




**Plataforma @firma**

---

**Actualización Certificados de Confianza**

Versión: 1.1

Fecha: 13/03/12

 <p>JUNTA DE ANDALUCÍA</p>	<p><b>Consejería de Hacienda y Administración Pública</b></p> <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p>	<p><b>Plataforma @firma</b></p> <p>Actualización de certificados de confianza</p>
---	---	---

## HOJA DE CONTROL

<b>Título</b>			
<b>Entregable</b>	Entregable del Proyecto @firma5		
<b>Nombre del Fichero</b>	Actualización_Certificados_Confianza_13_03_2012		
<b>Autor</b>	DGTHAE		
<b>Versión/Edición</b>	1.1	<b>Fecha Versión</b>	13/03/12
<b>Aprobado por</b>	José Ignacio Cortés Santos	<b>Fecha Aprobación</b>	13/03/12
		<b>Nº Total Páginas</b>	7


## REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
1.0	Primera versión del documento	Pablo Pizarro Armendáriz	UTE	13/03/12
1.1	Revisión del documento	José Ignacio Cortés Santos	SCAE	13/03/12

	<b>Consejería de Hacienda y Administración Pública</b>  <b>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</b>	<b>Plataforma @firma</b>  <b>Actualización de certificados de confianza</b>
---	---	---

## 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

 <p>JUNTA DE ANDALUCÍA</p>	<p><b>Consejería de Hacienda y Administración Pública</b></p> <p><b>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</b></p>	<p><b>Plataforma @firma</b></p> <p><b>Actualización de certificados de confianza</b></p>
---	--	--

## ÍNDICE

1.Introducción.....	5
2.Actualización certificado ANCERT.....	5
2.1.Modificación de Alias.....	5
2.2.Importar Certificado.....	5
2.3.Eliminar Certificado Antiguo.....	6
3.Actualización Certificado DNle FNMT.....	6
3.1.Modificación de Alias.....	6
3.2.Importar Certificado.....	7
3.3.Eliminar Certificado Antiguo.....	7

 <p>JUNTA DE ANDALUCÍA</p>	<p><b>Consejería de Hacienda y Administración Pública</b></p> <p><b>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</b></p>	<p><b>Plataforma @firma</b></p> <p><b>Actualización de certificados de confianza</b></p>
---	--	--

## 1. INTRODUCCIÓN

Este documento ha sido elaborado para indicar el proceso de actualización en la Plataforma @firma v5 de:

- Certificado de confianza para la validación de certificados ANCERT a través del protocolo OCSP.
- Certificado de confianza para la validación DNle mediante OCSP.

El documento se divide en dos secciones, para cada uno de los diferentes prestadores.

## 2. ACTUALIZACIÓN CERTIFICADO ANCERT

### 2.1. MODIFICACIÓN DE ALIAS

Selección del certificado que va a caducar el día 25/03/2012, para ello se debe seleccionar el keystore “**AlmacenConfianzaOCSP**” en el módulo “**Gestión de Keystores y contraseñas**”.

Actualmente existen dos certificados para la validación de certificados mediante OCSP contra ANCERT, uno para pre-producción y otro para el entorno de producción, estos dos certificados serán sustituidos por uno solo. Para ello modificar el certificado que contenga en el alias el common name “**cn=pre.ocsp.ac.ancert.com**” y “**cn=pre.ocsp.ac.ancert.com**” (siempre y cuando no se modificara cuando se importó). Modificar el alias de ambos, por ejemplo añadiéndole la cadena “old” al final, esto es simplemente para una vez importemos el nuevo certificado veamos claramente cuales eran los antiguos.

### 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.
- **Tercer paso:** Seleccionar el certificado recibido junto a este documento en la carpeta “Ancert” y pulsar sobre “Continuar”.

 <p>JUNTA DE ANDALUCÍA</p>	<p><b>Consejería de Hacienda y Administración Pública</b></p> <p>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</p>	<p><b>Plataforma @firma</b></p> <p>Actualización de certificados de confianza</p>
---	---	---

- **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 25 de Marzo de 2012. 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 los certificados antiguos (los certificados a los que 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**”. Los siguientes tres pasos deben ejecutarse para los dos certificados.

- **Primer paso:** se selecciona el certificado que se desea eliminar, donde el alias contiene el common name “**cn=pre.ocsp.ac.ancert.com**” o “**cn=pre.ocsp.ac.ancert.com**” 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.
- **Tercer paso:** Pulsamos sobre eliminar certificado y confirmamos la operación.

## 3. ACTUALIZACIÓN CERTIFICADO DNI<sup>E</sup> FNMT

### 3.1. MODIFICACIÓN DE ALIAS

Selección del certificado que va a caducar el día 15/03/2012, 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=av dnle fnmt,o=direccion general de la policia,ou=dnle,ou=fnmt**” (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.

 <p>JUNTA DE ANDALUCÍA</p>	<p><b>Consejería de Hacienda y Administración Pública</b></p> <p><b>Dirección General de Tecnologías para Hacienda y la Administración Electrónica</b></p>	<p><b>Plataforma @firma</b></p> <p>Actualización de certificados de confianza</p>
---	--	---

### 3.2. 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.
- **Tercer paso:** Seleccionar el certificado recibido junto a este documento en la carpeta “DNle” 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.

### 3.3. ELIMINAR CERTIFICADO ANTIGUO

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, donde el alias contiene el common name “**cn=av dnle fnmt**” 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 debe ser del 15 de Marzo de 2012.
- **Tercer paso:** Pulsamos sobre eliminar certificado y confirmamos la operación.