



Consejería de Hacienda y Administración Pública

@firma5

Actualización Certificado de Confianza de OCSP para APE de FNMT

Versión: 1.0

Fecha: 30/11/2011

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	Actualización Certificado de Confianza de OCSP para APE de FNMT		
Entregable	Entregable del Proyecto @firma5		
Nombre del Fichero	Actualización CertificadoAPE.doc		
Autor	Pablo Pizarro Armendáriz		
Versión/Edición	1.0	Fecha Versión	30/11/2011 1
Aprobado por	José Ignacio Cortés Santos	Fecha Aprobación	30/11/2011 1
		Nº Total Páginas	6

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
1.0	Primera versión del documento Versión 1.0	Pablo Pizarro Armendáriz		30/11/2011



Consejería de Hacienda y Administración Pública

Dirección General de Tecnologías para Hacienda y la Administración Electrónica

@firma5

Actualización de certificado de confianza para OCSP APE FNMT

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área	Nº Copias
Manuel Perera Domínguez	Jefe de Servicio	Servicio de Coordinación de Admón. Electrónica	1
José Ignacio Cortés Santos	Gabinete admón electrónica	Servicio de Coordinación de Admón. Electrónica	1



ÍNDICE

1. Introducción.....	5
2. Proceso de importación	5
2.1. Modificación de Alias	5
2.2. Importar Certificado.....	5
2.3. Eliminar Certificado Antiguo.....	6



1. INTRODUCCIÓN

Este documento ha sido elaborado para indicar el proceso de actualización en la Plataforma @firma 5 del certificado de confianza para la validación de certificados APE a través del protocolo OCSP ofrecido por FNMT-RCM.

El motivo de esta actualización es la caducidad del certificado actual del próximo 8 de diciembre. No obstante, FNMT-RCM va a realizar el cambio de certificado el próximo 5 de diciembre.

2. PROCESO DE IMPORTACIÓN

2.1. MODIFICACIÓN DE ALIAS

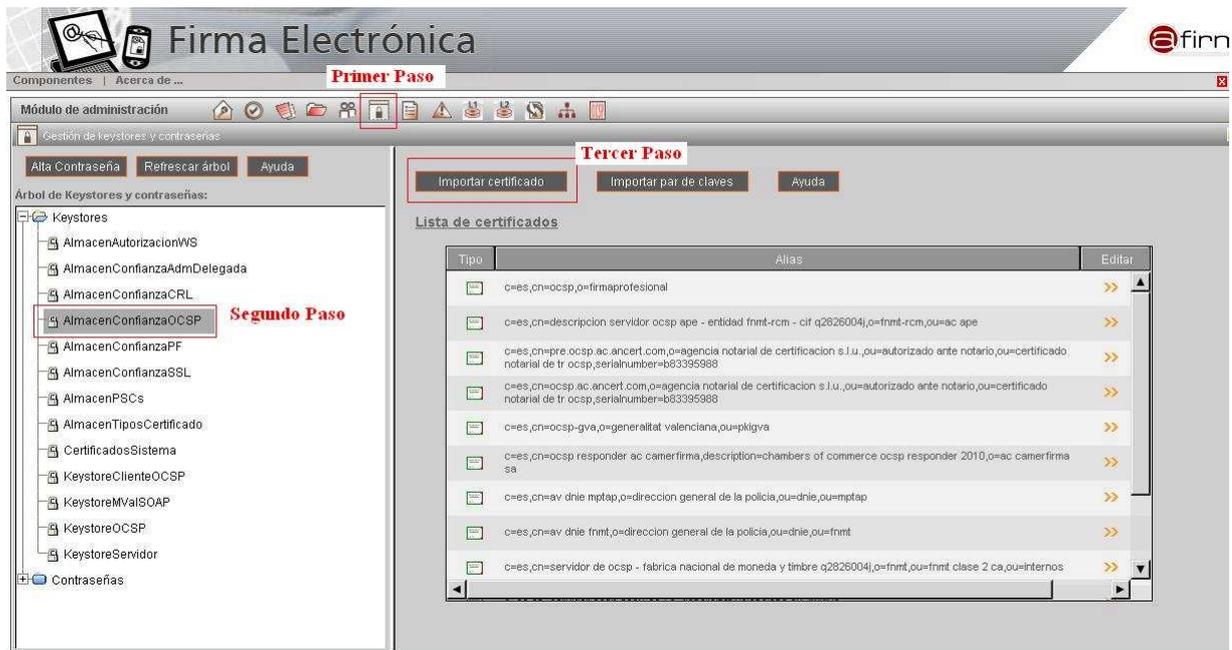
Selección del certificado que va a caducar el día 8/12/2011, para ello se debe seleccionar el keystore "**AlmacenConfianzaOCSP**" en el módulo "**Gestión de Keystores y contraseñas**".

El certificado debe tener un alias similar a "**c=es,cn=descripcion servidor ocsp ape - entidad fnmt-rcm - cif q2826004j,o=fnmt-rcm,ou=ac ape**" (siempre y cuando no se modificara cuando se importó). Modificar el alias, por ejemplo añadiéndole la cadena "old" al final, esto es simplemente para una vez importemos el nuevo certificado veamos claramente cuál era el antiguo.

2.2. IMPORTAR CERTIFICADO

A continuación se detallan los pasos a realizar para importar el certificado. Se considera que previamente el usuario se ha logado en la herramienta de administración del @firma y ya se encuentra en el módulo de "**Gestión de Keystores y contraseñas**".

- **Primer paso:** Seleccionar el keystore "AlmacenConfianzaOCSP".
- **Segundo paso:** Pulsa en "Importar certificado". Se solicitará que se vuelva a introducir el password del usuario.



The screenshot shows the 'Firma Electrónica' application interface. The main window is titled 'Módulo de administración' and 'Gestión de keystores y contraseñas'. On the left, there is a tree view of 'Keystores' with 'AlmacenConfianzaOCSP' selected. On the right, there is a 'Lista de certificados' table with columns 'Tipo', 'Alias', and 'Editar'. The table contains several rows of certificate information. The 'Importar certificado' button is highlighted in red.

- **Tercer paso:** Seleccionar el certificado recibido junto a este documento y pulsar sobre “Continuar”.
- **Cuarto paso:** Confirmar la importación del certificado.
- **Quinto paso:** Verificar que el certificado importado se encuentra en la lista de certificados. Para ello buscamos el alias mostrado en la pantalla anterior en la lista de certificados y

pulsamos sobre el icono editar:  , en la pantalla de edición verificamos la nueva fecha de caducidad.

2.3. ELIMINAR CERTIFICADO ANTIGUO

ATENCIÓN: No debe eliminar el certificado antiguo antes de la caducidad del mismo, es decir, deberá mantenerlo como mínimo hasta el próximo 8 de diciembre de 2011. Una vez superada esa fecha, podrá proceder a su eliminación según las instrucciones que se indican a continuación.

Una vez importado y verificado el nuevo certificado importado, se procede a eliminar el certificado antiguo (el certificado al que le modificamos el alias), para ello se recomienda seguir los pasos mostrados a continuación. Se considerará que el usuario está logado en la herramienta de administración y ha seleccionado el módulo “Gestión de Keystores y contraseñas” e igual que en el paso anterior ha seleccionado el keystore “AlmacenConfianzaOCSP”.



- **Primer paso:** se selecciona el certificado que se desea eliminar, con alias *“c=es,cn=descripcion servidor ocsp ape - entidad fnmt-rcm - cif q2826004j,o=fnmt-rcm,ou=ac ape”*. Para ello pulsar sobre el botón editar de dicho certificado:  .
- **Segundo paso:** Verificamos que dicho certificado es el que caduca próximamente.
- **Tercer paso:** Pulsamos sobre eliminar certificado y confirmamos la operación.