DECLARACIÓN BÁSICA DE CARACTERÍSTICAS Y REQUERIMIENTOS

PKI AC CAMERFIRMA SA

WEBSITES LEGALES

Versión 1.0

Idioma: **Castellano**
Fecha: Marzo 2016

Marzo 2016	V1.0	Redacción del documento

Índice de Contenido

1. Introducción

El presente documento presenta un extracto de las características y requerimientos de la PKI de Camerfirma, los cuales se establecen de forma completa en la DPC y en las correspondientes CP aplicables al certificado que se esté solicitando o con el que se esté operando.

Es altamente recomendable la lectura de la DPC en su totalidad, así como de las PC aplicables, para formar una idea clara de las especificaciones, objetivos, normas, derechos, responsabilidades y obligaciones por los cuales se rige la prestación del servicio de certificación.

La presente Declaración Básica se elabora conforme a la especificación técnica “ETSI TS 101 456: Policy Requirements for Certification Authorities issuing qualified certificates” En concreto, a lo recomendado en su anexo B para el “PKI Disclosure Statement”

2. Información de contacto de la AC

Esta PKI, está administrada y gestionada por el departamento jurídico de Camerfirma pudiendo ser contactado por los siguientes medios:

E-mail:	juridico@camerfirma.com
Teléfono:	+34 902 361 207
Fax:	+34 914 119 661
Dirección:	Camerfirma – Departamento Jurídico C/ Ribera del Loira, 122 - 8042 Madrid
Localización:	https://www.camerfirma.com/address

3. Tipos de certificado, procedimientos de validación y uso

Los Certificados Camerfirma para Websites Legales, permiten identificar y vincular un determinado dominio en Internet o URL a una entidad.

Los Certificados Camerfirma para Websites Legales dentro de la jerarquía "Chambers of Commerce Root" son los siguientes:

- Certificados para Servidor Seguro OV.
- Certificados de Servidor Seguro EV.
- Sede Electrónica Administrativa Nivel Alto.
- Sede Electrónica Administrativa Nivel Medio.

Los Certificados Camerfirma para Websites Legales pueden ser utilizados con los siguientes propósitos:

- Identificación de la entidad legal que controla un sitio web**:** Se ofrece una garantía razonable al usuario de un aplicativo cliente de navegación en Internet (navegador) de que el sitio al que se accede es controlado por la entidad identificada en el certificado mediante su nombre, dirección fiscal e identificación fiscal.
- Identificación de la URL: El usuario que accede a la URL para la cual se ha emitido el certificado puede comprobar los datos de la entidad que haya registrado ese dominio, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado.
- Negociación de Cifrado: Se permite el intercambio de información de claves para establecer un canal de comunicación cifrado entre el navegador y el sitio Web.
- Prevención de suplantación de identidad: Se asiste al usuario del navegador para asegurar la legitimidad de una entidad que declara gestionar un sitio Web, estableciendo un canal que sirva de ayuda para resolver problemas de direccionamientos relacionados con "phishing" y otras formas de fraude de identidad.

Los Certificados Camerfirma para Websites Legales no garantizan:

- La veracidad o legalidad del contenido del sitio Web.
- Que el suscriptor del certificado represente a una entidad comercialmente activa.
- Que el suscriptor del certificado cumple con las leyes actuales.
- Que el suscriptor del certificado es confiable, honesto o de reputación a la hora de realizar tratos comerciales.
- Que es seguro realizar negocios con el suscriptor del certificado.

La AC no se responsabilizará en ningún caso del contenido de las páginas web bajo la URL identificada en el certificado.

4. Limitaciones en la confianza

Los certificados deben emplearse para las funciones y finalidades establecidas en su correspondiente PC, sin que puedan emplearse para otras funciones y finalidades.

Según la legislación vigente, la responsabilidad de CAMERFIRMA y de la AR no se extiende a aquellos supuestos en los que la utilización indebida del certificado tiene su origen en conductas imputables al Firmante, y al Tercero que confía por:

- No haber proporcionado información adecuada, inicial o posteriormente como consecuencia de modificaciones de las circunstancias reflejadas en el certificado electrónico, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación;
- Haber incurrido en negligencia con respecto a la conservación de los datos de creación de firma y a su confidencialidad;
- No haber solicitado la suspensión o revocación de los datos del certificado electrónico en caso de duda sobre el mantenimiento de la confidencialidad;
- Haber utilizado la firma después de haber expirado el periodo de validez del certificado electrónico;
- Superar los límites que figuren en el certificado electrónico.
- En conductas imputables al Tercero que confía si éste actúa de forma negligente, es decir cuando no compruebe o tenga en cuenta las restricciones que figuran en el certificado en cuanto a sus posibles usos y límite de importe de las transacciones; o cuando no tenga en cuenta el estado de vigencia del certificado.
- De los daños ocasionados al firmante o terceros que confía por la inexactitud de los datos que consten en el certificado electrónico, si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible.

5. Obligaciones de los titulares

Será obligación de los titulares de un Certificado Camerfirma para Personas Legales:

1. Suministrar a la AC la información necesaria para realizar una correcta identificación
2. Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.
3. Custodiar su clave privada de manera diligente
4. Informar de la existencia de alguna causa de revocación.
5. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
6. No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación

6. Obligaciones de los Terceros que Confían

Será obligación de los Terceros que Confían en un certificado Camerfirma para Websites Legales:

1. Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
2. Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.
3. Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la PC pertinente.
4. Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

7. Limitación de responsabilidades

La AC no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

1. Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor
2. Por el uso de los certificados siempre y cuando exceda lo dispuesto en la normativa vigente y la Política de Certificación.
3. Por el uso indebido o fraudulento de los certificados o CRL emitidos por la AC.
4. Por el uso de la información contenida en el Certificado o en la CRL.
5. Por el incumplimiento de las obligaciones establecidas para el Suscriptor o Tercero que Confía en la normativa vigente, la PC o las prácticas correspondientes.
6. Por el perjuicio causado en el periodo de verificación de las causas de revocación.
7. Fraude en la información presentada por el solicitante.

8. Acuerdos, Declaración de Prácticas de Certificación y Políticas de Certificación aplicables

Todos los Acuerdos, DPC y PC aplicables se encuentran en la página web establecida al efecto: http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/

9. Política de protección de datos de carácter personal

Se determinará por la AC la información que deba ser considerada confidencial, debiendo cumplir en todo caso con la normativa vigente en materia de protección de datos y concretamente con lo dispuesto por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

Las autoridades de Registro que se constituyan en la PKI de Camerfirma verificarán que el solicitante de un certificado es informado y presta su consentimiento al tratamiento de sus datos de carácter personal, la finalidad que se les va a dar, a los destinatarios de los datos y su inclusión en el fichero declarado para dicho efecto por Camerfirma.

Los titulares de los datos podrán ejercer sus derechos de acceso, rectificación y oposición dirigiéndose a la dirección de contacto indicada en el presente documento.

Los datos contenidos en el Directorio de Certificados so consideran datos de carácter personal a efectos de lo dispuesto en la LOPD y demás normativa complementaria, motivo por el cual no se permite el acceso por parte de terceros.

10. Política de reembolsos

AC Camerfirma no tiene una política de reintegros específica, y se acoge a la normativa general vigente

11. Legislación aplicable, mecanismos de resolución de conflictos

11.1. Legislación aplicable

Las operaciones y funcionamiento de la PKI de Camerfirma, así como la DPC que sean de aplicación para cada tipo de certificado, estarán sujetas a la normativa que les sea aplicable, con especial atención a:

- Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

De igual manera, habrán de observarse las normas y procedimientos internos dictados por Camerfirma encaminadas a garantizar las exigencias de seguridad del citado Real Decreto.

11.2. Mecanismos de resolución de conflictos

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

12. Auditorías, certificaciones y sellos de confianza de la AC y los repositorios

Los objetivos de Camerfirma respecto a la seguridad y la calidad han sido fundamentalmente la obtención de la certificación ISO/IEC 27001, ISO/IEC 20000 y la realización de Auditorías internas bienales al Sistema de certificación Camerfirma, y fundamentalmente a las AR, para garantizar el cumplimiento de los procedimientos internos.

Camerfirma está sujeta a unas auditorias periódicas con el sello WEBTRUST for CA, WEBTRUST SSL BR y WEBTRUST SSL EV que asegura que los documentos de políticas y CPS tienen un formato y alcance adecuado a la vez que están completamente alineadas con su políticas y prácticas de certificación.

Camerfirma está también sujeta a los controles que realiza el organismo regulador nacional respecto a su actividad, siendo este el Ministerio de Industria del Gobierno de España

Se realizará una auditoría con una periodicidad mínima anual, salvo que se establezca un plazo menor por la normativa vigente.

La auditoría deberá verificar en todo caso:

- Que la AC tiene un sistema que garantice la calidad del servicio prestado.
- Que la AC cumple con los requerimientos de la Política de Certificación
- Que las Prácticas de Certificación de la AC se ajustan a lo establecido a la PC, con lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente.
- Que Camerfirma gestiona de forma adecuada la seguridad de sus sistemas de información.

Anexo I. Acrónimos

AC	Autoridad de Certificación.
AR	Autoridad de Registro
CRL	Certificate Revocation List. Lista de Certificados Revocados.
DPC	Declaración de Prácticas de Certificación.
EV	Extended Validation. Validación Extendida.
OV	Organization Validation. Validación de Organización.
PC	Política de Certificación
PKI	Public Key Infrastructure. Infraestructura de clave pública.
URL	Uniform Resource Locator. Localizador de Recursos Uniforme.