BANCO DE ESPAÑA
Eurosistema

11.05.2015

OID: 1.3.6.1.4.1.19484.2.2.101

Infraestructura de Clave Pública del Banco de España

Política de Certificación para certificados de componente de entidades externas

RESUMEN Este documento recoge la Política de Certificación (PC) que rige los certificados de componente emitidos por la Autoridad de Certificación Corporativa de la Infraestructura de Clave Pública (PKI) del Banco de España para entidades externas.

Hoja de Control

Título	Política de Certificación para certificados de componente de entidades externas
Autor	Departamento de Sistemas de Información
Versión	1.2
Fecha	11.05.2015

Registro de Cambios

Versión	**Fecha**	**Motivo del cambio**
1.0	5.04.2006	Primera versión
1.1	25.05.2010	Revisión tras implantación de servicios de fechado electrónico Renombrado de la Autoridad de Aprobación de Políticas a Autoridad de Administración de Políticas
1.2	11.05.2015	Actualización con motivo de la renovación de las Autoridades de Certificación

ÍNDICE

1 Introducción

1.1 Resumen

Este documento recoge la Política de Certificación (PC) que rige los certificados de componente emitidos por la Autoridad de Certificación Corporativa de la Infraestructura de Clave Pública del Banco de España (desde ahora PKIBDE) para entidades externas con las que el Banco intercambia información de forma telemática.

Esta Política de Certificación rige todos los certificados de componente emitidos por PKIBDE para entidades externas, en concreto los siguientes:

- Certificados genéricos para componentes de entidades externas.

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.

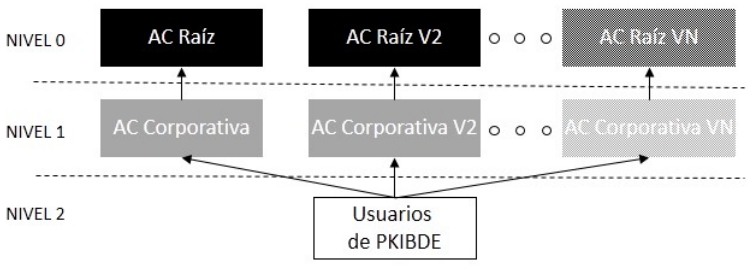
En esta PC se detalla y completa lo estipulado en la "Declaración de Prácticas de Certificación" (DPC) de la PKI del Banco de España, conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este 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 componente para entidades externas en su ciclo de vida, y sirve de guía de la relación entre la AC Corporativa y sus usuarios. 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 y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

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



[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.

1.2 Nombre del documento e identificación

Nombre del documento	Política de Certificación (PC) para certificados de entidades externas
Versión del documento	1.2
Estado del documento	Aprobada
Fecha de emisión	11.05.2015
OID (Object Identifier)	1.3.6.1.4.1.19484.2.2.101
Ubicación de la DPC	http://pki.bde.es/politicas
DPC Relacionada	Declaración de Prácticas 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 de PKIBDE.

1.3.2 Autoridades de Certificación

Se define Autoridades de Certificación de acuerdo con la Declaración de Prácticas de Certificación 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

- **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[2]:

1.3.2.2 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[3]:

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

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

- 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
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.

1.3.2.3 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[4]:

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
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.

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

1.3.3 Autoridades de Registro

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

La emisión de certificados de componente para entidades externas se realizará mediante la utilización de una serie de puestos remotos de Autoridad de Registro, los cuales permitirán a los diferentes Administradores Remotos de la AC designados por PKIBDE solicitar y descargar dichos certificados.

Estos Administradores dispondrán de certificados de autenticación emitidos por la AC Corporativa. Mediante estos certificados y haciendo uso de una interfaz de administración, actuarán en representación de los responsables de los componentes, generando peticiones de certificación/revocación. La AC comprobará si el puesto remoto está autorizado para el envío de peticiones y si es así las procesará. En el caso de una petición de certificación devolverá el certificado para que el Administrador Remoto se lo entregue al responsable del componente. En el caso de una petición de revocación devolverá el resultado de la operación.

1.3.4 Autoridad de Validación

Se define Autoridad de Validación de acuerdo con la Declaración de Prácticas de Certificación de PKIBDE.

1.3.5 Archivo de Claves

El Archivo de Claves definido en la Declaración de Prácticas de Certificación no tiene aplicación en esta política de certificación.

1.3.6 Titulares de los certificados

Se define Titular de acuerdo con la Declaración de Prácticas de Certificación de PKIBDE.

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

Entorno de Certificación	Titulares
AC Corporativa	Componentes (Sistemas y Servicios corporativos) de la entidad externa

Aunque se trata de certificados de componente, para cada uno debe haber una persona responsable. El tipo de personas que pueden serlo se recogen en la siguiente tabla:

Tipo de certificado	Responsable
Certificados genéricos para componentes de entidades externas	Responsable del componente de la entidad externa

1.3.7 Terceros aceptantes

Como Terceros Aceptantes se entienden aquellos que hagan uso de los certificados para identificar a los componentes (servidores, aplicaciones, código,…) para los que se ha expedido el certificado o para intercambiar con ellos información cifrada.

1.3.8 Otros afectados

Solicitantes: personas físicas que han solicitado la emisión de un certificado a PKIBDE para un componente de entidad externa.

Administradores Remotos de la AC: personas que dentro del Banco de España gestionan las peticiones de certificados de componente teniendo privilegios de administración remota de la AC.

1.4 Uso de los certificados

1.4.1 Usos apropiados de los certificados

Los certificados regulados por esta PC se utilizarán para la autenticación de componentes y el cifrado de comunicaciones en el entorno de los sistemas de información del Banco de España.
En la siguiente tabla se recoge con más detalle los usos apropiados en función del tipo de certificado de componente de que se trate:

Tipo de certificado	Usos apropiados
Certificados genéricos para componentes de entidad externa	Autenticación de componentes y cifrado de comunicaciones

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 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 PKI del Banco de España:

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.

Certificado electrónico: un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma (clave pública) 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, o sesión, terminando su utilidad una vez finalizada ésta.

Componente informático (o componente): cualquier dispositivo software o hardware susceptible de utilizar certificados electrónicos para su propio uso, con el objeto de identificarse o intercambiar datos firmados o cifrados con terceros aceptantes.

Directorio: repositorio de información al que se accede a través del protocolo LDAP.

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.

Infraestructura de Clave Pública: es el conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, cifrado, integridad

y no repudio, mediante el uso de criptografía de claves públicas y privadas y de certificados electrónicos.

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 física que solicita un certificado para sí mismo o para un componente informático.

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

Titular: persona o componente informático para el que se expide un certificado electrónico y es aceptado por éste o por su responsable en el caso de los certificados de componente.

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 Revocación de Certificados)

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

CDP: CRL Distribution Point (Punto de Distribución de CRLs)

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

CSR: Certificate Signing Request (petición de certificado). Conjunto de datos, que contienen una clave pública y su firma electrónica utilizando la clave privada asociada, enviado a la Autoridad de Certificación para la emisión de un certificado electrónico que contenga dicha clave pública

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

PIN: Personal Identification Number (número de identificación personal). Contraseña que protege el acceso a una tarjeta criptográfica.

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

PSC: Prestador de Servicios de Certificación.

PUK: PIN UnlocK Code (código o clave de desbloqueo del PIN). Contraseña que permite desbloquear una tarjeta criptográfica que ha sido bloqueada por introducción consecutiva de un PIN incorrecto.

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

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 ha de hacer referencia a la entidad propietaria del componente informático desde el que se va a utilizar el certificado. También se incluirá en el CN información sobre el mecanismo de identificación que se ha seguido para la emisión del certificado. Por otra parte, se especificará el tipo de componente informático a través de un prefijo en el CN.

El CN del certificado de componente será el siguiente:

Tipo de certificado	CN
Certificado genérico para componentes de entidades externas	CN=[EG] *CIF metodo_identif num_dif*

Siendo:

CIF, el código de identificación fiscal asignado por la Agencia Estatal de Administración Tributaria a la persona jurídica responsable del componente para el que se solicita el certificado.

metodo_identif, un identificador del mecanismo de reconocimiento que se ha llevado a cabo para la emisión del certificado, pudiendo tener los siguientes valores:

- **RI-<Código de unidad administrativa>**, si alguna unidad administrativa (UA) interna del Banco de España ha dado el visto bueno a la emisión del certificado, dicha UA será identificada por su código dentro del propio certificado.
- **RE-<Identificador de tipo de certificado utilizado en la solicitud[5]>**. En el certificado de componente que se emita se incluirá la información necesaria para identificar al PSC y a la política de certificación asociada al certificado con el que se firma la solicitud, si ésta ha sido firmada electrónicamente utilizando un certificado emitido por un PSC externo al Banco de España.

num_dif, un número que permitirá diferenciar entre certificados distintos generados para una misma entidad cuya emisión ha sido aprobada mediante el mismo método de identificación.

Un ejemplo del campo CN es el siguiente: *CN=[EG] G28000024 RI-C361A 0001*

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

- OU=COMPONENTES, O=<nombre de la entidad>, C=ES

Siendo <nombre de la entidad> el nombre de la identidad identificada por el CIF incluido en el atributo CN del certificado.

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.

[5] La lista de identificadores de tipos de certificado existentes está disponible en la dirección http://pki.bde.es

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. La utilización del CIF de componente garantiza la unicidad del DN. En el caso de que se emita más de un componente informático para una misma entidad, se diferenciarán dichos componentes por el mecanismo de identificación utilizado en la emisión del certificado. No podrá existir más de un certificado de componente informático de un mismo tipo para una misma entidad emitido utilizando un mismo mecanismo de identificación.

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

En los casos en que el par de claves de los certificados de componentes los genere la AC Corporativa no se aplicará este apartado.

En los casos en que el par de claves los genere la entidad propietaria del componente, la posesión de la clave privada, correspondiente a la clave pública para la que 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 componente para entidades externas 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.

Sin embargo, para garantizar que el componente informático desde el que se va a utilizar el certificado es propiedad de la entidad indicada en el propio certificado, existirán dos procedimientos de identificación alternativos:

a Que la solicitud de la emisión del certificado esté firmada electrónicamente utilizando un certificado de persona jurídica emitido por un PSC reconocido por el Banco de España a tal efecto. En tal caso, se incluirá en el CN del certificado un identificador que permita conocer qué PSC y bajo qué política de certificación concreta ha emitido el certificado con el que ha solicitado la emisión del certificado de componente. La validación de la identidad de la persona jurídica se habrá realizado conforme a los procedimientos establecidos por el PSC.

b Que la solicitud de la emisión del certificado esté firmada de forma manuscrita por una persona física que represente a la entidad propietaria del componente informático y que conste como tal en el Banco de España. En tal caso, se incluirá en el CN del certificado el código de la unidad administrativa encargada de validar la firma.

3.2.3 Autenticación de la identidad de una persona física

No aplica.

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

En el caso de que la solicitud del certificado se realice mediante la firma electrónica generada a través de un certificado de persona jurídica emitido por un PSC reconocido por el Banco de España, se presumirá que la persona física que está utilizando dicho certificado de persona jurídica tiene capacidad para hacerlo.

En los demás casos, las facultades de representación deberán constar previamente en el 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 componente emitidos por la AC Corporativa para entidades externas. Aunque estos certificados se van a almacenar en los propios componentes informáticos o 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 componente la ha de efectuar la persona designada como responsable de dicho componente por la entidad externa.
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 componente para entidades externas.

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

Existen dos tipos de proceso en función del mecanismo de solicitud utilizado.

Solicitud firmada electrónicamente mediante un certificado de persona jurídica emitido por un PSC

En este caso, el procedimiento es como sigue:

1 La solicitud se envía por correo electrónico firmado electrónicamente mediante un certificado de persona jurídica emitido por un PSC reconocido por el Banco de España a tales efectos. En cuanto al contenido de la petición existen dos posibilidades:

a Si la entidad opta por generar la pareja de claves, la solicitud ha de incluir la petición de certificado (CSR) con la clave pública así como la información necesaria para que la AC genere el certificado.

b Si la entidad decide que el Banco de España genere la pareja de claves, pública y privada, la solicitud incluye sólo la información necesaria para generar el certificado.

2 El administrador remoto recibirá el mensaje y verificará la firma electrónica. En caso de que la firma se verifique correctamente, solicitará a la Autoridad de Certificación:

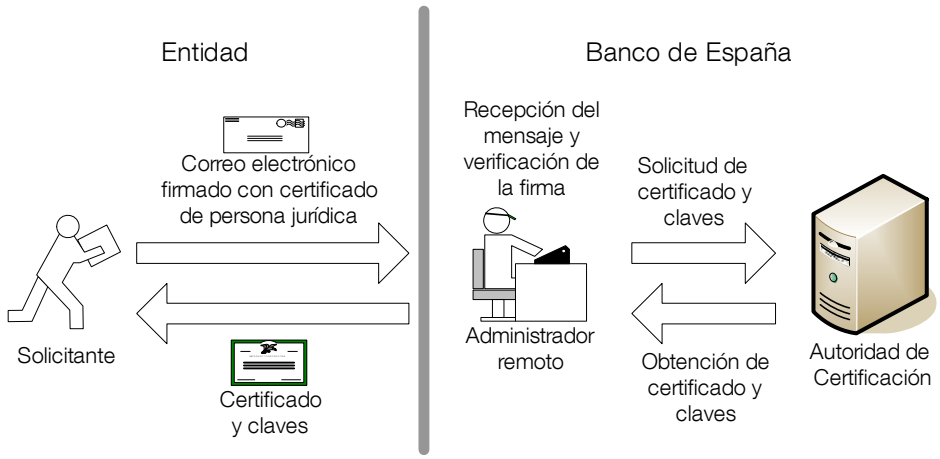
a La emisión del certificado, si la entidad ha enviado la solicitud de certificado (CSR) con la clave pública.

b La generación de una pareja de claves y la emisión del certificado asociado a la pública, si la entidad ha elegido esta opción.

3 La AC emite el certificado y, en su caso, genera la pareja de claves, y el administrador remoto descarga el correspondiente fichero con el certificado o bien un fichero con la clave privada y el certificado, cifrado por una contraseña conocida por él.

4 El Banco de España envía mediante correo electrónico al solicitante el certificado o el fichero con las claves. En este segundo caso, envía la contraseña a través de un mensaje de correo electrónico cifrado mediante el certificado de persona jurídica que la entidad utilizó para la firma de la solicitud.

En la siguiente figura se sintetiza el proceso descrito:



Solicitud firmada de forma manuscrita

En este caso, los pasos a seguir son los siguientes:

1 La solicitud ha de incluir un teléfono de contacto y la información necesaria para generar el certificado, así como el nombre o código de la unidad administrativa (departamento) del Banco de España que ha de validar la petición. Por otra parte:

a Si la entidad opta por generar la pareja de claves, la solicitud ha de incluir un disquete o CDROM con la petición de certificado (CSR), que ha de contener la clave pública.

b Si la entidad decide que el Banco de España genere la pareja de claves, se ha de indicar dicha opción en la solicitud.

2 La unidad administrativa del Banco indicada en la petición verificará la firma de la misma.

3 En caso de que la unidad administrativa correspondiente de el visto bueno a la emisión del certificado, un administrador remoto de la AC solicitará a ésta:

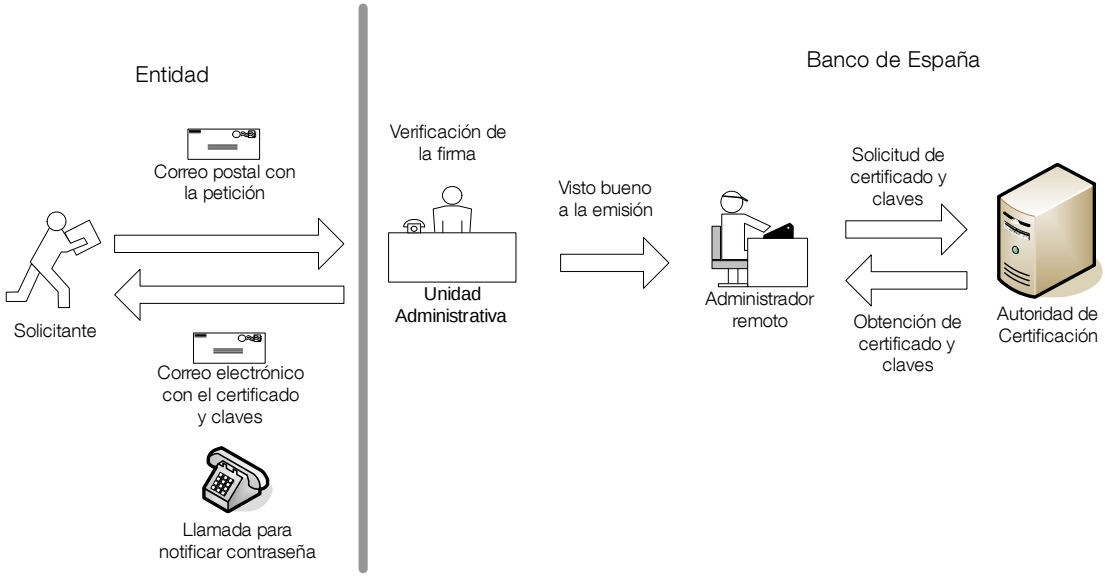
a La emisión del certificado, si la entidad ha enviado una petición de certificado (CSR) con la clave pública.

b La generación de una pareja de claves y la emisión del certificado asociado a la pública, si la entidad ha elegido esta opción.

4 La AC emite el certificado y, en su caso, genera la pareja de claves, y el administrador remoto descarga el correspondiente fichero con el certificado o bien un fichero con la clave privada y el certificado, cifrado por una contraseña conocida por él.

5 El Banco de España envía mediante correo electrónico al solicitante el certificado o el fichero cifrado con la clave privada y el certificado. En este segundo caso, notifica telefónicamente la contraseña con la que está cifrado dicho fichero.

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

La forma en la que se realiza la identificación y autenticación depende del modo en el que se haya realizado la petición:

- Si la petición se ha realizado por correo electrónico firmado con un certificado de persona jurídica emitido por un PSC reconocido a tal efecto por el Banco de España, la identificación y autenticación la realiza el administrador remoto mediante la firma electrónica.
- Si la petición se ha firmado de forma manuscrita, la identificación y la autenticación del solicitante la realiza la unidad administrativa indicada en la petición.

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.

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. del presente 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 de componente 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 componente 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. 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.

Los certificados de componente regulados por esta PC sólo pueden ser utilizados para prestar los siguientes servicios de seguridad:

Tipo de certificado	Usos apropiados
Certificados genéricos para componentes de entidad externa	Autenticación de componentes y cifrado de comunicaciones

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

Los Terceros Aceptantes sólo pueden depositar su confianza en los certificados para aquello que establece esta PC 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 componente 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 del componente titular del certificado.

4.7.3 Tramitación de las peticiones de renovación de certificados 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 del componente.

La identificación y autenticación para la renovación de un certificado de componente es la misma que para su emisión inicial.

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.

El proceso de renovación es análogo al de emisión inicial por lo que no se describe de nuevo.

4.7.4 Notificación de la emisión de un nuevo certificado al titular

Se notificará mediante correo electrónico.

4.7.5 Forma de aceptación del certificado con las claves cambiadas

El solicitante deberá confirmar la aceptación del certificado de componente y sus condiciones mediante firma del documento que se establezca al tal efecto.

4.7.6 Publicación del certificado con las nuevas claves por la AC

El certificado de componente 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 PC 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.

Un certificado de componente puede ser revocado por:

- 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 componente deja de estar en servicio.
- 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 del componente o por tercero autorizado o la persona física solicitante en representación de una persona jurídica.
- El certificado de una AR o 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 válido. La revocación no afectará a las obligaciones subyacentes creadas o comunicadas por esta PC 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 del titular, o cualquier otro hecho determinante que recomendara emprender dicha acción.

Asimismo, los responsables de los componentes también podrán 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 del componente de forma semejante a la descrita en el apartado 4.1.2 para la solicitud de emisión. Las tramitará siempre el Administrador remoto de la AC.

Además de esta vía ordinaria, los Operadores y Administradores de la PKI 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 componente 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 componente.

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'[6], aun no estando caducadas, no garantizan que dispongan de información de revocación actualizada.

4.9.7 Frecuencia de emisión de CRLs

Según lo especificado en la DPC de PKIBDE.

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

No existe un sistema en línea de verificación del estado de los certificados accesible para las entidades externas.

Las direcciones de acceso vía web a las CRL quedan reflejadas en el apartado *2.1 Repositorio*.

4.9.10 Requisitos de comprobación en-línea de revocación

No aplicable, ya que no existe un mecanismo de comprobación en-línea de revocación accesible por las entidades externas.

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 componente.

[6] 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.

4.9.14 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 de componente.

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
No estipulado.

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, están descritos en la DPC de PKIBDE.
En este apartado se recogen los controles de seguridad técnica para la emisión de certificados 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 componente para entidades externas, en el caso de que sea realizada por la AC Corporativa del Banco de España, se lleva a cabo en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3.
En el caso de que sea realizada por la entidad, se utilizarán las librerías criptográficas del navegador desde el que se realice la solicitud.

6.1.2 Entrega de la clave privada al titular

En los casos en que se entrega de clave privada por haberla generado la AC del Banco de España, esta entrega se efectúa mediante correo electrónico al responsable del componente adjuntando un fichero en formato PKCS#12, cifrado con una contraseña.
La contraseña se entregará de la siguiente forma:

- Si la solicitud del certificado se realizó mediante un correo electrónico firmado con un certificado de persona jurídica emitido por un PSC reconocido por el Banco de España para ese propósito, la contraseña se enviará mediante correo electrónico cifrado utilizando dicho certificado.
- Si la solicitud del certificado se realizó conforme a una firma manuscrita validada por una unidad administrativa interna del Banco de España, la contraseña se hará llegar telefónicamente al responsable del componente.

En los casos en que las claves hayan sido generadas por la entidad, no se produce entrega de clave privada.

6.1.3 Entrega de la clave publica al emisor del certificado

En los casos en que el par de claves lo haya generado la entidad, la clave pública se proporciona mediante un fichero en formato PKCS#10 adjunto a la solicitud, constituyendo la petición de certificado (CSR).
En los casos en que el par de claves lo haya generado la propia AC Corporativa, la clave pública se entregará dentro del fichero PKCS#12 indicado en el apartado anterior.

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 componente para persona jurídica es de 1024 bits.

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

La clave pública de los certificados de componente 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 utilizará para las operaciones de componentes que requieran autenticación, firma electrónica o cifrado frente a los sistemas de información del Banco de España.

A tal efecto, en los campos 'Key Usage' y 'Extended Key Usage' del certificado se han incluido los siguientes usos:

Tipo certificado	Key Usage	Extended Key Usage
Certificados genéricos de componentes para entidades externas	digitalSignature. dataEncipherment. keyEncipherment. keyAgreement	emailProtection clientAuth anyExtendedKeyUsage

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

6.2.1 Estándares para los módulos criptográficos

El módulo utilizado para la creación de claves utilizadas por la AC Corporativa de PKIBDE tiene la certificación FIPS 140-2 de nivel 3.

La puesta en marcha de cada una de las Autoridades de Certificación, contando con que se utiliza un módulo Criptográfico de seguridad (HSM) conlleva las siguientes tareas:

a Inicialización del estado del módulo HSM.

b Creación de las tarjetas de administración y de operador.

c Generación de las claves de la AC.

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

La clave privada, tanto de la AC Raíz como de AC Subordinada, se encuentra bajo control multipersona cuya activación se realiza mediante la inicialización del software de AC por medio de una combinación de operadores de la AC.

Éste es el único método de activación de dicha clave privada.

No se establece control multipersona para el acceso a las claves privadas de los certificados emitidos bajo esta PC.

6.2.3 Custodia de la clave privada

Las claves privadas de los certificados de componente se encuentran alojadas en el propio componente o en dispositivos adicionales, debiendo estar protegido el acceso a las operaciones con las mismas mediante contraseña.

6.2.4 Copia de seguridad de la clave privada

Dado que la responsabilidad de la custodia de las claves privadas corresponde a las entidades titulares de los certificados emitidos bajo esta PC, se recomienda a éstas últimas realizar copias de seguridad para evitar su pérdida o deterioro.

6.2.5 Archivo de la clave privada

La AC Corporativa una vez finalizado el proceso de emisión del certificado de componente conserva copia de su clave privada en los casos en que la haya generado.

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

No estipulado.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

En el caso de que la AC de PKIBDE genere las claves privadas, éstas son creadas en el módulo criptográfico de la AC Corporativa pero posteriormente no se conservan.

Esta PC no establece ningún requisito de almacenamiento en módulo criptográfico en el caso de que sea la entidad la que genera las claves privadas.

6.2.8 Método de activación de la clave privada

En los casos en que la clave privada la genera la AC se proporciona en un fichero PKCS#12 protegido mediante una contraseña. La entidad deberá importar la clave en el componente informático desde el que la utilizará, por lo que la activación posterior se hará conforme a las especificaciones de dicho componente.

En los casos en que la genera la entidad, su activación una vez obtenido el certificado, se hará conforme a las especificaciones del componente informático desde el que la entidad utilice la clave privada y el certificado.

6.2.9 Método de desactivación de la clave privada

No estipulado.

6.2.10 Método de destrucción de la clave privada

No estipulado.

6.2.11 Clasificación de los módulos criptográficos

Para el caso de que sea la Autoridad de Certificación la que realice la generación de las claves, los módulos criptográficos utilizados cumplen el estándar FIPS 140-2 nivel 3.

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 componentes y su par de claves asociados tienen un periodo de uso de 4 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 lo especificado en la DPC de PKIBDE.

6.4.2 Protección de los datos de activación

Según lo especificado en la DPC de PKIBDE.

6.4.3 Otros aspectos de los datos de activación

Según lo especificado en la DPC de PKIBDE.

6.5 Controles de seguridad informática

6.5.1 Requerimientos técnicos de seguridad específicos

Según lo especificado en la DPC de PKIBDE.

6.5.2 Evaluación de la seguridad informática

Según lo especificado en la DPC de PKIBDE.

6.6 Controles de seguridad del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Según lo especificado en la DPC de PKIBDE.

6.6.2 Controles de gestión de seguridad

Según lo especificado en la DPC de PKIBDE.

6.6.3 Controles de seguridad del ciclo de vida

Según lo especificado en la DPC de PKIBDE.

6.7 Controles de seguridad de la red

Según lo especificado en la DPC de PKIBDE.

6.8 Sellado de tiempo

Según lo especificado en la DPC de PKIBDE.

7 Perfiles de los Certificados, CRL y OCSP

7.1 Perfil de Certificado

7.1.1 Número de versión

Los certificados de componente emitidos por la AC Corporativa para entidades externas 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 no crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *SubjectAlternativeName*. Calificada como no crítica.
- *BasicConstraints*. Calificada como crítica.
- *CRLDistributionPoint*. Calificada como no crítica.
- *Auth. Information Access*. Calificada como no crítica.
- *NetscapeCertType*. Calificada como no crítica.
- *bdeCertType (1.3.6.1.4.1.19484.2.3.6)*. Calificada como no crítica.

A continuación se recogen los perfiles de los tipos de certificados de componente que emite PKIBDE para entidades externas:

Perfil de certificado genérico para componentes de entidades externas		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA-256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Validez	4 años	
6. Subject	CN=[EG] CIF_Entidad RI-<Cód unidad administrativa>[1] ó CN=[EG] CIF_Entidad RE-<Id.cert. usado en la solicitud>[2]-<Id de secuencia> OU=COMPONENTES O=<Nombre de la Entidad> C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud mínima de clave: 2048	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Authority Key Identifier		NO
keyIdentifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		SI
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	1	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	clientAuth, emailProtection, anyExtendedKeyUsage	NO
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	1.3.6.1.4.1.19484.2.2.101	

[1] <Cód unidad administrativa>: código de la unidad administrativa interna del Banco de España que ha aprobado la petición del certificado

[2] <Id.cert. usado en la solicitud>: identificador del Prestador de Servicios de Certificación y Política de Certificación que se ha utilizado para emitir el certificado de persona jurídica utilizado para solicitar el certificado de componente. La lista de identificadores posibles está ubicada en http://pki.bde.es

Notice Reference	Certificado de componente informático para Entidades externas 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 email según RFC 822 (opcional) 1.3.6.1.4.1.19484.2.3.8 Nombre de entidad (obligatorio) 1.3.6.1.4.1.19484.2.3.9 CIF de entidad (obligatorio) 1.3.6.1.4.1.19484.2.3.10 Tipo validación. (obligatorio)[1] 1.3.6.1.4.1.19484.2.3.11 Id. Validación (obligatorio)[2] 1.3.6.1.4.1.19484.2.3.12 Tipo código BE (opcional)[3] 1.3.6.1.4.1.19484.2.3.13 Código BE (opcional)[4] 1.3.6.1.4.1.19484.2.3.14 Número diferenc. (obligatorio)[5]	NO
7. Basic Constraints		SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
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)	EXTER_COMPONENTE_GENERICO	

[1] Tipo de validación: *RI*, aprobación de solicitud de certificado por una unidad administrativa interna del BE; *RE*, solicitud de certificado conforme a un certificado de persona jurídica emitido por un PSC externo

[2] Identificador de mecanismo de validación: código de la unidad administrativa que ha aprobado la petición del certificado o identificador del tipo de certificado de persona jurídica que se ha utilizado para solicitar el certificado

[3] Tipo de código Banco de España de la entidad. Podrá ser REN o SIC

[4] Valor del código Banco de España de la entidad. Podrá existir en caso de que la entidad disponga de un código asignado por el BE.

[5] Número diferenciador: Número utilizado para diferenciar certificados de una misma entidad.

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 los siguientes valores:

OU=COMPONENTE, O=<NOMBRE DE LA ENTIDAD>, 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. 2.2.101. 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 dos elementos de información, 'Policy Information':

- 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 '1.3.6.1.4.1.19484.2.2.101', 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.

Los servicios prestados por la AC en el contexto de esta PC son los servicios de emisión, renovación y revocación de certificados de componente.

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

Según lo especificado en la DPC de PKIBDE.

9.5.4 Obligaciones de los terceros aceptantes

Según lo especificado en la DPC de PKIBDE.

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.

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 aprobación por la AAP y 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.