

Políticas de Certificación Certificados Personales

Políticas de Certificación Certificados Personales	1
1 Certificados Personales	3
1.1 Los Certificados Personales	3
1.1.1 Política de Certificación	3
1.1.2 Definición y Finalidad	3
1.1.3 Publicación y Validez	3
1.1.4 Contenido	4
1.1.5 Estructura	4
1.2 Titular del Certificado	5
1.2.1 La aceptación del certificado	5
1.2.2 Obligaciones	5
1.2.3 Responsabilidad del SCR	5
1.2.4 Requisitos Técnicos	5
1.3 Emisión	6
1.3.1 Solicitud Presencial	6
1.3.2 Licencia de Uso	6
1.3.3 Renovación	6
1.4 Revocación	6
1.4.1 Efectos de la Revocación	6
1.4.2 Procedimiento de la Revocación	7

1 Certificados Personales

1.1 Los Certificados Personales

1.1.1 Política de Certificación

El presente documento recoge la Política de Certificación que el Servicio de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España, denominado Servicio de Certificación de los Registradores (SCR), aplica a los Certificados Personales. Esta Política desarrolla y complementa lo dispuesto en la Declaración de Prácticas de Certificación (CPS) y en el Reglamento del Servicio.

Los efectos legales de un certificado, así como los derechos y obligaciones asociados al mismo, se interpretarán en todo caso atendiendo a la CPS, el Reglamento y a la presente Política, en las versiones de los mismos publicadas en cada momento en la URL especificada en el propio certificado.

Antes de solicitar un certificado o de hacer uso del mismo como mecanismo de comprobación de firmas electrónicas, se recomienda leer el presente documento, al objeto de valorar adecuadamente la confianza que ofrece un certificado. No se podrá alegar la ignorancia de estas Condiciones para eximirse de las responsabilidades propias ni para exigir las a otra parte.

1.1.2 Definición y Finalidad

Los Certificados Personales acreditan la identidad de su titular, que será siempre una persona física. Únicamente podrán ser utilizados para firmar los documentos que se presenten ante los Registros y las Administraciones Públicas, así como en todas las comunicaciones que se realicen con éstos.

Los Certificados personales tienen como finalidad principal la firma de documentos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido. Los Certificados personales también pueden ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso.

1.1.3 Publicación y Validez

Los Certificados Personales vigentes se publican en el Directorio de Certificados, a efectos de que los usuarios de un certificado puedan comprobar la validez del mismo. El Directorio se publica según el estándar LDAP, en la URL `ldapsr.registradores.org`, puerto 389 y con cadena de entrada: `"o=Servicio de Certificación del Colegio de Registradores (SCR),c=es"`. El Directorio contiene también las listas de certificados revocados (CRLs), firmadas por el Servicio y que se actualizan cada vez que se revoca un certificado.

No se considerarán válidas las firmas electrónicas recibidas fuera del período de vigencia del certificado, salvo cuando se acredite que la firma fue realizada dentro de éste, mediante un sello de tiempo de los Registros o de otro sistema de sellado de tiempo reconocido por el Servicio de Certificación de los Registradores. Antes de dar por válida una firma electrónica será preciso verificar que el certificado que la respalda no ha sido revocado, para lo que habrá de consultarse el Directorio de Certificados.

El Servicio no dispone de mecanismos de recuperación de claves para esta clase de certificados, por lo que su uso para el cifrado de confidencialidad puede dar lugar a pérdidas irreversibles de información. Únicamente se recomienda el cifrado de mensajes, para garantizar la confidencialidad durante la transmisión.

1.1.4 Contenido

Los certificados están firmados electrónicamente por el Servicio de Certificación con la clave privada correspondiente a la clase de los certificados externos y se emiten de acuerdo con el estándar de la Unión Internacional de Telecomunicaciones, número X-509, versión 3.

La longitud de las claves certificadas es de 1024 bits. El período de vigencia es de dos años.

Los certificados tienen los siguientes campos con contenido fijo:

- *Datos del Servicio de Certificación*: Servicio de Certificación de los Registradores (SCR), Príncipe de Vergara 72, Madrid, scr@registradores.org
- *Clase de certificado*: Certificado externo.
- *Tipo de certificado*: Certificado personal.
- *Condiciones de Certificación*: https://www.registradores.org/scr/normativa/cp_f2.htm
- *País*: es
- *Comentario*: Limitado a actos inscribibles y comunicaciones con Registros, con Condiciones publicadas en: https://www.registradores.org/scr/normativa/cp_f2.htm

Además, se incluyen los siguientes campos de contenido variable:

- Código identificativo único del certificado.
- Nombre y apellidos del titular, número de identificación fiscal.
- Registro autorizante.
- Dirección postal.
- Dirección de correo electrónico del titular.
- Fechas de comienzo y fin del período de validez, incluyendo horas, minutos y segundos.

1.1.5 Estructura

La estructura del certificado, referente a su base de búsqueda, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	
O	Servicio de Certificación del Colegio de Registradores (SCR)	
OU	Certificado Externo	
OU	Certificado Personal	Cadena identificativa del tipo de certificado.
S	Registro Mercantil Emisor	Unidad de Tramitación en la que se generó el certificado
CN	NOMBRE <i>nombre apellidos</i> – NIF <i>nif</i>	

Tabla 1. Subject Personal

Campo	Valor	Descripción
C	ES	
O	Servicio de Certificación del Colegio de Registradores (SCR)	
OU	Certificado Propio	
OU	Certificado Raíz	
CN	Certificado de la Clave Secundaria para certificados externos	Cadena que indica que el certificado ha sido firmado por la CA Secundaria Externa. Los certificados firmados bajo esta CA secundaria son para el desarrollo de las actividades de terceros con los Registros y la interacción con las AAPP.
STREET	Príncipe de Vergara 72 28006 Madrid	
E	scr@registradores.org	

Tabla 2. Issuer

1.2 Titular del Certificado

1.2.1 La aceptación del certificado

El titular, al aceptar un certificado mediante la firma de la licencia, asume:

1. Que cada firma digital creada usando la clave privada correspondiente a la clave pública certificada es la firma electrónica del titular.
2. Que cada vez que el titular utiliza su certificado para acceder a cualquier tipo de información dicho acceso ha sido realizado por él personalmente.
3. Que el uso de la clave privada certificada es personal e intransferible, por lo que toda utilización que se haga de ella por terceras personas será bajo la responsabilidad y riesgo del titular.
4. Que acepta las limitaciones de uso correspondientes a la clase de certificado de que se trate y, en todo caso, que no usará la clave privada correspondiente a la pública certificada con el fin de firmar certificados o listas de certificados revocados.

1.2.2 Obligaciones

El Certificado personal debe ser utilizado de acuerdo con las finalidades propias del mismo, así como con lo establecido en la legislación española, en el Reglamento del Servicio, en las presentes Condiciones.

En particular, son obligaciones del titular:

1. Utilizar el certificado exclusivamente para los usos especificados en estas Condiciones de Certificación y en el propio certificado, y únicamente dentro de su período de vigencia.
2. Proteger y almacenar sus claves criptográficas privadas de forma confidencial e inaccesible a terceros no autorizados, adoptando las medidas de seguridad necesarias para conservarlas.
3. Mantener el secreto sobre la contraseña que protege su clave privada, así como sobre aquella que permite revocar el certificado.
4. Notificar inmediatamente a la Unidad de Tramitación correspondiente la pérdida o divulgación de la clave privada, o cualquier situación que pueda afectar a la validez del certificado, solicitando su revocación conforme a los procedimientos previstos en esta norma.

1.2.3 Responsabilidad del SCR

El Servicio de Certificación no responderá, en ningún caso, de la utilización que los titulares hagan de los certificados, ni de los errores de hecho o de interpretación que puedan cometer quienes validen una firma. En particular, el Servicio no tendrá responsabilidad alguna por:

1. Los daños y perjuicios, directos o indirectos, causados por la utilización de los certificados y de las claves certificadas para usos no permitidos o fuera de su período de vigencia, así como por la pérdida o divulgación de la clave privada del titular.
2. El contenido de los documentos firmados con una firma digital basada en un certificado emitido por él, ni por la información contenida en un servidor por el certificado.
3. Los daños o perjuicios directos o indirectos que sean consecuencia de los procedimientos o productos empleados para generar la pareja de claves asimétricas a certificar cuando sea el propio solicitante quien aporte las claves.
4. Los fallos o errores debidos a los equipos informáticos, navegadores o aplicaciones utilizados por el titular o por los terceros usuarios de los certificados.

1.2.4 Requisitos Técnicos

Para poder utilizar el certificado personal, el signatario deberá cumplir con los siguientes requerimientos mínimos de equipos y programas informáticos:

1. Un ordenador personal con acceso a Internet. Se recomienda el uso de un Pentium 166 MHz o superior, con 64 Mb de RAM, sistema operativo Windows 98 o superior, y navegador Netscape o Explorer, v.4 o superiores.

2. Un lector de tarjetas o dispositivo equivalente, compatible con el estándar PC/SC (Personal Computer/Smart Card), basado en la norma ISO 7816.

1.3 Emisión

1.3.1 Solicitud Presencial

El titular deberá personarse en la Unidad de Tramitación del Registro de su elección, con un documento acreditativo de su identidad, a los efectos firmar la solicitud de expedición del certificado, generar las claves del mismo, así como para asignar su correspondiente contraseña y firmar la licencia de uso.

El Registrador comprobará el documento de identidad aportado y la coincidencia de sus datos con los obrantes en la solicitud o formulario. Si el documento presentado es válido y está vigente y los datos coinciden con los de la solicitud, dará por superado el trámite de identificación.

Previamente a la emisión del certificado, la Unidad de Tramitación de los Registros comprobará si existe otro certificado de la misma clase y a nombre del mismo titular y, de ser así, procederá a su revocación.

A continuación se imprimirán dos copias de la licencia de uso, que firmará el titular, tras lo cual pondrá en marcha el dispositivo informático que le permitirá generar las claves dentro de su tarjeta criptográfica. El titular deberá introducir personalmente la contraseña de acceso a la tarjeta, de modo que ésta no sea conocida en ningún momento por el Servicio de Certificación. También deberá indicar una palabra secreta que le permitirá revocar el certificado a través del web del Servicio o de su sección de Atención Telefónica.

1.3.2 Licencia de Uso

El solicitante deberá firmar la licencia de uso del certificado, aceptando el mismo y las presentes Condiciones de Certificación. La licencia incluirá necesariamente los siguientes contenidos:

- Los datos personales del titular: nombre y apellidos, teléfono y dirección de correo electrónico.
- Una declaración del titular en la que, en su caso, manifiesta haber recibido la tarjeta conteniendo la clave privada y el certificado y en la que se compromete a utilizar ésta de acuerdo con lo dispuesto en el Reglamento y en las presentes Condiciones de Certificación.
- El consentimiento del solicitante para la cesión de sus datos de carácter personal al Servicio en la medida en que sean necesarios para que éste preste los servicios de certificación.

La licencia firmada manualmente quedará archivada en la Unidad de Tramitación Central durante 15 años.

1.3.3 Renovación

La Unidad de Tramitación Central notificará al titular por correo electrónico la futura expiración de los certificados, con al menos dos semanas de antelación a la fecha en que se produzca, indicando al titular los pasos a seguir para la obtención de un nuevo certificado.

1.4 Revocación

1.4.1 Efectos de la Revocación

La revocación de un certificado supone su total pérdida de validez y la exención de responsabilidad del Servicio de Certificación por cualquier daño producido como consecuencia del uso del certificado revocado con posterioridad a su revocación.

La revocación producirá efectos frente al solicitante desde el momento en que notifique la correspondiente solicitud a la Unidad de Inscripción y, frente a terceros, desde que sea publicada en el Directorio de Certificados. Será obligación del titular comprobar si la revocación del certificado ha sido publicada en el Directorio de Certificados.

1.4.2 Procedimiento de la Revocación

Para solicitar la revocación del certificado de forma presencial el titular, o la persona autorizada por el mismo, deberá personarse ante la Unidad de Tramitación Central y rellenar y firmar el formulario de solicitud de revocación. El formulario de solicitud de suspensión o revocación contendrá el nombre y apellidos del solicitante, dirección de correo electrónico y dirección postal. En el caso de que el solicitante sea una persona distinta del titular, sus datos y los del titular del certificado, así como documento fehaciente donde conste la autorización concedida por éste para pedir la revocación de su certificado. El operador comprobará los datos del formulario y la identidad del solicitante y procederá a la revocación del certificado, guardando el formulario firmado durante 15 años.

Por causa de urgencia podrá solicitarse la revocación de los certificados a través de la web del Servicio de Certificación o mediante una llamada telefónica a su Servicio de Asistencia Telefónica. En ambos casos, además de los datos del titular y del certificado, será preciso aportar la palabra secreta que se comunicó con este fin en el momento de la entrega del certificado. El operador de la Unidad de Tramitación Central procederá inmediatamente a la revocación del certificado. El titular deberá remitir posteriormente el formulario de solicitud a la Unidad de Tramitación Central por correo certificado u otro medio fehaciente.