RedAbogacía

ABOGACÍA ESPAÑOLA

Plan de renovación de certificados ACA 1024 bits y SHA1

Análisis implicaciones operativas

Confidencial

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/06/2016 9:48:49
Página: 3 de 14
REGISTRO SALIDA

RedAbogacía
ABOGACÍA ESPAÑOLA

ÍNDICE

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/06/2016 9:48:49
Página: 4 de 14
REGISTRO SALIDA

RedAbogacía
ABOGACÍA ESPAÑOLA

1. Antecedentes

Con motivo de la entrada en vigor, el próximo 6 de julio, del Reglamento Europeo 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, "ReiDAS"), la Autoridad de Certificación de la Abogacia (en adelante, "ACA") va a realizar un conjunto de acciones con el objetivo de adecuarse a esta nueva normativa y poder seguir emitiendo los certificados de Abogado con las máximas garantías de seguridad y calidad.

Adicionalmente, con la entrada en vigor de este Reglamento, el Ministerio de Industria, Energía y Turismo, en su calidad de Organismo Supervisor, nos ha informado de que **a partir del 1 de enero de 2017 empezarán a exigir de forma exclusiva el uso de certificados digitales con longitud de clave 2048 bits y algoritmo SHA2**.

2. Plan de acción

Las acciones que estamos realizando, con el objetivo de dar cumplimiento a los requerimientos anteriormente expuestos son las siguientes:

- **Abril 2016:** Hemos arrancado un proyecto de consultoría con la empresa SIA y Baker & McKenzie, para la adecuación de ACA al ReiDAS realizando un profundo análisis, jurídico, procedimental y técnico de nuestra Autoridad de Certificación para poder estar en disposición de superar, en su momento, la preceptiva auditoría que exige la mencionada norma europea a los Prestadores de Servicios de Confianza.

- **Mayo 2016:** En este mes de mayo, hemos realizado la migración de la autoridad de certificación raíz a tecnología más robusta (cambio de SHA1 a SHA2) y estamos en pleno proceso de creación de y adaptación de nuevas autoridades de certificación intermedias, para cubrir los requerimientos técnicos exigidos por el Reglamento.

- **Junio 2016**: Una vez finalizada la parte técnica y procedimental de la nueva Autoridad de certificación, el siguiente punto en el que estamos trabajando es comunicar a las Administraciones competentes esta nueva situación, así como al resto de administraciones públicas para la acreditación ante sus servicios telemáticos: plataforma @firma, AEAT, TGSS, Ministerio de Justicia, entre otras.

- **Septiembre 2016:** Como última fase del proyecto, previsiblemente a partir de septiembre, este Consejo General procederá a solicitar la renovación de los certificados de Abogado para la actualización de longitud de clave y algoritmo de firma. Para esta renovación se está desarrollado un aplicativo para que el Abogado pueda desde su despacho proceder a la renovación del certificado, de forma ágil y rápida, sin tener que desplazarse a su Colegio. Solo en el caso de las tarjetas con certificado SHA1 de 1024 será necesario que dicha renovación se realice en el Colegio ya que hay que cambiar la tarjeta ACA. Procederemos a informar de forma individualizada a aquellos Colegios que tengáis este tipo de certificados SHA1 de 1024.

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/06/2016 9:48:49
Página: 5 de 14
REGISTRO SALIDA

3. Implicaciones operativas para Colegios y Abogados

Derivado del plan de acción descrito en el apartado anterior, se deberá renovar el actual parque de certificados activos:

- ✓ Que tengan una longitud de clave de 1024 bits.
- ✓ Que tengan el algoritmo de firma SHA1.
- ✓ Que estén emitidos con la "antigua" jerarquía de certificación.

En base a estos requisitos se han definido dos tipos de renovación:

1. **Renovación prioritaria:** aplicable a aquellos certificados que no cumplen las exigencias del Ministerio de Industria, esto es, los certificados activos con longitud de clave de 1024 bits y/o algoritmo de firma SHA1. Esta renovación se debería **realizar antes de enero de 2017.**
2. **Renovación progresiva:** aplicable al resto de certificados con longitud de clave de 2048 bits y algoritmo de firma SHA2 pero que deben renovarse al estar emitidos con la "antigua" jerarquía. Estas renovaciones podrán extenderse **durante todo el año 2017** pudiéndose incluso alargar el plazo si así se necesitase.

Por otra parte se realizarán dos tipos de renovación de certificados **renovación Online** para los certificados en tarjeta de 2048 bits y **renovación en el Colegio** para los certificados que aún están emitidos en tarjetas de 1024 bits.

4. Datos certificados ACA a renovar

El parque de certificados activos por longitud de clave y algoritmo de firma es el que se detalla en la siguiente tabla.

	1024 bits	2048 bits	Renovación	Plazo renovación
SHA1	5.964	57.845	prioritaria	Antes de enero 2017
SHA2		47.810*	progresiva	Durante todo el año 2017
Tipo de renovación	En el Colegio	Online		

*a fecha 1 de junio 2016.

De estos datos se deriva que **antes de enero de 2017** se deberán realizar **63.809** renovaciones de certificados.

El resto de certificados activo que se emitan antes de cambiar de jerarquía de certificación (**47.810** a fecha 1 de junio de 2016) se podrán renovar a lo largo del año 2017.

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/06/2016 9:48:43
Página: 6 de 14
REGISTRO SALIDA

En el **Anexo 1** puede verse de forma gráfica la evolución tecnológica de la jerarquía de ACA y el parque actual de certificados asociados a cada Autoridad de Certificación.

5. Datos certificados ACA a renovar por Colegio.

Los Colegios podrán consultar los datos relativos a los certificados de sus abogados a través del portal ACA.

- En el **Anexo 2** se detalla cómo pueden los Colegios consultar cuántos certificados de 1024 bits que tendrán activos todavía activos en septiembre 2016 y que se tendrán por tanto que renovar en el Colegio.

- En el **Anexo 3** se detalla cómo pueden los Colegios consultar cuántos certificados se renovarán a partir de septiembre de 2016 de forma Online de forma prioritaria antes de enero de 2017.

- En el **Anexo 4** se detalla cómo pueden los Colegios consultar cuántos certificados se renovarán de forma Online de forma progresiva durante todo el año 2017.

6. Procedimiento de renovación prioritaria del certificado ACA

El procedimiento de renovación prioritaria dependerá del tipo de renovación.

6.1. Renovación en el Colegio

Esta renovación sólo aplica a los certificados que estén aún emitidos en tarjetas de 1024 bits.

En septiembre de 2016 se enviará una comunicación al correo electrónico del Abogado asociado al certificado indicando la necesidad de renovar y cambiar su tarjeta motivado por la evolución tecnológica de los certificados digitales y los requerimientos de Ministerio de Industria y se le instará a ponerse en contacto con el Colegio de Abogados para iniciar el proceso de renovación del certificado.

Se realizará una comunicación de apremio con periodicidad mensual para aquellos certificados que están pendientes de renovar.

Los Colegios de Abogados recibirán a los abogados y les emitirán un certificado en una nueva tarjeta de 2048 bits.

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/06/2016 9:48:49
Página: 7 de 14
REGISTRO SALIDA

6.2. Renovación Online

En septiembre de 2016 se enviará una comunicación al Abogado al correo electrónico del certificado indicando la necesidad de renovar el certificado motivado por la evolución tecnológica de los certificados digitales y los requerimientos de Ministerio de Industria y se le enviará el acceso al proceso de renovación Online junto con las instrucciones a seguir para la renovación.

La renovación Online consistirá en la **descarga de un ejecutable para instalar en el equipo del Colegiado** con las siguientes características:

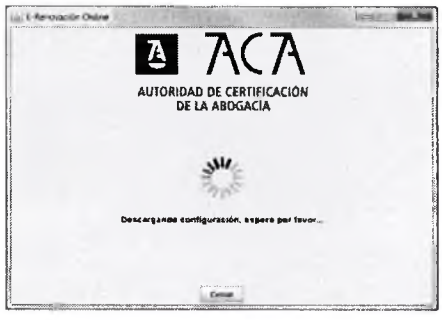
- ✓ Una vez instalada la aplicación de renovación, el Abogado con su tarjeta introducida en el lector, iniciará el proceso de renovación firmando digitalmente la petición.
- ✓ Mediante un canal cifrado se enviará la solicitud a la Autoridad de Certificación que devolverá un nuevo certificado emitido que se instalará en la tarjeta.
- ✓ Sólo se realizará una nueva emisión del certificado, no se volverán a generar claves en la tarjeta. Esto implicará una mayor agilidad del proceso y reducción de incidencias.
- ✓ La aplicación será multiidioma y compatible con Windows, Mac y Linux (Ubuntu).

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/09/2016 9:48:49
Página: 8 de 14
REGISTRO SALIDA

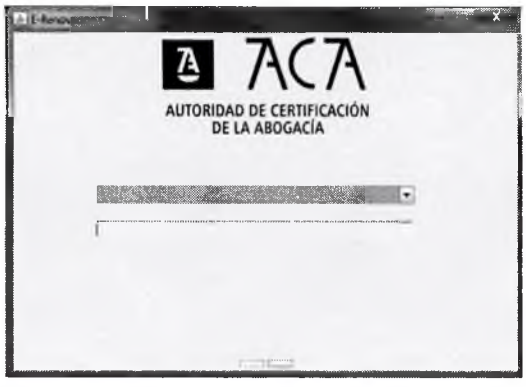
El proceso de renovación online, se realizará en tres pasos:

PASO 1: selección de idioma.

PASO 2: descarga de configuración.



PASO 3: selección del certificado a renovar y lanzamiento automático del proceso.



CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/06/2016 9:48:49
Página: 9 de 14
REGISTRO SALIDA

7. Procedimiento de renovación progresiva del certificado ACA

La renovación progresiva se realizará de forma exclusiva Online con la misma aplicación definida en el apartado anterior.

A partir de enero de 2017, se enviará de forma progresiva correos a los abogados para que actualicen su certificado digital a la nueva jerarquía enviándoles el acceso a la renovación y las instrucciones a seguir para realizarla.

Dependiendo del volumen de renovaciones realizadas, se podrán realizar acciones de difusión adicionales o implementar requisitos adicionales como por ejemplo que para acceder a algún servicio se "fuerce" a renovar primero el certificado.

8. Soporte a la renovación

El diseño de la aplicación de renovación Online se ha realizado para facilitar que el abogado pueda renovar su certificado de forma autónoma si bien desde el Consejo General de la Abogacía se ofrecerá el soporte a los usuarios que tengan algún tipo de incidencia a través de su Servicio de Soporte técnico.

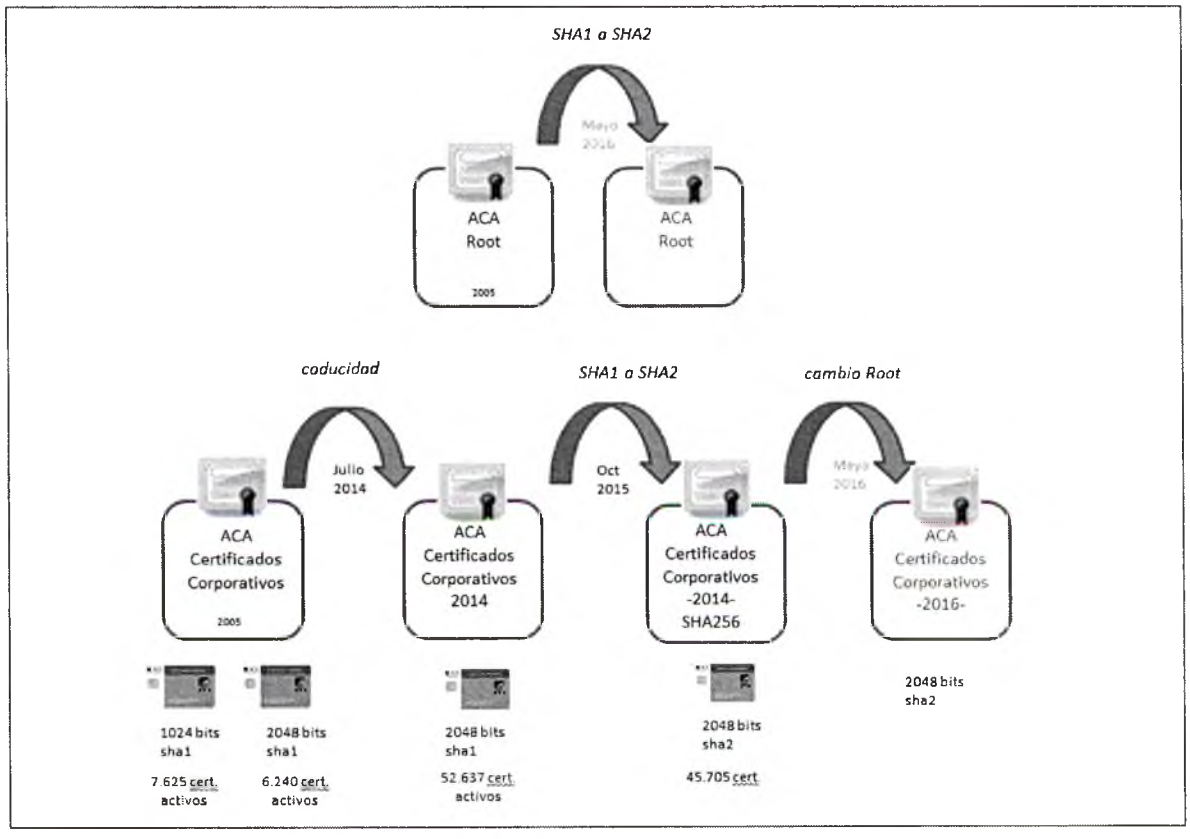
Se pondrá también a disposición de los usuarios materiales de guía en este proceso que serán publicados en nuestra web.

Se recomienda a los Colegios poner a disposición de los Abogados un equipo con la aplicación de renovación instalada para que puedan realizar este proceso también desde el propio Colegio desde un entorno controlado.

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/06/2016 9:48:49
Página: 10 de 14
REGISTRO SALIDA

ANEXO 1: Evolución tecnológica de la Jerarquía ACA

En la siguiente imagen puede verse de forma gráfica la evolución tecnológica de la jerarquía de certificación:



*Datos de certificados a mayo de 2016

Los cambios realizados y planificados sobre la jerarquía son los siguientes:

- ✓ En julio de 2014 por la caducidad de certificado se emitió un nuevo certificado de la CA subordinada.
- ✓ En octubre de 2015 se emitió un nuevo certificado de CA subordinada emitido con el algoritmo de firma SHA2.
- ✓ En mayo de 2016 se emitió un nuevo certificado de CA Raíz con el algoritmo de firma SHA2.
- ✓ En mayo de 2016 se emitió una nueva CA Subordinada con la nueva CA Raíz emitida en SHA2.

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/06/2016 9:48:49
Página: 11 de 14
REGISTRO SALIDA

ANEXO 2: Consulta de certificados de 1024 bits activos

Para comprobar desde el Colegio de Abogados cuántos abogados tienen un certificados de 1024 bits activo y que por tanto acudirán al Colegio para renovarlo, se debe acceder a www.acabogacia.org con un certificado de Operador, ir al apartado de Consulta de Certificados introducir los siguientes criterios de búsqueda:

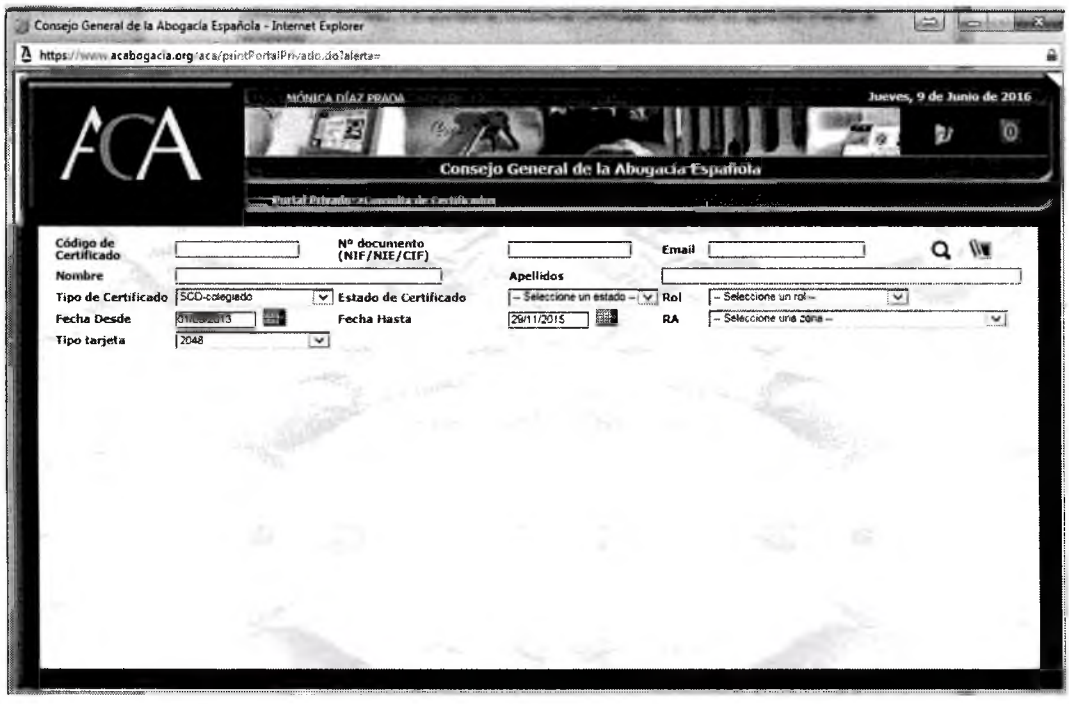
- Tipo de certificado: *SCD-colegiado*
- Estado del certificado: *En Vigor*
- Tipo de tarjeta: *1024*
- Fecha desde: *01 de septiembre de 2013*

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/06/2016 9:48:58
Página: 12 de 14
REGISTRO SALIDA

ANEXO 3: Consulta de certificados renovación Online prioritaria

Para comprobar desde el Colegio de Abogados cuántos abogados tienen un certificados de 2048 bits con SHA1 y que por lo tanto se tendrán que renovar de forma Online prioritaria antes de enero de 2017 se debe acceder a www.acabogacia.org con un certificado de Operador, ir al apartado de Consulta de Certificados introducir los siguientes criterios de búsqueda:

- Tipo de certificado: *SCD-colegiado*
- Estado del certificado: *En Vigor*
- Tipo de tarjeta: *2048*
- Fecha desde: *01 de septiembre de 2013*
- Fecha hasta: *29 de noviembre 2015*



CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/06/2016 9:48:49
Página: 13 de 14
REGISTRO SALIDA

ANEXO 4: Consulta de certificados renovación Online progresiva

Para comprobar desde el Colegio de Abogados cuántos abogados tienen un certificados de 2048 bits con SHA2 y que por lo tanto se tendrán que renovar de forma Online progresiva se debe acceder a www.acabogacia.org con un certificado de Operador, ir al apartado de Consulta de Certificados introducir los siguientes criterios de búsqueda:

- Tipo de certificado: *SCD-colegiado*
- Estado del certificado: *En Vigor*
- Fecha desde: *30 de noviembre 2015*

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA
Nº Registro: RS-09680
Of. Registro: Recoletos
14/06/2016 9:48:49
Página: 14 de 14
REGISTRO SALIDA