



Junta de Andalucía

Plataforma @firma

**Actualización Certificados de confianza de OCSP FNMT AC
Componentes Informáticos y FNMT AC Administración Pública**

Versión: v01r00

Fecha: 05/02/2021

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.

	Consejería de la Presidencia, Administración Pública e Interior Dirección General de Estrategia Digital y Gobierno Abierto	Plataforma @firma Actualización Certificados de confianza de OCSP FNMT AC Componentes Informáticos y FNMT AC Administración Pública
---	---	--

HOJA DE CONTROL

Título	Actualización Certificados de confianza de OCSP FNMT AC Componentes Informáticos y FNMT AC Administración Pública		
Entregable	Documentación Plataforma @firma		
Nombre del Fichero	202102~1		
Autor	SCAE		
Versión/Edición	v01r00	Fecha Versión	05/02/2021
Aprobado por	José Ignacio Cortés Santos	Fecha Aprobación	05/02/2021
		Nº Total Páginas	7

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r00	Primera versión del documento	UTE		05/02/2021

	Consejería de la Presidencia, Administración Pública e Interior Dirección General de Estrategia Digital y Gobierno Abierto	Plataforma @firma Actualización Certificados de confianza de OCSP FNMT AC Componentes Informáticos y FNMT AC Administración Pública
---	---	--

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 Certificados.....	5
2.1. Modificación de alias.....	5
2.2. Importar Certificados.....	5
2.3. Eliminar Certificados Antiguos.....	7

1. INTRODUCCIÓN

Este documento ha sido elaborado para indicar el proceso de actualización en la Plataforma @firma de los certificados de confianza para la validación de certificados emitidos por FNMT AC Componentes Informáticos y FNMT AC Administración Pública a través del protocolo OCSP. El motivo de esta actualización es la caducidad de los certificado actuales el día 14 de Febrero de 2021

Los nuevos certificados tienen validez hasta el 4 de Agosto de 2021.

2. ACTUALIZACIÓN CERTIFICADOS

2.1. MODIFICACIÓN DE ALIAS

Selección de los certificados que va a caducar el día 14/02/2021, 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 componentes inform\c3\la1ticos,o=fnmt-rcm,ou=ac componentes inform\c3\la1ticos**” o “**c=es,cn=servidor ocsp ac administraci\c3\b3n p\c3\bablica,o=fnmt-rcm,ou=ceres,serialnumber=q2826004j**” (siempre y cuando no se modificaran cuando se importaran). Modificar el alias, por ejemplo añadiéndole la cadena “**old**” al final, para diferenciar el antiguo certificado del nuevo que desea importarse.

2.2. IMPORTAR CERTIFICADOS

A continuación se detallan los pasos a realizar para importar los certificados. 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.

	Consejería de la Presidencia, Administración Pública e Interior Dirección General de Estrategia Digital y Gobierno Abierto	Plataforma @firma Actualización Certificados de confianza de OCSP FNMT AC Componentes Informáticos y FNMT AC Administración Pública
---	---	--

- **Tercer paso:** Seleccionar uno de los certificados 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 (04/08/2021).

2.3. ELIMINAR CERTIFICADOS ANTIGUOS

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 ocsp ac componentes inform\c3\la1ticos,o=fnmt-rcm,ou=ac componentes inform\c3\la1ticos**” o “**c=es,cn=servidor ocsp ac administraci\c3\b3n p\c3\bablica,o=fnmt-rcm,ou=ceres,serialnumber=q2826004j**”.
- **Segundo paso:** Verificamos que dicho certificado es el que deseamos eliminar, la fecha de caducidad debe ser del 14 de Febrero de 2021.
- **Tercer paso:** Pulsamos sobre eliminar certificado y confirmamos la operación.