Servicio Público de Empleo Estatal

CERTIFICADOS DE CIUDADANO

POLÍTICAS DE CERTIFICACIÓN

OID: 1.3.6.1.4.1.27781.1.2.1.1.2

Versión 1.0

Fecha: 16 de Noviembre de 2011

Índice

Capítulo 1. Introducción

1.1. Objeto

El presente documento recoge la Política de Certificación de la Autoridad de Certificación del Servicio Público de Empleo Estatal (SEPE), que define los mecanismos y procedimientos para la emisión, gestión, revocación, renovación y cualquier otro proceso que afecte al ciclo de vida de los certificados electrónicos de ciudadano y sus claves de firma asociadas.

Esta Política de Certificación se ha estructurado conforme a la normativa RFC-3647 *"Internet X.509 Public Key infrastructure Certificate Policy and Certification Practices Framework*". Cuando no se haya previsto nada en alguna sección aparecerá la frase "No Estipulado" o "No Aplica".

En cuanto al marco legislativo, se han seguido estas normativas:

- Ley 59/2003, de 19 de Diciembre, de Firma Electrónica.
- Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Real Decreto 1671/2009, de 6 de Noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Real Decreto 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.

1.2. Nombre e Identificación del documento

Nombre del documento	SEPE. Certificados de Ciudadano. Política de Certificación

Versión del documento	1.0
Estado del documento	Aprobado
Fecha de emisión	16/11/2011
OID (Object Identifier)	1.3.6.1.4.1.27781.1.2.1.1.2
Ubicación de la DPC	http://sede.sepe.gob.es/dpc

1.3. Participantes

1.3.1. Autoridad de Certificación

La AC del SEPE proporciona servicios de expedición y gestión de certificados a aquellos ciudadanos que necesiten realizar trámites que requieran el uso de firma electrónica y estén disponibles en la Sede Electrónica del SEPE.

En la Sede Electrónica, se publicará una relación actualizada de los trámites que hacen uso de estos certificados.

1.3.2. Autoridades de Registro

Actuarán como entidades de registro las Oficinas del SEPE, que verifican los datos del ciudadano en el momento de su alta en los Sistemas de Información del SEPE.

1.3.3. Suscriptores

Los suscriptores son los ciudadanos que obtienen y utilizan los certificados y claves emitidos por la AC del SEPE, para la realización de los trámites de la Sede Electrónica que requieren firma digital.

1.4. Uso de los certificados de ciudadano

Un certificado de ciudadano emitido por la AC del SEPE sólo puede ser utilizado para los propósitos explícitamente permitidos e indicados en esta Política de Certificación.

1.4.1. Usos apropiados de los certificados de ciudadano

Los certificados de ciudadano emitidos por la AC del SEPE se utilizarán para firmar electrónicamente trámites o documentos, cuyo ámbito de aplicación es el Servicio Público de Empleo Estatal.

1.4.2. Usos no permitidos de los certificados de ciudadano

Los certificados de ciudadano no podrán ser utilizados para propósitos diferentes a los indicados en esta política de certificación.

En particular, dichos certificados y sus claves asociadas no podrán utilizarse para cifrar ningún tipo de información, ni para realizar ningún tipo de autenticación, ya sea en la Sede Electrónica del SEPE o de otros organismos.

1.5. Política de administración de la Política de Certificación

El SEPE se reserva el derecho de hacer revisiones y actualizaciones de esta Política de Certificación si así lo estimase oportuno, y es el único organismo autorizado para hacer dichas modificaciones y publicarlas en el portal del SEPE.

1.5.1. Organización que administra la política de certificación

Nombre	Servicio Público de Empleo Estatal		
Dirección e-mail			
Dirección	C/ Condesa de Venadito 9 28027 - Madrid España		
Teléfono		**Fax**	

1.5.2. Procedimientos de aprobación de la política de certificación

La Subdirección General de Tecnología de la Información y Comunicaciones del SEPE acordará por unanimidad las modificaciones de esta Política de Certificación.

1.5.3. Actualizaciones de la política de certificación

Tras la aprobación de las modificaciones en la Política de Certificación de los certificados de ciudadano, el SEPE publicará la misma en la dirección **http://sede.sepe.gob.es/dpc**, reemplazando la Política de Certificación vigente en ese momento.

Capítulo 2. Identificación y Autenticación

En esta sección se establecen requisitos relativos a los procedimientos de identificación y autenticación que se utilizan durante el registro de los suscriptores, que tiene que realizarse con anterioridad a la emisión y entrega de certificados.

2.1.1. Tipos de Nombres

Los certificados emitidos por la AC del SEPE contienen el nombre distintivo del emisor y el destinatario del certificado en los campos “Issuer Name” y “Subject Name” respectivamente.

El nombre distintivo del “Issuer Name” contiene los siguientes campos:

- OU = AC SPEE
- O = SPEE
- C = ES

Para los certificados de ciudadano, en el nombre distintivo del “Subject Name” se incluyen los siguientes campos:

- CN = <Nombre> <Apellido1> <Apellido2>
- G = <Nombre>
- SERIALNUMBER = <DNI> ó <NIE>
- SN = <Apellido1>
- OU = AC SPEE
- O = SPEE
- C = ES

2.1.2. Necesidades de nombres significativos

Las normas seguidas por esta Política de Certificación garantizan que los nombres distintivos (DN) de los certificados son significativos para asociar de forma inequívoca la clave pública con una identidad única.

2.1.3. Anonimato o alias de los titulares

No aplica.

2.2. Autenticación inicial de la identidad

2.2.1. Métodos de prueba de la posesión de la clave privada

La generación del par de claves de ciudadano se realiza mediante la autenticación e identificación del mismo, cuando accede a un trámite de Sede Electrónica que requiere firma digital. Para ello el ciudadano utiliza una contraseña de acceso que solamente él conoce. De esta forma, se garantiza en todo momento que solamente el usuario autenticado e identificado por el sistema tiene acceso a la generación de su clave privada de firma para la realización de los trámites disponibles en Sede Electrónica.

2.2.2. Autenticación de la identidad de ciudadano

Para que a un ciudadano se le pueda emitir un certificado de firma debe cumplir los siguientes requisitos:

- Debe estar dado de alta en los Sistemas de Información del SEPE:
    - El ciudadano ya existe en los Sistemas de Información del SEPE, y solicita las credenciales de acceso a la Sede Electrónica del SEPE., verificándose previamente su identidad.
    - La solicitud de las credenciales de acceso puede hacerse presencialmente en una oficina del SEPE o bien de forma telemática a través de la propia Sede Electrónica y usando un certificado digital reconocido.
- En los Sistemas de Información deben constar, entre otros, los siguientes datos del usuario:
    - Nombre
    - Apellidos

- NIF
- País
- Provincia
- Código Postal
- Dirección
- Número de teléfono móvil (sin este dato el ciudadano no puede acceder a los servicios de firma digital del SEPE, ya que para realizar el proceso de firma se utiliza un segundo factor de autenticación basado en un pin de un solo uso que se envía al móvil del ciudadano vía SMS). Este dato sólo puede ser dado de alta y modificado en oficinas del SEPE.

- Una vez que el usuario pueda acceder al portal de Sede Electrónica, cuando el usuario vaya a realizar un trámite que requiera firma digital se le creará su certificado digital.

Tanto si el ciudadano se da de alta por primera vez en una Oficina del SEPE, como por el procedimiento de registro con certificado reconocido, se ha realizado previamente una identificación completa del mismo, mediante la verificación de los datos personales en documentos oficiales (DNI, NIE, DNIe, certificado FNMT, etc.).

2.3. Identificación y autenticación en las peticiones de renovación de claves y certificados

2.3.1. Identificación y autenticación

En el caso de una renovación de claves de firma y certificados, el ciudadano ya estaba dado de alta en los Sistemas de Información del SEPE, por tanto, no es necesario que realice ninguna tarea adicional de identificación/autenticación, salvo la entrada en el portal de Sede Electrónica con su usuario telemático y el acceso a un trámite de que requiera firma digital.

2.4. Identificación y autenticación para las peticiones de revocación de certificados

La revocación de los certificados de ciudadano vendrá indicada como una baja de la información del usuario en la AC del SEPE.

Para realizar una solicitud de baja, el ciudadano utilizará los medios a su disposición indicados en la Sede Electrónica del SEPE (formulario Contacte), introduciendo sus datos personales y el motivo de la baja de sus certificados.

Capítulo 3. Requisitos del ciclo de vida de los certificados

3.1. Solicitud de los certificados

3.1.1. Quién puede realizar una petición de certificado

Los ciudadanos que requieran realizar trámites de en la Sede Electrónica del SEPE, y que cumplan los siguientes requisitos:

- Debe estar dado de alta en los Sistemas de Información del SEPE.
- En los Sistemas de Información del SEPE deben constar, entre otros, los siguientes datos del usuario:
    - Nombre
    - Apellidos
    - NIF
    - País
    - Provincia
    - Código Postal
    - Dirección
    - Número de teléfono móvil (sin este dato el ciudadano no puede acceder a los servicios de firma digital del SEPE, ya que para realizar el proceso de firma se utiliza un segundo factor de autenticación basado en un pin de un solo uso que se envía al móvil del ciudadano vía SMS). Este dato sólo puede ser dado de alta y modificado en oficinas del SEPE.

- Una vez que el usuario pueda acceder al portal de Sede Electrónica, ya sea porque se le ha creado un usuario en una Oficina del SEPE o por una alta telemática, el usuario tiene que realizar un trámite que requiere firma digital.

3.1.2. Registro de las solicitudes de certificados

La AC del SEPE garantiza que los datos presentes en los certificados son exactos y completos y que las solicitudes quedan registradas en los archivos de auditoría de la Autoridad de Certificación.

3.2. Tramitación de solicitud de certificados

Una vez que el ciudadano acceda por primera vez a un trámite que requiera firma digital, se le mostrarán las Condiciones de Uso de los Certificados y si las acepta o no.

Si el usuario acepta las condiciones de uso, se le solicitará su contraseña de usuario de acceso a la Sede Electrónica.

En caso se autentique correctamente con su contraseña de acceso, se le enviará la petición de certificados a la AC del SEPE, que recopilará toda la información existente del usuario de los Sistemas de Información del SEPE, y procederá a generar una par de claves de firma y su certificado correspondiente.

3.2.1. Aprobación o denegación de la solicitud de certificados

Cuando al ciudadano se le muestran las Condiciones de Uso de los Certificados, se le ofrece la opción de aceptarlas o rechazarlas.

En caso de marcar la casilla “He leído y acepto las condiciones” y pulsar el botón “Continuar” se considera que el ciudadano acepta las condiciones y da su conformidad para que se generen sus claves y certificados en la AC del SEPE.

En caso de pulsar el botón “Cancelar” se considera que el ciudadano rechaza las condiciones y no desea que se generen sus claves y certificados en la AC del SEPE. En este caso se cierra la pantalla del trámite y se devuelve al usuario al Portal de la Sede Electrónica.

3.2.2. Plazo para procesar la solicitud de certificado

Una vez que el ciudadano acepta las condiciones de uso de los certificados e introduce su contraseña, la AC procesa inmediatamente la solicitud de emisión de certificados.

3.3. Emisión de certificados

3.3.1. Procedimiento para la emisión del certificado

La emisión del certificado tiene lugar una vez que la Autoridad de Certificación ha llevado a cabo las comprobaciones necesarias para validar la solicitud de certificación.

Los certificados se emiten automáticamente al recibir una solicitud válida, y una vez que el usuario ha dado su consentimiento mediante la aceptación de las condiciones de uso de los certificados.

3.3.2. Notificación al solicitante de la emisión por la AC del certificado

Cuando el ciudadano realiza por primera vez un trámite que requiera firma digital en la Sede Electrónica, y se autentica con su contraseña de usuario se le informa que se le van a generar los certificados y claves y que debe aceptar las Condiciones de Uso de los mismos.

3.4. Aceptación del certificado

3.4.1. Procedimientos para la aceptación del certificado

En el momento de la creación de sus certificados, el ciudadano es redirigido a la ventana “Creación de nuevo certificado”. En este momento el ciudadano marcará la casilla “He leído y acepto las condiciones” y pulsará el botón “Continuar”.

A continuación se mostrará una nueva ventana que solicita al usuario la introducción de su contraseña de acceso a la Sede Electrónica. La autenticación por medio de esta contraseña es el último paso antes de la generación de los certificados y claves.

3.4.2. Publicación del certificado

No estipulado.

3.4.3. Notificación de la emisión del certificado por la AC a otras Autoridades

No estipulado.

3.5. Par de claves y uso del certificado

3.5.1. Uso del certificado y de la clave privada por el titular

Los certificados solamente podrán ser utilizados para los usos descritos en la presente DPC y en la correspondiente Política de Certificación.

Tras la extinción de la vigencia o la revocación del certificado, el titular deberá dejar de usar la clave privada asociada, y los correspondientes certificados.

El uso principal de las claves privadas generadas para los ciudadanos es la firma digital de los trámites habilitados y disponibles en la Sede Electrónica del SEPE.

3.5.2. Uso del certificado y de la clave pública por los terceros aceptantes

No estipulado.

3.6. Renovación de certificados sin cambio de claves

En el ámbito de la AC del SEPE no se realizará renovación de certificados sin cambio de claves.

3.7. Renovación de certificados con cambio de clave

3.7.1. Motivos para la renovación con cambio de claves de un certificado

La renovación de certificados de ciudadanos con cambio de claves puede producirse por los siguientes motivos:

- Se ha alcanzado la fecha de caducidad de la clave privada de firma del ciudadano.

- Se ha alcanzado la fecha de caducidad del certificado del ciudadano.
- El usuario realiza un cambio de su contraseña en la Sede Electrónica del SEPE.
- El usuario requiere un cambio de datos en su certificado:
    - Nombre
    - Primer apellido
    - Segundo apellido
    - Orden de posición de los apellidos
    - Número de DNI ó NIE

3.7.2. Quién puede solicitar la renovación de un certificado

La renovación de las claves y certificados es automática, el ciudadano no realiza ninguna solicitud.

La AC del SEPE detectará automáticamente cualquiera de las condiciones especificadas en el punto 3.7.1, y procederá a la renovación automática de las claves y certificados cuando el usuario acceda a un trámite que requiera firma digital.

3.7.3. Tratamiento de la solicitud de renovación del certificado

En cualquier caso la renovación se realizará de forma automática y transparente para el ciudadano, en el momento en que el usuario acceda a realizar un trámite que requiere firma digital, y se autentique a su clave privada mediante la contraseña de acceso.

En este momento, si el sistema detecta alguna de las condiciones anteriores, se procederá, de forma transparente para el usuario, a realizar una renovación de sus claves y certificados.

3.7.4. Notificación de la emisión del nuevo certificado al titular

En caso de renovación por cambio de contraseña o datos del certificado, se le mostrará al ciudadano las condiciones de acceso, en casos de expiración de certificados y claves, el ciudadano no recibirá ninguna notificación.

3.8. Modificación de certificados

En el ámbito de la AC del SEPE no se permite la modificación de certificados de ciudadanos ya emitidos.

En caso de requerir cualquier modificación en un certificado de ciudadano ya emitido, se realizará una renovación de certificado con cambio de claves, en un proceso automático y totalmente transparente para el usuario.

3.9. Revocación y suspensión de certificados

La revocación de un certificado supone la pérdida de validez del mismo, y es irreversible.

La suspensión, en cambio, supone la pérdida de validez temporal de un certificado, y es reversible.

3.9.1. Causas de revocación de certificados

La revocación de los certificados y claves privadas de un ciudadano vendrá determinada cuando éste quiera darse de baja del portal de Sede Electrónica.

3.9.2. ¿Quién puede presentar la solicitud de revocación?

Cualquier ciudadano que haya realizado trámites en la Sede Electrónica, y que se le hayan generado claves y certificados para la firma digital de estos trámites.

3.9.3. Procedimiento de solicitud de revocación

El ciudadano que requiera la revocación de sus certificados solicitará una baja de sus datos mediante una solicitud al buzón CONTACTA

(**https://sede.sepe.gob.es/es/redtrabaja/contacte/contacteInternet.do**) de la Sede Electrónica del SEPE, indicando sus datos personales, y el motivo de la baja.

Una vez recibida la solicitud de baja, un administrador de la AC del SEPE procederá manualmente a dar de baja al usuario en la AC, realizando las siguientes tareas:

1º Búsqueda del usuario en la AC.

2º Revocación de todos los certificados del usuario.

3º Desactivación de los datos del usuario en la AC.

4º Eliminación de los datos del usuario en el repositorio de la AC.

3.9.4. Efectos de la revocación

El ciudadano titular del certificado revocado dejará de poder realizar trámites que requieran firma digital.

3.9.5. Plazo para la tramitación de la solicitud de revocación

La solicitud de revocación será tratada por los responsables de la AC del SEPE tan pronto como sea posible.

3.9.6. Requisitos especiales de revocación de clave comprometida

En caso de compromiso de la clave privada de un ciudadano, se procederá a su revocación inmediata y posterior desactivación en la AC del SEPE.

3.9.7. Causas de suspensión

En el ámbito de la Autoridad de Certificación del SEPE, no se contempla la suspensión (revocación temporal) de certificados de ciudadano. En todos los casos en los que sea necesario revocar un certificado, éste se revocará de forma permanente.

3.10. Servicio externo de consulta del estado del certificado

En SEPE no existe un servicio externo de validación de certificados.

Cada vez que un ciudadano accede a sus certificados, éstos son validados internamente por la aplicación que haga uso de los mismos.

3.11. Fin de la suscripción

La suscripción de un certificado de ciudadano expedido por la AC del SEPE puede finalizar en los siguientes casos:

- Revocación del certificado y de la correspondiente clave privada de firma (baja).
- Expiración del certificado.

3.12. Retención y recuperación de las claves

3.12.1. Políticas y prácticas de recuperación de claves

En el ámbito de la AC del SEPE no se realiza retención y recuperación de las claves privadas de firma de los ciudadanos.

3.12.2. Políticas y prácticas de encapsulamiento y recuperación de claves de sesión.

No estipulado.

Capítulo 4. Controles Técnicos de Seguridad

4.1. Generación e instalación del par de claves

4.1.1. Generación del par de claves

La generación de las claves del ciudadano se llevará a cabo de forma automática en la AC del SEPE, y el acceso a estas credenciales quedará protegido por la infraestructura y por la contraseña del ciudadano cuando éste realiza en la Sede Electrónica un trámite que requiera firma digital. Además, se utilizará un segundo factor de autenticación que consiste en una contraseña de un solo uso que se envía al usuario mediante un mensaje SMS al teléfono móvil registrado en los Sistemas de Información del SEPE.

4.1.2. Entrega de la clave privada al titular

El envío de la clave privada de firma se efectúa cuando el ciudadano realiza un trámite que requiera firma digital, y previa autenticación del mismo mediante los dos factores de autenticación (contraseña de acceso y contraseña de un solo uso enviado a su teléfono móvil).

4.1.3. Entrega de la clave pública al titular

Se siguen los mismos puntos que en el apartado anterior.

4.1.4. Longitud de las claves de ciudadano

La longitud de las claves de ciudadanos es de 1024 bits.

4.1.5. Parámetros de generación de la clave pública y verificación de la calidad

Los parámetros de clave pública son generados conforme a la norma PKCS#1. El algoritmo usado para la generación de las claves es RSA.

4.1.6. Usos admitidos de la clave (campo KeyUsage de X.509 v3)

La extensión "*keyUsage*" de los certificados indica el uso para el que deben ser utilizados según se recomienda en la norma RFC-3280, y debe establecerse como extensión crítica.

4.2. Protección de la clave privada

El acceso a las claves del ciudadano quedará protegido por la infraestructura y por la contraseña del ciudadano cuando éste realiza en la Sede Electrónica un trámite que requiera firma digital. Además, se utilizará un segundo factor de autenticación que consiste en una contraseña de un solo uso que se envía al usuario mediante un mensaje SMS al teléfono móvil del usuario, según figure en las bases de datos del SEPE. Este teléfono sólo puede modificarse presencialmente en las oficinas del SEPE.

4.2.1. Copia de seguridad y archivado de la clave privada

No se realizará copia de seguridad ni archivado de la clave privada de firma del ciudadano.

4.2.2. Método de activación de la clave privada

La activación de la clave privada de firma del ciudadano se produce cuando éste se autentica mediante la introducción de su contraseña de acceso a un trámite que requiera firma.

4.2.3. Método de desactivación de la clave privada

La desactivación de la clave privada de firma del ciudadano se produce cuando se completa el proceso de firma digital en el trámite. Esta eventualidad se le indica al usuario con el siguiente mensaje, después de completar dicho trámite: “El proceso de firma ha finalizado correctamente, por favor, espere a que se cierre la ventana”. Tras este proceso las claves desaparecen del equipo del usuario hasta que sea necesario su nuevo uso.

4.2.4. Proceso para la destrucción de la clave privada

La destrucción definitiva de la clave privada de firma de un ciudadano se produce cuando se le da de baja en la AC del SEPE. Este proceso de baja implica la revocación de los certificados del usuario, la desactivación de los mismos, y el borrado de los datos relativos al usuario en la AC.

4.3. Otros aspectos de la gestión de claves

4.3.1. Archivo de la clave pública

La AC del SEPE archiva las claves públicas y certificados del ciudadano, de acuerdo con lo establecido en este documento y en la Declaración de Prácticas de Certificación.

4.3.2. Periodos de validez del certificado y las claves

El periodo de utilización de las claves está determinado por el periodo de validez del certificado de modo que después de la expiración del certificado, las claves no podrán utilizarse, produciéndose el cese permanente de su funcionamiento para el uso para el que fueron generadas.

El tiempo de vida de la clave privada de firma y de los certificados de ciudadanos está estipulado en 3 años.

4.4. Datos de activación

4.4.1. Generación e instalación de los datos de activación

La contraseña de acceso a la clave privada de firma del ciudadano se genera cuando el usuario realiza por primera vez un trámite de Sede Electrónica que requiera firma digital.

La contraseña de un solo uso que el ciudadano recibe en su teléfono móvil se genera dinámicamente después de que el ciudadano se haya autenticado con su contraseña, y se destruye una vez que el ciudadano ha completado el proceso de firma digital.

4.4.2. Protección de los datos de activación

En el caso de la clave de firma de ciudadano, sólo éste conoce la contraseña de acceso a su clave privada, siendo por tanto el único responsable de la protección de los datos de activación de sus claves privadas.

La contraseña de acceso es confidencial, personal e intransferible y es el parámetro que protege las claves privadas permitiendo la utilización de los certificados en los servicios ofrecidos a través de una red de comunicaciones; por lo tanto, deben tenerse en cuenta unas normas de seguridad para su custodia y uso:

- Memorizar la contraseña y no anotarla en ningún documento físico ni electrónico que el titular conserve o transporte.
- No enviar ni comunicar la contraseña a nadie ni por ningún medio, ya sea vía telefónica, correo electrónico, etc.
- Es obligación del titular notificar la pérdida de control sobre su clave privada, a causa del compromiso de la contraseña, ya que es motivo de revocación del certificado asociado a dichas claves.
- Evitar escoger una contraseña relacionada con sus datos personales, así como cualquier otro código que pueda resultar fácilmente predecible por terceras personas (fecha de nacimiento, teléfono, series de números consecutivos, repeticiones de la misma cifra, secuencias de cifras que ya forman parte de su número de DNI, etc.).
- Se recomienda cambiar la contraseña de acceso periódicamente.

En el caso de la contraseña de un solo uso, ésta es enviada exclusivamente al teléfono móvil del ciudadano previamente autenticado, y solamente es válida para el trámite que el usuario está realizando en ese momento durante un periodo limitado de tiempo. La modificación del número de teléfono móvil asociado se ha de realizar presencialmente en una oficina del SEPE.

Capítulo 5. Perfil de los certificados

5.1. Perfil del certificado de ciudadano

El perfil y características de los certificados de ciudadano emitidos por la AC del SEPE sigue las especificaciones recogidas en la normativa "*RFC-3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002*".

5.1.1. Número de versión

Los certificados de identidad pública emitidos por la AC del SEPE utilizan el estándar X.509 versión 3 (X.509 v3).

5.1.2. Extensiones del certificado

Los campos y extensiones definidos en los certificados de ciudadano emitidos por la AC del SEPE son los siguientes:

5.1.2.1. Certificado de Ciudadano (Firma)

Nombre atributo	Valor	Tipo
Versión	V3	Campo v1
Número de serie	Secuencial	Campo v1
Algoritmo de firma	SHA1withRSAEncryption	Campo v1
Emisor	OU=AC SPEE, O=SPEE, C=ES	Campo v1
Validez	3 Años	Campo v1
Asunto	CN = <Nombre> <Apellido1> <Apellido2> G = <Nombre> SERIALNUMBER = NIF SN = <Apellido1>	Campo v1

	OU = AC SPEE O = SPEE C = ES	
Chave pública	RSA 1024 Bits	Campo v1
Uso de la clave	Firma digital	Extensión
Período de uso de la clave privada	3 años	Extensión
Bases del certificado	ID Directiva= 1.3.6.1.4.1.27781.1.2.1.1.1 ID de calificador de Directiva= CPS Calificador= http://www.redtrabaja.es/dpc	Extensión
Puntos de distribución de CRL	CN=CRLxx, OU=AC SPEE, O=SPEE, C=ES *(Donde xx es un número decimal consecutivo, comenzando por 01)*	Extensión
Authority Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora.	Extensión
Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto	Extensión
Restricciones básicas	Entidad Final	Extensión
Algoritmo de identificación	sha1	Extensión
1.2.840.113533.7.65.0	v7.1	Extensión
Firma Digital	No disponible	Extensión

5.1.3. Restricción de nombres

El nombre distintivo (DN) para los certificados de ciudadano es único y no ambiguo.

5.1.4. Identificador del objeto (OID) de la política de certificación

El SEPE dispone de un identificador único a partir del cual generar sus propios OIDs. Este identificador es 1.3.6.1.4.1.27781.

En esta extensión se ha cargado el OID asociado a la DPC del SEPE, el OID es 1.3.6.1.4.1.27781.1.2.1.1.1.

5.1.5. Utilización de la extensión "Policy Constraints"

Esta extensión contiene los siguientes elementos:

- OID de la DPC del SEPE:
    - 1.3.6.1.4.1.27781.1.2.1.1.2
- URL donde se publicará la DPC y la política de certificación de ciudadanos de la AC del SEPE:
    - http://www.redtrabaja.es/dpc

Capítulo 6. Requisitos comerciales y legales

6.1. Obligaciones y responsabilidad civil

6.1.1. Suscriptores

Se entiende por usuario del certificado al ciudadano con plena capacidad de obrar, que voluntariamente confía y hace uso del certificado emitido por el SEPE, del cual es titular.

Es obligación de los titulares de los certificados:

1º Suministrar a las Autoridades de Registro (oficinas del SEPE) información exacta, completa y veraz en relación a los datos que estas les soliciten para realizar el proceso de registro.

2º Conocer y aceptar las condiciones de utilización de los certificados.

3º Utilizar de forma correcta el certificado electrónico y sus claves.

4º Comunicar al SEPE, a través de los mecanismos que se habilitan a tal efecto, cualquier mal funcionamiento del certificado.

5º Proteger su contraseña de acceso a la Sede Electrónica del SEPE, tomando las precauciones razonables para evitar su pérdida, revelación o uso no autorizado, así como la contraseña de un solo uso enviada a su teléfono móvil durante el proceso de firma.

6º Cumplir las obligaciones que se establecen para el usuario en la DPC y en el artículo 23.1 de la LFE, así como en la Política de Certificación.

7º El ciudadano asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo informático o medio desde el cual emplee su certificado.

8º Así mismo, el ciudadano se responsabilizará de los riesgos derivados de la aceptación de una conexión segura sin haber realizado previamente la preceptiva verificación de la validez del certificado exhibido por el prestador de servicios. Los procedimientos para contrastar la seguridad de la conexión con dicho prestador de servicios deberán ser proporcionados por éste al ciudadano.