BANCO DE ESPAÑA

5.04.2006

OID: 1.3.6.1.4.1.19484.2.2.8.1.0

Infraestructura de Clave Pública del Banco de España

Política de Certificación para certificados de cifrado

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

Hoja de Control

Título	Política de Certificación para certificados de cifrado
Autor	Secretaría General Departamento Jurídico Departamento de Sistemas de Información y Procesos
Versión	1.0
Fecha	5.04.2006

Registro de Cambios

Versión	**Fecha**	**Motivo del cambio**
1.0	5.04.2006	Primera versión

ÍNDICE

1 Introducción

1.1 Resumen

Este documento recoge la Política de Certificación (PC) que rige los certificados de cifrado de personas emitidos por la Autoridad de Certificación Corporativa de la Infraestructura de Clave Pública (en adelante PKI) del Banco de España (desde ahora PKIBDE).

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.

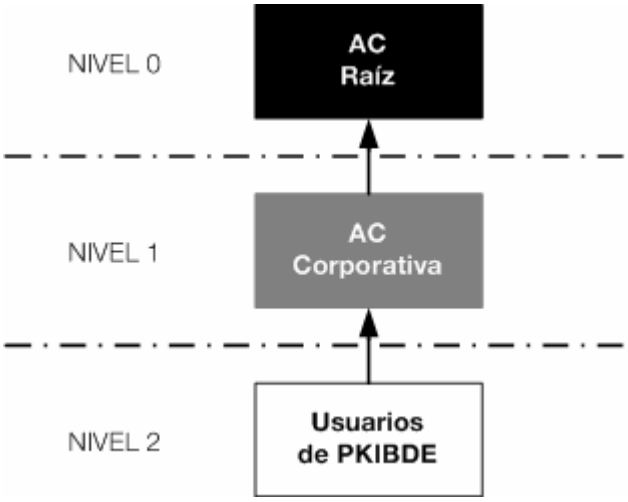
En esta PC se detalla y completa lo estipulado en la "Declaración de Prácticas de Certificación" (DPC) de la PKI del Banco de España (PKIBDE), conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas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



1.2 Nombre del documento e identificación

Nombre del documento	Política de Certificación (PC) para certificados de cifrado
Versión del documento	1.0
Estado del documento	Aprobado
Fecha de emisión	5/04/2006
OID (Object Identifier)	1.3.6.1.4.1.19484.2.2.8.1.0
Ubicación de la DPC	http://pki.bde.es/politicas
DPC Relacionada	Declaración de Prácticas de Certificación de la PKI del Banco de España OID 1.3.6.1.4.19484.2.2.1

1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes son:

- El Banco de España como titular de PKIBDE.
- La Autoridad de Aprobación 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 Aprobación de Políticas

Se define Autoridad de Aprobación 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 componen PKIBDE son:

- **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 Corporativa**: Autoridad de Certificación subordinada de la AC Raíz. Su función es la emisión de certificados para los usuarios de PKIBDE. Esta PC hace referencia a los certificados de cifrado emitidos por la misma. 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

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 cifrado se realiza con la intervención de la AR Corporativa, gestionándose las peticiones de modo remoto.

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

La presente Política de Certificación establece la existencia de un Archivo de Claves para el archivo y recuperación de las claves privadas de los certificados de cifrado. El Archivo de Claves garantiza la confidencialidad de la clave privada y su recuperación exige, como mínimo, la intervención de dos personas. En esta PC se regulan los procedimientos de petición y tramitación de recuperación de claves.

1.3.6 Titulares de los certificados

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

Los tipos de personas que pueden ser titulares de certificados de cifrado de la AC Corporativa se restringen a los recogidos en el siguiente cuadro:

Entorno de Certificación	Titulares
AC Corporativa	Empleados del Banco de España
	Colaboradores del Banco de España
	Personal de empresas contratadas con acceso a los sistemas de información del Banco de España

1.3.7 Terceros aceptantes

Como Terceros Aceptantes se entienden aquellos que hagan uso de los certificados para establecer comunicaciones cifradas con las personas titulares de certificados de cifrado de la AC Corporativa de PKIBDE.

1.3.8 Otros afectados

Solicitantes: personas físicas que han solicitado la emisión de un certificado a PKIBDE.
Administradores de usuarios: personas que dentro del Banco de España gestionan las peticiones de certificados personales y verifican su correcta obtención.
Administradores del Archivo de Claves: personas que dentro del Banco de España tienen acceso a los ficheros que contienen una copia de la clave privada de cifrado de cada usuario, sin tener acceso a las contraseñas con las que están cifrados dichos ficheros.

1.4 Uso de los certificados

1.4.1 Usos apropiados de los certificados

1 Los certificados emitidos por el Banco de España solamente podrán ser utilizados por:

a Las personas o entidades que deben relacionarse con él en función de las facultades y competencias que le atribuye la Ley 13/1994, de 1 de junio, y le confiere su naturaleza de Banco central y de miembro del sistema europeo de bancos centrales.

b Sus empleados o personal contratado, tanto en sus relaciones internas como en las externas que sean necesarias para el funcionamiento interno, propio u operativo de la Institución.

2 En el ámbito de lo dispuesto en el párrafo anterior, los certificados emitidos por PKIBDE podrán ser utilizados para actividades con trascendencia económica, con las limitaciones que, en su caso, se establezcan de acuerdo con lo dispuesto en el artículo 7.3 y artículo 11, letras h) e i) de la Ley de Firma Electrónica.

Los certificados regulados por esta PC se utilizarán para el cifrado de información de forma que sólo sea accesible por el titular del certificado.
Los certificados de cifrado pueden ser utilizados para prestar los siguientes servicios de seguridad:

- Cifrado de correos electrónicos.
- Cifrado de ficheros.
- Cifrado de transacciones.

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 Aprobación de Políticas (AAP) de la PKI del Banco de España:

Nombre	Autoridad de Aprobación de Políticas de la PKI del Banco de España		
Dirección e-mail	pkibde@bde.es		
Dirección	C/Alcalá, 522. 28027 - Madrid (España)		
Teléfono	+34913386610	**Fax**	+34913386870

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

La Comisión Ejecutiva del Banco de España es la Autoridad de Aprobación de Políticas (AAP) de PKIBDE, teniendo por tanto la competencia de la aprobación de la presente PC, así como de las Políticas de Certificación (PC).

La AAP también es la competente para aprobar las modificaciones de dichos documentos.

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, una de las cuales es la AC Corporativa.

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 Aprobación 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

El repositorio de PKIBDE está compuesto por un servicio de directorio vía Directorio Activo de Microsoft o vía LDAP, en ambos casos de uso interno del Banco de España, y un servicio Web, con acceso libre, que son los siguientes:

Repositorio para las CRLs de los certificados de AC Raíz:

- Directorio Activo (sólo para uso desde la red interna del Banco de España):

ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ, CN=SNTPKI01, CN=CDP, CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES ?authorityRevocationList ?base?objectclass=cRLDistributionPoint"

- LDAP (sólo para uso desde la red interna del Banco de España):

ldap://pkildap.bde.es/CN=CRL,CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ, CN=Internas, CN=PKI, CN=Configuration, DC=BDE, DC=ES ?authorityRevocationList ?base ?objectclass=cRLDistributionPoint"

- WEB:

http://pki.bde.es/crls/ACraiz.crl

Repositorio para las CRLs de los certificados de AC Corporativa:

- Directorio Activo (sólo para uso desde la red interna del Banco de España):

ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA, CN=SNT0053, CN=CDP, CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES ?certificateRevocationList?base?objectclass=cRLDistributionPoint"

- LDAP (sólo para uso desde la red interna del Banco de España):

ldap://pkildap.bde.es/CN=CRL,CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA, CN=Internas, CN=PKI, CN=Configuration, DC=BDE, DC=ES ?certificateRevocationList ?base ?objectclass=cRLDistributionPoint"

- WEB:

http://pki.bde.es/crls/ACcorporativa.crl

Servicio de validación en línea que implementa el protocolo OCSP:

- WEB: http://pkiva.bde.es (sólo para uso desde la red interna del Banco de España)

Para los certificados de la AC Raíz y AC Corporativa:

- WEB: http://pki.bde.es/certs/ACraiz.crt
- WEB: http://pki.bde.es/certs/ACcorporativa.crt

Para las DPC y las PC:

- http://pki.bde.es/politicas

Desde la página se accede a los siguientes documentos (X.Y indica la versión):

- PKIBdE_DPC-vX.Y.pdf
- PKIBdE_PC_CertCifrado-vX.Y.pdf

El repositorio de PKIBDE no contiene ninguna información de naturaleza confidencial.

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 contiene un identificador de que es un certificado de cifrado, '[C]', seguido del nombre y los dos apellidos.

Adicionalmente se utilizan los siguientes campos:

- SerialNumber= <Doc. Identificación> (OID: 2.5.4.5)
- PS= <Código Usuario> (OID: 2.5.4.65)

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

- OU=PERSONAS, 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. La utilización del código único de usuario garantiza la unicidad del DN.

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

El par de claves de los certificados de cifrado los generará la AC Corporativa, con lo que no se aplica este apartado.

3.2.2 Autenticación de la identidad de una persona jurídica

No está contemplada la emisión de certificados para personas jurídicas.

3.2.3 Autenticación de la identidad de una persona física

La autenticación inicial de la identidad de una persona física es presencial. El solicitante se ha de presentar ante su Administrador de usuarios debidamente identificado mediante su tarjeta de identificación.

3.2.4 Información no verificada sobre el solicitante

Toda la información recabada en el apartado anterior ha de ser verificada.

3.2.5 Comprobación de las facultades de representación

No estipulado al no estar contemplada la emisión de certificados para personas jurídicas.

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

La autenticación de la identidad de un individuo se puede dar de dos formas:

- **Presencial**: se utiliza en la emisión inicial del certificado, en caso de revocación del anterior o si la renovación anterior fue remota. El solicitante se ha de presentar ante su Administrador de usuarios debidamente identificado mediante su tarjeta de identificación.
- **Remota**: se utiliza en las renovaciones de certificados por caducidad en la que la anterior renovación haya sido presencial y el titular tenga su anterior certificado de autenticación en vigor. El solicitante se acredita de forma remota mediante su certificado de autenticación.

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

El proceso de identificación individual será presencial y con los mismos criterios que en una renovación de rutina.

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 cifrado personal emitidos por la AC Corporativa. Aunque estos certificados se van a almacenar en tarjetas criptográficas, no es objeto de esta Política de Certificación regular la gestión de dichas tarjetas, por lo que siempre se parte de que el solicitante del certificado ha obtenido previamente su tarjeta criptográfica.
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 cifrado está referida a dos tipos de colectivos:

- Empleados: se entiende que la petición se efectúa automáticamente por el hecho de su incorporación a la plantilla del Banco de España. El empleado debe acudir al Administrador de Usuarios que tenga asignado con su tarjeta criptográfica para que éste le identifique, le registre previamente en la PKI y active la emisión del certificado.
- Colaboradores y subcontratados: la petición la debe hacer el Departamento en el que estén asignados en función de su necesidad de acceder a los Sistemas de Información. El colaborador o subcontratado deberá ir al Administrador de Usuarios que tenga asignado con su tarjeta criptográfica para que dicho Administrador le identifique, le registre previamente en la PKI y active la emisión del certificado.

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 cifrado. El Administrador de la PKI podrá recabar del solicitante la documentación que considere oportuna.

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

Este proceso se realiza conjuntamente con el de obtención del certificado de autenticación, observándose los siguientes trámites:

1 El solicitante, una vez que tiene tarjeta criptográfica, se dirige al Administrador de Usuarios que tiene asignado.

2 El Administrador de Usuarios le identifica y comprueba que está autorizado a tener certificado de cifrado y que posee una tarjeta criptográfica válida.

3 El Administrador de Usuarios, utilizando la transacción de Emisión de Certificados, introduce los datos del solicitante y activa la petición a la AC. La transacción genera el envío de una contraseña de un solo uso en dos partes para poder generar el certificado, una dirigida al solicitante y la otra al Administrador de Usuarios

4 La AC Corporativa, una vez recibida la petición, mantiene ésta en estado latente a la espera de que el solicitante, vía web, active el proceso utilizando la contraseña.

5 El solicitante, utilizando las dos partes de la contraseña y su código de usuario, activa el proceso de generación del certificado en la AC.

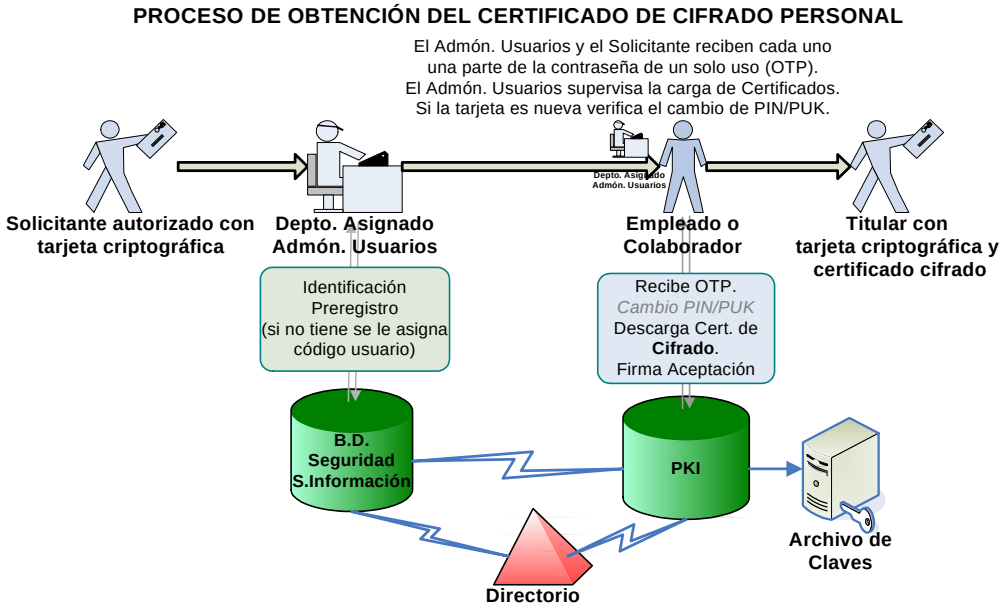
6 La AC Corporativa genera el par de claves y el certificado y pone el certificado y la clave privada en formato PKCS#12 para su descarga por el solicitante.

7 Si la tarjeta es nueva, el solicitante, bajo la supervisión del Administrador de Usuarios, cambia el PIN/PUK de la tarjeta.

8 El solicitante, bajo la supervisión del Administrador de Usuarios, descarga el certificado a la tarjeta.

9 El solicitante firma el documento de Aceptación de las Condiciones de uso de los Certificados Personales y adquiere así la condición de titular del certificado. Dicho documento le es proporcionado y lo recoge, una vez firmado, el Administrador de Usuarios.

Las responsabilidades de los solicitantes no recogidas en este apartado se incluyen en la Declaración de Prácticas de Certificación (DPC) de PKIBDE.
En la siguiente figura se sintetiza el proceso de obtención del certificado de cifrado personal.



Además del proceso descrito, un Administrador remoto de la AC puede introducir directamente una solicitud de certificado y obtener la clave privada y el certificado en formato PKCS#12 para su entrega a un solicitante.

4.2 Tramitación de las solicitudes de certificados

4.2.1 Realización de las funciones de identificación y autenticación

La identificación y autenticación se realiza de dos maneras, en función del tipo de solicitud:

- Emisión inicial, renovación por pérdida o cambio de tarjeta o renovación tras una renovación en línea anterior: en todos estos casos la identificación y autenticación la realiza el Administrador de Usuarios.
- Renovación remota: la identificación y autenticación se efectúa electrónicamente utilizando el certificado de autenticación en vigor del titular. Este tipo de renovación se alterna con la anterior.

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.
La AC Corporativa puede negarse a emitir un certificado de cualquier solicitante basándose exclusivamente en su propio criterio, sin que ello implique contraer responsabilidad alguna por las consecuencias que puedan derivarse de tal negativa.
Las solicitudes de certificados de los empleados del Banco de España se aprueban por su condición de tales, mientras que la de los colaboradores y subcontratados requieren, para ser aprobadas, la previa petición de los certificados por parte del Departamento en el que estén asignados.

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.

El solicitante dispone de un periodo limitado de 7 días naturales para activar la generación y descarga del certificado. Pasado ese periodo la petición queda anulada.

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 disponibilidad del certificado de cifrado mediante correo electrónico.

4.4 Aceptación del certificado

4.4.1 Forma en la que se acepta el certificado

El solicitante deberá confirmar la aceptación del certificado de cifrado y sus condiciones mediante firma manuscrita en las renovaciones presenciales o mediante firma electrónica en las que se hagan en línea.

4.4.2 Publicación del certificado por la AC

El certificado de cifrado 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.
Tras la expiración o revocación del certificado el titular dejará de usar la clave privada.
Los certificados de Cifrado regulados por esta PC sólo pueden ser utilizados para prestar los siguientes servicios de seguridad:

- Cifrado de correos electrónicos.
- Cifrado de ficheros
- Cifrado de transacciones.

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 cifrado 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 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. Asimismo, si alguna información del titular ha cambiado ésta deberá ser verificada y registrada con el acuerdo del titular.

La identificación y autenticación para la renovación de un certificado de cifrado contempla de forma general, dos casos:

- Renovación por caducidad del certificado siendo la renovación anterior presencial: en este caso la renovación se podrá realizar de forma remota identificándose mediante un certificado de autenticación de PKIBDE en vigor.
- Renovación por caducidad del certificado siendo la renovación anterior en línea o renovación por otras causas: en este caso la renovación se solicitará de forma presencial en los puestos de registro que se establezcan de igual forma que en el caso de la emisión inicial.

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

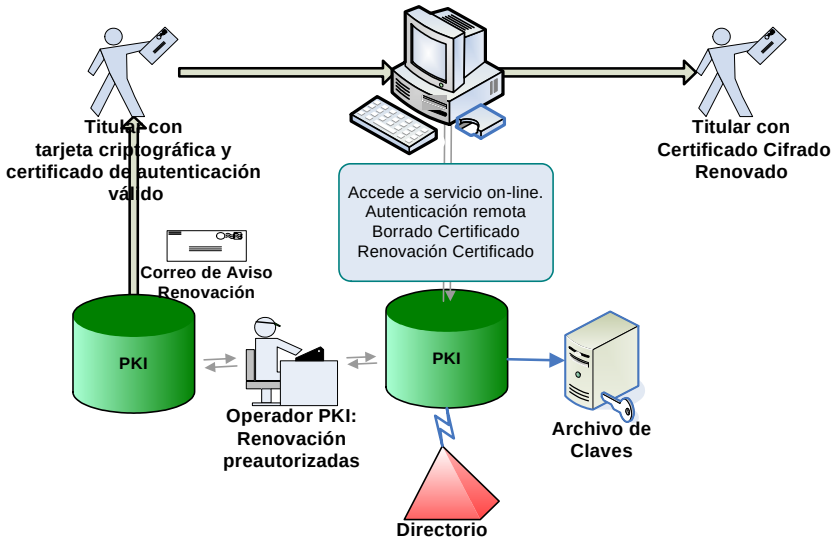
En cualquier caso la renovación de un certificado está supeditada a:

- Que lo solicite en debido tiempo y forma, siguiendo las instrucciones y normas que PKIBDE especifica a tal efecto. Sólo se puede solicitar la renovación de un certificado dentro de sus últimos 12 meses de vigencia.
- 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.

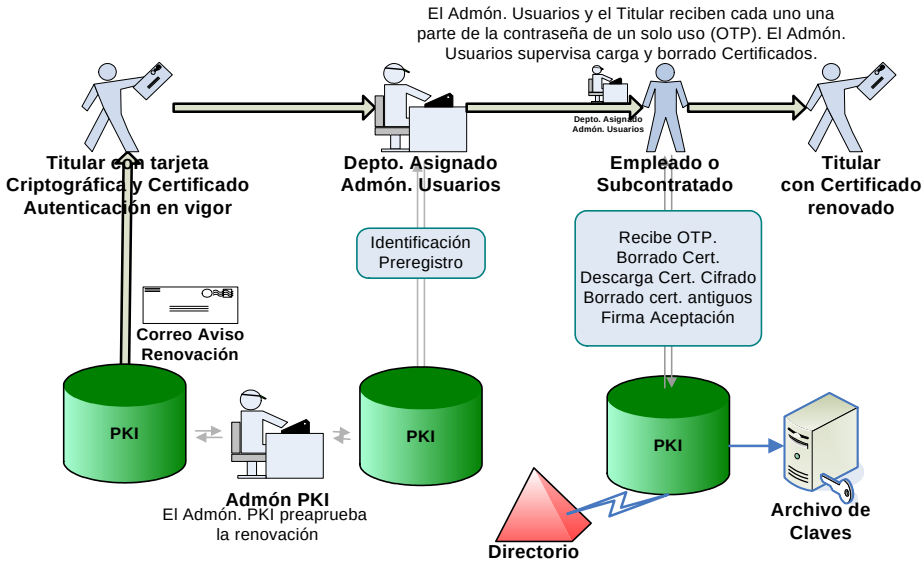
En los siguientes diagramas se recoge de forma sintética los dos procesos de renovación de certificados de cifrado:

- Renovación remota (on-line): como describe el diagrama, salvo la preautorización, toda la gestión la realiza el propio titular.
- Renovación presencial: en este caso, al igual que en la emisión inicial, participa el Administrador de Usuarios y el titular se ha de personar ante él.

PROCESO DE RENOVACIÓN ON-LINE DE LOS CERTIFICADOS DE CIFRADO CON CERTIFICADO DE AUTENTICACIÓN VÁLIDO



PROCESO DE RENOVACIÓN PRESENCIAL CERTIFICADOS CIFRADO



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

En el caso de la renovación remota el titular confirma electrónicamente la aceptación del certificado y en el caso de las renovaciones presenciales ha de firmar la aceptación al Administrador de Usuarios.

4.7.6 Publicación del certificado con las nuevas claves por la AC

El certificado de cifrado 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 Revocación de Certificados (CRL) de acceso público.

Un certificado de cifrado personal 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 el Formulario de aceptación de las condiciones de los servicios de certificación de la autoridad de certificación del Banco de España, en la DPC o en la presente PC.
- El titular de un certificado deja de pertenecer al grupo, 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 titular o por tercero autorizado.
- 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.

Adicionalmente, los certificados de cifrado personal revocados serán eliminados del directorio en el que estaban publicados.

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 titulares de certificados también podrán solicitar la revocación de sus certificados, debiendo hacerlo de acuerdo con las condiciones especificadas en el apartado 4.9.3.

La política de identificación para las solicitudes de revocación podrá ser la misma que para el registro inicial. La política de autenticación aceptará solicitudes de revocación firmadas electrónicamente por el titular del certificado, siempre que lo haga con un certificado en vigor diferente del que solicita sea revocado.

4.9.3 Procedimiento de solicitud de revocación

El titular o persona que solicite la revocación la debe presentar ante su Administrador de Usuarios, identificándose e indicando la causa de la solicitud.

El Administrador de Usuarios tramitará siempre las solicitudes de revocación de aquellos titulares que tenga asignados. La solicitud se realiza mediante una transacción dentro de la Aplicación de Seguridad Informática.

Además de este procedimiento ordinario, los Operadores y Administradores de la PKI podrán revocar de modo inmediato cualquier certificado caso de que llegue a su conocimiento la existencia de alguna causa que motive la 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 cifrado 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 cifrado.

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 CRLs guardadas en memoria 'cache' [1], aun no estando caducadas, no garantizan que dispongan de información de revocación actualizada.

Para los certificados de cifrado el procedimiento ordinario de comprobación de la validez de un certificado será la consulta a la Autoridad de Validación del Banco de España, la cual mediante protocolo OCSP indicará el estado del certificado.

4.9.7 Frecuencia de emisión de CRLs

PKIBDE publicará una nueva CRL en su repositorio en el momento que se produzca cualquier revocación, y, en último caso, a intervalos no superiores a 24 horas (aunque no se hayan producido modificaciones en la CRL) para las ACs subordinadas y de 15 años para la AC Raíz.

[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 6 horas.

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

PKIBDE proporciona un servidor web donde publica las CRLs para la verificación del estado de los certificados que emite. Asimismo, existe una Autoridad de Validación que, mediante el protocolo OCSP, permite verificar el estado de los certificados.

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

4.9.10 Requisitos de comprobación en-línea de revocación

En el caso de utilizar la Autoridad de Validación el Tercero Aceptante debe de 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 revocación 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

La suspensión de la vigencia de los certificados se aplicará, entre otros, en los siguientes casos:

- Cambio temporal de alguna de las características del titular del certificado que aconsejen la suspensión de los certificados mientras dure el mismo. Al retornarse a la situación inicial se levantará la suspensión del certificado.
- Comunicación por el titular del certificado de un posible compromiso de sus claves. En el caso de que la sospecha, por su grado de certeza, no aconseje la revocación inmediata, se suspenderán los certificados del titular mientras se averigua el posible compromiso de las claves. Al término del análisis se determinará si se revocan los certificados o si se levanta la suspensión.
- Resolución judicial o administrativa que lo ordene.

4.9.14 Quién puede solicitar la suspensión

La solicitud la puede iniciar el titular del certificado.

4.9.15 Procedimiento para la solicitud de suspensión

La solicitud de suspensión la tramitará el Administrador de Usuarios mediante la transacción en el sistema de Administración establecido a tal efecto. Por el mismo método se solicitará el levantamiento de la suspensión cuando proceda éste.

En cualquier caso, se le comunicará al titular del certificado tanto el comienzo de la suspensión como su fin por correo electrónico.

4.9.16 Límites del periodo de suspensión

Por defecto PKIBDE suspenderá los certificados de forma provisional por un plazo máximo de 1 año, plazo tras el cual se revocará el certificado, salvo que se hubiera levantado previamente la suspensión del certificado.

Si durante el tiempo de suspensión del certificado éste caduca o se solicita su revocación, se producirán las mismas consecuencias que para los certificados no suspendidos en esos mismos casos de caducidad o revocación.

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

Las claves privadas correspondientes a los certificados de cifrado personales se archivan, con lo que procede regular la forma en que se pueden recuperar dichas claves del 'Archivo de Claves'.

En la recuperación de claves de cifrado se han de distinguir dos casos, dependiendo de si el solicitante es el titular o un tercero. En el caso de que el solicitante sea un tercero, hace falta el concurso de dos figuras separadas, como se describe más adelante, de forma que nadie de forma autónoma pueda acceder a la clave de cifrado de un tercero:

El solicitante es el titular:

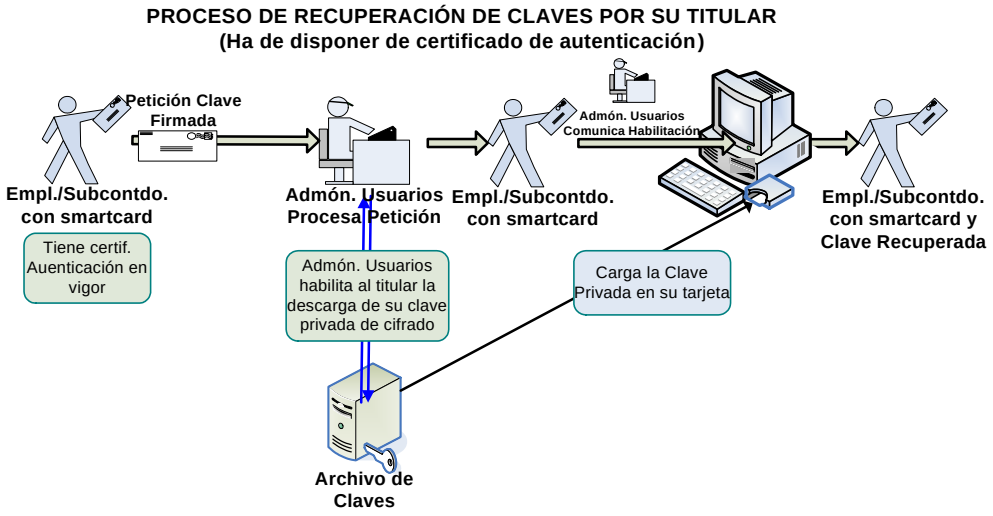
Se considera que el titular está autorizado a recuperar sus propias claves. Ha de disponer de tarjeta con certificados de autenticación y firma, normal o provisional, para poder hacer la petición y recuperar la clave. El titular ha de solicitar a su Administrador de Usuarios que el habilite la recuperación de la clave privada de cifrado. Una vez que el Administrador de Usuarios le habilite la recuperación, el titular podrá descargar dicha clave autenticándose mediante su certificado de autenticación.

El solicitante es otra persona diferente del titular:

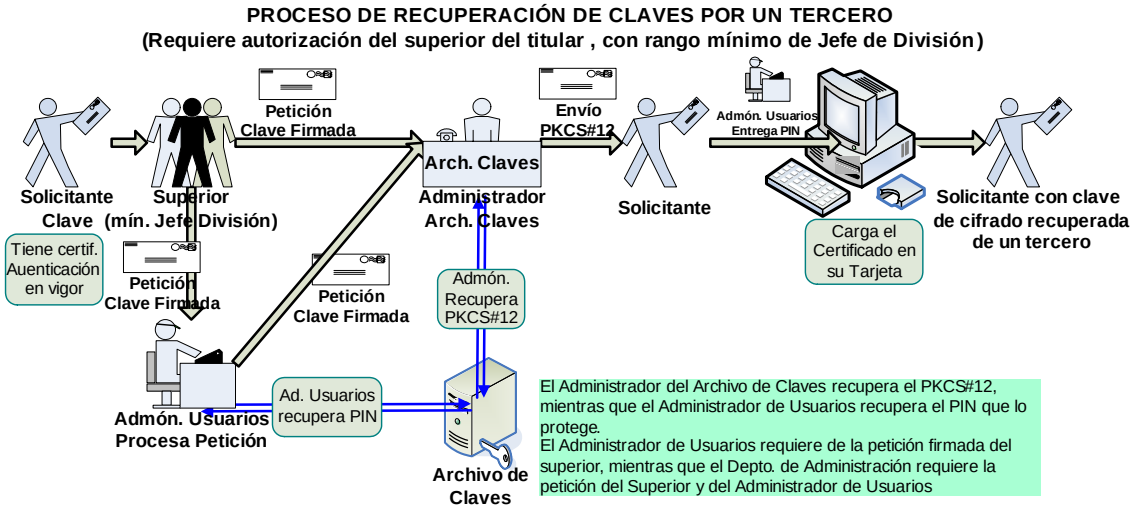
La petición de la solicitud de recuperación ha de autorizarla el superior jerárquico del titular con nivel profesional de Jefe de División, como mínimo, y el Administrador de Usuarios correspondiente. En el caso de la Alta Dirección se establecerá un procedimiento especial. El superior ha de remitir su petición firmada al Administrador de Usuarios y a la Unidad de Administración y Presupuestos del Departamento de Sistemas de Información. El Administrador de Usuarios, por su parte, ha de confirmar la petición a la misma Unidad mediante correo firmado. Una vez cursada la petición los intervinientes actúan de la siguiente forma:

- **Administradores del Archivo de Claves**: tienen acceso para descargar los ficheros PKCS#12 con las claves privadas del Archivo de Claves, sin embargo no tiene acceso a los PIN que los protegen. Tras validar la petición recibida remite el fichero PKCS#12 al solicitante autorizado de la clave.
- **Administradores de Usuarios**: tienen acceso para descargar los PIN de los PKCS#12 del Archivo de Claves, pero no pueden acceder a los PKCS#12. Cuando el solicitante autorizado reciba el fichero PKCS#12 le proporciona el PIN y supervisa la obtención de la clave privada.

En la siguiente figura se recoge el proceso de recuperación de claves por su titular:



En la siguiente figura se recoge el proceso de recuperación de claves por un tercero. Es preciso que la solicitud de recuperación la autorice un Superior, con rango mínimo de Jefe de División, y el Administrador de Usuarios. Los Administradores del Archivo de Claves deben recibir las peticiones firmadas de ambos para recuperar el PKCS#12:



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

No aplicable.

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 Numero 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

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

Las claves para los certificados de cifrado emitidos por la AC Corporativa se generan en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3 que tiene instalados dicha AC.

6.1.2 Entrega de la clave privada al titular

La entrega de la clave privada se efectúa mediante la descarga por el titular de un fichero en formato PKCS#12. Para garantizar la seguridad de la entrega se comunica la disponibilidad de la generación y posterior descarga del certificado mediante correo electrónico, y se proporciona una parte de la contraseña de un solo uso a utilizar. El resto de la contraseña se comunica al Administrador de Usuarios que tramitó la petición.

La generación del par de claves y el certificado lo activa el solicitante, así como su descarga, en presencia de su Administrador el cual le proporciona su parte de contraseña. El software de descarga fuerza a que el certificado y la clave privada se instalen en la tarjeta criptográfica del titular, impidiendo que pueda guardar copia del PKCS#12 en su disco duro.

6.1.3 Entrega de la clave publica al emisor del certificado

La clave pública la genera la propia AC Corporativa, por lo que no procede esta entrega.

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 cifrado 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 cifrado está codificada de acuerdo con RFC 3280 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)

La clave definida por la presente política, y por consiguiente el certificado asociado, se utilizará para la verificación de la identidad del titular del certificado 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:

Key Usage:

- Digital Signature
- Key Agreement

Extended Key Usage:

- emailProtection
- 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.

En cuanto a las tarjetas criptográficas, aptas como dispositivos seguros de creación de firma, cumplen el nivel de seguridad CC EAL4+, aunque también son admisibles las certificaciones equivalentes ITSEC E3 o FIPS 140-2 Nivel 2.

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

Según lo especificado en la DPC de PKIBDE.

6.2.3 Custodia de la clave privada

Las claves privadas de los certificados de cifrado se encuentran alojadas en tarjetas criptográficas, no siendo exportadas una vez instaladas en ningún caso y estando protegido el acceso a las operaciones con las mismas mediante PIN.

La AC Corporativa, una vez generado el par de claves, guarda cifrada la clave privada de cifrado en el 'Archivo de Claves' del que dispone, con el objeto de poder recuperar dicha clave. La recuperación de una clave privada de cifrado del 'Archivo de Claves' exige la intervención de dos personas: una para recuperar la clave en formato PKCS#12 y otra para recuperar el PIN que lo protege. En el apartado *4.12.1 Prácticas y políticas de custodia y recuperación de claves* se regula el procedimiento de recuperación.

6.2.4 Copia de seguridad de la clave privada

Según lo especificado en la DPC de PKIBDE.

6.2.5 Archivo de la clave privada

La AC Corporativa, una vez generado el par de claves, guarda cifrada la clave privada de cifrado en el 'Archivo de Claves' del que dispone. La recuperación de una clave privada de cifrado del 'Archivo de Claves' exige la intervención de dos personas: una para recuperar la clave en formato PKCS#12 y otra para recuperar el PIN que lo protege. En el apartado *4.12.1 Prácticas y políticas de custodia y recuperación de claves* se regula el procedimiento de recuperación.

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

Según lo especificado en la DPC de PKIBDE.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas se crean en el módulo criptográfico de la AC Corporativa pero posteriormente no se conservan.

6.2.8 Método de activación de la clave privada

La clave privada se proporciona en un fichero PKCS#12 protegido mediante una contraseña de un solo uso. Una vez descargado e instalado en la tarjeta criptográfica su uso se controla mediante el PIN de la tarjeta.

6.2.9 Método de desactivación de la clave privada

Se puede desactivar retirando la tarjeta del lector o pasado el tiempo establecido tras la introducción del PIN.

6.2.10 Método de destrucción de la clave privada

Según lo especificado en la DPC de PKIBDE.

6.2.11 Clasificación de los módulos criptográficos

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

El certificado de cifrado 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 cifrado personales 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:

- *KeyUsage*. Calificada como crítica.
- *BasicConstraint*. Calificada como crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *SubjectAlternativeName*. Calificada como no crítica.
- *CRLDistributionPoint*. Calificada como no crítica.

CAMPO	CONTENIDO	CRÍTICA para extensiones
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA-1WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA, O=BANCO DE ESPAÑA, C=ES	
5. Validez	4 años	
6. Subject	CN=[C] Nombre Apellido1 Apellido 2 SerialNumber=NIF PS=Código Usuario OU=PERSONAS O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 1024(big string)	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
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	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora.	NO
3. KeyUsage		SI
Digital Signature	0	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	1	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	

CAMPO	CONTENIDO	CRÍTICA para extensiones
4. extKeyUsage	emailProtection, anyExtendedKeyUsage	NO
5. privateKeyUsagePeriod	No se utilizará	
6. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. © 2004 Banco de España. Todos los derechos reservados. (C/Alcalá 48, 28014 Madrid-España)	
7.Policy Mappings	No se utilizará	
8. Subject Alternate Names	UPN (User´s Principal Name de Windows 2000) Dirección email según RFC 822 1.3.6.1.4.1.19484.2.3.1 Nombre 1.3.6.1.4.1.19484.2.3.2 Apellido1 1.3.6.1.4.1.19484.2.3.3 Apellido2 1.3.6.1.4.1.19484.2.3.4 Nº de empleado BDE 1.3.6.1.4.1.19484.2.3.5 Código Usuario BDE 1.3.6.1.4.1.19484.2.3.7 Documento Identificación	NO
9. Issuer Alternate Names	No se utilizará	
10. Subject Directory Attributes	No se utilizará	
11. Basic Constraints	CA	SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
12. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20 DE%20ESPA%D1A%20-%20AC%20CORPORATIVA,CN=snt0053,CN=CDP, CN=Public%20Key%20Services,CN=Services,CN=Configuration, DC=BDE, DC=ES ?certificateRevocationList?base?objectclass= cRLDistributionPoint (2) LDAP: ldap://pkildap.bde.es/CN=CRL,CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA, CN=Internas, CN=PKI, CN=Configuration, DC=BDE, DC=ES ?certificateRevocationList ?base ?objectclass=cRLDistributionPoint (3)HTTP http://pki.bde.es/certs/ACcorporativa.crl	NO
13. Auth. Information Access	OCSP http://pkiva.bde.es CA http://pki.bde.es/certs/ACraiz.crt	NO
14.netscapeCertType	No procede	
15. netscapeRevocationURL	No procede	
16. netscapeCAPolicyURL	No procede	
17. netscapeComment	No procede	
18. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	CIFRADO	

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)

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.

Los atributos CN (Common Name), serialNumber y PS (pseudonym) del DN serán los que distingan a los DN entre sí. La letra C entre corchetes en el CN identifica al certificado de cifrado. El resto de atributos tendrán lo siguientes valores fijos:

OU=PERSONAS, 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 1.3.6.1.4.1.19484.2.2.8 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':

- URL CPS: contiene la URL a la DPC y a la PC que rigen el certificado.
- Notice Referente: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

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

PKIBDE soporta y utiliza CRLs X.509 versión 2 (v2).

7.2.2 CRL y extensiones

No estipulado.

7.3 Perfil de OCSP

7.3.1 Número(s) de versión

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de PKIBDE.

7.3.2 Extensiones OCSP

Según lo especificado en la Declaración de Prácticas de Certificación (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.
La Autoridad de Certificación Corporativa de PKIBDE actuará relacionando una determinada clave pública con su titular mediante la emisión de un certificado de cifrado, todo ello de conformidad con los términos de esta PC y de la DPC.
Los servicios prestados por la AC en el contexto de esta PC son los servicios de emisión, renovación y revocación de certificados de cifrado personales, a los que se accede mediante los Puestos de Administración remotos de la AC desplegados a tal efecto.

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 BDEPKI, 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.