POLÍTICA DE CERTIFICACIÓN DE CERTIFICADOS FEREN (FIRMA ELECTRONICA RECONOCIDA NOTARIAL)

Versión 1.0
Fecha: 25/10/2004

Índice

1 INTRODUCCION

1.1. Presentación

El **CONSEJO GENERAL DEL NOTARIADO,** en su calidad de Prestador de Servicios de Certificación, ha delegado en la **Agencia Notarial de Certificación, S.L.U**. **(ANCERT) –constituida exclusivamente por el propio Consejo-** los medios técnicos necesarios para la emisión de certificados electrónicos reconocidos. **ANCERT** dispone de la Autoridad de Certificación raíz **ANCERT Certificados CGN** que ha expedido un *Certificado* raíz para la Autoridad de Certificación subordinada **ANCERT Certificados FERN**, para a su vez emitir los *Certificado*s electrónicos denominados **Certificados FEREN.**

El presente documento recoge la *Política de Certificación* de la Autoridad de Certificación subordinada **ANCERT Certificados FERN** para la emisión de los **Certificados FEREN.** Esta Política de Certificación detalla y completa lo definido en la *Declaración de Prácticas de Certificación* de **ANCERT**, recogiendo su ámbito de aplicación, las características técnicas de este tipo de *Certificado*, el conjunto de reglas que indican los procedimientos seguidos en la prestación de servicios de certificación, tales como el ciclo de vida de los *Certificado*s, así como sus condiciones de uso.

Esta Política de Certificación, junto con la *Declaración de Prácticas de Certificación* de ANCERT, está especialmente dirigida a cualquiera que confíe de buena fe en este tipo de *Certificado*s.

Los conceptos y terminología de la presente *Política de Certificación* deberán interpretarse de acuerdo con el punto “1.8 Definiciones y Acrónimos” de la *Declaración de Prácticas de Certificación*.

ANCERT Certificados FERN emite los **Certificados FEREN** para todos los Notarios establecidos en territorio español. El Decano de cada Colegio Notarial del territorio español es el responsable del registro de sus Colegiados, actuando como *Autoridad de Registro*. Por su parte el Presidente de la Junta de Decanos actúa como *Autoridad de Registro* para todos los Decanos del territorio español. Los Decanos de los Colegios Notariales y el Presidente de la Junta de Decanos (en adelante la *Autoridad de Registro*) son responsables del registro e identificación de los Notarios y Notarios Decanos. Se utilizan Tarjetas *Criptográficas* como único soporte de los *Certificados,* denominadas *Tarjetas FEREN*.

Los documentos electrónicos firmados con este tipo de Certificados son los únicos que servirán para la comunicación de los documentos públicos en los términos prevenidos en el artículo 3, número 6, a) de la Ley 59/2003.

Los **Certificados FEREN** son *Certificados* electrónicos reconocidos y son utilizados para generar la firma electrónica que garantiza la identidad del *Suscriptor* del certificado, de acuerdo con lo establecido por los artículos 11 y siguientes de la Ley 59/2003 de Firma Electrónica y lo dispuesto en los artículos 110 y siguientes de la Ley 24/2001.

La huella digital de esta Autoridad de Certificación subordinada basada en el algoritmo SHA-1 es:

BB5A 6CDF 6882 BDA1 9DFC 8260 5911 BA96 3BB0 A651

1.2. Identificación

Política de Certificación de **ANCERT Certificados FERN** de los **Certificados FEREN**:

- *OID: 1.3.6.1.4.1.18920.4.1.1.1*

1.3. Directorio de *Certificados*

ANCERT Certificados FERN dispone de un servicio de Directorio de *Certificados* el cual es operativo durante las 24 horas de los 7 días de la semana. En caso de que se interrumpiera dicho servicio por causa de fuerza mayor, y por tanto ajena a dicha Autoridad de Certificación, el servicio se restablecerá en el estrictamente menor tiempo posible.

1.4. Publicación

ANCERT Certificados FERN mantendrá el *Directorio de Certificados* que podrá ser consultado libremente vía Web las 24 horas de los 7 días de la semana en la dirección http://www.ancert.com. En el *Directorio de Certificados* de **ANCERT Certificados FERN** se podrá consultar el estado de los *Certificados*.

Así mismo podrán consultarse las *Listas Certificados Revocados*, la presente *Política de Certificación*, la *Declaración de Prácticas de Certificación* y el *Certificado* raíz de **ANCERT Certificados FERN**.

1.5. Frecuencia de actualizaciones

Cuando **ANCERT Certificados FERN,** en virtud de su actividad como *Prestador de Servicios de Certificación,* disponga de información actualizada la publicará oportunamente.

1.6. Control de Acceso al *Directorio de Certificados*

ANCERT Certificados FERN no limita el acceso de lectura a las informaciones establecidas en los puntos 1.3 y 1.4 pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o eliminar información registrada, a fin de proteger la integridad y autenticidad de la misma. **ANCERT Certificados FERN** utiliza sistemas fiables para el registro de *Certificados*, pudiendo únicamente personas autorizadas hacer modificaciones.

2 DESCRIPCIÓN DEL *CERTIFICADO*

2.1. Ámbito de aplicación

ANCERT Certificados FERN expide los **Certificados FEREN** a personas físicas, en su nombre propio. Además de las menciones que más adelante se explicitan este tipo de certificados deberá recoger ineludiblemente la condición de Notario y la plaza donde ejerce su ministerio el titular del *Certificado*.

2.2. Tipo de *Certificado*

Los **Certificados FEREN** son *Certificados reconocidos,* en los términos del artículo 11 de la Ley 59/2003, de Firma Electrónica, es decir, son *Certificado*s electrónicos expedidos por un *Prestador de Servicios de Certificación* cumpliendo los requisitos establecidos en dicha Ley 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.

La Ley sólo considera Firma Electrónica reconocida la firma electrónica avanzada basada en un *Certificado reconocido* y generada mediante un *Dispositivo seguro de Creación de Firma*. Por ello, la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

2.3. Usos del *Certificado*

Los **Certificados FEREN** se utilizan para la Firma electrónica reconocida de documentos electrónicos o mensajes electrónicos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido, entendiendo por ello lo siguiente:

Autenticidad de origen

Asegura que el documento o la comunicación electrónica provienen del dispositivo de creación de firma de la persona o entidad de quien dice provenir. Esta característica se obtiene mediante la firma electrónica reconocida. El receptor de un mensaje firmado electrónicamente puede verificar esa firma a través del **Certificado FEREN** del *Suscriptor*.

No repudio de origen

Evita que el emisor de un determinado mensaje pueda negar, si ello le conviene, la emisión del mismo. Para ello se utiliza la firma electrónica reconocida. El receptor de un mensaje firmado digitalmente puede verificar esa firma a través del **Certificado FEREN** del *Suscriptor*. De esta forma puede demostrar la identidad del emisor del mensaje sin que éste pueda repudiarlo.

Integridad

Permite comprobar que un documento electrónico firmado con *Firma electrónica reconocida* no ha sido modificado por ningún agente externo. Para garantizar la integridad, la criptografía utiliza las capacidades matemáticas de las funciones de resumen (funciones de *hash*), utilizadas en combinación con la firma electrónica. El procedimiento se centra en firmar electrónicamente un resumen único del documento electrónico con la clave privada del suscriptor de forma que cualquier alteración del documento revierte en una alteración de su resumen.

2.3.1 Uso permitido del Certificado

Podrá utilizarse el **Certificado FEREN** para cifrar o descifrar documentos electrónicos bajo su exclusiva responsabilidad. Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de tales usos quedan a cargo del *Suscriptor*. En ningún caso podrán *las Autoridades de Registro* ni el *Suscriptor* ni los terceros perjudicados reclamar a **ANCERT Certificados FERN** compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los *Certificado*s para fines de cifrado de confidencialidad.

2.4. Limitaciones de uso

2.4.1 Usos prohibidos

No se permite usar los **Certificados FEREN** para usos diferentes a los previstos en los puntos 2.3. y 2.3.1. A título enunciativo, se prohíbe el uso de los **Certificados FEREN** para:

1) fines contrarios al propio del mismo, a sus propósitos y funcionalidades, y a su correcta utilización.
2) firmar otro *Certificado* o aplicaciones informáticas.
3) generar sellos de tiempo.
4) prestar servicios a título gratuito u oneroso, tales como servicios de OCSP, de facturación electrónica, de generación de *Listas de Revocación o de s*ervicios de notificación.
5) fines contrarios a la legislación vigente en España sobre prestación de servicios de certificación o firma electrónica en el momento de utilizar el *Certificado*.
6) fines contrarios a lo establecido en la *Declaración de Prácticas de Certificación*, en esta *Política de Certificación*.

2.4.2 Limitación de cuantías

Los **Certificados FEREN** emitidos por **ANCERT Certificados FERN** se conceden sin limitación de uso por razón de la cuantía.

3 IDENTIFICACION Y AUTENTICACION

3.1. Nombre del Certificado FEREN

En esta sección se establecen los requisitos relativos a los procedimientos de identificación y autenticación que han de utilizarse durante el registro de los *Suscriptores* de **Certificados FEREN**, los cuales deben realizarse con anterioridad a la expedición de los *Certificado*s.

3.1.1 Nombre distintivo en el campo *Subject* del *Certificado*

Todos los **Certificados FEREN** contienen un nombre distintivo X.500 en el campo *Subject*, que incluye los campos que se desarrollan en el punto 4.5.1 de esta *Política de Certificación*.

3.1.2 Identidad alternativa en el campo *Subject* del *Certificado*

Todos los **Certificados FEREN** contienen una identidad alternativa X.500 en el campo *Subject*, que incluye los campos que se desarrollan en el punto 4.5.2 de esta *Política de Certificación*.

3.1.3 Nombre del *Suscriptor* persona física

En los **Certificados FEREN** el nombre del *Suscriptor* está compuesto únicamente por su nombre y apellidos.

3.1.4 Uso de pseudónimos

No pueden utilizarse pseudónimos para identificar a una persona física.

3.1.5 Interpretación del formato de nombres

Todos los nombres de personas físicas están escritos utilizando lenguaje natural, prescindiendo de acentos. En ningún caso se pueden modificar los nombres y apellidos, excepto para adaptarlos al formato y longitud del componente *CommonName* en el que se insertan.

3.2. Comprobación de la identidad de los *Suscriptores*

El proceso de identificación y autenticación lo realizarán, como *Autoridad de Registro,* exclusivamente los Decanos y miembros de las Juntas Directivas de los Colegios Notariales para los Notarios Colegiados y el Presidente de la Junta de Decanos para los Notarios Decanos.

Los tipos de documentos que son necesarios para acreditar la identidad del *Suscriptor* pueden ser exclusivamente el Documento Nacional de Identidad, pasaporte, o

cualquier otro medio admitido en derecho, siempre que contenga al menos la siguiente información:

a) Nombre y apellidos
b) Lugar y fecha de nacimiento
c) Numero de Identidad reconocido legalmente
d) Otros atributos del Solicitante

4 CICLO DE VIDA DEL *CERTIFICADO*

4.1. Solicitud

Los *Certificado*s que incorporen firma electrónica reconocida se regirán en cuanto a los requisitos para su solicitud, generación, entrega, conservación y revocación por lo que contractualmente se acuerde entre **ANCERT Certificados FERN** y *las Autoridades de Registro*, con las especialidades que se contienen en la presente *Política de Certificación.*

En todo caso, previamente a efectuar la solicitud del *Certificado*, *las Autoridades de Registro* identificarán a los *Suscriptores* mediante el Documento Nacional de Identidad vigente, u otros medios admitidos en derecho a efectos de identificación descritos en el punto 3.2 de este documento.

4.2. Emisión

Los trámites a seguir para la emisión de las claves y el *Certificado* del *Solicitante* son los siguientes:

1. Los Decanos o miembros de las Juntas Directivas del Colegio Notarial o el Presidente de la Junta de Decanos, en su caso, como *Autoridades de Registro* introducirán en el Lector de Tarjetas de su ordenador su *Tarjeta Criptográfica* con el *Certificado* que les autentica como *Autoridades de Registro* y accederán a la aplicación de registro.
2. Una vez autenticado, el Decano o miembro de las Juntas Directivas del Colegio Notarial o el Presidente de la Junta de Decanos, en su caso, introducirá en el Lector de Tarjetas la *Tarjeta Criptográfica* del Notario o Decano, que previamente les ha sido entregada junto a los códigos PIN y PUK correspondientes en sobre cerrado.
3. *Las Autoridades de Registro* completarán el formulario de registro con los datos de los *Suscriptores* y solicitarán la emisión del *Certificado*.
4. En este momento, la aplicación de registro solicitará el PIN correspondiente a la *Tarjeta Criptográfica* del *Suscriptor*, para activar el procedimiento de generación de claves.
5. En ese momento se generará el par de claves en la *Tarjeta Criptográfica* del *Suscriptor*, enviando la petición a **ANCERT Certificados FERN**, la cual generará el *Certificado* y lo remitirá vía SSL al ordenador del Decano del

Colegio Notarial o del Presidente de la Junta de Decanos, en su caso, quedando almacenado automáticamente en la *Tarjeta Criptográfica* del *Suscriptor*.

El soporte para el almacenamiento de las claves y el *Certificado* será siempre una *Tarjeta Criptográfica*, considerada como un *Dispositivo seguro de creación de firma*, con capacidades criptográficas de generación de los *Datos de creación y de verificación de Firma*, lo que permite garantizar que la clave privada no abandona nunca la Tarjeta Criptográfica y que por lo tanto la Tarjeta Criptográfica no puede ser duplicada. Para realizar una firma o activar la tarjeta es necesario introducir el Código Secreto de Activación (PIN) que solamente debe conocer el Suscriptor de la Tarjeta. Tres intentos consecutivos erróneos en la introducción del PIN provocan un bloqueo de la Tarjeta. Para desbloquear la Tarjeta, el *Suscriptor* deberá introducir el código PUK y del mismo modo tres intentos consecutivos erróneos en la introducción del PUK provocan el bloqueo irreversible de la Tarjeta.

La creación de las claves Pública y Privada (1024 bits RSA) la realiza la propia tarjeta internamente, de tal forma que se garantiza tanto la robustez de las claves como la imposibilidad de un compromiso de las mismas en el proceso de generación.

Los *Datos de creación de Firma* permanecerán siempre bajo el exclusivo control del *Suscriptor* de los mismos, no guardándose copia de ellos ni **ANCERT Certificados FERN** ni la *Autoridad de Registro.*

4.3. Publicación del *Certificado*

Una vez emitido el *Certificado* **ANCERT Certificados FERN** publicará automáticamente una copia del mismo en el *Directorio de Certificados* de **ANCERT Certificados FERN**.

4.4. Entrega del Certificado

Una vez emitido el certificado, el Notario o el Decano de un Colegio Notarial recibirá la *Tarjeta Criptográfica* firmando la correspondiente acta de entrega.

4.5. Composición del *Certificado*

4.5.1 Composición del nombre distintivo del Subject de Certificados FEREN

Los datos personales del Solicitante acreditados durante el proceso de solicitud del Certificado componen el nombre distintivo (DN) del Solicitante conforme al estándar X.500, la composición del cual es la siguiente:

Campo	***Descripción***

EA	e-mail del Notario
CN	Nombre y Apellidos del Notario
GN	Nombre del Notario
SU	Apellidos del Notario
SN	NIF del Notario
OU	Código de notaría
OU	Colegio Notarial
OU	NOTARIO
O	CONSEJO GENERAL DEL NOTARIADO
L	Población
ST	Provincia
C	País

Una vez compuesto el nombre distintivo que identificará al *Suscriptor*, se crea la correspondiente entrada en el directorio, asegurando que el nombre distintivo es único en toda la infraestructura del *Prestador de Servicios de Certificación*.

4.5.2 Composición de la identidad alternativa del *Subject* de *Certificados FEREN*

Campo	***Descripción***
Email	Email del Suscriptor

Se utiliza la extensión subjectAltName definida en X.509 versión 3 para ofrecer la información del e-mail.

4.5.3 Perfil del Certificado FEREN

Las extensiones utilizadas por los certificados emitidos bajo el amparo de la presente política son:

CAMPO	**VALOR**
Versión	V3
SerialNumber	1F8C 20FF 1F76 45EE 5E50 8D6E EDEE 65E2
Issuer(Emisor)	
CommonName	ANCERT Certificados FERN
Organization	Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988
Locality	Paseo del General Martinez Campos 46-6a planta
State	Madrid
Country	ES

Valido desde	La fecha de emisión
Valido hasta	Tres años después de la emisión
Clave Pública	Octet String Contienindeo la clave pública del suscriptor
Extended Key Usage	TLS web client authentication (OID 1.3.6.1.5.5.7.3.2) E-mail protection (OID 1.3.6.1.5.5.7.3.4)
CRL Distribution Points	Distribution Point Name (uRI) “http://www.ancert.com/crl/ANCERTFERN.crl" “http://www2.ancert.com/crl/ ANCERTFERN.crl" “http://www3.ancert.com/crl/ ANCERTFERN.crl"
Certificate Policy Extensions	
PolicyIdentifier	1.3.6.1.4.1.18920.4.1.1.1
CPSuri	http://www.ancert.com/cps
Usernotice	Este certificado se expide como Certificado Reconocido de acuerdo con la legislacion vigente. La declaracion de practicas de certificacion y la politica de certificacion que rigen el funcionamiento de este certificado se encuentran disponibles en http://www.ancert.com
Key Usage	digital signature non-repudiation key encipherment data encipherment
Netscape Certificate Type	SSL client S/MIME client
Basic Contraints	Ca False Path Lengh Constraint 0
Authority Key Identifier	EC57 9FC8 7622 6FCC 3AAE 5BF0 2DA1 6258 D18D 02CC
Authority Information Access	
AccessMethod	1.3.6.1.5.5.7.48.1
accessLocation	uRI = http://ocsp.ac.ancert.com/ocsp.xuda
Algoritmo de firma	sha1RSA

4.6. Caducidad

Los *Certificados* emitidos por **ANCERT Certificados FERN** tendrán un periodo de validez de tres (3) años contados a partir del momento de la emisión del *Certificado*, sin perjuicio de que durante su vigencia concurra cualquier causa de extinción de las establecidas en la *Declaración de Prácticas de Certificación*.

Fuera de este periodo de validez los *Certificado*s se considerarán inválidos para cualquier tipo de operación cesando de esta manera los servicios de certificación ofrecidos por el *PSC*, siendo necesaria la emisión de uno nuevo en caso de que el *Suscriptor* desee seguir utilizando los servicios de **ANCERT Certificados FERN**. Ésta notificará al *Suscriptor*, mediante correo electrónico, la expiración de sus *Certificado*s

con una antelación de un mes. Tal notificación se realiza exclusivamente para la conveniencia del notificado en el proceso de obtención de un nuevo *Certificado*. Transcurrido este período el *Certificado* caducará.

El *Certificado* tendrá efectos frente a terceros de buena fe desde el momento de su publicación en el *Directorio de Certificados* de **ANCERT Certificados FERN**.

4.7. Extinción y suspensión

4.7.1 Revocación

Los **Certificados FEREN** son revocables. En cuanto a los sujetos que pueden solicitar la revocación, las causas y los efectos de la misma y el momento de producción de tales efectos, se estará a lo dispuesto en la *CPS* de ANCERT.

La solicitud de revocación de los **Certificados FEREN** se realizará:

- A solicitud de *la Autoridad de Registro*. Ésta podrá solicitar la revocación de los certificados emitidos según lo determinado en la CPS de ANCERT o bien,

- A instancia de **ANCERT Certificados FERN** la cual podrá proceder a la revocación del *Certificado* cuando por medio fehaciente haya tenido conocimiento cierto de la concurrencia con respecto al mismo de alguna de las causas de revocación enumeradas en la *CPS* de ANCERT.

En todos los casos, una vez revocado el *Certificado*, la revocación será publicada en el *Directorio de Certificados* de **ANCERT Certificados FERN,** produciendo desde ese mismo instante efectos respecto a terceros, e incluida en la *Lista de Certificados Revocados* en el plazo máximo previsto de veinticuatro (24) horas.

4.7.2 Suspensión

Los **Certificados FEREN** pueden ser suspendidos. En cuanto a los sujetos que pueden solicitar la suspensión, las causas y los efectos de la misma y el momento de producción de tales efectos, se estará a lo dispuesto en la *CPS* de ANCERT.

El procedimiento de suspensión de los **Certificados FEREN** será diferente en función del origen de la solicitud de revocación:

- A solicitud de *la Autoridad de Registro*. Ésta podrá solicitar la suspensión los certificados emitidos según lo determinado en la CPS de ANCERT o bien,

- **ANCERT Certificados FERN** podrá proceder a la suspensión del *Certificado* cuando por medio fehaciente haya tenido conocimiento cierto de la concurrencia con respecto al mismo de alguna de las causas de revocación enumeradas en la *CPS* de ANCERT.

En todos los casos, una vez suspendido el *Certificado*, la suspensión será publicada en el *Directorio de Certificados* de ANCERT, produciendo desde ese mismo instante

efectos respecto a terceros, e incluida en la *Lista de Certificados Revocados* en el plazo máximo previsto de veinticuatro (24) horas.

4.7.3 Levantamiento de la suspensión del *Certificado*

La *Autoridad de Registro* podrá proceder a la solicitud del levantamiento de la suspensión durante los sesenta (60) días siguientes a su suspensión en caso de que el *Certificado* haya sido suspendido por *la Autoridad de Registro*.

En el caso de que la suspensión haya provenido de **ANCERT Certificados FERN**, ésta únicamente podrá proceder a levantar la suspensión del *Certificado* cuando por medio fehaciente halla tenido conocimiento cierto de la desaparición de la causa que motivó la suspensión. En este caso, inmediatamente después procederá a eliminar el *Certificado* de la *Lista de Certificados Revocados*.

En todos los casos, una vez levantada la suspensión del *Certificado*, la misma será publicada en el acto en el *Directorio de Certificados* de ANCERT, produciendo desde ese mismo instante efectos respecto a terceros, e incluida en la *Lista de Certificados Revocados* en el plazo máximo previsto de veinticuatro (24) horas.

4.7.4 Procedimiento de Extinción

ANCERT Certificados FERN extinguirá el *Certificado,* además de los casos de revocación descritos, cuando por medio fehaciente haya tenido conocimiento cierto de la concurrencia con respecto al mismo de alguna de las restantes causas de extinción enumeradas en la *CPS* de ANCERT.

4.7.5 Efectos comunes de la extinción y suspensión

En los casos de extinción de *Certificados,* por causa de revocación o cualquier otra de las previstas en la *CPS* de ANCERT o en la Ley, o en los casos de suspensión, **ANCERT Certificados FERN** hará constar inmediatamente en el *Directorio de Certificados y* cada veinticuatro (24) horas en la *Lista de Revocación de Certificados,* exceptuando en este caso la caducidad del *Certificado*, la extinción o suspensión de la vigencia de los *Certificado*s electrónicos en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia.

El Suscriptor cuyo certificado haya sido suspendido o revocado debe ser informado de dicho hecho, así como, en su caso, del levantamiento de la suspensión, por lo que **ANCERT** notificará dicha información por correo electrónico o postal o incluso por teléfono cuando no haya sido posible la notificación en alguna de las dos formas anteriores.

No obstante lo dispuesto en el párrafo anterior, la notificación se entenderá debidamente cumplimentada cuando haya sido realizada por correo electrónica a la dirección que aparezca en el certificado y que, por tanto, habrá sido admitida previamente por el usuario del certificado.

Si no obstante el sistema produjera un mensaje de error o rechazara la comunicación, se entenderá que ANCERT ha cumplido suficientemente la notificación cuando ésta haya sido estampeada. A fin de justificar ulteriormente el cumplimiento de la debida diligencia, ANCERT conservará durante quince años el comprobante electrónico de haber realizado la comunicación de la revocación o suspensión.

La extinción o suspensión de la vigencia de un *Certificado* electrónico no tendrá efectos retroactivos.

La extinción o suspensión de la vigencia de un *Certificado* electrónico se mantendrá accesible en el directorio de *Listas de Certificados Revocados* al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

5 Obligaciones y responsabilidades

Sin perjuicio de las obligaciones y responsabilidades particulares establecidas en la presente *Política de Certificación*, los *Suscriptores*, *las Autoridades de Registro*, **ANCERT Certificados FERN,** los *Terceros de confianza*, y en general todas las partes participantes en la actividad de certificación de los **Certificados FEREN** deberán cumplir lo previsto en los puntos “6 OBLIGACIONES” y “7 RESPONSABILIDADES” de la *Declaración de Prácticas de Certificación*.