



Plataforma @firma

Actualización Certificado de confianza de OCSP para FNMT-APE

Versión: v01r01

Fecha: 07/11/2012

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 FNMT-APE		
Entregable	Documentación Plataforma @firma		
DNombre del Fichero	20121106-Actualizacion Certificado OCSP FNMT-APE		
Autor	SCAE		
Versión/Edición	v01r01	Fecha Versión	06/11/2012
Aprobado por	José Ignacio Cortés Santos	Fecha Aprobación	07/11/2012
		Nº Total Páginas	6

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r00	Primera versión del documento	Ernesto Salgado Suárez		06/11/2012
v01r01	Revisión del documento	José Ignacio Cortés Santos		07/11/2012

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
Ernesto Salgado Suárez	Soporte @firma	Soporte de Administración Electrónica	1

ÍNDICE

1.Introducción.....	5
2.Actualización Certificado.....	5
2.1.Modificación de Alias.....	5
2.2.Importar Certificado.....	5
2.3.Eliminar Certificado Antiguo.....	5

1. INTRODUCCIÓN

Este documento describe el proceso de actualización en la Plataforma @firma del certificado de confianza para la validación de certificados de FNMT-APE a través del protocolo OCSP. El motivo de esta actualización es la caducidad del certificado actual el próximo día 09 de noviembre de 2012.

2. ACTUALIZACIÓN CERTIFICADO

2.1. MODIFICACIÓN DE ALIAS

Selección del certificado que va a caducar el día 09/11/2012, para ello se debe seleccionar el keystore "**AlmacenConfianzaOCSP**" en el módulo "**Gestión de Keystores y contraseñas**".

El certificado debe tener en el alias el common name "**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 diferenciamos claramente 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 identificado correctamente en la herramienta de administración de @firma y 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 la contraseña del usuario.
- **Tercer paso:** Seleccionar el certificado adjunto a este documento en la carpeta "**OCSP FNMT-APE**" 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 (22/04/2013)

2.3. ELIMINAR CERTIFICADO ANTIGUO

Este paso debe realizarse una vez caducado el certificado actual, con fecha posterior al 9 de noviembre de 2012.

Una vez importado y verificado el nuevo certificado importado, y **con fecha posterior a la caducidad del certificado actual**, 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 identificado 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, donde el alias contiene el common name “**c=es,cn=descripcion servidor ocsp ape - entidad fnmt-rcm**” y termina con la cadena “**old**”. Es el certificado cuyo alias modificamos en el paso “2.1 Modificación de Alias”. Para ello pulsar sobre el botón editar de dicho certificado.
- **Segundo paso:** Verificamos que dicho certificado es el que deseamos eliminar, la fecha de caducidad debe ser del 09 de Noviembre de 2012.
- **Tercer paso:** Pulsamos sobre eliminar certificado y confirmamos la operación.