



## **Plataforma @firma**

---

### **Actualización Certificado de confianza de OCSP AC FNMT Usuarios**

Versión: v01r00

Fecha: 20/05/2019

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.

 <b>JUNTA DE ANDALUCÍA</b>	<b>Consejería de Hacienda, Industria y Energía</b> <b>Dirección General de Política Digital</b>	<b>Plataforma @firma</b> <b>Actualización Certificado de confianza de OCSP AC FNMT Usuarios</b>
--	--	--

## HOJA DE CONTROL

<b>Título</b>	Actualización Certificado de confianza de OCSP AC FNMT Usuarios		
<b>Entregable</b>	Documentación Plataforma @firma		
<b>Nombre del Fichero</b>	20190520-Actualizacion Certificado Servidor OCSP AC FNMT Usuarios		
<b>Autor</b>	SCAE		
<b>Versión/Edición</b>	v01r00	<b>Fecha Versión</b>	09/05/2019
<b>Aprobado por</b>	José Ignacio Cortés Santos	<b>Fecha Aprobación</b>	20/05/2019
		<b>Nº Total Páginas</b>	6

## REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r00	Primera versión del documento	UTE		20/05/2019

## CONTROL DE DISTRIBUCIÓN

<b>Nombre y Apellidos</b>	<b>Cargo</b>	<b>Área</b>	<b>Nº Copias</b>
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
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.....	5

## 1. INTRODUCCIÓN

Este documento ha sido elaborado para indicar el proceso de actualización en la Plataforma @firma del certificado de confianza para la validación mediante el protocolo OCSP de los certificados emitidos por AC FNMT Usuarios. El día **20 de mayo de 2019 a las 16:30**, FNMT procederá a realizar el cambio del certificado que firma las respuestas OCSP, en la validación de los certificados emitidos por la Autoridad de Certificación AC Usuarios FNMT-RCM. El motivo de esta actualización es la caducidad del certificado actual el día 22 de mayo de 2019.

El nuevo certificado tiene validez hasta el 08 de noviembre de 2019.

## 2. ACTUALIZACIÓN CERTIFICADO

### 2.1. MODIFICACIÓN DE ALIAS

Selección del certificado que va a caducar el día 22/05/2019, 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 fnmt usuarios,o=fnmt-rcm,ou=ceres**" (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 (08/11/2019).

### 2.3. ELIMINAR CERTIFICADO ANTIGUO

Una vez importados y verificados los nuevos certificados, **con fecha posterior a la caducidad del certificado antiguo** 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=servidor ocsp ac fnmt usuarios,o=fnmt-rcm,ou=ceres**” 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 22 de mayo de 2019.
- **Tercer paso:** Pulsamos sobre eliminar certificado y confirmamos la operación.