



---

Agencia Notarial  
de Certificación

**POLÍTICA DE CERTIFICACIÓN DE  
CERTIFICADOS CORPORATIVOS DE ACCESO  
PARA AYUNTAMIENTOS**

**Versión 3.0**  
**Fecha: 28/03/2013**

## Índice

<b>1</b>	<b>INTRODUCCION .....</b>	<b>3</b>
1.1.	PRESENTACIÓN .....	3
1.2.	IDENTIFICACIÓN .....	3
1.3.	DEFINICIONES .....	3
<b>2</b>	<b>DESCRIPCIÓN DEL CERTIFICADO .....</b>	<b>4</b>
2.1.	ÁMBITO DE APLICACIÓN.....	4
2.2.	TIPO DE CERTIFICADO .....	5
2.3.	USOS DEL CERTIFICADO.....	5
2.4.	USOS PROHIBIDOS .....	5
<b>3</b>	<b>IDENTIFICACION Y AUTENTICACION .....</b>	<b>5</b>
3.1.	NOMBRE DEL CERTIFICADO CORPORATIVO DE ACCESO .....	5
3.1.1	Nombre distintivo en el campo <i>Subject</i> del <i>Certificado</i> .....	5
3.1.2	Nombre del <i>Suscriptor</i> .....	5
3.2.	COMPROBACIÓN DE LA IDENTIDAD DE LOS SUSCRIPTORES .....	5
<b>4</b>	<b>CICLO DE VIDA DEL CERTIFICADO .....</b>	<b>6</b>
4.1.	SOLICITUD.....	6
4.2.	EMISIÓN .....	6
4.3.	COMPOSICIÓN DEL <i>CERTIFICADO</i> .....	6
4.3.1	Composición del nombre distintivo del <i>Subject</i> de Certificados Corporativos de Acceso para Ayuntamientos .....	6
4.3.2	Perfil del Certificado Corporativo de Acceso para Ayuntamientos .....	7
4.4.	CADUCIDAD .....	7
4.5.	EXTINCIÓN Y SUSPENSIÓN.....	8
4.5.1	Revocación .....	8
4.5.2	Suspensión.....	8
4.5.3	Procedimiento de Extinción.....	8
4.5.4	Efectos comunes de la extinción .....	8
<b>5</b>	<b>OBLIGACIONES Y RESPONSABILIDADES .....</b>	<b>9</b>
5.1.	OBLIGACIONES.....	9
5.1.1	Obligaciones de ANCERT Certificados Corporativos de Acceso .....	9
5.1.2	Obligaciones del Suscriptor.....	9
5.2.	RESPONSABILIDADES .....	9
5.2.1	Responsabilidades de ANCERT Certificados Corporativos de Acceso... ..	9
5.2.2	Responsabilidad del Suscriptor .....	10
<b>6.</b>	<b>PROPIEDAD INTELECTUAL E INDUSTRIAL.....</b>	<b>10</b>

# 1 INTRODUCCION

## 1.1. Presentación

El presente documento recoge la *Política de Certificación* de la Autoridad de Certificación **ANCERT Certificados Corporativos de Acceso** para los **Certificados Corporativos de Acceso para Ayuntamientos**. Esta *Política de Certificación* define su ámbito de aplicación, las características técnicas, el conjunto de reglas que regulan los procedimientos seguidos en la prestación de servicios de certificación, tales como el ciclo de vida de los *Certificados* y sus condiciones de uso.

**ANCERT Certificados Corporativos de Acceso** es la *Autoridad de Certificación* subordinada para quien la *Autoridad de Certificación* raíz **ANCERT Certificados Redes Privadas** ha expedido un *Certificado raíz* para, a su vez, poder emitir los *Certificados* electrónicos **Certificados Corporativos de Acceso para Ayuntamientos**. La *Autoridad de Certificación raíz ANCERT Certificados Redes Privadas* es una *Autoridad de Certificación* creada por la entidad **Agencia Notarial de Certificación, S.L.U.**

Los **Certificados Corporativos de Acceso para Ayuntamientos** se emiten a los *Ayuntamientos* del territorio español y, en determinados casos, también a las *entidades gestoras* designadas por ellos del *Impuesto sobre el Incremento de Valor de los Terrenos de naturaleza Urbana* (comúnmente llamado *Plusvalía*), a las cuales los *Ayuntamientos* hayan delegado la gestión de dicho Impuesto (en adelante las *entidades gestoras*). **ANCERT Certificados Corporativos de Acceso** registrará a los *Suscriptores* de los *Certificados*, actuando como Autoridad de Registro. Se utilizan archivos informáticos como único soporte de los *Certificados*.

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

DEB1 D24D EA75 2094 4DA3 DEFB 26C1 ABE0 45D0 FCE5

## 1.2. Identificación

*Política de Certificación* de **ANCERT Certificados Corporativos de Acceso** de los **Certificados Corporativos de Acceso para Ayuntamientos**:

- *OID*: 1.3.6.1.4.1.18920.2.3.1.1.

## 1.3. Definiciones

A los efectos de determinar el alcance de los conceptos que son utilizados en la presente *Política de Certificación*, deberá entenderse:

- *Autoridad de Certificación o Prestador de Servicios de Certificación*: es aquella persona física o jurídica que expide *Certificados electrónicos*, pudiendo prestar además otros servicios.
- *Autoridad de Registro*: entidad que realiza la comprobación de la identidad de los *Solicitantes y Suscriptores de Certificados*.
- *Certificado*: documento electrónico *firmado electrónicamente* por un *Prestador de Servicios de Certificación*. En la presente *Política de Certificación* cuando se haga referencia a *Certificado* se entenderá realizada al *Certificado* emitido por **ANCERT Certificados Corporativos de Acceso**.

- *Certificado raíz*: Certificado cuyo *Suscriptor* es una *Autoridad de Certificación* perteneciente a la jerarquía de la entidad Agencia Notarial de Certificación, S.L.U. como *Prestador de Servicios de Certificación*, y que contiene los Datos de verificación de Firma de dicha Autoridad firmado con los Datos de creación de Firma de la misma como *Prestador de Servicios de Certificación*.
- *Función hash*: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la *Función hash*.
- *Hash o Huella digital*: resultado de tamaño fijo que se obtiene tras aplicar una *función hash* a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.
- *Listas de Revocación de Certificados o Listas de Certificados Revocados*: lista donde figuran exclusivamente las relaciones de *Certificados* revocados (no los caducados).
- *Número de serie de Certificado*: valor entero y único que está asociado inequívocamente con un *Certificado* expedido por **ANCERT Certificados Corporativos de Acceso**.
- *OID (Object Identifier)*: valor, de naturaleza jerárquica y comprensivo de una secuencia de componentes variables aunque siempre constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que tienen la propiedad de ser únicos entre el resto de OID.
- *Política de Certificación*: documento que establece las condiciones de uso y los procedimientos seguidos por **ANCERT Certificados Corporativos de Acceso** para emitir *Certificados*.
- *SHA-1*: Secure Hash Algorithm (algoritmo seguro de resumen –hash-). Desarrollado por el NIST y revisado en 1994 (*SHA-1*). El algoritmo consiste en tomar mensajes de menos de 264 bits y generar un resumen de 160 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es prácticamente nula.
- *Solicitante*: persona/s física/s que en nombre de los *Ayuntamientos y entidades gestoras*, solicitan la emisión de un *Certificado*.
- *Suscriptor*: el titular del *Certificado*. El concepto de *Suscriptor*, será referido en los *Certificados* y en las aplicaciones informáticas relacionadas con su emisión como al *Ayuntamiento y entidades gestoras* en cuyo *Subject* aparece el NIF de dichos organismos.
- *X.500*: estándar desarrollado por la UIT que define las recomendaciones del directorio. Se corresponde con el estándar ISO/IEC 9594-1: 1993. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511, X.518, X.519, X.520, X.521 y X.525.

## 2 DESCRIPCIÓN DEL CERTIFICADO

### 2.1. Ámbito de aplicación

**ANCERT Certificados Corporativos de Acceso** expide los **Certificados Corporativos de Acceso para Ayuntamientos** a *Ayuntamiento* y, en su caso, *entidades gestoras* a los únicos efectos de acceder al portal de servicios para Ayuntamientos provisto por ANCERT.

Dicho *Índice de Plusvalías* está regulado en la Orden del Ministerio de Justicia 469/2003, de 19 de febrero, por la que se regula el Índice informatizado de los Notarios para dar cumplimiento a lo dispuesto en el artículo 7 del Real Decreto 1643/2000.

## 2.2. Tipo de Certificado

Los **Certificados Corporativos de Acceso para Ayuntamientos** son *Certificados electrónicos* no regulados por la Ley 59/2003, de Firma Electrónica. Son documentos firmados electrónicamente por un *Prestador de Servicios de Certificación*, que identifican al *Ayuntamiento o entidad gestora* frente a la aplicación de *Índice de Plusvalías* titularidad de la Agencia Notarial de Certificación S.L. Unipersonal.

Dicho *Certificado* electrónico no identifica al *Suscriptor* en ningún otro ámbito.

## 2.3. Usos del Certificado

Los **Certificados Corporativos de Acceso para Ayuntamientos** se utilizan exclusivamente para acceder al portal de servicios para Ayuntamientos provisto por ANCERT.

## 2.4. Usos prohibidos

No se permite usar los **Certificados Corporativos de Acceso para Ayuntamientos** para cualquier fin que no sea el enunciado en el punto 2.3.

# 3 IDENTIFICACION Y AUTENTICACION

## 3.1. Nombre del Certificado Corporativo de Acceso

En esta sección se establecen los nombres de los campos del *Certificado* que vinculan al *Ayuntamiento o entidad gestora* frente al portal de servicios para Ayuntamientos titularidad de la Agencia Notarial de Certificación S.L. Unipersonal.

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

Todos los **Certificados Corporativos de Acceso para Ayuntamientos** contienen un nombre distintivo X.500 en el campo *Subject*, que incluye los campos que se desarrollan en el punto 4.3.1 de esta *Política de Certificación*.

### 3.1.2 Nombre del *Suscriptor*

En los **Certificados Corporativos de Acceso para Ayuntamientos** el *Suscriptor* se identifica mediante el campo CN que contiene el NIF del *Ayuntamiento o entidad gestora*.

## 3.2. Comprobación de la identidad de los Suscriptores

El proceso de identificación y autenticación lo realizará **ANCERT Certificados Corporativos de Acceso**, la cual actuará como Autoridad de Registro según se dispone en el siguiente apartado.

## 4 CICLO DE VIDA DEL CERTIFICADO

### 4.1. Solicitud

El proceso para la obtención del *Certificado* consiste en lo siguiente:

1. El *Ayuntamiento o entidad gestora* deberá cumplimentar el formulario disponible en la sección *Solicitud del Certificado* de la página Web [www.ancert.com/ayuntamientos](http://www.ancert.com/ayuntamientos) y enviarlo telemáticamente mediante el botón disponible a pie del formulario.
2. Con el objetivo de certificar la veracidad de los datos proporcionados, el *Ayuntamiento o entidad gestora* debe imprimir en papel el formulario de *Solicitud del Certificado* cumplimentado, sellarlo con el sello del Ayuntamiento, firmarlo el Sr. Secretario con el visto bueno del Sr. Alcalde, y enviarlo por correo postal a **ANCERT Certificados Corporativos de Acceso**.

### 4.2. Emisión

Una vez **ANCERT Certificados Corporativos de Acceso** haya recibido el formulario debidamente firmado, se procederá del siguiente modo:

1. **ANCERT Certificados Corporativos de Acceso** enviará al *Ayuntamiento* y, en su caso, a la *entidad gestora*, un correo electrónico a la dirección de e-mail que se haya especificado en el formulario, adjuntando un enlace, el cual le llevará a la página Web donde podrá descargar el *Certificado* según los pasos siguientes.
2. Al mismo tiempo **ANCERT Certificados Corporativos de Acceso** les enviará por correo postal una carta acompañando el código secreto de instalación del *Certificado*.
3. Una vez recibidos los envíos referidos en los anteriores punto 1 y 2, el *Ayuntamiento* y, en su caso, la *entidad gestora*, accediendo al enlace referido en el punto 1, podrán, una vez descargado previamente, instalarse el *Certificado* utilizando el código secreto proporcionado.
4. Una vez instalado el *Certificado*, el *Ayuntamiento o entidad gestora* podrá acceder al portal de servicios para Ayuntamientos.

### 4.3. Composición del *Certificado*

#### 4.3.1 Composición del nombre distintivo del *Subject* de Certificados Corporativos de Acceso para Ayuntamientos

El nombre distintivo (DN) del *Certificado* conforme al estándar X.500, tendrá la siguiente composición:

CN	NIF del Ayuntamiento	
O	Organización	Acceso PV
C	País	ES

### 4.3.2 Perfil del Certificado Corporativo de Acceso para Ayuntamientos

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

CAMPO	VALOR
<b>Versión</b>	V3
<b>SerialNumber</b>	75F8 F232 195C 80CD 669F 64A8 20F2 65E6
<b>Issuer(Emisor)</b>	
CommonName	ANCERT Certificados Corporativos de Acceso
Organization	Agencia Notarial de Certificación S.L. Unipersonal - CIF B83395988
Locality	Paseo del General Martínez Campos 46-6a planta
State	Madrid
Country	ES
<b>Valido desde</b>	La fecha de emisión
<b>Valido hasta</b>	Tres años después de la emisión
<b>Clave Pública</b>	Octet String Contiene la clave pública del suscriptor
<b>Extended Key Usage</b>	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)
<b>CRL Distribution Points</b>	Distribution Point Name (uRI) "http://www.ancert.com/crl/ANCERTCCA.crl" "http://www2.ancert.com/crl/ANCERTCCA.crl" "http://www3.ancert.com/crl/ANCERTCCA.crl"
<b>Certificate Policy Extensions</b>	
PolicyIdentifier	1.3.6.1.4.1.18920.2.3.1.1
CPSuri	<a href="http://www.ancert.com/cps">http://www.ancert.com/cps</a>
Usernotice	Agencia Notarial de Certificación. La declaración de prácticas de certificación que rige el funcionamiento de la presente autoridad se encuentra disponible en <a href="http://www.ancert.com/cps">http://www.ancert.com/cps</a>
<b>Key Usage</b>	digital signature non-repudiation key encipherment data encipherment
<b>Netscape Certificate Type</b>	SSL client S/MIME client
<b>Basic Constraints</b>	Ca False Path Length Constraint 0
<b>Authority Key Identifier (Numero de Serie)</b>	D9B9 F4A2 6125 B9F3 427D E9CD CEC3 85AD 2641 4BC9
<b>Authority Information Access</b>	
AccessMethod	1.3.6.1.5.5.7.48.1
accessLocation	uRI = <a href="http://ocsp.ac.ancert.com/ocsp.xuda">http://ocsp.ac.ancert.com/ocsp.xuda</a>
<b>Algoritmo de firma</b>	sha1RSA

### 4.4. Caducidad

Los *Certificados* emitidos por **ANCERT Certificados Corporativos de Acceso** tendrán un periodo de validez de tres (3) años contados a partir del momento de la emisión del *Certificado*.

Fuera de este periodo de validez los *Certificados* se considerarán inválidos para cualquier tipo de operación cesando de esta manera los servicios de certificación ofrecidos por el *Prestador de Servicios de Certificación*, siendo necesaria la emisión de uno nuevo en caso de que el *Suscriptor* desee seguir utilizando los servicios de **ANCERT Certificados Corporativos de Acceso**.

## 4.5. Extinción y suspensión

### 4.5.1 Revocación

Los **Certificados Corporativos de Acceso para Ayuntamientos** 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 a continuación.

La solicitud de revocación de los **Certificados Corporativos de Acceso para Ayuntamientos** se realizará:

- A instancia del *Ayuntamiento o entidad gestora*. Ésta podrá solicitar la revocación de los certificados emitidos, solicitándolo mediante la remisión de una carta por correo postal firmada por el Sr. Secretario con el visto bueno del Sr. Alcalde.
- A instancia de **ANCERT Certificados Corporativos de Acceso**, en caso de que tenga conocimiento cierto de que concurre algún supuesto de uso ilegítimo del *Certificado* o contrario a lo que se especifica en esta *Política de Certificación*.

### 4.5.2 Suspensión

No se contempla la suspensión en este tipo de *Certificados*.

### 4.5.3 Procedimiento de Extinción

**ANCERT Certificados Corporativos de Acceso** extinguirá el *Certificado*, además de los casos que prevea la Ley, cuando por medio fehaciente haya tenido conocimiento cierto de la concurrencia con respecto al mismo de alguna de las restantes causas de revocación anteriormente enumeradas.

### 4.5.4 Efectos comunes de la extinción

En los casos de extinción de *Certificados*, por causa de revocación o cualquier otra legal, **ANCERT Certificados Corporativos de Acceso** hará constar en la *Lista de Revocación de Certificados* correspondiente la extinción de la vigencia de los *Certificados*, exceptuando en este caso la caducidad del *Certificado*, en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción de su vigencia.

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

La extinción de la vigencia de un *Certificado* electrónico se mantendrá accesible en el la *Lista de Revocación de Certificados* al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

## 5 Obligaciones y responsabilidades

### 5.1. Obligaciones

#### 5.1.1 Obligaciones de ANCERT Certificados Corporativos de Acceso

ANCERT Certificados Corporativos de Acceso se obliga a:

1. Cumplir todas aquellas obligaciones impuestas por la presente *Política de Certificación*.
2. Cumplir todas las previsiones de la normativa sobre protección de datos de carácter personal.
3. Emitir los *Certificados* solicitados ajustándose a las normas y procedimientos establecidos en la presente *Política de Certificación*.

#### 5.1.2 Obligaciones del Suscriptor

Son obligaciones del *Suscriptor*:

1. Solicitar y recibir el *Certificado* siguiendo los procedimientos descritos en la presente *Política de Certificación*.
2. Mantener el compromiso para todo el periodo de vigencia del *Certificado*, de que toda la información contenida en el *Certificado* es cierta y se compromete a notificar cualquier modificación, actualización o inexactitud de la misma.
3. Utilizar el *Certificado* exclusivamente dentro de los límites especificados en el momento de su concesión.
4. No utilizar el *Certificado* desde el momento que solicita su revocación o fuera del periodo de validez.
5. Proteger y custodiar de forma diligente el *Certificado*, las claves, el soporte de las mismas, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.
6. Notificar a **ANCERT Certificados Corporativos de Acceso** la pérdida o divulgación de la *Clave Privada*, o cualquier situación que pueda afectar a la validez del *Certificado*, o su confidencialidad, solicitando su revocación en forma inmediata.
7. Conocer y cumplir con todas aquellas obligaciones impuestas en esta *Política de Certificación*.
8. No reproducir, comunicar, distribuir o transformar el *Certificado* y la clave privada correspondiente.

### 5.2. Responsabilidades

#### 5.2.1 Responsabilidades de ANCERT Certificados Corporativos de Acceso

ANCERT Certificados Corporativos de Acceso responderá en el caso de incumplimiento de todas aquellas obligaciones impuestas por la presente *Política de Certificación* y la normativa existente en materia de prestación de servicios de certificación, excepto respecto de los daños y perjuicios causados por las siguientes causas:

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 *Suscriptor*, o por el uso incorrecto de los soportes que contienen los *Certificados* y las claves.

4. Caso fortuito o fuerza mayor tales como los desastres naturales, la guerra, los cortes en el suministro electrónico o en el funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el *Suscriptor*.

### 5.2.2 Responsabilidad del Suscriptor

El *Suscriptor*, sean los Ayuntamientos o las *entidades gestoras*, deberá cumplir íntegramente lo previsto en la presente *Política de Certificación*, eximiendo de cualquier responsabilidad al *Prestador de Servicios de Certificación ANCERT Certificados Corporativos de Acceso* en caso del incumplimiento de la misma, y en concreto, en los supuestos de que el *Certificado* no sea utilizado exclusivamente para el uso indicado en el punto 2.3, siendo, en dichos casos, exclusivamente el *Suscriptor* el responsable de cualquier daño o perjuicio ocasionado por dicho uso no permitido.

## 6. Propiedad Intelectual e Industrial

**ANCERT Certificados Corporativos de Acceso** es titular en exclusiva de todos los derechos, incluidos los derechos de explotación, sobre la Lista de Revocación 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 a la Lista de Revocación de Certificados estando prohibida la reproducción, comunicación pública, distribución, transformación o reordenación salvo cuando esté expresamente autorizada por ANCERT o por la Ley.

Asimismo, **ANCERT Certificados Corporativos de Acceso** es titular de todos los mismos derechos de propiedad intelectual e industrial respecto a la presente Declaración de Prácticas de Certificación, de las claves criptográficas, de los Certificados Electrónicos y de 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 ANCERT 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>

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 **ANCERT Certificados Corporativos de Acceso** pone a disposición de los Suscriptores de Certificados.