



Junta de Andalucía

Plataforma @firma

**Actualización Certificados Actualización Certificado de confianza de
OCSP AC RAIZ FNMT-RCM**

Versión: v01r00

Fecha: 02/07/2020

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 Certificados Actualización Certificado de confianza de OCSP AC RAIZ FNMT-RCM		
Entregable	Documentación Plataforma @firma		
Nombre del Fichero	20200702-Actualizacion Certificado Servidor OCSP AC RAIZ FNMT-RCM		
Autor	SCAE		
Versión/Edición	v01r00	Fecha Versión	02/07/2020
Aprobado por	José Ignacio Cortés Santos	Fecha Aprobación	02/07/2020
		Nº Total Páginas	7

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r00	Primera versión del documento	UTE		02/07/2020



CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área	Nº Copias
Manuel Escobar Montes	Jefe de Servicio	Servicio de Coordinación de Admón. Electrónica	1
José Ignacio Cortés Santos	Gabinete admón electrónica	Servicio de Coordinación de Admón. Electrónica	1
Francisco Javier Toro Ferreira	Soporte @firma	Soporte de Administración Electrónica	1
Miguel Angel Ager Vázquez	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.....	7



1. INTRODUCCIÓN

Este documento ha sido elaborado para indicar el proceso de actualización en la Plataforma @firma del certificado de confianza para la validación de certificados emitidos por RAIZ FNMT-RCM a través del protocolo OCSP. El motivo de esta actualización es la caducidad del actual certificado el día 13 de julio de 2020 y su sustitución el martes **7 de julio de 2020 a las 16:30 horas**.

El nuevo certificado tienen validez hasta el 1 de enero de 2021.

2. ACTUALIZACIÓN CERTIFICADO

2.1. MODIFICACIÓN DE ALIAS

Selección del certificado que va a caducar el día 13/07/2020, 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=servidor ocsp ac raiz fnmt-rcm,o=fnmt-rcm,ou=ac raiz fnmt-rcm**” (siempre y cuando no se modificara cuando se importó). Modificar el alias, por ejemplo añadiéndole la cadena “**old**” al final, para diferenciar el antiguo certificado del nuevo que desea importarse.

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 “**certificado**” 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 (01/01/2021).



2.3. ELIMINAR CERTIFICADO ANTIGUO

Opcionalmente, una vez importado y verificado el nuevo certificado, con fecha posterior a la caducidad del certificado antiguo (el certificado al que le modificamos el alias), se procederá a su eliminación. 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=servidor ocs ac componentes inform\c3\la1ticos,o=fnmt-rcm,ou=ac componentes inform\c3\la1ticos**” .
- **Segundo paso:** Verificamos que dicho certificado es el que deseamos eliminar, la fecha de caducidad debe ser del 12 de marzo de 2020.
- **Tercer paso:** Pulsamos sobre eliminar certificado y confirmamos la operación.