Condiciones Generales de Emisión de los Certificados del Consejo General del Notariado

Agencia Notarial de Certificación

ancert
Agencia Notarial de Certificación

1. Información general

1.1. Control documental

Proyecto:	**Condiciones Generales de Emisión**
Entidad de destino:	**Agencia Notarial de Certificación**
Código de referencia:	**-**
Versión:	**1.1**
Fecha de la edición:	**22/11/2017**
Archivo:	**CG emisión CGN v1r0.docx**

1.2. Control de versiones

Versión	**Partes que cambian**	**Descripción del cambio**	**Fecha cambio**	**Fecha publicación**
1.0	Todo	Original	01/09/2014	03/11/2014
1.1	Todo	Revisión Reglamento (UE) 910/2014	22/11/2017	28/11/2017

Condiciones generales de emisión de los Certificados para el Consejo General del Notariado

Este documento tiene por objeto establecer las condiciones generales de emisión, entre la Agencia Notarial de Certificación (Ancert) y el Consejo General del Notariado (CGN), para los certificados emitidos agrupados dentro de la "Clase Certificados del Consejo del Notariado", en adelante "Certificados CGN".

Estas condiciones se encuentran disponibles para su descarga en la dirección electrónica: http://www.ancert.com/condiciones

CLÁUSULAS

PRIMERA. Objeto y documentación de los servicios de certificación

Estas condiciones generales de emisión regulan los servicios de certificación de la Agencia Notarial de Certificación al Consejo General del Notariado y sus organismos dependientes, que se convierten en los suscriptores de los certificados.

El objeto de los servicios de certificación es el suministro de los elementos técnicos de firma electrónica y servicios accesorios de la misma, y que se concretan en el suministro de certificados, en su caso en una tarjeta, con la consideración legal de dispositivo cualificado de creación de firma, y del software necesario.

Los servicios de certificación de la Agencia Notarial de Certificación se regulan técnicamente y operativamente por la Declaración de Prácticas de Certificación de la Clase Certificados CGN, y por sus actualizaciones posteriores, así como por documentación complementaria suministrada.

La Declaración de Prácticas de Certificación y la documentación de procedimientos de suscriptor de la Agencia Notarial de Certificación, que se modifican según se indica periódicamente en el Depósito de certificados, consultables en la página http://www.ancert.com, se incorporan a estas condiciones generales por referencia. En caso de discrepancia, el significado de los términos contenidos en estas condiciones generales de emisión prevalecerá respecto de lo que se establece en la Declaración de Prácticas de Certificación.

SEGUNDA. Clases y características de los Certificados CGN

Los "Certificados CGN" agrupan los certificados expedidos por Ancert a los Notarios establecidos en una plaza del territorio español (certificados FEREN), los Notarios que ostentan cargos dentro de la organización del CGN o de los Colegios Notariales (certificados de cargo) y a los empleados de Notarías y Colegios Notariales del territorio español (certificados de empleados).

Para los certificados que se emiten, de clase "Certificados CGN", los suscriptores son:

- Certificados FEREN: El Consejo General del Notariado, que es la persona jurídica identificada en el certificado.
- Certificados de Cargo: El Consejo General del Notariado o el Colegio Notarial, que es la persona jurídica identificada en el certificado.
- Certificados de Empleado: La Notaría o Colegio Notarial (donde trabaja el empleado), que es la persona jurídica identificada en el certificado.

2.1. Certificados FEREN

Los Certificados FEREN son certificados cualificados, en los términos del artículo 28 del Reglamento (UE) 910/2014; es decir, son certificados electrónicos expedidos por la Agencia Notarial de Certificación cumpliendo los requisitos establecidos en dicho Reglamento en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que prestan.

Los Certificados FEREN permiten tres funcionalidades, emitiéndose un Certificado para cada una de ellas:

- La creación de la firma electrónica cualificada, que es la firma electrónica avanzada basada en un certificado cualificado y que se genera mediante un dispositivo cualificado de creación de firma, teniendo respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.
- La autenticación personal en sistemas electrónicos de información, en presencia física o a distancia.
- El cifrado y el descifrado de documentos electrónicos, con recuperación de clave.

Se utiliza una tarjeta criptográfica como único soporte para los tres certificados, con la garantía de dispositivo cualificado de creación de firma, en los términos del artículo 29 del Reglamento (UE) 910/2014.

Los certificados pueden contener informaciones personales adicionales (por ejemplo, la pertenencia a un Colegio Notarial, etc.), siempre que no se trate de datos especialmente protegidos, de acuerdo con el artículo 7 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

La tarjeta suministrada contiene tres certificados, diferenciados por el uso a que pueden destinarse:

- Certificado FEREN de firma electrónica cualificada.
- Certificado FEREN de autenticación.
- Certificado FEREN de cifrado.

2.1.1. Certificado FEREN de firma electrónica cualificada

Este certificado se utiliza para la firma electrónica cualificada de documentos electrónicos o mensajes electrónicos, garantizando la autenticidad del emisor entendiendo por ello el

aseguramiento de que el documento o la comunicación electrónica provienen del dispositivo de creación de firma de la persona de quien dice provenir.

Los Certificados FEREN de firma electrónica cualificada se utilizan también para garantizar la integridad del contenido, entendiendo por ello que permiten comprobar que un documento electrónico no ha sido modificado por ningún agente externo.

Para garantizar la integridad, la criptografía utiliza las capacidades matemáticas de las funciones de resumen (en inglés, unciones de *hash*), utilizadas en combinación con la firma digital. El procedimiento se centra en firmar digitalmente un resumen único del documento electrónico con la clave privada del poseedor de claves de forma que cualquier alteración del documento revierte en una alteración de su resumen.

Además de los anteriores aspectos, sólo los Certificados FEREN de firma electrónica cualificada garantizan la irrefutabilidad de los mensajes, basada en el conocimiento de su contenido (función también denominada "no repudio de origen"), entendiendo por ello evitar que el emisor de un determinado mensaje pueda negar, si ello le conviene, la emisión del mismo o su contenido.

Esta característica se obtiene mediante la firma electrónica cualificada, que es la firma electrónica avanzada basada en un certificado cualificado y que se genera mediante un dispositivo cualificado de creación de firma, teniendo respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

El receptor de un mensaje firmado electrónicamente puede verificar esa firma a través del Certificado FEREN de firma electrónica cualificada del suscriptor.

Los Certificados FEREN de firma electrónica cualificada se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.18920.4.1.1.2.1

2.1.2. Certificado FEREN de autenticación

Este certificado se utiliza para la confirmación de la identidad del emisor de mensajes o documentos, en las operaciones de autenticación que el mismo realiza, a través de protocolos técnicos de autenticación como SSL, TLS, WTLS u otros que resulten idóneos.

Adicionalmente, en determinadas aplicaciones se puede emplear este certificado para garantizar la autenticidad del origen de los mensajes, y la integridad de los mismos, pero sin garantía legal de la comprensión y aceptación del contenido, como por ejemplo en aplicaciones de correo electrónico seguro.

Los Certificados FEREN de autenticación se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.18920.4.1.1.2.2

2.1.3. Certificado FEREN de cifrado

Este certificado se utiliza para cifrar o descifrar mensajes o documentos electrónicos bajo la exclusiva responsabilidad de la persona identificada en el certificado.

El certificado permite que cualquier persona, pueda producir mensajes con garantía de confidencialidad, que únicamente podrá leer el suscriptor del certificado, siempre que posea la

clave privada del certificado, incluso con posterioridad a la expiración, ordinaria o anticipada, del certificado.

Los Certificados FEREN de cifrado se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.18920.4.1.1.2.3

2.2. Certificados de Cargo

Los Certificados de Cargo son certificados cualificados, en los términos del artículo 28 del Reglamento (UE) 910/2014; es decir, son certificados electrónicos expedidos por la Agencia Notarial de Certificación cumpliendo los requisitos establecidos en dicho Reglamento en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que prestan.

Los Certificados de Cargo permiten tres funcionalidades, emitiéndose un Certificado para cada una de ellas:

- La creación de la firma electrónica cualificada, que es la firma electrónica avanzada basada en un certificado cualificado y que se genera mediante un dispositivo cualificado de creación de firma, teniendo respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.
- La autenticación personal en sistemas electrónicos de información, en presencia física o a distancia.
- El cifrado y el descifrado de documentos electrónicos, con recuperación de clave.

Se utiliza una tarjeta criptográfica como único soporte para los tres certificados, con la garantía de dispositivo cualificado de creación de firma, en los términos del artículo 29 del Reglamento (UE) 910/2014.

Los certificados pueden contener informaciones personales adicionales (por ejemplo, el cargo ocupado dentro de la estructura organizativa del Consejo General del Notariado, etc.), siempre que no se trate de datos especialmente protegidos, de acuerdo con el artículo 7 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

La tarjeta suministrada contiene tres certificados, diferenciados por el uso a que pueden destinarse:

- Certificado de Cargo de firma electrónica cualificada.
- Certificado de Cargo de autenticación.
- Certificado de Cargo de cifrado.

2.2.1. Certificado de Cargo de firma electrónica cualificada

Este certificado se utiliza para la firma electrónica cualificada de documentos electrónicos o mensajes electrónicos, garantizando la autenticidad del emisor entendiendo por ello el aseguramiento de que el documento o la comunicación electrónica provienen del dispositivo de creación de firma de la persona de quien dice provenir.

Los Certificados de Cargo de firma electrónica cualificada se utilizan también para garantizar la integridad del contenido, entendiendo por ello que permiten comprobar que un documento electrónico no ha sido modificado por ningún agente externo.

Para garantizar la integridad, la criptografía utiliza las capacidades matemáticas de las funciones de resumen (en inglés, unciones de *hash*), utilizadas en combinación con la firma digital. El procedimiento se centra en firmar digitalmente un resumen único del documento electrónico con la clave privada del poseedor de claves de forma que cualquier alteración del documento revierte en una alteración de su resumen.

Además de los anteriores aspectos, sólo los Certificados de Cargo de firma electrónica cualificada garantizan la irrefutabilidad de los mensajes, basada en el conocimiento de su contenido (función también denominada "no repudio de origen"), entendiendo por ello evitar que el emisor de un determinado mensaje pueda negar, si ello le conviene, la emisión del mismo o su contenido.

Esta característica se obtiene mediante la firma electrónica cualificada, que es la firma electrónica avanzada basada en un certificado cualificado y que se genera mediante un dispositivo cualificado de creación de firma, teniendo respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

El receptor de un mensaje firmado electrónicamente puede verificar esa firma a través del Certificado de Cargo de firma electrónica cualificada del suscriptor.

Los Certificados de Cargo de firma electrónica cualificada se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.18920.4.1.2.2.1

2.2.2. Certificado de Cargo de autenticación

Este certificado se utiliza para la confirmación de la identidad del emisor de mensajes o documentos, en las operaciones de autenticación que el mismo realiza, a través de protocolos técnicos de autenticación como SSL, TLS, WTLS u otros que resulten idóneos.

Adicionalmente, en determinadas aplicaciones se puede emplear este certificado para garantizar la autenticidad del origen de los mensajes, y la integridad de los mismos, pero sin garantía legal de la comprensión y aceptación del contenido, como por ejemplo en aplicaciones de correo electrónico seguro.

Los Certificados de Cargo de autenticación se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.18920.4.1.2.2.2

2.2.3. Certificado de Cargo de cifrado

Este certificado se utiliza para cifrar o descifrar mensajes o documentos electrónicos bajo la exclusiva responsabilidad de la persona identificada en el certificado.

El certificado permite que cualquier persona, pueda producir mensajes con garantía de confidencialidad, que únicamente podrá leer el suscriptor del certificado, siempre que posea la clave privada del certificado, incluso con posterioridad a la expiración, ordinaria o anticipada, del certificado.

Los Certificados de Cargo de cifrado se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.18920.4.1.2.2.3

2.3. Certificados de Empleados

Los Certificados de Empleados son certificados cualificados, en los términos del artículo 28 del Reglamento (UE) 910/2014; es decir, son certificados electrónicos expedidos por la Agencia Notarial de Certificación cumpliendo los requisitos establecidos en dicho Reglamento en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que prestan.

Los Certificados de Empleados permiten tres funcionalidades, emitiéndose un Certificado para cada una de ellas:

- La creación de la firma electrónica cualificada, que es la firma electrónica avanzada basada en un certificado cualificado y que se genera mediante un dispositivo cualificado de creación de firma, teniendo respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.
- La autenticación personal en sistemas electrónicos de información, en presencia física o a distancia.
- El cifrado y el descifrado de documentos electrónicos, con recuperación de clave.

Se utiliza una tarjeta criptográfica como único soporte para los tres certificados, con la garantía de dispositivo cualificado de creación de firma, en los términos del artículo 29 del Reglamento (UE) 910/2014.

Los certificados pueden contener informaciones personales adicionales (por ejemplo, el cargo ocupado dentro de la estructura organizativa del Consejo General del Notariado, etc.), siempre que no se trate de datos especialmente protegidos, de acuerdo con el artículo 7 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

La tarjeta suministrada contiene dos certificados, diferenciados por el uso a que pueden destinarse:

- Certificado de Empleado de firma electrónica cualificada.
- Certificado de Empleado de autenticación.

Opcionalmente, la tarjeta suministrada contiene un tercer certificado para el uso de cifrado:

- Certificado de Empleado de cifrado.

2.2.1. Certificado de Empleado de firma electrónica cualificada

Este certificado se utiliza para la firma electrónica cualificada de documentos electrónicos o mensajes electrónicos, garantizando la autenticidad del emisor entendiendo por ello el aseguramiento de que el documento o la comunicación electrónica provienen del dispositivo de creación de firma de la persona de quien dice provenir.

Los Certificados de Empleado de firma electrónica cualificada se utilizan también para garantizar la integridad del contenido, entendiendo por ello que permiten comprobar que un documento electrónico no ha sido modificado por ningún agente externo.

Para garantizar la integridad, la criptografía utiliza las capacidades matemáticas de las funciones de resumen (en inglés, unciones de *hash*), utilizadas en combinación con la firma digital. El procedimiento se centra en firmar digitalmente un resumen único del documento electrónico con la clave privada del poseedor de claves de forma que cualquier alteración del documento revierte en una alteración de su resumen.

Además de los anteriores aspectos, sólo los Certificados de Empleado de firma electrónica cualificada garantizan la irrefutabilidad de los mensajes, basada en el conocimiento de su contenido (función también denominada "no repudio de origen"), entendiendo por ello evitar que el emisor de un determinado mensaje pueda negar, si ello le conviene, la emisión del mismo o su contenido.

Esta característica se obtiene mediante la firma electrónica cualificada, que es la firma electrónica avanzada basada en un certificado cualificado y que se genera mediante un dispositivo cualificado de creación de firma, teniendo respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

El receptor de un mensaje firmado electrónicamente puede verificar esa firma a través del Certificado de Empleado de firma electrónica cualificada del suscriptor.

Los Certificados de Empleado de firma electrónica cualificada se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.18920.4.2.1.2.1

2.2.2. Certificado de Empleado de autenticación

Este certificado se utiliza para la confirmación de la identidad del emisor de mensajes o documentos, en las operaciones de autenticación que el mismo realiza, a través de protocolos técnicos de autenticación como SSL, TLS, WTLS u otros que resulten idóneos.

Adicionalmente, en determinadas aplicaciones se puede emplear este certificado para garantizar la autenticidad del origen de los mensajes, y la integridad de los mismos, pero sin garantía legal de la comprensión y aceptación del contenido, como por ejemplo en aplicaciones de correo electrónico seguro.

Los Certificados de Empleado de autenticación se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.18920.4.2.1.2.2

2.2.3. Certificado de Empleado de cifrado

Este certificado se utiliza para cifrar o descifrar mensajes o documentos electrónicos bajo la exclusiva responsabilidad de la persona identificada en el certificado.

El certificado permite que cualquier persona, pueda producir mensajes con garantía de confidencialidad, que únicamente podrá leer el suscriptor del certificado, siempre que posea la clave privada del certificado, incluso con posterioridad a la expiración, ordinaria o anticipada, del certificado.

Los Certificados de Empleado de cifrado se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.18920.4.2.1.2.3

2.4. Duración de los certificados

Los Certificados CGN tendrán un periodo de validez de tres años desde el día en que sean emitidos.

La fecha de expiración de los certificados figura indicada dentro los mismos certificados.

La duración de los certificados queda condicionada a que los mismos no sean revocados, por las causas que se indican en la Declaración de Prácticas de Certificación.

TERCERA. Limitaciones y prohibiciones de uso de los Certificados CGN

3.1. Límites de uso

Los Certificados CGN deben emplearse para su función propia y finalidad establecida en la cláusula segunda de estas condiciones generales, sin que puedan emplearse en otras funciones y con otras finalidades.

Asimismo, los certificados deberán emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento

3.2. Usos prohibidos

Los Certificados CGN no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (CRL) o informaciones de estado de certificados (mediante servidores OCSP o similares), excepto cuando se autorice expresamente.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de usos limitados y/o prohibidos quedan a cargo del suscriptor. En ningún caso podrá el suscriptor o los terceros perjudicados reclamar a la Agencia Notarial de Certificación, o al Consejo General del Notariado, compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los certificados para los usos limitados y/o prohibidos.

CUARTA. Obligaciones del suscriptor, y en su caso, del poseedor de claves.

4.1. Personal responsable de la ejecución de los procedimientos

Las entidades de registro son las personas físicas o jurídicas que asisten a la Agencia Notarial en las tareas de emisión y gestión de los certificados, y en concreto, en las tareas de:

- Contratación del servicio de certificación a entidades finales.
- Identificación y autenticación de la identidad y circunstancias personales de las personas que reciben los certificados.
- Generación de certificados y entrega de dispositivos cualificados de creación de firma a los suscriptores.
- Almacenamiento de documentos en relación con los servicios de certificación.

4.2. Solicitud del servicio y generación de las claves

El suscriptor solicitará y autorizará a la persona actuante como entidad de registro correspondiente de la Agencia Notarial de Certificación, que genere las claves del suscriptor, privada y pública, correspondientes a las funcionalidades de identificación, firma y cifrado, o de acceso, dentro de un dispositivo cualificado de creación de firma electrónica (la tarjeta que recibe el poseedor de claves), cuando proceda, y que realice la emisión de los certificados correspondientes.

Para la clase de certificados "ANCERT Certificados FEREN" actúa como Entidad de Registro el Decano de cada Colegio Notarial para sus Colegiados, así como el Presidente de la Junta de Decanos para todos los Decanos.

Para la clase de certificados "ANCERT Certificados de Cargo" actúa como Entidad de Registro el Presidente del Consejo General del Notariado para los miembros del Consejo y los Decanos, así como los Decanos para los miembros de las Juntas Directivas y cargos de Distritos de sus respectivos Colegios Notariales.

Para la clase de certificados emitidos por la Autoridad de Certificación subordinada "ANCERT Certificados para Empleados V2" actúa como Entidad de Registro el Notario para los empleados de su Notaría, así como el Secretario de los Colegios Notariales para los empleados de los mismos.

4.3. Veracidad de la información

El suscriptor se responsabilizará de que toda la información incluida, por cualquier medio, en la solicitud de los certificados y en los mismos certificados sea exacta, completa para la finalidad de los certificados y esté actualizada en todo momento.

El suscriptor debe informar inmediatamente a la Agencia Notarial de Certificación de cualquier inexactitud en el certificado, detectada una vez se haya emitido, así como de los cambios que se produzcan en la información aportada por el poseedor de claves para la emisión del certificado.

4.4. Entrega y aceptación del servicio

El suscriptor queda vinculado y acepta estas condiciones generales de emisión desde la solicitud del mismo.

La aceptación del certificado por parte del suscriptor, se entiende producida desde el momento de su emisión y entrega al poseedor de claves por la Agencia Notarial de Certificación y firma ante la Entidad de Registro la correspondiente hoja de entrega.

4.5. Poseedores de claves del subscriptor

El suscriptor se obliga a informar los poseedores de claves de los términos y condiciones relativos al uso de los certificados, así como de los procedimientos internos de gestión de certificados que pueda establecer adicionalmente a los provistos por la Agencia Notarial de Certificación.

4.6. Obligaciones de custodia

El suscriptor, por medio del poseedor de claves, se obliga a custodiar el código de identificación personal, la tarjeta o cualquier otro elemento técnico entregado por la Agencia Notarial de Certificación, las claves privadas y, cuando proceda, las especificaciones propiedad de la Agencia Notarial de Certificación que le sean suministradas.

En caso de pérdida o robo de la clave privada del certificado, o en caso de que el poseedor de claves y/o el suscriptor sospechen que la clave privada ha perdido fiabilidad por cualquier motivo, deben notificarlo inmediatamente a la Entidad de Registro correspondiente y/o a la Agencia Notarial de Certificación

4.7. Obligaciones de uso correcto

El suscriptor, a través del poseedor de claves, debe utilizar el servicio de certificación prestado por la Agencia Notarial de Certificación exclusivamente para los usos autorizados en estas condiciones generales y en la Declaración de Prácticas de Certificación, excepto declaración expresa y por escrito en otro sentido realizada por la Agencia Notarial de Certificación.

El suscriptor, por medio del poseedor de claves, se obliga a utilizar el servicio de certificación digital, la pareja clave pública/clave privada, la tarjeta y cualquier otro elemento técnico entregado por la Autoridad de Registro correspondiente y los certificados, de acuerdo con estas condiciones generales, las condiciones particulares que en su caso resulten aplicables, y con cualquier otra instrucción, manual o procedimiento suministrados por la referida Autoridad de Registro o por la Agencia Notarial de Certificación al suscriptor y/o poseedor de claves.

QUINTA. Obligaciones de la Agencia Notarial de Certificación, y de la Autoridad de Registro por delegación de la Agencia Notarial de Certificación

5.1. Obligaciones previas a la expedición de los Certificados CGN.

Antes de expedir los certificados, la Agencia Notarial de Certificación, y por delegación, la Autoridad de Registro correspondiente para cada tipo de certificado, se obligan a lo siguiente:

a) Comprobar la identidad y circunstancias personales del futuro poseedor de claves de los certificados, de acuerdo con la Declaración de Prácticas de Certificación.

b) Verificar que toda la información contenida en la solicitud de los certificados es exacta y que incluye toda la información prescrita para los certificados cualificados.

c) Asegurar que el futuro poseedor de claves de los certificados recibe la posesión de los datos de creación de firma electrónica correspondientes a los datos de verificación de firma que constan en el certificado de firma electrónica, mediante la entrega de la tarjeta.

d) Garantizar la complementariedad de los datos de creación y verificación de firma generados.

e) Asegurar que el futuro solicitante de los certificados ha recibido, o en caso contrario, proporcionar la siguiente información mínima por escrito o por vía electrónica, mediante un texto de divulgación de certificados:

> 1) Las obligaciones del poseedor de claves, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos e información sobre la tarjeta, en su condición de dispositivo cualificado de creación y de verificación de firma electrónica compatible con los datos de firma y con los certificados expedidos.
>
> 2) Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.
>
> 3) El método utilizado por la Agencia Notarial de Certificación para comprobar la identidad del futuro poseedor de claves u otros datos que figuren en el Certificado.
>
> 4) Las condiciones precisas de utilización de los certificados, sus posibles límites de uso y la forma en que la Agencia Notarial de Certificación garantiza su responsabilidad patrimonial.
>
> 5) Las demás informaciones relevantes contenidas en la Declaración de Prácticas de Certificación.

ANCERT se obliga al registro de los datos del certificado y a su emisión posterior al suscriptor, para lo cual debe realizar las comprobaciones que considere oportunas respecto de la identidad y otras informaciones personales y complementarias de los suscriptores y, cuando resulte procedente, de los poseedores de claves.

Estas comprobaciones deben incluir la justificación documental aportada por el suscriptor y, si ANCERT lo considera necesario, cualquier otro documento e información relevantes, facilitados por el suscriptor, por el poseedor de claves, o por terceras personas.

En el caso que ANCERT detecte errores en los datos que se deben incluir en los certificados o que justifican estos datos, podrá realizar los cambios que considere necesarios antes de emitir el certificado o suspender el proceso de emisión y gestionar con el suscriptor la incidencia correspondiente. En caso de que ANCERT corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, deberá notificar los datos finalmente certificados al suscriptor.

ANCERT se reserva el derecho a no emitir el certificado, cuando la justificación documental aportada resulte insuficiente para la correcta identificación y autenticación del suscriptor y/o del poseedor de claves.

Las anteriores obligaciones quedarán en suspenso en los casos en que el suscriptor actúe como entidad de registro y disponga de los elementos técnicos correspondientes a la generación de claves, emisión de certificados y grabación de tarjetas corporativas.

5.2. Obligaciones simultáneas o posteriores a la expedición de los Certificados CGN.

Simultánea o posteriormente a la expedición de los Certificados, la Agencia Notarial de Certificación se obliga a:

a) No almacenar ni copiar los datos de creación de firma del poseedor de claves.

b) Mantener un Depósito actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del depósito se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

c) Demostrar la fiabilidad necesaria para prestar servicios de certificación.

d) Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.

e) Emplear personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos.

f) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica, y en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

g) Conservar registrada por cualquier medio seguro toda la información y documentación relativa a los certificados cualificados y las Declaraciones de Prácticas de Certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.

h) Utilizar sistemas fiables para almacenar los certificados cualificados que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el suscriptor haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

i) Revocar el Certificado y a publicar ese hecho de un modo inmediato en sus sistemas de información de estado de certificados, así como en el Depósito de certificado, una vez recibida la correspondiente solicitud de revocación. La solicitud de revocación deberá ser cursada en la forma prevenida en la Declaración de Prácticas Certificación.

j) Poner a disposición de los usuarios los medios necesarios para verificar la autenticidad de los certificados emitidos.

k) Facilitar el acceso por medios telemáticos a la Declaración de Prácticas de Certificación vigente en cada momento, así como a las informaciones descritas en la misma.

l) Cumplir todas las previsiones aplicables de la normativa sobre protección de datos de carácter personal.

m) Emitir los certificados solicitados ajustándose a las normas y procedimientos establecidos en la Declaración de Prácticas de Certificación.

n) Cumplir todas aquellas obligaciones impuestas por la Declaración de Prácticas Certificación y por la normativa vigente en materia de Firma electrónica y prestación de servicios de certificación.

SEXTA. Garantías

6.1. Garantía de la Agencia Notarial de Certificación por los servicios de certificación digital

La Agencia Notarial de Certificación garantiza que la clave privada de la entidad de certificación utilizada para emitir certificados no ha sido comprometida, a no ser que haya comunicado lo contrario mediante el registro de certificación, de acuerdo con la Declaración de Prácticas de Certificación.

La Agencia Notarial de Certificación únicamente garantiza al suscriptor, en el momento de la emisión del certificado, que:

a) Todos los Certificados CGN son cualificados y, cuando procede, funcionan en dispositivo cualificado de creación de firma, en los términos previstos en la Reglamento (UE) 910/2014, de 19 de diciembre.

b) La Agencia Notarial de Certificación no ha originado ni ha introducido declaraciones falsas o erróneas en la información de ningún certificado, ni ha dejado de incluir información necesaria aportada y verificada por el suscriptor.

c) Todos los certificados cumplen los requisitos formales y de contenido previstos en la Declaración de Prácticas de Certificación.

d) La Agencia Notarial de Certificación ha cumplido los procedimientos descritos en la Declaración de Prácticas de Certificación.

La Agencia Notarial de Certificación aplica una diligencia razonable para asegurar que cada producto suministrado en la prestación de sus servicios se encuentra libre de virus informático, gusanos y otros códigos ilícitos, y se obliga a comunicar al suscriptor cualquier virus, gusano u otros códigos ilícitos descubiertos posteriormente en cualquier producto.

6.2. Exclusiones de la garantía

La Agencia Notarial de Certificación no garantiza software alguno que utilice el suscriptor de certificados o el poseedor de claves o cualquier otra persona para generar, verificar o utilizar de otra forma firma digital alguna o certificado digital emitido por la Agencia Notarial de Certificación, excepto cuando exista una declaración escrita de la Agencia Notarial de Certificación en sentido contrario.

SÉPTIMA. Responsabilidad del suscriptor

El suscriptor debe responder ante cualquier persona por el incumplimiento de sus obligaciones según los términos de estas condiciones generales, y en todo caso, de su actividad como Entidad de Registro y del uso indebido del certificado, o de la no veracidad o exactitud de la información aportada en todo momento a la Agencia Notarial de Certificación o a terceros.

El suscriptor es responsable de todas las comunicaciones electrónicas firmadas o protegidas electrónicamente, cuando el certificado haya sido válidamente verificado mediante los mecanismos y las condiciones establecidos por la Agencia Notarial de Certificación en la Declaración de Prácticas de Certificación.

El suscriptor se compromete a mantener indemne a la Agencia Notarial de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida,

gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a la Agencia Notarial de Certificación, la entidad de registro o cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

OCTAVA. Responsabilidad de la Agencia Notarial de Certificación

8.1. Responsabilidad como prestador de servicios de certificación

La Agencia Notarial de Certificación responde ante el suscriptor y cualquier tercera persona por el incumplimiento de las obligaciones legalmente impuestas por el Reglamento (UE) 910/2014, y según los términos de estas condiciones generales.

La Agencia Notarial de Certificación no será responsable:

a) En los casos previstos en el artículo 13 del Reglamento (UE) 910/2014.

b) De las informaciones contenidas en los certificados, siempre que su contenido cumpla estas condiciones generales y la Declaración de Prácticas de Certificación.

c) De los daños y perjuicios causados por los siguientes motivos:

1) El incumplimiento de las obligaciones que corresponden a cada suscriptor de los certificados.

2) La utilización de los certificados y/o claves certificadas por ellos, para usos no permitidos en el certificado, o por su utilización fuera del periodo de vigencia del certificado.

3) La pérdida, divulgación o compromiso de la clave privada del poseedor de claves; o por el uso incorrecto de los soportes que contienen los certificados y las claves.

4) El contenido concreto de los documentos a los que se incorpora la firma electrónica cualificada basada en el certificado emitido, dado que la Agencia Notarial de Certificación no tiene conocimiento de los documentos que se firman.

5) Caso fortuito o fuerza mayor tales como los desastres naturales o la guerra, o los cortes en el suministro electrónico o en el funcionamiento defectuoso de los equipos informáticos utilizados por el suscriptor o por los terceros.

Sin perjuicio de lo anterior, la Agencia Notarial de Certificación no garantiza los algoritmos criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que haya aplicado la diligencia debida según el estado de la técnica en cada

momento, y haya actuado conforme a lo dispuesto en la Declaración de Prácticas de Certificación, y en el Reglamento (UE) 910/2014 y su normativa de aplicación.

8.2. Adecuación de los productos que hacen uso de la identificación, la firma electrónica o el cifrado

La Agencia Notarial de Certificación no se hace responsable de la adecuación de los productos y servicios relacionados con la certificación digital, la identificación, la firma electrónica o el cifrado existentes en el mercado que sean utilizados en aplicaciones informáticas del suscriptor, excepto cuando la Agencia Notarial de Certificación los suministre. En este caso, las partes quedarán sujetas a las correspondientes condiciones de uso.

NOVENA. Lugar de prestación de la actividad

El lugar de cumplimiento de las obligaciones de la Agencia Notarial de Certificación relativas a los servicios de certificación digital y, en su caso, licencias de uso de software es el domicilio de la Agencia Notarial de Certificación, Paseo del General Martínez Campos 46, 6ª planta, 28010 Madrid.

DÉCIMA. Licencia de software

La Agencia Notarial de Certificación concede al suscriptor, con carácter no exclusivo e intransferible, licencia para utilizar las copias del software recibido de la Agencia Notarial de Certificación para la operación de la tarjeta, así como para la producción de la firma electrónica y los restantes servicios criptográficos por parte de los poseedores de claves.

El suscriptor puede hacer copias del software únicamente con el fin de archivo o copia de seguridad.

En caso de que cualquier persona diferente de la Agencia Notarial de Certificación realice modificaciones en el software suministrado, todas las garantías respeto al software quedarán inmediatamente canceladas.

UNDÉCIMA. Propiedad de los certificados y las tarjetas

Los certificados y las tarjetas de los poseedores de claves suministradas permanecen propiedad de la Agencia Notarial de Certificación, que se reserva el derecho discrecional de retirar o sustituir las tarjetas con certificados emitidos, por razones de seguridad, cuando queden obsoletas tecnológicamente o por cualquier otro motivo justificado.

DUODÉCIMA.- Propiedad Intelectual e Industrial

La Agencia Notarial de Certificación es titular en exclusiva de todos los derechos, incluidos los derechos de explotación, sobre el Depósito de Certificados, la Lista de Revocación de Certificados y los restantes mecanismos de información de estado de certificados, en los términos señalados en el Texto Refundido de la Ley de Propiedad Intelectual aprobado mediante Real Decreto Legislativo 1/1996, de 12 de abril, incluido el derecho sui generis reconocido en el artículo 133 de la citada Ley.

Se permite el acceso al Depósito de Certificados, las Listas de Revocación de Certificados y los restantes mecanismos de información de estado de certificados, estando prohibida la reproducción, comunicación pública, distribución, transformación o reordenación salvo cuando esté expresamente autorizada por la Agencia Notarial de Certificación o por la Ley.

Se autoriza expresamente la obtención y conservación de la información necesaria para formar evidencia de la verificación de cada firma electrónica.

Asimismo, la Agencia Notarial de Certificación es titular de todos los mismos derechos de propiedad intelectual e industrial respecto a la Declaración de Prácticas de Certificación y la información de la actividad de prestación de los servicios de certificación, respecto de los cuales se concede únicamente a los suscriptores un derecho de uso.

Los OID propiedad de la Agencia Notarial de Certificación han sido registrados en la IANA (Internet Assigned Number Authority) bajo la rama 1.3.6.1.4.1, habiéndose asignado el número 18920 (ANCERT), siendo dicha información pública en:

http://www.iana.org/assignments/enterprise-numbers

Igualmente queda prohibido el uso total o parcial de cualquiera de los OID asignados a la Agencia Notarial de Certificados salvo para los usos previstos en los certificados o en el Depósito de Certificados.

Queda prohibida cualquier extracción y/o reutilización de la totalidad o de una parte sustancial de los contenidos o de las bases de datos que la Agencia Notarial de Certificación pone a disposición de los suscriptores de certificados.

DÉCIMOTERCERA. Protección de los datos personales

La Agencia Notarial de Certificación es titular de un conjunto de ficheros de datos de carácter personal relativos a los datos de identificación y autenticación de los usuarios de los servicios de certificación digital, tal y como se especifica en la Declaración de Prácticas de Certificación.

La Agencia Notarial de Certificación obtiene los datos personales que figuran en los ficheros por captación de los datos por parte del solicitante, a través del Consejo General del Notariado, los Colegios Notariales y las Notarías que actúan como Entidad de Registro, en las condiciones previstas en la normativa sobre firma electrónica y sobre protección de datos de carácter personal.

La Agencia Notarial de Certificación se obliga a cumplir la normativa sobre firma electrónica y sobre protección de datos de carácter personal, en especial con respecto a la inscripción y la correcta gestión de los ficheros de datos personales, con las medidas de seguridad correspondientes.

La Agencia Notarial de Certificación tiene la condición de Responsable del Fichero en tanto que decide sobre la finalidad, contenido y uso del tratamiento de los datos de carácter personal y las Entidades de Registro se consideran Encargadas del Tratamiento, las cuales deben utilizar los

datos contenidos en dichos Ficheros, única y exclusivamente para los fines que figuran en su Declaración de Prácticas de Certificación.

La Agencia Notarial de Certificación queda exonerada de cualquier responsabilidad que se pudiera generar por el incumplimiento por parte de las personas Encargadas del Tratamiento de sus obligaciones descritas. En dichos supuestos de incumplimiento, éstas serán consideradas como responsables del tratamiento y responderán de las infracciones en que hubiese incurrido personalmente.

DÉCIMOCUARTA. Ley aplicable, y jurisdición comptente.

Las presentes condiciones de emisión serán interpretadas y serán ejecutadas en sus propios términos y, en todo aquello no previsto, las partes se regirán por el Reglamento (UE) 910/2014, por la legislación administrativa aplicable y, subsidiariamente, por la legislación civil y mercantil que regula el régimen de las obligaciones y los contratos.

La jurisdicción competente es la que se indica en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

DÉCIMOQUINTA. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación.

Las cláusulas de las presentes condiciones de emisión son independientes entre sí, motivo por el cual si cualquier cláusula es considerada inválida o inaplicable, el resto de cláusulas seguirán siendo aplicables, excepto acuerdo expreso en contrario de las partes.

Asimismo, la invalidez de una cláusula no afectará al resto de las cláusulas del contrato, que se mantendrán vigentes en tanto en cuanto no finalice la relación jurídica entre las partes por cualquiera de las causas mencionadas en las presentes condiciones generales de emisión.

Tras la finalización de la prestación de servicios entre las partes los requisitos relativos a obligaciones y responsabilidad, auditoría de conformidad y confidencialidad, según los términos de la Declaración de Prácticas de Certificación, continarán vigentes.

Las condiciones generales de emisión contienen la voluntad completa y todos los acuerdos entre las partes.

Las partes procederán a la notificación de la información de que se trate, ya sea de forma presencial en las instalaciones de la Entidad de Registro correspondiente, o a distancia por comunicación escrita y/o vía web en la dirección que se habilite para ello.

DÉCIMOSEXTA. Resolución

La resolución tendrá lugar en los casos siguientes:

a) Por incumplimiento por la otra parte, de cualquiera de sus obligaciones especificadas en la Declaración de Prácticas de Certificación.

b) Por concurrencia de cualquier otra causa de resolución anticipada establecida por la legislación vigente y, especialmente, por la legislación vigente de firma electrónica y certificación digital.