de keystores y contraseñas

Alta Contraseña Refrescar árbol Ayuda

Arbol de Keystores y contraseñas:

- Keystores
 - AlmacenAutorizacionWS
 - AlmacenConfianzaAdmDelegada
 - AlmacenConfianzaCRL
 - AlmacenConfianzaOCSP
 - AlmacenConfianzaPF
 - AlmacenConfianzaSSL
 - AlmacenPSCs
 - AlmacenTiposCertificado
 - CertificadosSistema
 - KeystoreClienteOCSP
 - KeystoreMValSOAP
 - KeystoreOCSP
 - KeystoreServidor
- Contraseñas

Importar certificado Importar par de claves Ayuda

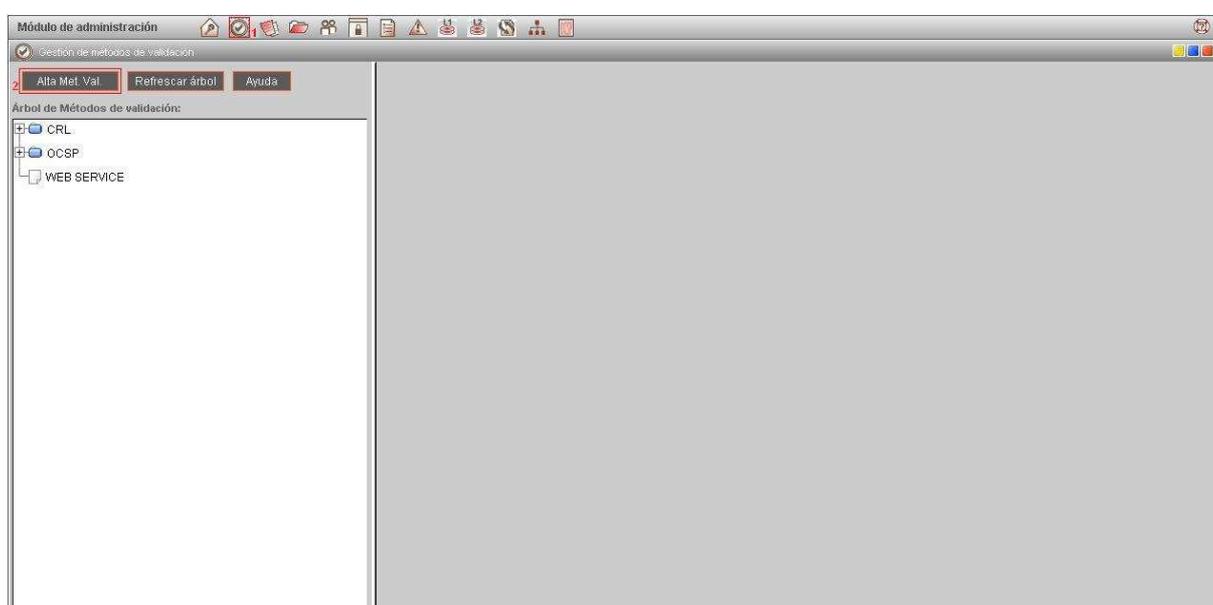
Lista de certificados

Tipo	Alias	Editar
	c=es, o=frmt-rcm, ou=ac ape	>>
	c=es, cn=ocsp.acancert.com, p=agencia notarial de certificación s.l.u., ou=autorizado ante notario, ou=certificado notarial de tr ocsp, serialnumber=683395988	>>
	c=es, cn=ocsp-gva, o=generalitat_valenciana, ou=pligva	>>
	c=es, cn=av dnle mpr, o=direccion general de la policia, ou=dnle, ou=mpr - sha2	>>
	c=es, cn=av dnle mpr, o=direccion general de la policia, ou=dnle, ou=mpr - sha1	>>
	c=es, cn=av dnle mpr, o=direccion general de la policia, ou=desarrollo, ou=dnle, ou=mpr	>>
	c=es, cn=av dnle frmt, o=direccion general de la policia, ou=dnle, ou=frmt - sha2	>>
	c=es, cn=av dnle frmt, o=direccion general de la policia, ou=dnle, ou=frmt - sha1	>>
	c=es, cn=servidor de ocsp - fabrica nacional de moneda y timbre q2826004, o=frmt, ou=frmt clase 2 ca, ou=internos	>>
	c=es, cn=servidor ocsp.ecov-ca2, o=generalitat_valenciana, ou=pligva	>>

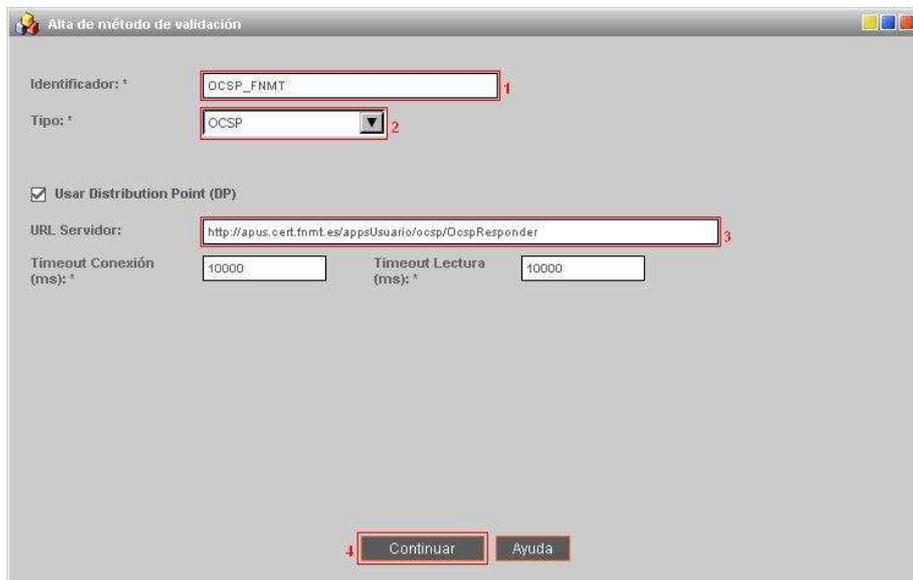
3 Gestión de métodos de validación

Una vez configurado el KeystoreClienteOCSP ya se puede configurar el método de validación OCSP para la firma electrónica de las peticiones. Las pantallas de configuración siguientes pertenecen a la gestión de métodos de validación y siguen el ejemplo anterior para integrarse con el servicio OCSP de la FNMT-RCM.

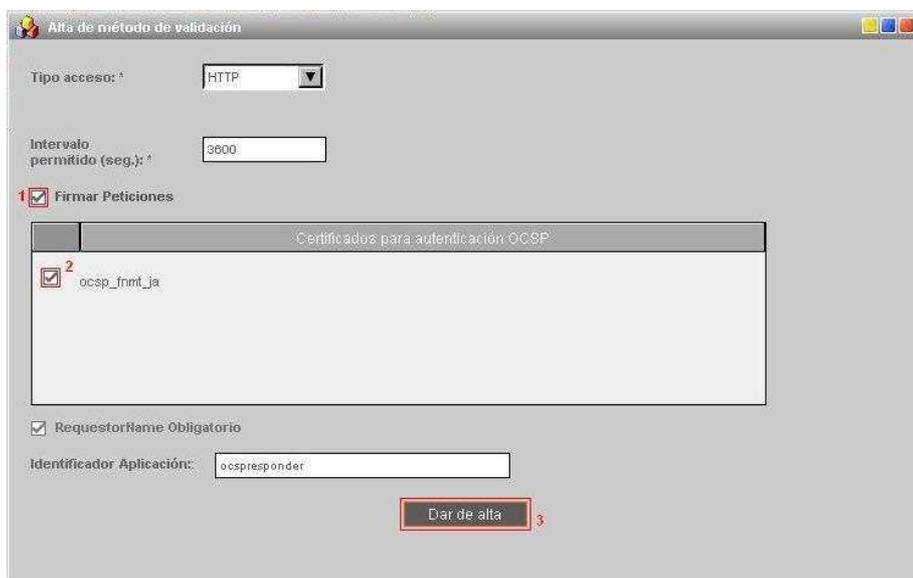
1. Se procede a dar de alta un nuevo método de validación. Si se ha importado alguna política de emitida por la Junta de Andalucía podrá modificarse el método de validación OCSP_FNMT en lugar de dar de alta uno nuevo.



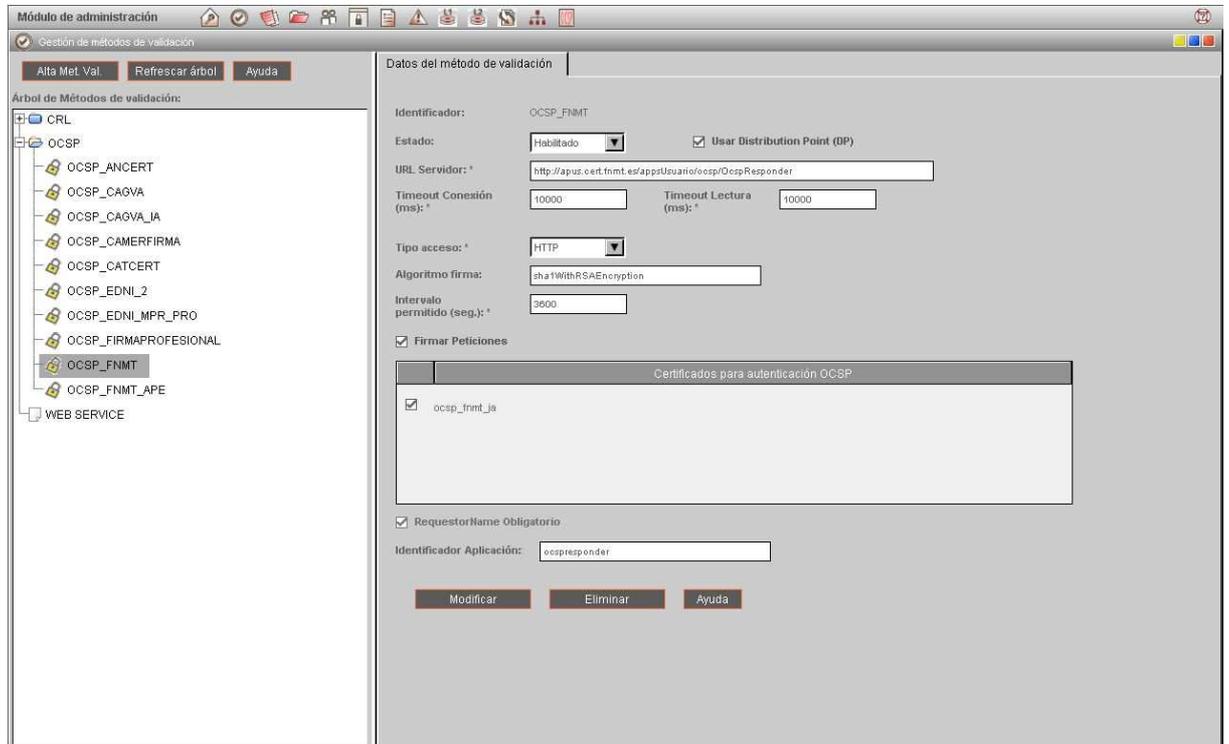
2. Se configura el nombre, tipo OCSP y la URL que ofrece el servicio antes de continuar. El resto de propiedades deben dejarse por defecto.
 - a. Identificador – Nombre del nuevo método de validación (OCSP_FNMT)
 - b. Tipo – OCSP
 - c. Usar Distribution Point (DP) – Se usará el punto de distribución indicado en el certificado que se valide cada vez, omitiendo la URL base del servicio configurado.
 - d. URS servidor – Es obligatorio configurar la URL de acceso al servicio OCSP que se está configurando, pero al estar DP activado siempre se usará la URL del servicio OCSP indicada por cada certificado.
 - e. Timeouts – Tiempo máximo de conexión y de lectura en milisegundos.



3. En esta ventana seleccionamos la casilla para firma de peticiones y el alias configurado en punto 6 del apartado anterior, correspondiente al certificado obtenido para la firma electrónica de las peticiones OCSP.
 - a. Tipo de acceso – Debe ser HTTP.
 - b. Intervalo permitido – Desfase de actualización del estado de revocación permitido en el OCSP.
 - c. Firmar Peticiones – Aquí se indica que el OCSP es privado y se selecciona el alias a usar de entre los contenidos en el KeystoreClienteOCSP.
 - d. RequestorName Obligatorio – Propiedad exclusiva para la integración de @firma con un servicio OCSP de otro @firma. Debe indicarse un identificador de aplicación por defecto, pero no será usado en los procesos OCSP. Se usa por defecto el identificador 'ocspresponder'.



4. Finalmente ya se tiene configurado el método de validación.

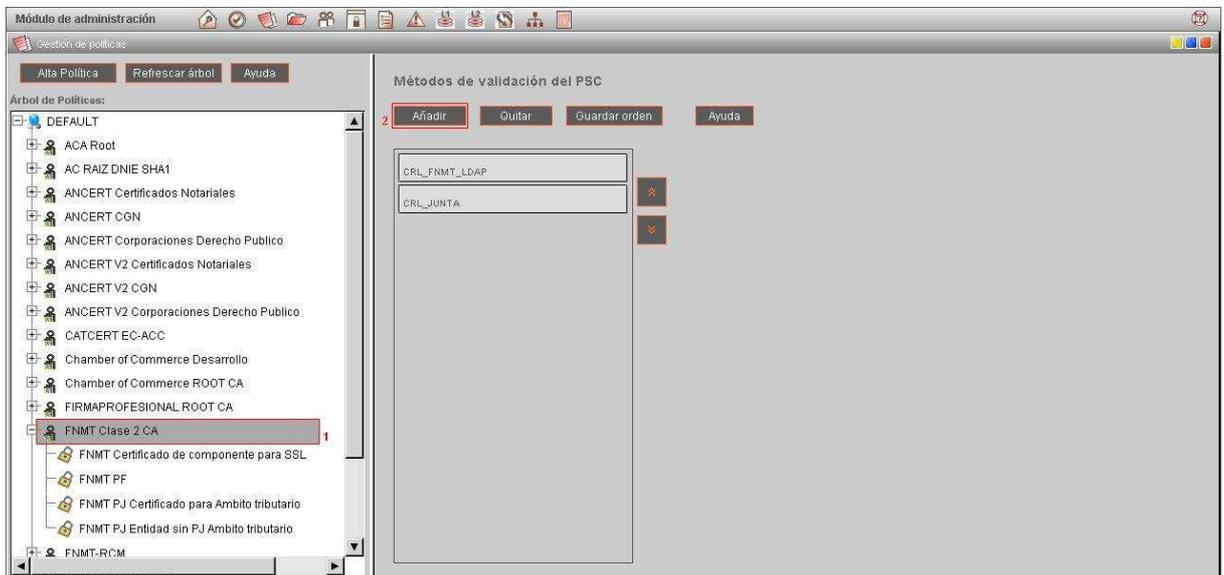


The screenshot displays the 'Módulo de administración' interface for managing validation methods. On the left, a tree view shows the 'Arbol de Métodos de validación' with 'OCSP' expanded and 'OCSP_FNMT' selected. The main area, titled 'Datos del método de validación', shows the configuration for 'OCSP_FNMT'. The status is 'Habilitado' and 'Usar Distribution Point (BP)' is checked. The server URL is 'http://apus.cert.fnmt.es/appt/usuario/ocsp/OcspResponder'. Connection and reading timeouts are both set to 10000 ms. The access type is 'HTTP' and the signature algorithm is 'sha1WithRSAEncryption'. The allowed interval is 3000 seconds. The 'Firmar Peticiones' checkbox is checked, and a table below it lists 'ocsp_fnmt_ja' as a certificate for authentication. The 'RequestorName Obligatorio' checkbox is also checked, and the application identifier is 'ocspresponder'. At the bottom, there are buttons for 'Modificar', 'Eliminar', and 'Ayuda'.

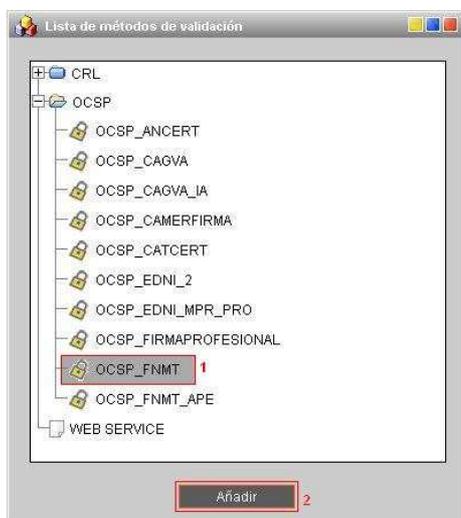
4 Gestión de políticas

Ya configurados los keystores y el método de validación únicamente falta activarlo en la política usada, junto con el resto de métodos de validación del PSC en concreto. En este ejemplo se refiere al PSC FNMT Clase 2 CA, de forma que se tendrá que incluir el nuevo método para que se utilice en la validación de los certificados emitidos por este PSC.

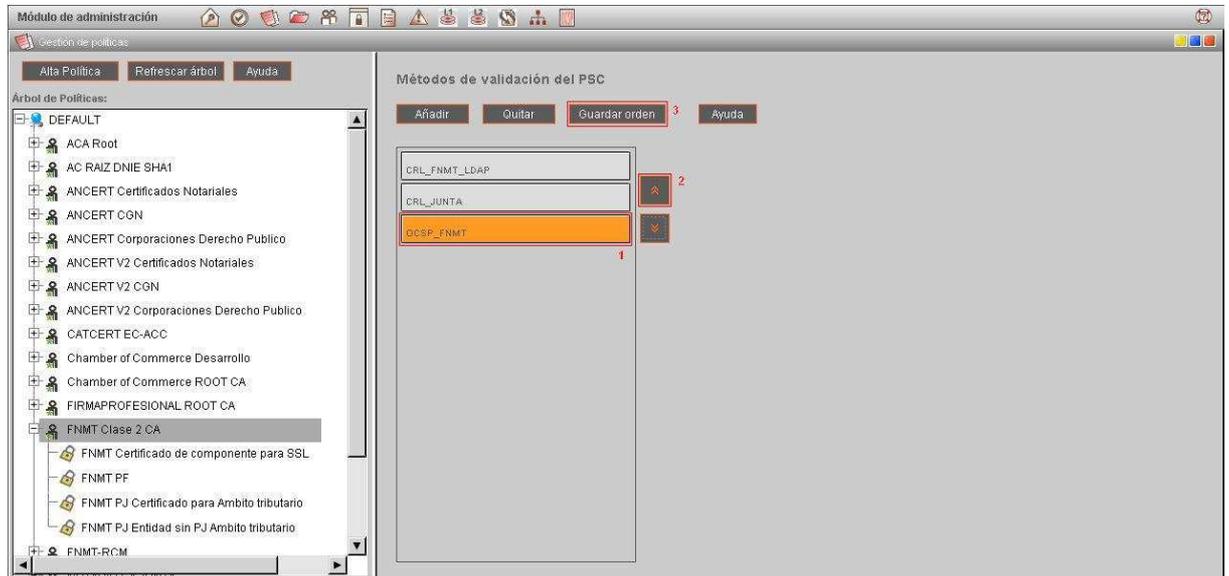
1. En la gestión de políticas se selecciona el PSC correspondiente y se añade un nuevo método de validación. En función del PSC correspondiente al OCSP configurado puede seleccionarse una CA o SubCA, pero nunca un certificado final. Esto significa que todos los certificados emitidos por la CA/subCA seleccionada usarán los métodos de validación configurados.



2. Se selecciona el método OCSP configurado y se añade a la lista.



3. Se establece el orden de uso conveniente para la validación, situando OCSP_FNMT el primero.



4. Ya se dispone del resultado final de la lista de métodos de validación y la plataforma configurada para hacer uso del servicio OCSP.

