BANCO DE ESPAÑA
Eurosistema

15.12.2017

OID: 1.3.6.1.4.1.19484.2.2.11

Infraestructura de Clave Pública del Banco de España

Política de Certificación para Certificados de Autoridad de Sellado de Tiempo

Este documento recoge la Política de Certificación (PC) que regula los certificados emitidos por la AC Corporativa para la Autoridad de Sellado de Tiempo del Banco de España

Hoja de Control

Título	Política de Certificación de certificados de Autoridad de Sellado de Tiempo
Autor	Departamento de Sistemas de Información
Versión	1.2
Fecha	15.12.2017

Registro de Cambios

Versión	**Fecha**	**Motivo del cambio**
1.0	21.05.2010	Primera versión
1.1	11.05.2015	Actualización con motivo de la renovación de las Autoridades de Certificación
1.2	15.12.2017	Actualización con objeto de definir las nuevas extensiones propietarias bdeIssuerName y bdeIssuerVAT

ÍNDICE

1 Introducción

1.1 Resumen

Este documento recoge la Política de Certificación (PC) que rige la emisión de Certificados de Autoridad de Sellado de Tiempo (en adelante TSA) por parte de la Infraestructura de Clave Pública del Banco de España (en adelante PKIBDE). En particular, esta PC rige la emisión de Certificados a la Autoridad de Sellado de Tiempo del Banco de España, TSABDE.

Desde el punto de vista de la norma X.509 v3, una PC es un conjunto de reglas que definen la aplicabilidad o uso de un certificado en una comunidad de usuarios, sistemas o clase particular de aplicaciones que tengan en común una serie de requisitos de seguridad.

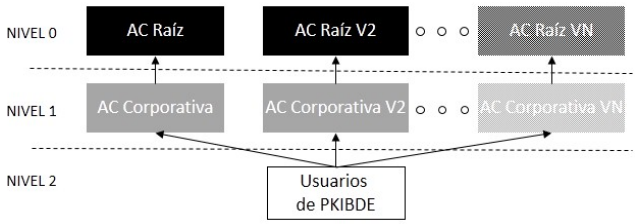
En esta PC se detalla y completa lo estipulado en la "Declaración de Prácticas de Certificación" (DPC) de la PKI del Banco de España (PKIBDE), conteniendo las reglas por las que se rige el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

La presente PC, salvo en el apartado 9 en el que existe una ligera desviación, se ha estructurado conforme a lo dispuesto por el grupo de trabajo PKIX del IETF (Internet Engineering Task Force), en su documento de referencia RFC 3647 (aprobado en Noviembre de 2003) *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*". A fin de dotar de un carácter uniforme al documento y facilitar su lectura y análisis, se incluyen todas las secciones establecidas en la RFC 3647. Cuando no se haya previsto nada en alguna sección aparecerá la frase "No estipulado". Adicionalmente a los epígrafes establecidos en la RFC 3647, se ha incluido un nuevo capítulo dedicado a la Protección de Datos de Carácter Personal para dar cumplimiento a la legislación española en la materia.

La PC incluye todas las actividades encaminadas a la gestión de los certificados de la Autoridad de Sellado de Tiempo en su ciclo de vida. En consecuencia, todas las partes involucradas tienen la obligación de conocer la PC y ajustar su actividad a lo dispuesto en la misma.

Esta PC asume que el lector conoce los conceptos de PKI, certificado, firma electrónica, TSA, servicios de sellado de tiempo, y sello de tiempo.

La arquitectura general, a nivel jerárquico, de la PKI del Banco de España es la siguiente[1]:



1.2 Nombre del documento e identificación

Nombre del documento	Política de Certificación (PC) para Certificados de Autoridad de Sellado de Tiempo de la PKIBDE
Versión del documento	1.2
Estado del documento	Aprobado
Fecha de emisión	15.12.2017
Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.19484.2.2.11
Ubicación de la DPC	http://pki.bde.es/politicas
DPC Relacionada	Declaración de Practicas de Certificación de la PKI del Banco de España OID 1.3.6.1.4.1.19484.2.2.1

1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes son:

- El Banco de España como titular de PKIBDE.
- La Autoridad de Administración de Políticas.
- Las Autoridades de Certificación.
- Las Autoridades de Registro.
- Las Autoridades de Validación.
- El Archivo de Claves.
- Los Solicitantes y Titulares de los certificados emitidos por PKIBDE.
- Los Terceros Aceptantes de los certificados emitidos por PKIBDE.

1.3.1 Autoridad de Administración de Políticas

Se define Autoridad de Administración de Políticas de acuerdo con la Declaración de Prácticas de Certificación (en adelante DPC) de PKIBDE.

[1] Sucesivas renovaciones de las Autoridades de Certificación, sean Raíz o Corporativas, se señalarán con un número de versionado, tal y como se muestra en la imagen.

1.3.2 Autoridades de Certificación

Se define Autoridades de Certificación de acuerdo con la DPC de PKIBDE.

Las Autoridades de Certificación que actualmente componen PKIBDE son:

1.3.2.1 Autoridades de Certificación Raíz

- **AC Raíz**: Autoridad de Certificación de primer nivel. Esta AC sólo emite certificados para sí misma y sus AC Subordinadas. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece. Sus datos más relevantes son:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Número de serie	F16D 7586 5D7C CF92 41AD A17A CD9A 3DE2
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2004-07-08 11:34:12 hasta 2034-07-08 11:34:12
Huella digital (SHA-1)	2B60 DE7D 3337 8BF7 5B67 8B10 77BB F951 6029 D6A8
Algoritmos criptográficos	SHA-1 / RSA 2048

- **AC Raíz V2**: Autoridad de Certificación de primer nivel. Esta AC sólo emite certificados para sí misma y sus AC Subordinadas. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece. Se emiten tres certificados válidos, utilizando el mismo par de claves, para esta AC:

  - Con algoritmo SHA-1[1]:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	25B4 07F6 4A5C F9F1 5547 7951 2040 982B
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 12:42:33 hasta 2045-05-04 12:42:33
Huella digital (SHA-1)	A84A 2C75 2746 B21B 567F 8B07 EC2A FCB9 7551 046A
Algoritmos criptográficos	SHA-1 / RSA 4096

  - Con algoritmo SHA-256:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	4554 22D4 E876 1BFC 5547 4D19 4E85 6E37
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 12:42:33 hasta 2045-05-04 12:42:33
Huella digital (SHA-1)	ACBC CB74 406A 5588 EB88 2F5F 5994 9DDC B831 7986

[1] Este certificado sólo se utilizará en sistemas que no soporten los algoritmos superiores

Algoritmos criptográficos	SHA-256 / RSA 4096

- Con algoritmo SHA-512:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	19D8 C7AA 668C 3E0F 5547 7970 D573 00FC
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 12:42:33 hasta 2045-05-04 12:42:33
Huella digital (SHA-1)	2AD9 E9BF FCDD B5D4 46C9 7A3A D4BB 6DCE A3B1 219C
Algoritmos criptográficos	SHA-512 / RSA 4096

La AC Raíz V2 ha sido emitida para sustituir a la AC Raíz de Banco de España, con motivo de la actualización criptográfica de los algoritmos y tamaños de clave utilizados de acuerdo a las recomendaciones internacionales. Ambas AC Raíz son válidas, sin embargo, hasta su fecha de caducidad.

1.3.2.2 Autoridades de Certificación Intermedias

- **AC Corporativa**: Autoridad de Certificación subordinada de la AC Raíz. Su función es la emisión de certificados para los usuarios de PKIBDE. Sus datos más relevantes son:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA, O=BANCO DE ESPAÑA, C=ES
Número de serie	366A 524D A5E4 4AF8 4108 A140 9B9B 76EB
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2004-07-29 9:03:28 hasta 2019-07-29 9:03:28
Huella digital (SHA-1)	ABE6 1ED2 5AF6 4253 F77B 322F 6F21 3729 B539 1BDA
Algoritmos criptográficos	SHA-1 / RSA 2048

- **AC Corporativa V2**: Autoridad de Certificación subordinada de la AC Raíz. Su función es la emisión de certificados para los usuarios de PKIBDE. Se emiten tres certificados válidos para esta AC:

- Con algoritmo SHA-1[1]:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	5F8B 48ED 492D 5236 5547 7730 704F 397F
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES

[1] Este certificado sólo se utilizará en sistemas que no soporten los algoritmos superiores

Periodo de validez	Desde 2015-05-04 18:00:00 hasta 2030-05-04 18:00:00
Huella digital (SHA-1)	4832 0271 9F45 67EB 42E4 4A13 04DE D1F7 7B7B 7EE9
Algoritmos criptográficos	SHA-1 / RSA 4096

- Con algoritmo SHA-256:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	18D8 765B E681 86C6 5547 76F5 9227 2480
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 18:00:00 hasta 2030-05-04 18:00:00
Huella digital (SHA-1)	A8F0 5CAC 9C65 18C0 8FF6 3F82 C338 DE46 D8B9 3E38
Algoritmos criptográficos	SHA-256 / RSA 4096

- Con algoritmo SHA-512:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	293F 0A37 5B54 D2D2 5547 7749 5728 B9B6
Nombre distintivo del emisor	CN= BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 18:00:00 hasta 2030-05-04 18:00:00
Huella digital (SHA-1)	B3CF 4285 869F 6C07 45B1 D69C 8EC2 7683 6953 DE5E
Algoritmos criptográficos	SHA-512 / RSA 4096

La AC Corporativa V2 ha sido emitida para sustituir a la AC Corporativa de Banco de España, con motivo de la actualización criptográfica de los algoritmos y tamaños de clave utilizados de acuerdo a las recomendaciones internacionales.

Ambas AC Intermedias son válidas hasta su fecha de caducidad o su revocación. Sin embargo, la AC Corporativa dejará de prestar servicio de emisión de certificados de entidad final a partir de la fecha de entrada en servicio de la AC Corporativa V2 manteniéndose únicamente para permitir la revocación de certificados previamente emitidos por ella.

1.3.3 Autoridades de Registro

Se definen las Autoridades de Registro de acuerdo con la Declaración de Prácticas de Certificación de PKIBDE.

La emisión de Certificados de TSA la realizarán los propios Administradores de PKIBDE, los cuales actuarán como Autoridades de Registro para comprobar los datos de los solicitantes y generar

peticiones de certificación/revocación, utilizando directamente la administración de la AC Corporativa.

1.3.4 Autoridad de Validación

Se define Autoridad de Validación de acuerdo con la DPC de PKIBDE.

1.3.5 Archivo de claves

El Archivo de Claves definido en la DPC no tiene aplicación en esta política de certificación.

1.3.6 Titulares de los certificados

Se define Titular de acuerdo con la DPC de PKIBDE.

Los tipos de entidades que pueden ser titulares de Certificados a los que se refiere esta PC se restringen a los recogidos en el siguiente cuadro:

Entorno de Certificación	Titulares
AC Corporativa	Autoridad de Sellado de Tiempos

Cabe recordar que estas Autoridades de Sellado de Tiempos pueden ser internas (ej: TSABDE) o externas al Banco de España. En ambos casos, para cada TSA debe haber una persona responsable. El tipo de personas que pueden serlo se recogen en la siguiente tabla:

Tipo de certificado	Responsable
Certificados de Autoridad de Sellado de Tiempo	Responsable de la Autoridad de Sellado de Tiempo

1.3.7 Terceros aceptantes

Se definen los terceros aceptantes según lo especificado en la DPC de PKIBDE. En particular, serán los que reconozcan y hagan uso de los Sellos de Tiempo emitidos por una TSA, cuyo certificado haya sido emitido por PKIBDE según esta PC.

1.3.8 Otros afectados

Solicitante: son los responsables de la Autoridad de Sellado de Tiempo.

Administrador de la AC: personas que dentro del Banco de España gestionan las peticiones de certificados de TSA teniendo privilegios de administración de la AC.

1.4 Uso de los certificados

1.4.1 Usos apropiados de los certificados

La Autoridad de Sellado de Tiempo titular del certificado deberá tener implantada una "Política de Sellado de Tiempo" conforme a buenas prácticas reconocidas, para la prestación de servicios de sellado de tiempo.

Asimismo, deberá disponer de un documento actualizado de "Políticas y Prácticas de Sellado de Tiempo" que recoja dicha política implantada, accesible de forma pública y gratuita, y en el que figuren sus responsables y se describan sus obligaciones y responsabilidades, procesos y procedimientos para la gestión y operación de la TSA, ciclo de vida de las claves, mecanismos de seguridad, etc.

En la siguiente tabla se recoge con más detalle el uso apropiado de los certificados:

Tipo de certificado	Usos apropiados
Certificados de Autoridad de Sellado de Tiempo	Prestación de servicios de sellado de tiempo (conforme a las "Políticas y Prácticas de Sellado de Tiempo" de la TSA)

1.4.2 Limitaciones y restricciones en el uso de los certificados

Cualquier uso no incluido en el apartado anterior queda excluido.

1.5 Administración de las políticas

1.5.1 El Banco de España como titular de PKIBDE

Esta PC es propiedad del Banco de España:

Nombre	Banco de España		
Dirección e-mail	pkibde@bde.es		
Dirección	C/Alcalá, 48. 28014 - Madrid (España)		
Teléfono	+34913385000	**Fax**	+34915310059

1.5.2 Persona de contacto

Esta PC está administrada por la Autoridad de Administración de Políticas (AAP) de la PKIBDE.

Nombre	Departamento de Sistemas de Información Autoridad de Administración de Políticas de la PKI del Banco de España		
Dirección e-mail	pkibde@bde.es		
Dirección	C/Alcalá, 522. 28027 - Madrid (España)		
Teléfono	+34913386666	**Fax**	+34913386875

1.5.3 Determinación de la adecuación de la DPC de una AC externa a las Políticas de Certificación de PKIBDE

Según lo especificado en la DPC de PKIBDE.

1.5.4 Procedimientos de Aprobación de esta PC

Según lo especificado en la DPC de PKIBDE.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

En el ámbito de esta PC se utilizan las siguientes denominaciones:

Autenticación: procedimiento de comprobación de la identidad de un solicitante o titular de certificados de PKIBDE.

Autoridad de Sellado de Tiempo (TSA): autoridad que expide sellos de tiempo.

Certificado electrónico: un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. Esta es la definición de la Ley 59/2003 que en este documento se extiende a los casos en que la vinculación de los datos de verificación de firma se hace a un componente informático.

Clave Pública y Clave Privada: la criptografía asimétrica en la que se basa la PKI emplea un par de claves en la que lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado y, si procede, por el Archivo de Claves.

Clave de Sesión: clave que establece para cifrar una comunicación entre dos entidades. La clave se establece de forma específica para cada comunicación, sesión, terminando su utilidad una vez finalizada ésta.

Directorio: Repositorio de información que sigue el estándar X.500 de ITU-T.

Identificación: procedimiento de reconocimiento de la identidad de un solicitante o titular de certificados de PKIBDE.

Identificador de usuario: conjunto de caracteres que se utilizan para la identificación unívoca de un usuario en un sistema.

Jerarquía de confianza: Conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una AC de nivel superior garantiza la confiabilidad de una o varias de nivel inferior. En el caso de PKIBDE, la jerarquía tiene dos niveles, la AC Raíz en el nivel superior garantiza la confianza de sus AC subordinadas.

Prestador de Servicios de Certificación: persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Solicitante: persona que solicita un certificado para sí mismo, para una persona jurídica o para una Autoridad de Sellado de Tiempos.

Tercero Aceptante: persona o entidad diferente del titular que decide aceptar y confiar en un certificado emitido por PKIBDE.

Titular: persona, componente informático o entidad (ej: Autoridad de Sellado de Tiempo) para el que se expide un certificado electrónico y es aceptado por éste o por su solicitante.

UTC (Tiempo Universal Coordinado): zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo. Definido en ITU-R Recommendation TF.460-5

UTC(k): escala de tiempo realizada por el laboratorio "k" y mantenida en acuerdo con UTC, con el objetivo de alcanzar un margen de +-100 ns con respecto a ella (Recommendation TF.536-1)

Suscriptor: entidad que solicita los servicios de la TSA y que ha aceptado explícita o implícitamente sus términos y condiciones.

Política de sellado de tiempo (time-stamp policy): conjunto de reglas que regulan la aplicabilidad del sellado de tiempo sobre una comunidad determinada y/o su aplicación con unos requisitos de seguridad comunes.

Declaración de prácticas de TSA: declaración de las prácticas que una TSA realiza en la emisión de tokens de sellado de tiempo.

Sello de tiempo (time-stamp token): documento firmado electrónicamente por la TSA que liga la representación de un dato a un tiempo concreto, estableciendo por lo tanto que dicho dato existía antes de dicho momento.

Sistema TSA: conjunto de productos IT y otros componentes organizados para dar soporte al suministro de servicios de sellado de tiempo.

Unidad de Sellado de Tiempo: conjunto de hardware y software que tiene una sola clave activa de firma de sellos de tiempo en un momento dado.

1.6.2 Acrónimos

AAP: Autoridad de Administración de Políticas

AC: Autoridad de Certificación

AR: Autoridad de Registro

AV: Autoridad de Validación.

CRL: Certificate Revocation List (Lista de Certificados Revocados)

C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CEN: Comité Européen de Normalisation

CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CWA: CEN Workshop Agreement

DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.

DPC: Declaración de Prácticas de Certificación

ETSI: European Telecommunications Standard Institute

FIPS: Federal Information Processing Standard (Estándar USA de procesado de información)

HSM: Hardware Security Module. Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.

IETF: Internet Engineering Task Force (Organismo de estandarización de Internet)

LDAP: Lightweight Directory Access Protocol (Protocolo de acceso a servicios de directorio)

O: Organization. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

OCSP: Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.

OID: Object identifier (Identificador de objeto único)

OU: Organizacional Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

PC: Política de Certificación

PKCS: Public Key Infrastructure Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.

PKI: Public Key Infrastructure (Infraestructura de Clave Pública)

PKIBDE: PKI del Banco de España.

PKIX: Grupo de trabajo dentro del IETF (Internet Engineering Task Group) constituido con el objeto de desarrollar las especificación relacionadas con las PKI e Internet.

RFC: Request For Comments (Estándar emitido por la IETF)

TSA: Time Stamping Authority (Autoridad de Sellado de Tiempo)

TSU: Time Stamping Unit (Unidad de Sellado de Tiempo)

UTC: Universal Time Coordinated (Tiempo Universal Coordinado)

2 Repositorios y publicación de información

2.1 Repositorios

Según lo especificado en la DPC de PKIBDE.

2.2 Publicación de información de certificación

Según lo especificado en la DPC de PKIBDE.

2.3 Temporalidad o frecuencia de publicación

Según lo especificado en la DPC de PKIBDE.

2.4 Controles de acceso a los repositorios

Según lo especificado en la DPC de PKIBDE.

3 Identificación y autenticación de los titulares de los certificados

3.1 Nombres

3.1.1 Tipos de nombres

Los certificados emitidos por PKIBDE contienen el nombre distintivo (*Distinguished Name* o DN) X.500 del emisor y el del destinatario del certificado en los campos *issuer name* y *subject name* respectivamente.

El atributo CN (*Common Name*) del DN hará referencia al código asignado a la Autoridad de Sellado de Tiempo titular del certificado.

En caso de que haya más de una TSU para una misma Autoridad de Sellado de Tiempo, el CN deberá estar finalizado por un código numérico que identifique unívocamente a cada TSU.

El CN del certificado de componente será el siguiente:

Tipo de certificado	CN
Certificados de Autoridad de Sellado de Tiempo	CN=BANCO DE ESPAÑA – TSA *TEXTO_LIBRE*

Siendo *TEXTO_LIBRE* un texto libre que permitirá diferenciar entre certificados distintos generados para una misma Autoridad de Sellado de Tiempos que dispone de varias TSUs.

El resto de atributos del DN tendrán los siguientes valores fijos:

O=BANCO DE ESPAÑA, C=ES

3.1.2 Necesidad de que los nombres sean significativos

En todos los casos los nombres distintivos de los certificados han de ser significativos y se aplicarán las reglas establecidas en el apartado anterior para ello.

3.1.3 Reglas para interpretar varios formatos de nombres

La regla utilizada por PKIBDE para interpretar los nombres distintivos de los titulares de los certificados que emite es ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.4 Unicidad de los nombres

El DN de los certificados no puede estar repetido.

En el caso de que se emita más de un certificado para una misma TSA por disponer de varias TSUs, estos certificados se diferenciarán por un número distintivo al final de su correspondiente CN.

No podrá existir más de un certificado para una misma TSU, dada una TSA determinada.

3.1.5 Procedimientos de resolución de conflictos sobre nombres

Cualquier conflicto concerniente a la propiedad de nombres se resolverá según lo estipulado en el punto *9.13 Reclamaciones y jurisdicción* de este documento.

3.1.6 Reconocimiento, autenticación y papel de las marcas registradas

No estipulado.

3.2 Validación de la identidad inicial

3.2.1 Medio de prueba de posesión de la clave privada

La posesión de la clave privada, correspondiente a la clave pública para la que el responsable de la TSA solicita que se genere el certificado, quedará probada mediante el envío de la solicitud de certificación, en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

3.2.2 Autenticación de la identidad de una persona jurídica

Los certificados de Autoridad de Sellado de Tiempo no son certificados electrónicos de persona jurídica según lo definido en artículo 7 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

3.2.3 Autenticación de la identidad de una persona física

La autenticación de individuos en el marco de esta política se hará mediante la firma electrónica de la solicitud utilizando un certificado de persona física emitido por un PSC reconocido por el Banco de España a tal efecto o por PKIBDE. La validación de la identidad de la persona física se habrá realizado conforme a los procedimientos establecidos por el PSC o por PKIBDE.

3.2.4 Información no verificada sobre el solicitante

No se verificará la propiedad de los nombres de dominio ni de las direcciones de correo electrónico, en caso de que sea necesario incluirlos dentro del certificado.

3.2.5 Comprobación de las facultades de representación

El solicitante habrá de ser el responsable de la TSA del Banco de España.

3.2.6 Criterios para operar con AC externas

Según lo especificado en la DPC de PKIBDE.

3.3 Identificación y autenticación en las peticiones de renovación de claves

3.3.1 Identificación y autenticación por una renovación de claves de rutina

El proceso de identificación individual será el mismo que en la validación inicial.

3.3.2 Identificación y autenticación por una renovación de claves tras una revocación

El proceso de identificación individual será el mismo que en la validación inicial.

4 Requisitos operacionales para el ciclo de vida de los certificados

En este capítulo se recogen los requisitos operacionales para el ciclo de vida de los certificados de la Autoridad de Sellado de Tiempo emitidos por la AC Corporativa.

Aunque estos certificados deben ser almacenados en hardware criptográfico de soporte, no es objeto de esta Política de Certificación regular la gestión de dichos elementos.

Por otro lado, en este capítulo se van a emplear algunas ilustraciones para facilitar su comprensión. En el caso de que existiera alguna diferencia o discrepancia entre lo recogido en el texto y lo recogido en las ilustraciones prevalecería siempre el texto, dado el carácter necesariamente sintético de las ilustraciones.

4.1 Solicitud de certificados

4.1.1 Quién puede efectuar una solicitud

La petición de un certificado de Autoridad de Sellado de Tiempo la ha de efectuar la persona responsable de la TSA mediante un certificado de persona física. Dicho responsable deberá disponer de la facultad de representación necesaria que le acredite como tal.

La solicitud del certificado no implica su obtención si el solicitante no cumple los requisitos establecidos en la DPC y en esta PC para certificados de TSA.

4.1.2 Registro de las solicitudes de certificados y responsabilidades de los solicitantes

1 La solicitud se envía por correo electrónico al Banco de España. La firma electrónica podrá realizarse o bien sobre el propio documento de solicitud, o bien sobre el correo electrónico utilizado para enviar la petición, mediante alguno de los certificados de persona física del responsable de la TSA emitido por un PSC reconocido por el Banco de España a tales efectos o bien por la propia PKIBDE.

En cuanto al contenido de la solicitud, ha de incluir la petición de certificado (CSR) con la clave pública asociada así como la información necesaria para que la AC genere el certificado.

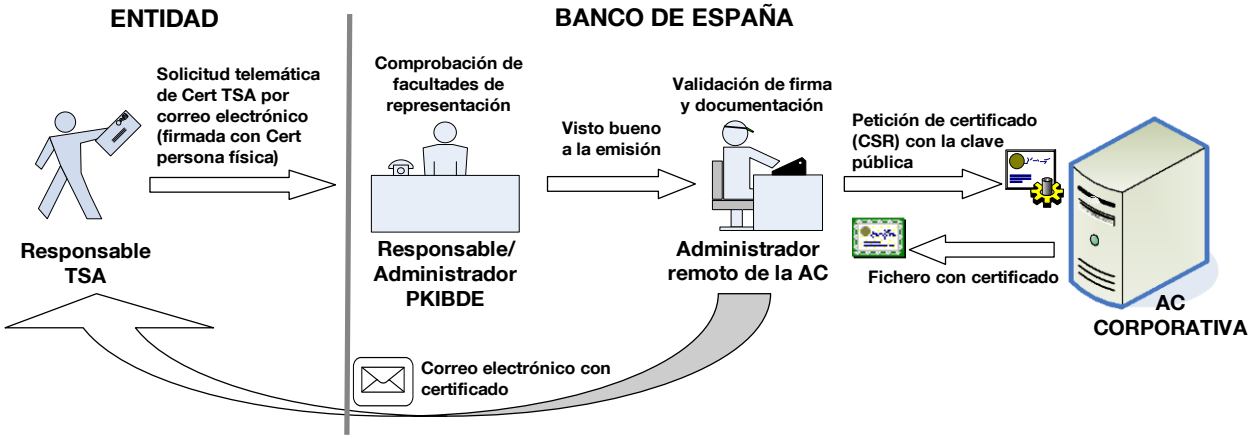
2 El administrador o responsable de PKIBDE verificará las facultades de representación del solicitante previamente disponibles en el Banco de España, como paso previo para dar el visto bueno a la emisión del certificado.

3 Un administrador remoto de la AC recibirá el mensaje de correo electrónico con el visto bueno previo, verificará la firma electrónica correspondiente, y realizará las comprobaciones necesarias sobre los datos e información aportados por el solicitante. Si todo es correcto, el administrador remoto se conectará para solicitar la emisión del certificado a partir de la petición de certificado (CSR) con la clave pública.

4 La AC emite el certificado, y posteriormente el administrador remoto descarga el correspondiente fichero.

5 El Banco de España envía mediante correo electrónico al solicitante el certificado.

En la siguiente figura se sintetiza el proceso descrito:



4.2 Tramitación de las solicitudes de certificados

4.2.1 Realización de las funciones de identificación y autenticación

El administrador o responsable de PKIBDE realizará la identificación y autenticación del solicitante mediante la validación de la firma electrónica de la solicitud o del correo electrónico utilizado para enviarla.

4.2.2 Aprobación o denegación de las solicitudes de certificados

La emisión del certificado tendrá lugar una vez que PKIBDE haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación.

A tal efecto, PKIBDE o sus administradores y responsables podrán recabar del solicitante la documentación que consideren oportuna.

4.2.3 Plazo para la tramitación de las solicitudes de certificados

La AC Corporativa de PKIBDE no se hace responsable de las demoras que puedan surgir en el periodo comprendido entre la solicitud del certificado, la publicación en el repositorio de PKIBDE y la entrega del mismo. La AC Corporativa tramitará las peticiones con la mayor diligencia posible.

4.3 Emisión de certificados

4.3.1 Actuaciones de la AC durante la emisión del certificado

La emisión del certificado implica la autorización definitiva de la solicitud por parte de la AC.

Cuando la AC Corporativa de PKIBDE emita un certificado de acuerdo con una solicitud de certificación, efectuará las notificaciones que se establecen en el apartado 4.3.2 de este capítulo.

Todos los certificados iniciarán su vigencia en el momento de su emisión, salvo que se indique en los mismos una fecha y hora posterior a su entrada en vigor, que no será posterior a los 15 días naturales desde su emisión. El periodo de vigencia estará sujeto a una posible extinción anticipada, temporal o definitiva, cuando se den las causas que motiven la suspensión o revocación del certificado.

4.3.2 Notificación al solicitante de la emisión por la AC del certificado

El solicitante conocerá la emisión del certificado mediante correo electrónico.

4.4 Aceptación del certificado

4.4.1 Forma en la que se acepta el certificado

El solicitante estará aceptando implícitamente la DPC y PC así como el certificado por el hecho de solicitarlo.

4.4.2 Publicación del certificado por la AC

El certificado de la Autoridad de Sellado de Tiempo se publicará en el repositorio de PKIBDE.

4.4.3 Notificación de la emisión del certificado por la AC a otras Autoridades

No procede.

4.5 Par de claves y uso del certificado

4.5.1 Uso de la clave privada y del certificado por el titular

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta PC y de acuerdo con lo establecido en los campos 'Key Usage' y 'Extended Key Usage' del certificado, y con lo establecido en sus "Políticas y Prácticas de Sellado de Tiempo". Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso establecidas en la DPC y PC y sólo para lo que éstas establezcan.

Tras la expiración o revocación del certificado el titular deberá dejar de usar la clave privada.

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

Los Terceros Aceptantes sólo deben depositar su confianza en los certificados para aquello que establece esta PC y las "Políticas y Prácticas de Sellado de Tiempo" de la TSA, y de acuerdo con lo establecido en el campo 'Key Usage' del certificado.

Los Terceros Aceptantes han de realizar las operaciones de clave pública de manera satisfactoria para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en la DPC y en esta PC. Asimismo, se obligan a las condiciones de uso establecidas en estos documentos.

4.6 Renovación de certificados sin cambio de claves

4.6.1 Circunstancias para la renovación de certificados sin cambio de claves

Todas las renovaciones de certificados realizadas en el ámbito de esta PC se realizarán con cambio de claves. En consecuencia, no se recogen el resto de los puntos del apartado 4.6 (4.6.2 a 4.6.7) que establece la RFC 3647, lo que implica, a efectos de esta PC, su no estipulación.

4.7 Renovación de certificados con cambio de claves

4.7.1 Circunstancias para una renovación con cambio claves de un certificado

Un Certificado de TSA puede ser renovado, entre otros, por los siguientes motivos:
- Expiración del periodo de validez.
- Cambio de datos contenidos en el certificado.
- Claves comprometidas o pérdida de fiabilidad de las mismas.
- Cambio de formato.

Todas las renovaciones, con independencia de su causa, se realizarán con cambio de claves.

4.7.2 Quién puede pedir la renovación de un certificado

La renovación la debe solicitar el responsable de la TSA.

4.7.3 Tramitación de las peticiones de renovación con cambio de claves

La AC comprobará en el proceso de renovación que la información utilizada para verificar la identidad y atributos del titular es todavía válida. Si alguna información del titular ha cambiado ésta deberá ser verificada y registrada con el acuerdo del responsable de la TSA.

Los requisitos de renovación serán los mismos que para la emisión inicial del certificado.

Si alguna de las condiciones establecidas en esta PC han cambiado se deberá asegurar que tal hecho es conocido por el responsable de la TSA y que éste está de acuerdo con las mismas.

En cualquier caso la renovación de un certificado está supeditada a:
- Que lo solicite en debido tiempo y forma, siguiendo las instrucciones y normas que PKIBDE especifica a tal efecto.
- Que la AC no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación / suspensión del certificado.
- Que la solicitud de renovación de servicios de prestación se refiera al mismo tipo de certificado emitido inicialmente.

4.7.4 Notificación de la emisión de un nuevo certificado al titular

Se notificará mediante correo electrónico al responsable de la TSA.

4.7.5 Forma de aceptación del certificado con las claves cambiadas

El solicitante estará aceptando implícitamente la DPC y PC así como el certificado por el hecho de renovarlo.

4.7.6 Publicación del certificado con las nuevas claves por la AC

El Certificado de TSA se publicará en el repositorio de PKIBDE.

4.7.7 Notificación de la emisión del certificado por la AC a otras Autoridades

No estipulado.

4.8 Modificación de certificados

4.8.1 Circunstancias para la modificación de un certificado

Todas las modificaciones de certificados realizadas en el ámbito de esta PC se tratarán como una renovación de certificados, por lo que son de aplicación los apartados anteriores al respecto.

En consecuencia, no se recogen el resto de subapartados del apartado 4.8 (4.8.2 a 4.8.7) que establece la RFC 3647, lo que implica a efectos de esta Declaración que no han sido regulados.

4.9 Revocación y suspensión de certificados

4.9.1 Circunstancias para la revocación

La revocación de un certificado es el acto por el cual se deja sin efecto la validez de un certificado antes de su caducidad. El efecto de la revocación de un certificado es la pérdida de vigencia del mismo, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación. La revocación de un certificado impide el uso legítimo del mismo por parte del titular.

La revocación de un certificado implica su publicación en la Lista de Certificados Revocados (CRL) de acceso público.

Causas de revocación:

- El robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del titular.
- El mal uso deliberado de claves y certificados, o la falta de observancia o contravención de los requerimientos operacionales contenidos en la DPC o en la presente PC.
- El cese de la TSA en sus funciones, circunstancia que le facultaba para la posesión del certificado.
- Cese de la actividad de PKIBDE.
- Emisión defectuosa de un certificado debido a que:
    1. No se ha cumplido un requisito material para la emisión del certificado.
    2. La creencia razonable de que un dato fundamental relativo al certificado es o puede ser falso.
    3. Existencia de un error de entrada de datos u otro error de proceso.
- El par de claves generado por un titular se revela como “débil”.
- La información contenida en un certificado o utilizada para realizar su solicitud deviene en inexacta.
- Por orden formulada por el responsable de la TSA o por tercero autorizado o la persona física solicitante en representación de una persona jurídica.
- El certificado de una AC superior en la jerarquía de confianza del certificado es revocado.
- Por la concurrencia de cualquier otra causa especificada en la presente PC o en la DPC.

La revocación tiene como principal efecto sobre el certificado la terminación inmediata y anticipada del periodo de validez del mismo, deviniendo el certificado como no valido. La revocación no afectará a las obligaciones subyacentes creadas o comunicadas por esta DPC ni tendrá efectos retroactivos.

4.9.2 Quien puede solicitar la revocación

PKIBDE o cualquiera de las Autoridades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada de la TSA, o cualquier otro hecho que recomendara emprender dicha acción.

Asimismo, el responsable de la TSA también podrá solicitar la revocación de sus certificados, debiendo hacerlo de acuerdo con las condiciones especificadas en el apartado 4.9.3.

4.9.3 Procedimiento de solicitud de revocación

Las solicitudes de revocación las realizará el responsable de la TSA de forma semejante a la descrita en el apartado 4.1.2 para la solicitud de emisión. Las tramitará siempre el Administrador o Responsable de PKIBDE.

Además de esta vía ordinaria, los Operadores y Administradores de PKIBDE podrán revocar de modo inmediato cualquier certificado en caso de que llegue a su conocimiento alguna de las causas de revocación.

4.9.4 Periodo de gracia de la solicitud de revocación

La revocación se llevará a cabo de forma inmediata a la tramitación de cada solicitud verificada como válida. Por tanto, no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la solicitud de revocación.

4.9.5 Plazo en el que la AC debe resolver la solicitud de revocación

La solicitud de revocación de un certificado de TSA debe ser atendida con la máxima celeridad, sin que en ningún caso su tratamiento pueda ser superior a 24 horas.

4.9.6 Requisitos de verificación de las revocaciones por los terceros aceptantes

La verificación de las revocaciones es obligatoria para cada uso de los certificados de TSA.

Los terceros aceptantes deberán comprobar la validez de la CRL previamente a cada uno de sus usos y descargar la nueva CRL del repositorio de PKIBDE al finalizar el periodo de validez de la que posean. Las listas de CRLs guardadas en memoria 'cache'[1], aun no estando caducadas, no garantizan que dispongan de información de revocación actualizada.

Opcionalmente, se puede emplear una Autoridad de Validación de PKIBDE (en caso de estar disponible según se establece en el apartado 2.1 de esta PC) para verificar de forma online el estado de revocación del certificado.

4.9.7 Frecuencia de emisión de CRLs

Según lo especificado en la DPC de PKIBDE.

[1] Memoria 'caché': memoria donde se guardan los datos necesarios para que el sistema opere con más rapidez en lugar de obtenerlos en cada operación de la fuente de datos. Su uso puede suponer un riesgo de operar con datos no actuales.

4.9.8 Tiempo máximo entre la generación y la publicación de las CRL

El tiempo máximo admisible entre la generación de la CRL y su publicación en el repositorio es de 1 hora.

4.9.9 Disponibilidad de un sistema en línea de verificación del estado de los certificados

Opcionalmente, PKIBDE dispone de un sistema en línea (Autoridad de Validación) de verificación del estado de los certificados.

Las direcciones de acceso vía web a las CRL y a la Autoridad de Validación, así como sus características y restricciones de uso, quedan reflejadas en el apartado *2.1 Repositorio*.

4.9.10 Requisitos de comprobación en-línea de revocación

En el caso de utilizar una Autoridad de Validación, el tercer aceptante debe disponer de un software que sea capaz de operar con el protocolo OCSP para obtener la información sobre el certificado.

4.9.11 Otras formas de divulgación de información de revocación disponibles

No estipulado.

4.9.12 Requisitos especiales de renovación de claves comprometidas

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al compromiso de la clave privada.

4.9.13 Causas para la suspensión

No se contempla la posibilidad de suspensión de certificados de TSA.

4.9.14 Quién puede solicitar la suspensión

No estipulado.

4.9.15 Procedimiento para la solicitud de suspensión

No estipulado.

4.9.16 Límites del periodo de suspensión

No estipulado.

4.10 Servicios de información del estado de certificados

4.10.1 Características operativas

Según lo especificado en la DPC de PKIBDE.

4.10.2 Disponibilidad del servicio

Según lo especificado en la DPC de PKIBDE.

4.10.3 Características adicionales

Según lo especificado en la DPC de PKIBDE.

4.11 Extinción de la validez de un certificado

La extinción de la validez de un certificado se produce en los siguientes casos:

- Revocación anticipada del certificado por cualquiera de las causas recogidas en el apartado 4.9.1.
- Expiración de la vigencia del certificado.

Si no se solicita la renovación del certificado la extinción de su validez supondrá la extinción de la relación entre el titular y la AC.

4.12 Custodia y recuperación de claves

4.12.1 Prácticas y políticas de custodia y recuperación de claves

No se efectúa archivo de la clave privada de los certificados utilizados por TSA

4.12.2 Prácticas y políticas de protección y recuperación de la clave de sesión

No estipulado.

5 Controles de seguridad física, instalaciones, gestión y operacionales

5.1 Controles físicos

5.1.1 Ubicación física y construcción

Según lo especificado en la DPC de PKIBDE.

5.1.2 Acceso físico

Según lo especificado en la DPC de PKIBDE.

5.1.3 Alimentación eléctrica y aire acondicionado

Según lo especificado en la DPC de PKIBDE.

5.1.4 Exposición al agua

Según lo especificado en la DPC de PKIBDE.

5.1.5 Protección y prevención de incendios

Según lo especificado en la DPC de PKIBDE.

5.1.6 Sistema de almacenamiento

Según lo especificado en la DPC de PKIBDE.

5.1.7 Eliminación de residuos

Según lo especificado en la DPC de PKIBDE.

5.1.8 Copias de seguridad fuera de las instalaciones

Según lo especificado en la DPC de PKIBDE.

5.2 Controles de procedimiento

5.2.1 Roles responsables del control y gestión de la PKI

Según lo especificado en la DPC de PKIBDE.

5.2.2 Número de personas requeridas por tarea

Según lo especificado en la DPC de PKIBDE.

5.2.3 Identificación y autenticación para cada usuario

Según lo especificado en la DPC de PKIBDE.

5.2.4 Roles que requieren segregación de funciones

Según lo especificado en la DPC de PKIBDE.

5.3 Controles de personal

5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

Según lo especificado en la DPC de PKIBDE.

5.3.2 Procedimientos de comprobación de antecedentes

Según lo especificado en la DPC de PKIBDE.

5.3.3 Requerimientos de formación

Según lo especificado en la DPC de PKIBDE.

5.3.4 Requerimientos y frecuencia de actualización de la formación

Según lo especificado en la DPC de PKIBDE.

5.3.5 Frecuencia y secuencia de rotación de tareas

Según lo especificado en la DPC de PKIBDE.

5.3.6 Sanciones por acciones no autorizadas

Según lo especificado en la DPC de PKIBDE.

5.3.7 Requisitos de contratación de terceros

Según lo especificado en la DPC de PKIBDE.

5.3.8 Documentación proporcionada al personal

Según lo especificado en la DPC de PKIBDE.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de eventos registrados

Según lo especificado en la DPC de PKIBDE.

5.4.2 Frecuencia de procesado de registros de auditoría

Según lo especificado en la DPC de PKIBDE.

5.4.3 Periodo de conservación de los registros de auditoría

Según lo especificado en la DPC de PKIBDE.

5.4.4 Protección de los registros de auditoría

Según lo especificado en la DPC de PKIBDE.

5.4.5 Procedimientos de respaldo de los registros de auditoría

Según lo especificado en la DPC de PKIBDE.

5.4.6 Sistema de recogida de información de auditoría (interno vs externo)

Según lo especificado en la DPC de PKIBDE.

5.4.7 Notificación al sujeto causa del evento

Según lo especificado en la DPC de PKIBDE.

5.4.8 Análisis de vulnerabilidades

Según lo especificado en la DPC de PKIBDE.

5.5 Archivo de registros

5.5.1 Tipo de eventos archivados

Según lo especificado en la DPC de PKIBDE.

5.5.2 Periodo de conservación de registros

Según lo especificado en la DPC de PKIBDE.

5.5.3 Protección del archivo

Según lo especificado en la DPC de PKIBDE.

5.5.4 Procedimientos de copia de respaldo del archivo

Según lo especificado en la DPC de PKIBDE.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Según lo especificado en la DPC de PKIBDE.

5.5.6 Sistema de archivo de información de auditoría (interno vs externo)

Según lo especificado en la DPC de PKIBDE.

5.5.7 Procedimientos para obtener y verificar información archivada

Según lo especificado en la DPC de PKIBDE.

5.6 Cambio de claves de una AC

Según lo especificado en la DPC de PKIBDE.

5.7 Recuperación en caso de compromiso de una clave o catástrofe

5.7.1 Procedimientos de gestión de incidentes y compromisos

Según lo especificado en la DPC de PKIBDE.

5.7.2 Alteración de los recursos hardware, software y/o datos

Según lo especificado en la DPC de PKIBDE.

5.7.3 Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad

Según lo especificado en la DPC de PKIBDE.

5.7.4 Instalación después de un desastre natural u otro tipo de catástrofe

Según lo especificado en la DPC de PKIBDE.

5.8 Cese de una AC o AR

5.8.1 Autoridad de Certificación

Según lo especificado en la DPC de PKIBDE.

5.8.2 Autoridad de Registro

Según lo especificado en la DPC de PKIBDE.

6 Controles de Seguridad Técnica

Los controles de seguridad técnica para los componentes internos de PKIBDE, y concretamente para AC Raíz y AC Corporativa en los procesos de emisión y firma de certificados de TSA, están descritos en la Declaración de Prácticas de Certificación (DPC) de PKIBDE.

En este apartado se recogen los controles de seguridad técnica a cumplir por una Autoridad de Sellado de Tiempo titular de un certificado emitido bajo esta PC.

6.1 Generación e Instalación del par de claves

6.1.1 Generación del par de claves

La generación de claves para los certificados de Autoridad de Sellado de Tiempo se debe llevar a cabo por la propia TSA en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3 o similar, y según tenga establecido en sus Políticas y Prácticas de Sellado de Tiempo.

6.1.2 Entrega de la clave privada al titular

No procede, puesto que la clave privada siempre la debe generar la TSA

6.1.3 Entrega de la clave publica al emisor del certificado

La clave pública se proporciona mediante un fichero en formato PKCS#10 adjunto a la solicitud, constituyendo la petición de certificado (CSR).

6.1.4 Entrega de la clave pública de la AC a los terceros aceptantes

La clave pública de la AC Corporativa está incluida en el certificado de dicha AC. El certificado de la AC Corporativa no viene incluido en el certificado generado para el titular. El certificado de la AC Corporativa debe ser obtenido del repositorio especificado en este documento donde queda a disposición de los titulares de certificados y terceros aceptantes para realizar cualquier tipo de comprobación.

6.1.5 Tamaño de las claves

El tamaño mínimo de las claves de los Certificados de TSA es de 2048 bits.

6.1.6 Parámetros de generación de la clave pública y verificación de la calidad

La clave pública de los Certificados de TSA está codificada de acuerdo con RFC 5280 y PKCS#1. El algoritmo de generación de claves es el RSA.

6.1.7 Fines del uso de la clave (campo KeyUsage de X.509 v3)

Las claves definidas por la presente política, y por consiguiente los certificados asociados, se utilizarán para la prestación de servicios de sellado de tiempo y, en particular, para la emisión de sellos de tiempo por parte de la TSA titular del certificado.

A tal efecto, en los campos '*Key Usage*' y '*Extended Key Usage*' de los certificados se han incluido los siguientes usos:

Tipo de certificado	Key Usage	Extended Key Usage
Certificado de TSA	digitalSignature nonRepudiation	TimeStamping

6.2 Protección de la clave privada y controles de ingeniería de los módulos criptográficos

6.2.1 Estándares para los módulos criptográficos

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

En particular, deberá disponer de un nivel de seguridad equivalente o superior a FIPS 140-2 de nivel 3.

6.2.2 Control multipersona (k de n) de la clave privada

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.2.3 Custodia de la clave privada

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

En particular, las claves privadas de los Certificados de la TSA deben estar alojadas en dispositivos de hardware criptográfico con certificación equivalente o superior a FIPS-2 de nivel 3, y accesibles únicamente por la TSA.

6.2.4 Copia de seguridad de la clave privada

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.2.5 Archivo de la clave privada

Esta PC prohíbe el archivo de la clave privada de la TSA en un lugar distinto a un módulo criptográfico.

6.2.6 Transferencia de la clave privada a/desde el módulo criptográfico

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

En particular, las claves privadas se deben generar en el módulo criptográfico en el momento de la creación de cada una de las Unidades de Sellado de Tiempo (TSU) que conforman la TSA, y se guardan cifradas.

6.2.8 Método de activación de la clave privada

La activación por parte de la TSA de la clave privada asociada al certificado emitido según esta PC, se realizará según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.2.9 Método de desactivación de la clave privada

La desactivación por parte de la TSA de la clave privada asociada al certificado emitido según esta PC, se realizará según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.2.10 Método de destrucción de la clave privada

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.2.11 Clasificación de los módulos criptográficos

El módulo criptográfico de la TSA debe contar con certificación equivalente o superior a FIPS-2 de nivel 3. Las especificaciones concretas han de estar reflejadas en sus Políticas y Prácticas de Sellado de Tiempo.

6.3 Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

Según lo especificado en la DPC de PKIBDE.

6.3.2 Periodos operativos de los certificados y periodo de uso para el par de claves

Los Certificados de TSA y su par de claves asociados tienen un periodo de uso de 8 años, si bien en el momento de su emisión la AC Corporativa puede establecer periodos inferiores.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.4.2 Protección de los datos de activación

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.4.3 Otros aspectos de los datos de activación

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.5 Controles de seguridad informática

6.5.1 Requerimientos técnicos de seguridad específicos

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.5.2 Evaluación de la seguridad informática

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.6 Controles de seguridad del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.6.2 Controles de gestión de seguridad

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.6.3 Controles de seguridad del ciclo de vida

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.7 Controles de seguridad de la red

Según tenga especificado la TSA en sus Políticas y Prácticas de Sellado de Tiempo.

6.8 Sellado de tiempo

Los certificados emitidos bajo esta PC se podrán utilizar para la prestación de servicios de sellado de tiempo por parte de la TSA titular, y conforme tenga especificado en sus Políticas y Prácticas de Sellado de Tiempo.

En este sentido, dicha TSA deberá garantizar la seguridad de la hora incluida en los sellos de tiempo que emite, mediante su sincronización periódica con una fuente de tiempos fiable.

7 Perfiles de los Certificados, CRL y OCSP

7.1 Perfil de Certificado

7.1.1 Número de versión

Los Certificados de Autoridad de Sellado de Tiempo (TSA) emitidos por la AC Corporativa utilizan el estándar X.509 versión 3 (X.509 v3)

7.1.2 Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- *Subject Key Identifier*. Calificada como no crítica.
- *Authority Key Identifier*. Calificada como no crítica.
- *KeyUsage*. Calificada como crítica.
- *extKeyUsage*. Calificada como crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *BasicConstraint*. Calificada como crítica.
- *CRLDistributionPoint*. Calificada como no crítica.
- *Auth. Information Access*. Calificada como no crítica.
- *Subject Alternate Name*. Calificada como no crítica.
- *bdeCertType (1.3.6.1.4.1.19484.2.3.6)*. Calificada como no crítica.
- *bdeIssuerName* (*1.3.6.1.4.1.19484.2.3.17*). Calificada como no crítica.
- *bdeIssuerVAT (1.3.6.1.4.1.19484.2.3.18)*. Calificada como no crítica.

A continuación se recoge el perfil de los certificados de Autoridad de Sellado de Tiempo que emite PKIBDE.

Perfil de certificado de TSA de la PKI		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA–AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Validez	1 año	
6. Subject	CN=BANCO DE ESPAÑA-TSA *TEXTO_LIBRE*[1] O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 2048 (bit string)	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la TSA.	NO
2. Authority Key Identifier		NO
keyIdentifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora	
3. KeyUsage		SI
Digital Signature	1	
Non Repudiation	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	Time Stamping	SI
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1 (DPC)	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. @2015 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.11 (PC)	
Notice Reference	Certificado de Autoridad de Sellado de Tiempo sujeto a la Declaración de Prácticas de Certificación del Banco de España. @2015 Banco de España. Todos los derechos reservados.	
6. Subject Alternate Names	Dirección URL=http://pkitsa.bde.es	

[1] Texto libre que permitirá diferenciar entre certificados distintos generados para una misma Autoridad de Sellado de Tiempos que dispone de varias TSUs

Perfil de certificado de TSA de la PKI

CAMPO	CONTENIDO	CRÍTICA para extensiones
7. Basic Constraints		SI
Subject Type	Entidad Final	
Path Length Constraint	No se utilizará	
8. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	NO
9. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
10. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	AUTORIDAD DE SELLADO DE TIEMPO	NO
11. bdeIssuerName (1.3.6.1.4.1.19484.2.3.17)	BANCO DE ESPAÑA	NO
12. bdeIssuerVAT (1.3.6.1.4.1.19484.2.3.18)	VATES-V28000024	NO

7.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:
- SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
- SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- SHA-512 with RSA Encryption (1.2.840.113549.1.1.13)

7.1.4 Formatos de nombres

Los certificados emitidos por PKIBDE contienen el *Distinguished Name* X.500 del emisor y el del destinatario del certificado en los campos *issuer name* y *subject name* respectivamente.

7.1.5 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a *distinguished names* X.500, que son únicos y no ambiguos.

El atributo CN (*Common Name*) del DN será el que distingue a los DN entre sí. El resto de atributos tendrán lo siguientes valores fijos:

O=BANCO DE ESPAÑA, C=ES

7.1.6 Identificador de objeto (OID) de la Política de Certificación

El OID de la presente PC es 1.3.6.1.4.1.19484.2.2.11 Se le añade una extensión de formato X.Y que recoge la versión de la PC.

7.1.7 Uso de la extensión "PolicyConstraints"

No estipulado.

7.1.8 Sintaxis y semántica de los "PolicyQualifier"

La extensión Certificate Policies contiene los siguientes 'Policy Qualifiers':
- Elemento con identificador '1.3.6.1.4.1.19484.2.2.1', que se corresponde con la DPC. Incluye los calificadores: 'URL CPS' con la dirección web en la que se puede acceder a la DPC y a esta PC; 'Notice Reference' con una nota de texto sobre la DPC aplicable.
- Elemento con identificador '1.3.6.1.4.1.19484.2.2.11', que se corresponde con esta PC. Incluye el calificador 'Notice Reference' con una nota de texto sobre esta PC.

Dentro del apartado *7.1.2 Extensiones del certificado* se puede ver su contenido para los certificados regulados por esa política.

7.1.9 Tratamiento semántico para la extensión critica "CertificatePolicy"

No estipulado.

7.2 Perfil de CRL

7.2.1 Número de versión

Según lo especificado en la DPC de PKIBDE.

7.2.2 CRL y extensiones

Según lo especificado en la DPC de PKIBDE.

7.3 Perfil de OCSP

7.3.1 Número(s) de versión

Según lo especificado en la DPC de PKIBDE.

7.3.2 Extensiones OCSP

Según lo especificado en la DPC de PKIBDE.

8 Auditorías de cumplimiento y otros controles

8.1 Frecuencia o circunstancias de los controles para cada Autoridad

Según lo especificado en la DPC de PKIBDE.

8.2 Identificación/cualificación del auditor

Según lo especificado en la DPC de PKIBDE.

8.3 Relación entre el auditor y la Autoridad auditada

Según lo especificado en la DPC de PKIBDE.

8.4 Aspectos cubiertos por los controles

Según lo especificado en la DPC de PKIBDE.

8.5 Acciones a tomar como resultado de la detección de deficiencias

Según lo especificado en la DPC de PKIBDE.

8.6 Comunicación de resultados

Según lo especificado en la DPC de PKIBDE.

9 Otras cuestiones legales y de actividad

9.1 Tarifas

9.1.1 Tarifas de emisión de certificado o renovación

No se aplica ninguna tarifa sobre la emisión o renovación de certificados bajo el amparo de la presente Política de Certificación.

9.1.2 Tarifas de acceso a los certificados

El acceso a los certificados emitidos bajo esta Política es gratuito y por tanto no hay ninguna tarifa de aplicación sobre el mismo.

9.1.3 Tarifas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los certificados es libre y gratuita y por tanto no se aplicará ninguna tarifa.

9.1.4 Tarifas de otros servicios tales como información de políticas

No se aplicará ninguna tarifa por el servicio de información sobre esta política ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la redacción del presente documento.

9.1.5 Política de reembolso

Al no existir ninguna tarifa de aplicación para esta Política de Certificación no es necesaria ninguna política de reintegros.

9.2 Confidencialidad de la información

9.2.1 Ámbito de la información confidencial

Según lo especificado en la DPC de PKIBDE.

9.2.2 Información no confidencial

Según lo especificado en la DPC de PKIBDE.

9.2.3 Deber de secreto profesional

Según lo especificado en la DPC de PKIBDE.

9.3 Protección de la información personal

9.3.1 Política de protección de datos de carácter personal

Según lo especificado en la DPC de PKIBDE.

9.3.2 Información tratada como privada

Según lo especificado en la DPC de PKIBDE.

9.3.3 Información no calificada como privada

Según lo especificado en la DPC de PKIBDE.

9.3.4 Responsabilidad de la protección de los datos de carácter personal

Según lo especificado en la DPC de PKIBDE.

9.3.5 Comunicación y consentimiento para usar datos de carácter personal

Según lo especificado en la DPC de PKIBDE.

9.3.6 Revelación en el marco de un proceso judicial

Según lo especificado en la DPC de PKIBDE.

9.3.7 Otras circunstancias de publicación de información

Según lo especificado en la DPC de PKIBDE.

9.4 Derechos de propiedad Intelectual

Según lo especificado en la DPC de PKIBDE.

9.5 Obligaciones

9.5.1 Obligaciones de la AC

Según lo especificado en la DPC de PKIBDE.

9.5.2 Obligaciones de la AR

Según lo especificado en la DPC de PKIBDE.

9.5.3 Obligaciones de los titulares de los certificados

Sin perjuicio de lo especificado en la DPC de PKIBDE, las Autoridades de Sellado de Tiempo titulares de los certificados emitidos bajo la presente PC tendrán además las obligaciones siguientes:

- Tener implantada una "Política de Sellado de Tiempo" conforme a buenas prácticas reconocidas, para la prestación de servicios de sellado de tiempo.
- Disponer de un documento actualizado de "Políticas y Prácticas de Sellado de Tiempo" que recoja dicha política implantada, accesible de forma pública y gratuita, y en el que figuren sus responsables y se describan sus obligaciones y responsabilidades, procesos y procedimientos para la gestión y operación de la TSA, ciclo de vida de las claves, mecanismos de seguridad, etc.
- Garantizar el cumplimiento de todas las consideraciones, y prestar los servicios de sellado de tiempo conforme a los requisitos y procedimientos descritos en dicho documento de "Políticas y Prácticas de Sellado de Tiempo"
- Adherirse a cualquier recomendación y obligación adicional indicada por el Banco de España para la prestación de servicios de sellado de tiempo en esta PC.

9.5.4 Obligaciones de los terceros aceptantes

Sin perjuicio de lo especificado en la DPC de PKIBDE, los terceros aceptantes de los servicios de sellado de tiempo que se prestan mediante los certificados emitidos bajo esta PC, tendrán además las obligaciones siguientes:

- Tener conocimiento y asumir cualquier limitación en el uso de los sellos de tiempo firmados con los certificados emitidos bajo esta PC, indicada por las "Políticas y Prácticas de Sellado de Tiempo" correspondientes.
- Tener conocimiento y asumir cualquier otra precaución que tuviera establecida mediante acuerdo con la Autoridad de Sellado de Tiempo, para la obtención de servicios de sellado de tiempo.

9.5.5 Obligaciones de otros participantes

Según lo especificado en la DPC de PKIBDE.

9.6 Responsabilidades

9.6.1 Responsabilidades de PKIBDE

Según lo especificado en la DPC de PKIBDE.

9.6.2 Exención de responsabilidades de PKIBDE

Según lo especificado en la DPC de PKIBDE.

Del mismo modo, PKIBDE en tanto que Prestador de Servicios de Certificación, no se responsabiliza de los servicios de sellado de tiempo ofrecidos mediante sus certificados, y en particular, del contenido, fiabilidad y precisión de la hora incluida en los sellos de tiempo firmados y emitidos con sus certificados.

Asimismo, tampoco se responsabiliza por los daños y perjuicios que se pudieran derivar por parte del prestador de los servicios de sellado de tiempo, causados por el incumplimiento de las obligaciones y responsabilidades recogidas sus "Políticas y Prácticas de Sellado de Tiempo" o en esta PC.

9.6.3 Alcance de la cobertura

Según lo especificado en la DPC de PKIBDE.

9.7 Limitaciones de pérdidas

Según lo especificado en la DPC de PKIBDE.

9.8 Periodo de validez

9.8.1 Plazo

Esta PC entrará en vigor desde el momento de su publicación en el repositorio de PKIBDE.

Esta PC está en vigor mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la AC Corporativa, ocasión en que obligatoriamente se emitirá una nueva versión.

9.8.2 Sustitución y derogación de la PC

Esta PC será siempre sustituida por una nueva versión con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad.

Cuando la PC quede derogada se retirará del repositorio público de PKIBDE, si bien se conservará durante 15 años.

9.8.3 Efectos de la finalización

Las obligaciones y restricciones que establece esta PC, en referencia a auditorías, información confidencial, obligaciones y responsabilidades de PKIBDE, nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

9.9 Notificaciones individuales y comunicaciones con los participantes

Según lo especificado en la DPC de PKIBDE.

9.10 Procedimientos de cambios en las especificaciones

9.10.1 Procedimiento para los cambios

Según lo especificado en la DPC de PKIBDE.

9.10.2 Periodo y mecanismo de notificación

Según lo especificado en la DPC de PKIBDE.

9.10.3 Circunstancias en las que el OID debe ser cambiado

Según lo especificado en la DPC de PKIBDE.

9.11 Reclamaciones y jurisdicción

Según lo especificado en la DPC de PKIBDE.

9.12 Normativa aplicable

Según lo especificado en la DPC de PKIBDE.

9.13 Cumplimiento de la normativa aplicable

Según lo especificado en la DPC de PKIBDE.

9.14 Estipulaciones diversas

9.14.1 Cláusula de aceptación completa

Según lo especificado en la DPC de PKIBDE.

9.14.2 Independencia

En el caso que una o más estipulaciones de esta PC sea o llegase a ser inválida, nula, o inexigible legalmente, se entenderá por no puesta, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la PC careciera ésta de toda eficacia jurídica.

9.14.3 Resolución por la vía judicial

No estipulado.

9.15 Otras estipulaciones

No estipulado.

10 Protección de datos de carácter personal

10.1 Régimen jurídico de protección de datos

Según lo especificado en la DPC de PKIBDE.

10.2 Creación del fichero e inscripción registral

Según lo especificado en la DPC de PKIBDE.

10.3 Documento de seguridad LOPD

Según lo especificado en la DPC de PKIBDE.