BANCO DE ESPAÑA
Eurosistema

11.05.2015

OID: 1.3.6.1.4.1.19484.2.2.1

Infraestructura de Clave Pública del Banco de España

Declaración de Prácticas de Certificación

RESUMEN Este documento recoge la Declaración de Prácticas de Certificación (DPC) que rige el funcionamiento y operaciones de la Infraestructura de Clave Pública (PKI) del Banco de España.

Esta DPC se aplica a todos los intervinientes relacionados con la jerarquía de la PKI del Banco de España, incluyendo Autoridades de Certificación (AC), Autoridades de Registro, Solicitantes, Titulares de certificados y Terceros Aceptantes, entre otros.

Hoja de Control

Título	Declaración de Prácticas de Certificación
Autor	Secretaría General Departamento Jurídico Departamento de Sistemas de Información
Versión	1.5
Fecha	11.05.2015

Registro de Cambios

Versión	**Fecha**	**Motivo del cambio**
1.0	5.04.2006	Primera versión
1.1	25.10.2006	Inclusión de nuevas extensiones propietarias (apartado 7.1.2)
1.2	25.05.2010	Revisión tras implantación de servicios de fechado electrónico Aclaración de la descripción del procedimiento de aprobación de la DPC y PC, renombrando la Autoridad de Aprobación de Políticas por Autoridad de Administración de Políticas
1.3	07.07.2011	Revisión de las responsabilidades de BdE
1.4	20.10.2014	Consolidación en un único documento de las políticas de certificación de todos los certificados para usuario interno del Banco de España
1.5	11.05.2015	Actualización con motivo de la renovación de las Autoridades de Certificación

ÍNDICE

CONTENIDO, DERECHOS Y OBLIGACIONES ESTABLECIDOS EN ESTA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Este apartado constituye una síntesis del contenido, derechos y obligaciones establecidos en la presente Declaración de Prácticas de Certificación (DPC). Su enunciado ha de ser complementado con la correspondiente Política de Certificación (PC) aplicable al certificado que se esté solicitando o con el que se esté operando.

Es recomendable la lectura completa de esta DPC, así como de las PC que sean de aplicación, para entender los objetivos, especificaciones, normas, derechos, obligaciones y responsabilidades que rigen la prestación del servicio de certificación.

- Esta DPC y los documentos relacionados regulan todo el ciclo de vida de los certificados electrónicos desde su solicitud hasta su extinción o revocación, así como las relaciones que se establecen entre el solicitante/titular del certificado, la Autoridad de Certificación y los terceros aceptantes. Asimismo contempla tanto los certificados electrónicos regulados por la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, como los certificados electrónicos de componentes informáticos, no contemplados en dicha Ley.

- Las Autoridades de Certificación de la PKI del Banco de España emiten diversos tipos de certificados, para los que existen Políticas de Certificación (PC) específicas. En consecuencia, el solicitante de cualquier tipo de certificado ha de conocer esta DPC y la PC que en cada caso le sea de aplicación para poder solicitar y usar de forma correcta el certificado. Lo estipulado en las Políticas de Certificación específicas prevalecerá sobre lo regulado en esta DPC.

- En esta DPC y en las PC relacionadas se establece la delimitación de responsabilidades de las diferentes partes intervinientes así como las limitaciones de las mismas ante posibles daños y perjuicios.

- Tanto la DPC como el resto de documentos relacionados están a disposición de los Solicitantes, Titulares y Terceros Aceptantes de los certificados en la web http://pki.bde.es.

- El titular debe hacer un uso apropiado del certificado, y será de su exclusiva responsabilidad la utilización del certificado de forma diferente a la prevista en la DPC y en la PC correspondiente

- El titular del certificado deberá comunicar a la Autoridad de Certificación cualquier modificación o variación de los datos que se proporcionaron para la obtención del certificado, tanto si éstos se recogieron o no en el propio certificado.

- La custodia de la clave privada por el titular del certificado es requisito fundamental para la seguridad del sistema. En consecuencia, resulta obligado informar de manera inmediata a la Autoridad de Certificación cuando exista alguna de las causas de revocación/suspensión de la vigencia del certificado establecidas en la DPC. Así, se podrá suspender/revocar el certificado comprometido y evitar su uso ilegítimo por un tercero no autorizado.

- La persona que pretenda confiar en un certificado es responsable de verificar, utilizando las fuentes de información que se ponen a su disposición, que el certificado y el resto de certificados de la cadena de confianza son válidos y no han caducado o han sido suspendidos o revocados.

- En esta DPC y en las PC relacionadas se establece la delimitación de responsabilidades de las diferentes partes intervinientes así como las limitaciones de las mismas ante posibles daños y perjuicios.

Para más información, consulte la página web establecida al efecto cuya dirección es http://pki.bde.es o póngase en contacto con la Autoridad de Certificación mediante la dirección de correo electrónico pkibde@bde.es.

1 Introducción

1.1 Resumen

Este documento recoge la Declaración de Prácticas de Certificación (DPC) que rige el funcionamiento y operaciones de la Infraestructura de Clave Pública (en adelante PKI) del Banco de España (desde ahora PKIBDE).

Esta DPC se aplica a todos los intervinientes relacionados con la jerarquía de la PKI del Banco de España, incluyendo Autoridades de Certificación (AC), Autoridades de Registro, Solicitantes y Titulares de certificados y Terceros Aceptantes, entre otros.

La presente DPC, 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 normativa española en la materia.

Asimismo, para el desarrollo de su contenido, se ha tenido en cuenta a los estándares europeos, entre los que cabe destacar los siguientes:

- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats
- ETSI TS 101 862: Qualified Certificate Profile.
- ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.

Igualmente, se ha considerado como normativa básica aplicable a la materia:

- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica (BOE de 20).
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal (BOE de 15).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual (BOE de 22).
- Circular del Banco de España 2/2005, de 25 de febrero, sobre ficheros automatizados con datos de carácter personal gestionados por el Banco de España (BOE de 22 de marzo), y sus posteriores actualizaciones.

Esta DPC recoge la política de servicios, así como la declaración del nivel de garantía ofrecido, mediante la descripción de las medidas técnicas y organizativas establecidas para garantizar el nivel de seguridad de la PKI.

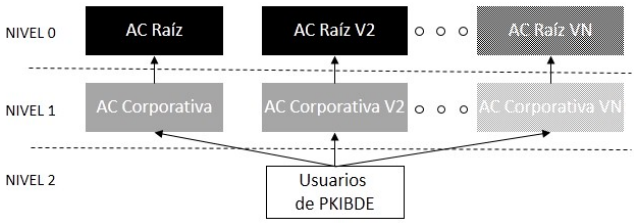
La DPC incluye todas las actividades encaminadas a la gestión de los certificados electrónicos en su ciclo de vida, y sirve de guía de la relación entre PKIBDE y sus usuarios. En consecuencia, todas las partes involucradas tienen la obligación de conocer la DPC y las Políticas de Certificación (PCs) aplicables y ajustar su actividad a lo dispuesto en la misma.

La Ley 59/2003, de 19 de diciembre, de Firma Electrónica, en su artículo 6 limita la cualidad de titular de los certificados electrónicos a las personas físicas y jurídicas. Ello no obstante, la presente Declaración de Prácticas de Certificación se aplica tanto a los certificados asociados a personas físicas y por tanto sujetos a la mencionada Ley, como a otra categoría diferente de certificados que son los vinculados a los componentes informáticos, esto es, a los sistemas y servicios corporativos.

Esta DPC 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	Declaración de Practicas de Certificación de la PKI del Banco de España
Versión del documento	1.5
Estado del documento	Borrador
Fecha de emisión	11.05.2015
OID (Object Identifier)	1.3.6.1.4.1.19484.2.2.1
Ubicación de la DPC	http://pki.bde.es/politicas

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

La Autoridad de Administración de Políticas (AAP) es la organización establecida dentro del Departamento de Sistemas de Información del Banco de España como responsable de la administración de la presente DPC y de las Políticas de Certificación de PKIBDE.

Asimismo, la AAP es la encargada, en caso de que se tuviese que evaluar la posibilidad de que una AC externa interactúe con PKIBDE, de determinar la adecuación de la DPC de dicha AC a la Política de Certificación afectada.

La AAP es responsable de analizar los informes de las auditorías, totales o parciales, que se hagan de PKIBDE, así como de determinar, en caso necesario, las acciones correctoras a ejecutar.

1.3.2 Autoridades de Certificación

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la emisión de certificados electrónicos y de la asignación a sus titulares. Así mismo efectúan la renovación y revocación de los mencionados certificados y la generación de claves públicas y privadas, cuando así lo establecen sus prácticas y políticas.

Las Autoridades de Certificación que actualmente componen PKIBDE son:

1.3.2.1 Autoridades de Certificación Raíz

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

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

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

  - Con algoritmo SHA-1[2]:

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

  - Con algoritmo SHA-256:

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

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

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

1.3.2.2 Autoridades de Certificación Intermedias

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

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

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

  - Con algoritmo SHA-1[3]:

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

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

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

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

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

1.3.3 Autoridades de Registro

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la verificación de la identidad de los solicitantes de certificados electrónicos y, si procede, de los atributos asociados a los mismos.

Las Autoridades de Registro (AR) llevarán a cabo la identificación de los solicitantes de certificados conforme a las normas de esta DPC y el acuerdo suscrito con la AC. En el caso de que las AR sean del Banco de España no será precisa la firma de ningún acuerdo y las relaciones entre ambas se regirán por la presente DPC y las PC que sean de aplicación.

Las Autoridades de Registro competentes para la gestión de solicitudes de certificación se encuentran definidas en la Política de Certificación correspondiente a cada tipo de certificado.

La AC podrá valerse de una o varias Autoridades de Registro (AR) elegidas libremente para la prestación del servicio de certificación.

1.3.4 Autoridad de Validación

La Autoridad de Validación (AV) es el sistema informático junto con las políticas y procedimientos correspondientes que tiene como función la comprobación del estado de los certificados emitidos por PKIBDE, proporcionando un servicio compatible con los protocolos *Online Certificate Status Protocol* (OCSP)[4] y *Lightweigth Online Certificate Status Protocol*[5], que determinan el estado actual de un certificado electrónico a solicitud de un Tercero Aceptante sin requerir el acceso a listas de revocación de certificados.

Este mecanismo de validación es complementario a la publicación de las listas de revocación de certificados (CRL).

1.3.5 Archivo de Claves

Las Políticas de Certificación podrán establecer la existencia de un Archivo de Claves, que es un sistema informático que, junto con las políticas y procedimientos correspondientes, permite el archivo y recuperación de las claves privadas de los titulares de los certificados que se regulen. El Archivo de Claves deberá garantizar la confidencialidad de la clave privada y su recuperación deberá exigir, como mínimo, la intervención de dos personas. En las PC se deberán regular los procedimientos de petición y tramitación de recuperación de claves.

De acuerdo con la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, en ningún caso se archivaran las claves privadas asociadas a certificados electrónicos de firma.

[4] RFC 6960

[5] RFC 5019

1.3.6 Titulares de los certificados

Se denomina Titular de un certificado a toda aquella persona física o componente informático para el que se emite un certificado en el ámbito de PKIBDE. La titularidad es efectiva una vez que el certificado es emitido por la AC y aceptado por su solicitante.

Los tipos de entidades que pueden ser titulares de certificados de PKIBDE se encuentran definidos y limitados por cada Política de Certificación. De forma genérica, y sin perjuicio de lo establecido por la Política de Certificación aplicable en cada caso, pueden observarse, en la siguiente tabla, algunas clases de titulares existentes en PKIBDE:

Entorno de Certificación	Titulares
AC Corporativa	Empleados del Banco de España
	Personal de empresas contratadas y colaboradores externos que trabajan en las instalaciones del Banco
	Componentes informáticos internos
	Componentes informáticos de entidades externas
	Entidades de PKIBDE
	Autoridad de Sellado de Tiempo del Banco de España (TSABDE)

1.3.7 Terceros aceptantes

Los Terceros Aceptantes son las personas o entidades diferentes del titular que deciden aceptar y confiar en un certificado emitido por PKIBDE

Las Políticas de Certificación correspondientes a cada tipo de certificado son quienes determinan los Terceros Aceptantes de cada certificado. No es objetivo de esta DPC su determinación.

1.3.8 Otros afectados

Solicitantes: personas físicas, así como los responsables de componentes informáticos, 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 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

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 Por sus empleados o personal contratado, tanto en sus relaciones internas como externas que sean necesarias para el funcionamiento interno, propio u operativo de la Institución, así como por aplicaciones informáticas puestas a disposición de dichas personas.

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.

Las Políticas de Certificación correspondientes a cada tipo de certificado son las que determinan los usos apropiados que debe darse a cada certificado. No es objetivo de esta DPC la determinación de dichos usos.

1.4.2 Limitaciones y restricciones en el uso de los certificados

Los certificados deben emplearse de acuerdo con las funciones y finalidades definidas en su correspondiente PC, sin que puedan utilizarse para otras tareas y otros fines no contemplados en aquella.

Igualmente, los certificados deben emplearse únicamente de acuerdo con la legislación que le sea aplicable especialmente teniendo en cuenta las restricciones de importación y exportación en materia de criptografía existentes en cada momento.

Los certificados, salvo en los casos en que así lo especifique la PC, no pueden utilizarse para actuar ni como Autoridad de Registro ni como Autoridad de Certificación, firmando certificados de clave pública de ningún tipo ni listas de revocación de certificados (CRL).

Los servicios de certificación que ofrece PKIBDE, no han sido diseñados ni autorizados para ser utilizados en actividades de alto riesgo o que requieran una actividad a prueba de fallos, como las relativas al funcionamiento de instalaciones hospitalarias, nucleares, de control de tráfico aéreo o ferroviario, o cualquier otra donde un fallo pudiera conllevar la muerte, lesiones personales o daños graves al medioambiente.

Las Políticas de Certificación correspondientes a cada tipo de certificado pueden determinar limitaciones y restricciones adicionales en el uso de los certificados. No es objetivo de esta DPC la determinación de dichas limitaciones y restricciones adicionales.

1.5 Administración de las políticas

1.5.1 Banco de España como titular de PKIBDE

Esta DPC 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 DPC está administrada por la Autoridad de Administración de Políticas (AAP) de la PKI del Banco de España, perteneciente al Departamento de Sistemas de Información:

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

En el caso de que se tuviese que evaluar la posibilidad de que una AC externa interactúe con PKIBDE, la Autoridad de Administración de Políticas de PKIBDE es la responsable de determinar la adecuación de la DPC de la AC externa a la Política de Certificación afectada. Los procedimientos para determinar la adecuación se recogen en la PC que tenga prevista la posibilidad de operar con otras AC.

1.5.4 Procedimiento de aprobación de esta DPC

La Comisión Ejecutiva del Banco de España es la responsable de la aprobación de la presente DPC y de las distintas Políticas de Certificación (PC), aunque ha autorizado a la Autoridad de Administración de Políticas (AAP) de PKIBDE, perteneciente al Departamento de Sistemas de Información, a la realización y publicación de las necesarias actualizaciones de dichos documentos, informando de todo ello periódicamente.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

En el ámbito de esta DPC 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, las AC Raíz en el nivel superior garantizan 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

PKIBDE hace uso de varios repositorios, descritos a continuación:

- Un servicio de directorio vía **Directorio Activo** de Microsoft, de uso interno del Banco de España, donde se publica la información indicada a continuación:
    - CRLs de los certificados de las AC Raíz (ARL):
        - ARL de AC Raíz:

          ```
          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
          ```

        - ARL de AC Raíz V2:

          ```
          ldap:///CN=BANCO%20DE%20ESPA%D1A-
          AC%20RAIZ%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Serv
          ices,CN=Configuration,DC=BDE,DC=ES?authorityRevocationList?base?ob
          jectclass=cRLDistributionPoint
          ```

    - CRLs de los certificados de las AC Corporativa:
        - CRL de AC Corporativa

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

        - CRL de AC Corporativa V2

          ```
          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?certificateRevocationLis
          t?base?objectclass=cRLDistributionPoint
          ```

    - Certificados de las AC Raíz en vigor:
        - Certificado de AC Raíz

          ```
          ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ,
          CN=Certification%20Authorities,CN=Public%20Key%20Services,CN=Servi
          ces,CN=Configuration,DC=BDE,DC=ES?cACertificate?base?objectclass=c
          ertificationAuthority
          ```

        - Certificado de AC Raíz V2

          ```
          ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ%20V2,
          CN=Certification%20Authorities,CN=Public%20Key%20Services,CN=Servi
          ces,CN=Configuration,DC=BDE,DC=ES?cACertificate?base?objectclass=c
          ertificationAuthority
          ```

    - Certificados de las AC Corporativas en vigor:
        - Certificado de AC Corporativa

          ```
          ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA,
          CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=
          BDE,DC=ES?cACertificate?base?objectclass=certificationAuthority
          ```

        - Certificado de AC Corporativa V2

          ```
          ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,
          CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=
          BDE,DC=ES?cACertificate?base?objectclass=certificationAuthority
          ```

    - Últimos certificados válidos emitidos por las AC Corporativas para un titular, asociados a su cuenta de dominio del Banco de España.

- Un servicio de directorio vía **Directorio LDAP**, de uso interno del Banco de España, donde se publica la información indicada a continuación:
    - CRLs de los certificados de las AC Raíz (ARL):
        - ARL de AC Raíz:

          ```
          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
          ```

    - CRLs de los certificados de las AC Corporativa:
        - CRL de AC Corporativa:

```
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
```

- Una **página Web** accesible desde la red VPN del Banco de España (sólo accesible a miembros de esa VPN):
    - CRLs de los certificados de las AC Raíz (ARL):
        - ARL de AC Raíz: http://pki.redbde.es/crls/ACraiz.crl
        - ARL de AC Raíz V2: http://pki.redbde.es/crls/ACraizv2.crl
    - CRLs de los certificados de las AC Corporativa:
        - CRL de AC Corporativa: http://pki.redbde.es/crls/ACcorporativa.crl
        - CRL de AC Corporativa V2: http://pki.redbde.es/crls/ACcorporativav2.crl
- Una **página Web** accesible desde Internet con acceso libre:
    - CRLs de los certificados de las AC Raíz (ARL):
        - ARL de AC Raíz: http://pki.bde.es/crls/ACraiz.crl
        - ARL de AC Raíz V2: http://pki.bde.es/crls/ACraizv2.crl
    - CRLs de los certificados de las AC Corporativa:
        - CRL de AC Corporativa: http://pki.bde.es/crls/ACcorporativa.crl
        - CRL de AC Corporativa V2: http://pki.bde.es/crls/ACcorporativav2.crl
    - Certificados de las AC Raíz:
        - Certificado de AC Raíz: http://pki.bde.es/certs/ACraiz.crt
        - Certificado de AC Raíz V2: http://pki.bde.es/certs/ACraizv2.crt
    - Certificados de las AC Corporativas:
        - Certificado de AC Corporativa: http://pki.bde.es/certs/ACcorporativa.crt
        - Certificado de AC Corporativa V2: http://pki.bde.es/certs/ACcorporativav2.crt
    - Certificados de entidad final:
        - Certificado de la Autoridad de Sellado de Tiempo: http://pki.bde.es/certs/TSAcorporativa.crt
    - Documentación de Políticas y Prácticas de Certificación (X.Y indica la versión): http://pki.bde.es/politicas
        - Declaración de Prácticas de Certificación: http://pki.bde.es/politicas/PKIBdE_DPC-vX.Y.pdf
        - Política de Certificación para certificados de usuario interno: http://pki.bde.es/politicas/PKIBdE_PC_CertUsuarioInterno-vX.Y.pdf
        - Política de Certificación para certificados personales de autenticación para dispositivos móviles: http://pki.bde.es/politicas/PKIBdE_PC_CertAutenticacionMovil-vX.Y.pdf
        - Política de Certificación para certificados de componente informático para uso interno: http://pki.bde.es/politicas/PKIBdE_PC_CertComponentes-vX.Y.pdf
        - Política de Certificación para certificados de componente informático para entidades externas: http://pki.bde.es/politicas/PKIBdE_PC_CertComponentesEntidadesExternas-vX.Y.pdf
        - Política de Certificación para certificados de Autoridad de Sellado de Tiempo: http://pki.bde.es/politicas/PKIBdE_PC_CertTSA_vX.Y.pdf
        - Políticas y Prácticas de Sellado de Tiempo: http://pki.bde.es/politicas/PKIBdE_PST_y_DPST-vX.Y.pdf
- Un servicio de **validación en línea** del estado de revocación de certificados, que implementa el protocolo OCSP, accesible externamente al Banco de España a través de Internet:
    - http://ocsp.bde.es

- Un servicio de **validación en línea** del estado de revocación de certificados, que implementa el protocolo OCSP, accesible externamente al Banco de España a través de la red VPN del Sistema Europeo de Bancos Centrales:
    - http://ocsp-pkibde.es.escb.eu
- Un servicio de **validación en línea** del estado de revocación de certificados, de uso interno del Banco de España:
    - http://ocsp.bde.es

Los repositorios de PKIBDE no contienen, en ningún caso, información de naturaleza confidencial.

2.2 Publicación de información de certificación

Es obligación de las ACs pertenecientes a la jerarquía de confianza de PKIBDE publicar la información relativa a sus prácticas, a sus certificados y al estado actual de dichos certificados.

La presente DPC es pública y se encuentra disponible en el sitio Web de PKIBDE, al que se hace referencia en el apartado 2.1 *Repositorio*, en formato PDF.

Las Políticas de Certificación de PKIBDE son públicas y se encuentran disponibles en el sitio Web de PKIBDE, al que se hace referencia en el apartado 2.1 *Repositorio*, en formato PDF.

Las listas de revocación de certificados (CRL) por PKIBDE son públicas y se encuentran disponibles, en formato CRL v2, en el repositorio y sitio Web de PKIBDE al que se hace referencia en el apartado 2.1 Repositorio.

Las listas de revocación de certificados estarán firmadas electrónicamente por las AC de PKIBDE que las emitan.

La información sobre el estado de los certificados se podrá consultar accediendo directamente a las CRL o mediante el servicio de validación en línea disponible que implementa el protocolo OCSP.

2.3 Temporalidad o frecuencia de publicación

La DPC y las Políticas de Certificación se publicarán en el momento de su creación y se volverán a publicar en el momento en que se apruebe cualquier modificación sobre las mismas. Las modificaciones se harán públicas en el sitio web referido en el apartado 2.1 *Repositorios*.

La AC añadirá los certificados revocados a la CRL pertinente dentro del periodo de tiempo estipulado en el punto 4.9.7 Frecuencia de emisión de CRLs.

2.4 Controles de acceso a los repositorios

El acceso para la lectura a las DPC y PC es abierto, pero sólo PKIBDE está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. Para ello PKIBDE establecerá controles que impidan a personas no autorizadas manipular la información contenida en los repositorios.

3 Identificación y autenticación de los titulares de Certificados

3.1 Nombres

3.1.1 Tipos de nombres

Todos los titulares de certificados requieren un nombre distintivo (Distinguished Name) conforme con el estándar X.500.

El procedimiento de asignación de los nombres distintivos viene dado por la política a tal efecto desarrollada y descrita en el documento de Política de Certificación correspondiente al certificado en cuestión. Esta política debe estar en consonancia con las directrices generales descritas en este capítulo de la DPC.

3.1.2 Necesidad de que los nombres sean significativos

En todos los casos se recomienda que los nombres distintivos de los titulares de los certificados sean significativos.

En cualquier supuesto el dotar a los nombres distintivos de significado viene dado por la política a tal efecto desarrollada y descrita en el documento de Política de Certificación correspondiente al certificado en cuestión.

3.1.3 Reglas para interpretar varios formatos de nombres

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

3.1.4 Unicidad de los nombres

El conjunto de nombre distintivo (distinguished name) más el contenido de la extensión KeyUsage debe ser único y no ambiguo.

Las Políticas de Certificación establecerán los procedimientos de garantía de la unicidad.

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 9.11 *Reclamaciones y jurisdicción* de esta DPC.

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 caso de que el par de claves sea generado por el solicitante del certificado, 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 petición de certificado (CSR), en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

Este procedimiento podrá ser modificado por el que establezca en cada caso la Política de Certificación aplicable.

3.2.2 Autenticación de la identidad de una persona jurídica

En caso de que sea aplicable, cada PC establecerá el procedimiento de autenticación de la identidad de una persona jurídica.

3.2.3 Autenticación de la identidad de una persona física

La Política de Certificación aplicable a cada tipo de certificado definirá el procedimiento de identificación individual.

No se considerará que el proceso deba ser menos estricto que otros procedimientos de identificación utilizados por el Banco de España.

Como norma general no se emplearán métodos de identificación remotos distintos a la firma electrónica realizada con certificados emitidos por la propia PKIBDE, o bien por Prestadores de Servicios de Certificación admitidos por el Banco de España.

En cada PC se establecerá la información a proporcionar por el solicitante, determinándose entre otros aspectos los siguientes:

- Tipos de documentos de identidad válidos para la identificación.
- Procedimiento de identificación por la AC o AR del individuo.
- Necesidad o no de identificación presencial.
- Forma de acreditar la pertenencia a una determinada organización.

3.2.4 Información no verificada sobre el solicitante

Cada PC establecerá qué parte de la información suministrada en la solicitud de un certificado no se verifica necesariamente.

3.2.5 Comprobación de las facultades de representación

En los casos de emisión de certificados de componentes informáticos la verificación de las facultades del responsable para la solicitud de los mismos vendrá establecida en la PC específica.

3.2.6 Criterios para operar con AC externas

Antes de establecer relaciones de interactividad con AC externas se ha de determinar la adecuación de dichas AC al cumplimiento de ciertos requisitos. Los criterios mínimos, que pueden ser ampliados en cada caso por la AAP, para considerar a una AC adecuada para interaccionar con PKIBDE son:

- La AC externa ha de proporcionar un nivel de seguridad en la gestión de los certificados, a lo largo de su ciclo de vida, como mínimo, igual al de la PKIBDE. Esta exigencia se recogerá en la DPC y PC correspondientes y en su cumplimiento por la AC.

- Ha de cumplir el estándar ETSI TS 101 456: *Policy Requirements for certification authorities issuing qualified certificates* o equivalente.

- Deberá aportar el informe de auditoría de una Autoridad externa de reconocido prestigio relativa a sus operaciones como medio de verificación del nivel de seguridad existente. La AAP podrá declarar exentas de este requisito a las AC pertenecientes a Administraciones Públicas o al Sistema Europeo de Bancos Centrales.

- Establecer un convenio de colaboración en el que se fijen los compromisos adquiridos en materia de seguridad para los certificados incluidos en la interacción.

Aunque una AC cumpla los requisitos anteriores la AAP podrá denegar la solicitud de interactividad sin necesidad de aportar ninguna justificación.

La interactividad puede llevarse a cabo mediante certificación cruzada, certificación unilateral u otras formas.

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 y autenticación individual se define por la Política de Certificación aplicable a cada tipo de certificado.

Como norma general no se emplearán métodos de identificación/autenticación remotos distintos a la firma electrónica realizada con certificados emitidos por la propia PKIBDE.

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

El proceso de identificación y autenticación individual se define por la Política de Certificación aplicable a cada tipo de certificado, debiendo ser como mínimo tan estricto como el aplicado en la solicitud inicial del certificado.

Como norma general no se emplearán métodos de identificación/autenticación remotos distintos a la firma electrónica realizada con certificados emitidos por la propia PKIBDE.

4 Requisitos operacionales para el ciclo de vida de los certificados

4.1 Solicitud de certificados

4.1.1 Quién puede efectuar una solicitud

En cada Política de Certificación se concreta quién puede solicitar un certificado y la información que se debe suministrar en la solicitud. Asimismo, la PC establece los pasos que deben seguirse para llevar a cabo este proceso.

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

En general, es atribución de cada Autoridad de Registro de PKIBDE determinar la adecuación del tipo de certificado a las características de las funciones del solicitante, de acuerdo con lo previsto en la Política de Certificación aplicable en cada caso. La Autoridad de Registro podrá autorizar o denegar la solicitud de certificación.

Las solicitudes de los certificados, una vez completadas, serán enviadas a la Autoridad de Certificación por la Autoridad de Registro de PKIBDE.

Como regla general, todo solicitante que desee un certificado deberá:

- Cumplimentar el formulario de solicitud del certificado con toda la información que PKIBDE requiera para la emisión del mismo. Cabe destacar que no toda la información solicitada aparecerá en el certificado y que ésta será conservada, de manera confidencial, por la Autoridad de Certificación de acuerdo con la normativa vigente en materia de Protección de Datos de Carácter Personal.
- Entregar la solicitud de certificado, que incluye la clave pública, a la AR correspondiente, en el caso de que el par de claves lo haya generado el solicitante y el certificado se genere directamente a partir de la solicitud. En la correspondiente PC se establecerá el procedimiento de entrega.

La existencia del formulario de solicitud y en general el procedimiento de solicitud de certificados a PKIBDE queda definido en la Política de Certificación correspondiente a cada uno de los certificados.

4.2 Tramitación de las solicitudes de certificados

4.2.1 Realización de las funciones de identificación y autenticación

El proceso de identificación individual se define por la Política de Certificación aplicable a cada tipo de certificado. El proceso debe ser tan estricto como otros procedimientos de identificación utilizados por el Banco de España.

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. El procedimiento por el que se determina la naturaleza y la forma de realizar dichas comprobaciones se establece en la Política de Certificación correspondiente.

PKIBDE 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 pudieran derivarse de tal negativa.

4.2.3 Plazo para la tramitación de las solicitudes de certificados

Las AC de PKIBDE no se hacen responsables de las demoras que pueda surgir en el periodo comprendido entre la solicitud del certificado, la publicación en el repositorio de PKIBDE, si procede, y la entrega del mismo. En todo caso se establecerán plazos mínimos para la tramitación de las solicitudes de los certificados en las PC correspondientes.

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 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 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.

Todo lo especificado en este apartado queda supeditado a lo estipulado por las distintas Políticas de Certificación para la emisión de certificados acogidos a las mismas.

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

Cada PC establecerá la forma por la que el solicitante haya de conocer la emisión de su certificado.

4.4 Aceptación del certificado

4.4.1 Forma en la que se acepta el certificado

La aceptación del certificado es la acción mediante la cual su titular da inicio a sus obligaciones respecto a la PKI del Banco de España.

Los certificados que exijan una identificación presencial llevarán aparejada la aceptación explícita del titular del certificado y el reconocimiento de que está de acuerdo en los términos y condiciones contenidos en el formulario de aceptación de las condiciones de los servicios de certificación de la autoridad de certificación del Banco de España que rige los derechos y obligaciones entre PKIBDE y el titular y de que éste conoce la existencia de la presente Declaración de Prácticas de Certificación, que recoge técnica y operativamente los servicios de certificación electrónica prestados por PKIBDE.

En la PC correspondiente se podrán detallar o ampliar la forma en que se acepta el certificado.

4.4.2 Publicación del certificado por la AC

En cada PC se establecerá la publicación del certificado en el repositorio de PKIBDE.

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

Cuando la AC de PKIBDE emita un certificado de acuerdo con una solicitud de certificación tramitada a través de una AR, enviará una copia del mismo a la AR que remitió la solicitud.

4.5 Par de claves y uso del certificado

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

Las responsabilidades y limitaciones de uso del par de claves y del certificado se establecerán en la correspondiente PC.

El titular sólo podrá utilizar la clave privada y el certificado para los usos autorizados en la 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.

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 establezca la correspondiente 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 esta DPC y en la correspondiente PC. Asimismo, se obligan a las condiciones de uso establecidas en dichos 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 DPC 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 Declaración, 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

El proceso de renovación de certificados dependerá de la Política de Certificación aplicable a cada tipo de certificado.

Un certificado puede ser renovado, entre otros, por los siguientes motivos:

- Expiración, o cercanía en la 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 de certificados en el ámbito de esta DPC se realizarán con cambio de claves.

4.7.2 Quién puede pedir la renovación de los certificados

El titular del certificado deberá solicitar la renovación, si bien no todos los certificados prevén esta posibilidad. En cada Política de Certificación se establecerá quien puede solicitar la renovación 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 titular.

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

- Renovación por caducidad de un certificado de usuario interno: 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.

- Renovación de un certificado de componente: todas las renovaciones se realizarán de forma remota, efectuando la solicitud mediante la identificación con un certificado válido emitido por PKIBDE u otro PSC admitido por el BE o bien mediante otros mecanismos definidos en las políticas de certificación.

Estas directrices están supeditadas a la Política de Certificación aplicada a cada certificado, prevaleciendo siempre sobre lo estipulado en este apartado.

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

- Que se 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 los servicios de prestación se refiera al mismo tipo de certificado emitido inicialmente.

4.7.4 Notificación de la emisión de un nuevo certificado al titular

En cada PC se establecerá la forma en que el solicitante será informado de que ha sido emitido el correspondiente certificado a su nombre.

4.7.5 Forma de aceptación del certificado con las claves cambiadas

En cada PC se establecerá la forma de aceptación.

4.7.6 Publicación del certificado con las nuevas claves por la AC

En cada PC se establecerá, si procede, el procedimiento de la publicación del certificado en el repositorio de PKIBDE.

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

Cuando la AC de PKIBDE emita un certificado de acuerdo con una solicitud de certificación tramitada a través de una AR, enviará una copia del mismo a la AR que remitió la solicitud

4.8 Modificación de certificados

4.8.1 Circunstancias para la modificación de un certificado

Se habla de modificación de un certificado cuando se emite uno nuevo debido a cambios en la información del certificado no relacionados con su clave pública o expiración del periodo de validez.

Las modificaciones de los certificados pueden venir dadas por diferentes motivos tales como:

- Cambio de nombre.
- Cambio en las funciones dentro de la organización.
- Reorganización como resultado del cambio en el Nombre Distintitivo.

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

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

4.9 Revocación y suspensión de certificados

4.9.1 Circunstancias para la revocación

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

El proceso de solicitud de revocación se define en la Política de Certificación aplicable a cada tipo de certificado.

La revocación de un certificado implica su publicación en la Lista de Certificados Revocados (CRL) de acceso público. Al expirar el periodo de validez de un Certificado revocado, éste dejará de estar incluido en la CRL.

Causas de revocación:

Sin perjuicio de lo dispuesto en la normativa aplicable un certificado podrá 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 , la PC asociada o de la presente DPC.

- El titular de un certificado deja de pertenecer al grupo, circunstancia que le facultaba para la posesión del certificado.

- El 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 DPC o en las correspondientes Políticas de Certificación establecidas para cada tipo de Certificado.

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 DPC ni tendrá efectos retroactivos.

4.9.2 Quien puede solicitar la revocación

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

Asimismo, los titulares de certificados o sus responsables, en el caso de los certificados de componente, 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.

Las distintas Políticas de Certificación podrán definir otros procedimientos de identificación que sean más rigurosos.

4.9.3 Procedimiento de solicitud de revocación

El procedimiento para la solicitud de la revocación de cada tipo de certificado se definirá en la Política de Certificación correspondiente.

De forma general y sin perjuicio de lo definido en las PC se establece que:

- Se comunicará al titular del certificado la revocación del mismo mediante correo electrónico. Tras la revocación del certificado el titular deberá cesar en el uso de la clave privada que se corresponda con aquel.

- La solicitud de revocación de un certificado recibida con posterioridad a su fecha de caducidad no será atendida.

La información a suministrar para solicitar la revocación de un certificado se establecerá a expensas de lo especificado en la correspondiente Política de Certificación.

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

Cada PC establecerá el tiempo máximo para la resolución de una solicitud de revocación, si bien se establece como norma general que se haga en menos de 24 horas.

4.9.6 Requisitos de verificación de las revocaciones por los terceros aceptantes

La verificación de las revocaciones, ya sea mediante consulta directa de la CRL o protocolo OCSP, es obligatoria para cada uso de los certificados por los Terceros Aceptantes.

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 revocación de certificados guardadas en memoria 'caché'[6], aun no estando caducadas, no garantizan que dispongan de información de revocación actualizada.

Opcionalmente, salvo que la PC de aplicación establezca lo contrario, se podrá recurrir a la Autoridad de Validación para verificar las revocaciones.

Cuando la PC de aplicación admita otras formas de divulgación de información de revocación, los requisitos para la comprobación de dicha información se especificarán en la propia PC.

4.9.7 Frecuencia de emisión de CRLs

PKIBDE publicará una nueva CRL en su repositorio en el momento en que se produzca cualquier revocación. En cualquier caso, PKIBDE publicará una nueva CRL en su repositorio a intervalos no superiores a 24 horas para las ACs Subordinadas y a 15 años para la AC Raíz, aunque no se hayan producido modificaciones en la CRL, es decir, aunque no se haya revocado ningún certificado desde la última publicación.

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

Cada PC establecerá el tiempo máximo admisible entre la generación de la CRL y su publicación en el repositorio.

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*.

[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.

4.9.10 Requisitos de comprobación en línea de revocación

En el caso de recurrir a la Autoridad de Validación el Tercero Aceptante debe disponer de un software que sea capaz de operar con el protocolo OCSP para obtener la información sobre el certificado.

4.9.11 Otras formas de divulgación de información de revocación disponibles

Algunas PC pueden admitir a otras formas de aviso de revocación.

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 (en el caso de que dicha operación esté contemplada por la PC correspondiente), entre otros, en los siguientes casos:

- Cambio temporal de alguna de las circunstancias 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. Las características y requisitos para la suspensión se establecerán en la correspondiente Política de Certificación.
- 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 puede presentarla el titular del certificado o la persona que se establezca en la PC correspondiente.

4.9.15 Procedimiento para la solicitud de suspensión

Cada PC establecerá el procedimiento para la solicitud de suspensión.

4.9.16 Límites del periodo de suspensión

Sin perjuicio de lo definido en las Políticas de Certificación, PKIBDE suspenderá la vigencia de los certificados 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

PKIBDE dispone como mínimo de dos servicios que proporcionan información sobre el estado de los certificados emitidos por su AC:

- Publicación de las listas de revocación de certificados (CRL). El acceso a las CRL se puede hacer vía Active Directory o LDAP (sólo Terceros Aceptantes ubicados en la red interna del Banco de España) y HTTP (todos los Terceros Aceptantes).
- Servicio de validación en línea (Autoridad de Validación, AV) que implementa Online Certificate Status Protocol siguiendo la RFC 6960 y Lightweight Online Certificate Status Protocol siguiendo la RFC 5019. Mediante el uso de ese protocolo se determina el estado actual de un certificado

electrónico sin requerir las CRLs. Un cliente de OCSP envía una petición sobre el estado del certificado a la AV, la cual, tras consultar la información del estado de revocación de certificados de que dispone, o bien a servicios OCSP de terceros, ofrece una respuesta sobre el estado del certificado vía HTTP.

4.10.2 Disponibilidad del servicio

El servicio, en sus dos variantes, está disponible de forma ininterrumpida todos los días del año, tanto para los Terceros Aceptantes internos del Banco de España como para los Terceros Aceptantes externos.

4.10.3 Características adicionales

Para hacer uso del Servicio de validación en línea es responsabilidad del Tercero Aceptante disponer de un Cliente OCSP que cumpla la RFC 6960 o RFC 5019.

4.11 Extinción de la validez de un certificado

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

- Revocación 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

En cada PC donde se establezca el archivo de claves privadas se identificarán las políticas y prácticas para el registro y recuperación de claves.

No se archivará la clave privada de ningún certificado que tenga autorizada la funcionalidad de firma electrónica no repudiable. Esto se podrá comprobar verificando que la extensión 'Key Usage' tenga el código igual a 1 en el campo 'Non Repudiation'

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

En los casos en que sea de aplicación, la PC correspondiente identificará las políticas y prácticas para la protección y recuperación de la clave de sesión.

5 Controles de seguridad física, instalaciones, gestión y operacionales

5.1 Controles físicos

Los aspectos referentes a los controles de seguridad física se encuentran recogidos en detalle en la documentación que el Servicio de Seguridad y Departamento de Sistemas de Información del Banco de España han desarrollado a tal efecto. En este apartado se van a recoger las medidas adoptadas más relevantes.

5.1.1 Ubicación física y construcción

Los edificios donde se encuentra ubicada la infraestructura de PKIBDE disponen de medidas de seguridad de control de acceso, de forma que se permite la entrada a los mismos a las personas debidamente autorizadas.

Todas las operaciones críticas de PKIBDE se realizan en recintos físicamente seguros, con niveles de seguridad específicos para los elementos más críticos. Estos sistemas están separados de otros del Banco de España, de forma que sólo el personal autorizado pueda acceder a ellos.

Los Centros de Proceso de Datos de PKIBDE cumplen los siguientes requisitos físicos:

a Están alejados de salidas de humos para evitar posibles daños por incendios en otras plantas.

b Ausencia de ventanas al exterior del edificio.

c Cámaras de vigilancia en las áreas de acceso restringido.

d Control de acceso basado en tarjeta y contraseña.

e Sistemas de protección y prevención de incendios: detectores, extintores, formación del personal para actuar ante incendios, etc.

f Existencia de mamparas transparentes, limitando las distintas zonas, que permitan observar las salas desde pasillos de acceso, para detectar intrusiones o actividades ilícitas en su interior.

g Protección del cableado contra daños e interceptación tanto de la transmisión de datos como de telefonía.

5.1.2 Acceso físico

Se dispone de un completo sistema de control de acceso físico de personas a la entrada y a la salida que conforman varios niveles de control. Todas las operaciones sensibles se realizan dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a las máquinas y aplicaciones críticas.

Los sistemas de PKIBDE estarán separados de otros sistemas del Banco de España de forma que únicamente el personal autorizado pueda acceder a ellos, y se garantice la independencia de los otros sistemas informáticos.

Las áreas de carga y descarga están aisladas y permanentemente vigiladas por medios humanos y técnicos.

5.1.3 Alimentación eléctrica y aire acondicionado

Las salas donde se ubican los equipos de la infraestructura de PKIBDE disponen de suministro de electricidad y aire acondicionado adecuado a los requisitos de los equipos en ellas instalados. La infraestructura está protegida contra caídas de tensión o cualquier anomalía en el suministro eléctrico. Aquellos sistemas que lo requieren disponen de unidades de alimentación permanente así como de grupo electrógeno.

5.1.4 Exposición al agua

Se han tomado las medidas adecuadas para prevenir la exposición al agua de los equipos y el cableado.

5.1.5 Protección y prevención de incendios

Las salas disponen de los medios adecuados -detectores- para la protección de su contenido contra incendios.

El cableado se encuentra en falso suelo o falso techo y se dispone de los medios adecuados -detectores en suelo y techo- para la protección del mismo contra incendios.

5.1.6 Sistema de almacenamiento

PKIBDE ha establecido los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva.

PKIBDE ha dispuesto planes de copia de respaldo, los mismos que para el resto de la infraestructura central del Banco de España, de toda la información sensible y de aquella considerada como necesaria para la persistencia de su actividad.

5.1.7 Eliminación de residuos

Se ha adoptado una política de gestión de residuos que garantiza la destrucción de cualquier material que pudiera contener información, así como una política de gestión de los soportes removibles.

5.1.8 Copias de seguridad fuera de las instalaciones

PKIBDE dispone de copias de seguridad en dos locales propios que reúnen las medidas precisas de seguridad y con una separación física adecuada.

5.2 Controles de procedimiento

Por razones de seguridad, la información relativa a los controles de procedimiento se considera materia confidencial y solo se incluye una parte de la misma.

PKIBDE procura que toda la gestión, tanto la relativa a los procedimientos operacionales como a la de administración, se lleve a cabo de forma segura, conforme a lo establecido en este documento, realizando auditorías periódicas. (Véase el capítulo 8 *Auditorías de Cumplimiento y otros Controles de Conformidad*).

Asimismo, se ha diseñado una segregación de funciones para evitar que una sola persona pueda conseguir el control total de la infraestructura.

5.2.1 Roles responsables del control y gestión de la PKI

Se distinguen los siguientes responsables para el control y gestión del sistema:

5.2.1.1 Roles de gestión de los módulos de seguridad hardware

- *Administradores del HSM*: Se define un conjunto de 7 Administradores para el HSM de las AC Raíz y 6 para las AC Corporativa, cada uno con una tarjeta criptográfica de control de acceso a su función. Para la realización de las operaciones que requieran un papel de Administradores es necesario introducir en el lector del HSM un total de 2 tarjetas de las 7 ó 6 definidas, según se trate de las AC Raíz o las AC Corporativa. Los Administradores del HSM se encargan de realizar las siguientes operaciones:

1 Recuperación de la funcionalidad del hardware criptográfico en caso de fallo de un HSM.

2 Recuperación de claves en caso de borrado accidental.

3 Sustitución de un conjunto de tarjetas de administrador. Esta operación solo es necesaria realizarla si se desea ampliar o reducir el conjunto de tarjetas de administrador.

4 Sustitución de un conjunto de tarjetas de operador. Esta operación solo es necesaria realizarla si se desea ampliar o reducir el conjunto de tarjetas de operador o sustituir el existente por deterioro

5 Ampliación del número de HSM integrados en la infraestructura.

6 Dado que se opera en modo FIPS140-2 Nivel 3, autorización para la generación de conjuntos de tarjetas de operador y claves. Esta operación solo se requiere durante la ceremonia de generación de claves para las ACs.

- *Operadores del HSM*: Se define un conjunto de 5 operadores tanto para la AC Raíz como para la AC Corporativa, cada uno con una tarjeta criptográfica de control de acceso a su función. Para la utilización de las claves protegidas por el conjunto de tarjetas de operador es necesario introducir en el lector del HSM dos tarjetas de operador. Los Operadores del HSM se encargan de realizar las siguientes operaciones:

1 Activación de claves para su utilización. Esto significa que cada vez que se inicie una AC, se requerirá la inserción de las tarjetas de operador asociadas a las claves.

2 Autorización para la generación de claves de aplicación, aunque esta autorización puede ser realizada también por un administrador. Esta operación solo se requiere durante la ceremonia de generación de claves para las ACs.

3 Arranque de la interfaz de configuración de las AC y del resto de entidades que conforman la PKI. Mediante esta interfaz, el operador podrá modificar las políticas de certificación y definir los administradores remotos de la AC.

Las operaciones realizadas por los operadores son más frecuentes que las realizadas por los administradores, teniendo que intervenir cada vez que sea necesario volver a configurar la AC o volver a arrancar uno de los procesos involucrados en PKIBDE.

5.2.1.2 Roles de gestión del software de PKI

Oficiales de Registro: una vez iniciados los procesos de la PKI por parte de los operadores del HSM, las tareas de Administración / Gestión del ciclo de vida de los certificados emitidos por los operadores de registro. Estos operadores se encargarán de:

1 Emisión de certificados para las distintas entidades que comprenden la PKI.

2 Emisión de certificados para componentes informáticos (ej. servidores, aplicaciones, etc).

3 Emisión de certificados para usuarios finales, en los casos en los que así se contemple en las Políticas de Certificación

4 Revocación y suspensión de certificados.

Cada operador de registro deberá disponer de un certificado para autenticarse.

Administrador de Sistemas: responsable del funcionamiento de los sistemas que componen la PKI, del hardware y del software base. La responsabilidad de este perfil incluye, entre otros, la administración del sistema de base de datos, del repositorio de información y de los sistemas operativos, así como configuración de los lectores de tarjetas.

Oficial de Seguridad: responsable de la definición y verificación de las políticas y procedimientos de seguridad.

Autoridad de Administración de Políticas: autoridad responsable de la administración de las políticas de certificación.

Administrador de Auditoría: responsable de las tareas de ejecución y revisión de auditorías internas del sistema.

Administrador de Backup: responsable de las tareas de ejecución y revisión de las copias de seguridad del sistema.

Administradores de Usuarios: responsables de las tramitaciones de peticiones de los certificados personales, del control de su correcta descarga por los titulares y de la aceptación por estos de las condiciones de uso.

5.2.2 Número de personas requeridas por tarea

Se requiere un mínimo de dos personas con capacidad profesional suficiente para realizar las tareas de Administración y Operación de los HSM recogidas en el apartado 5.2.1 *Roles responsables del control y gestión de la PKI*.

5.2.3 Identificación y autenticación para cada usuario

Los Administradores y Operadores de HSM se identifican y autentican en los HSM mediante técnicas de secreto compartido en tarjetas criptográficas específicas de los HSM.

El resto de usuarios autorizados de PKIBDE se identifican mediante certificados electrónicos emitidos por la propia PKI y se autentican por medio de tarjetas criptográficas.

5.2.4 Roles que requieren segregación de funciones

La asignación de personal garantizará que se cumplen las siguientes reglas de incompatibilidad:

- Un Administrador de HSM no puede ser Administrador de Auditoría.
- Un Administrador de Sistemas no puede ser ni Oficial de Seguridad ni Administrador de Auditoría.
- Un Oficial de Seguridad no puede ser Administrador de Sistemas ni Administrador de Auditoría.
- Un Administrador de Auditoría no puede ser ni Administrador de HSM, ni Administrador de Sistemas, ni Oficial de Registro, ni Oficial de Seguridad.

5.3 Controles de personal

5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

Todo el personal que preste sus servicios en el ámbito de la PKIBDE deberá poseer el conocimiento, experiencia y formación suficientes, para el mejor cometido de las funciones asignadas.

Para ello, el Banco de España llevará a cabo los procesos de selección de personal que estime precisos con objeto de que el perfil profesional del empleado se adecue lo más posible a las características propias de las tareas a desarrollar.

5.3.2 Procedimientos de comprobación de antecedentes

Según los procedimientos de selección de personal establecidos por el Banco de España.

5.3.3 Requerimientos de formación

Según los procedimientos establecidos por el Banco de España.

En particular, el personal relacionado con la explotación de la PKI, recibirá la formación necesaria para asegurar la correcta realización de sus funciones. Se incluyen en la formación los siguientes aspectos:

- Entrega de una copia de la Declaración de Prácticas de Certificación.
- Concienciación sobre la seguridad física, lógica y técnica
- Operación del software y hardware para cada papel específico.
- Procedimientos de seguridad para cada rol específico.
- Procedimientos de operación y administración para cada rol específico.
- Procedimientos para la recuperación de la operación de la PKI en caso de desastres.

5.3.4 Requerimientos y frecuencia de actualización de la formación

Según los procedimientos establecidos por el Banco de España.

5.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado.

5.3.6 Sanciones por actuaciones no autorizadas

La comisión de acciones no autorizadas será calificada como falta laboral y sancionada conforme a lo preceptuado en el Reglamento de Trabajo del Banco de España y en el Estatuto de los Trabajadores, sin perjuicio de las responsabilidades de otra índole en que pudiera incurrirse.

5.3.7 Requisitos de contratación de terceros

Se aplicará la normativa general del Banco de España para las contrataciones.

5.3.8 Documentación proporcionada al personal

Se facilitará el acceso a la normativa de seguridad de obligado cumplimiento junto con la presente DPC y las contenidas en las PC que sean de aplicación.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de eventos registrados

Las operaciones se dividen en eventos, por lo que se guarda información sobre uno o más eventos para cada operación relevante. Los eventos registrados poseen, como mínimo, la información siguiente:

Categoría: Indica la importancia del evento.

- Informativo: los eventos de esta categoría contienen información sobre operaciones realizadas con éxito.
- Marca: cada vez que empieza y termina una sesión de administración, se registra un evento de esta categoría.
- Advertencia: indica que se ha detectado un hecho inusual durante una operación, pero que no provocó que la operación fallara (p.ej. una petición de lote denegada).
- Error: indica el fallo de una operación debido a un error predecible (p.ej. un lote que no se ha procesado porque la AR pidió una plantilla de certificación para la cual no estaba autorizada).
- Error Fatal: indica que ha ocurrido una circunstancia excepcional durante una operación (p.ej. una tabla de base de datos a la que no se puede acceder).

Fecha: Fecha y hora en la que ocurrió el evento.

Autor: Nombre distintivo de la Autoridad que generó el evento.

Rol: Tipo de Autoridad que generó el evento.

Tipo evento: Identifica el tipo del evento, distinguiendo, entre otros, los eventos criptográficos, de interfaz de usuario, de librería.

Id. Evento: Número que identifica exclusivamente a un evento de entre un grupo de eventos del mismo tipo, generados por un mismo módulo.

Módulo: Identifica el módulo que generó el evento. Los posibles módulos son:

- AC.
- AR.
- Repositorio de información.
- Librerías de control de almacenamiento de información.

Nivel: Número que indica el nivel en que se encuentra el evento. Los eventos producidos por algunas operaciones están organizados de forma jerárquica, por lo que un evento puede agrupar otros eventos de nivel inferior, en función de la complejidad de la operación. Para eventos de primer nivel, este campo indicará un valor de 1. Para los de segundo nivel, y sucesivos, indicará el valor correspondiente. Se asignará un valor de 0 a los eventos en los que esta característica no sea aplicable.

Observaciones: Representación textual del evento. Para algunos eventos, la descripción va seguida de una lista de parámetros cuyos valores variarán dependiendo de los datos sobre los que se ejecutó la operación.

Algunos ejemplos de los parámetros que se incluyen para la descripción del evento "Certificado generado" son: el número de serie, el nombre distintivo del titular del certificado emitido y la plantilla de certificación que se ha aplicado.

Los eventos registrados en la Base de Datos pueden estar sujetos al tipo de certificado, quedando especificado en la correspondiente Política de Certificación.

5.4.2 Frecuencia de procesado de registros de auditoría

Los registros se analizarán de manera manual cuando sea necesario, o bien haciendo uso de herramientas automáticas, no existiendo una frecuencia definida para dicho proceso.

5.4.3 Periodo de conservación de los registros de auditoría

La información generada por los registros de auditoría se mantiene en línea hasta que es archivada. Una vez archivados, los registros de auditoría se conservarán, al menos, durante 5 años.

5.4.4 Protección de los registros de auditoría

Los eventos registrados por la PKI están protegidos mediante cifrado, de forma que nadie, salvo las propias aplicaciones de visualización de eventos, con su debido control de accesos, pueda acceder a ellos.

La destrucción de un archivo de auditoría solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Coordinador de Seguridad y el Administrador de Auditorías de PKIBDE. Tal destrucción se puede iniciar por la recomendación escrita de cualquiera de estas tres Autoridades o del administrador del servicio auditado.

5.4.5 Procedimientos de respaldo de los registros de auditoría

Las copias de respaldo de los registros de auditoría se realizan según las medidas estándar establecidas por el Banco de España para las copias de respaldo de las Bases de Datos de los Ordenadores Centrales.

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

El sistema de recopilación de información de auditoría de la PKI es una combinación de procesos automáticos y manuales ejecutados por las aplicaciones de la PKI. Todos los registros de auditoría de las ACs, ARs, y Administradores Remotos se almacenan en los sistemas internos de PKIBDE.

Todos los elementos significativos existentes en PKIBDE se acumulan en una Base de Datos. Los procedimientos de control de seguridad empleados en PKIBDE se basan en la tecnología de construcción empleada en la base de datos.

Las características de este sistema son las siguientes:

- Permite verificar la integridad de la base de datos, es decir, detecta una posible manipulación fraudulenta de los datos.

- Asegura el no repudio por parte de los autores de las operaciones realizadas sobre los datos. Esto se consigue mediante las firmas electrónicas.

- Guarda un registro histórico de actualización de datos, es decir, almacena versiones sucesivas de cada registro resultante de diferentes operaciones realizadas sobre él. Esto permite guardar un registro de las operaciones realizadas y evita que se pierdan firmas electrónicas realizadas anteriormente por otros usuarios cuando se actualizan los datos.

La siguiente lista es un resumen de los posibles peligros a los que una base de datos puede estar expuesta y que pueden detectarse con las pruebas de integridad:

- Inserción o alteración fraudulenta de un registro de sesión.

- Supresión fraudulenta de sesiones intermedias.
- Inserción, alteración o supresión fraudulenta de un registro histórico.
- Inserción, alteración o supresión fraudulenta del registro de una tabla de consultas.

5.4.7 Notificación al sujeto causa del evento

No se prevé la notificación automática de la acción de los ficheros de registro de auditoría al causante del evento.

5.4.8 Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto con el Plan de Auditoría del Banco de España.

5.5 Archivo de registros

5.5.1 Tipo de eventos archivados

Cada Autoridad de Certificación definida en PKIBDE conserva toda la información relevante sobre las operaciones realizadas con los certificados durante los periodos de tiempo establecidos, manteniendo un registro de eventos.

Las operaciones registradas incluyen las realizadas por los administradores que utilizan las aplicaciones de administración de los elementos de PKIBDE, así como toda la información relacionada con el proceso de registro.

Los tipos de datos o ficheros que son archivados son, entre otros, los siguientes:

- Datos relacionados con el procedimiento de registro y solicitud de certificados
- Los especificados en el punto 5.4.1.
- El fichero histórico de claves.

5.5.2 Periodo de conservación de registros

Toda la información y documentación relativa a los certificados se conservarán durante 15 años, plazo que en el caso de los certificados reconocidos deriva de un mandato legal

Para los registros de auditoría se estará a lo especificado en el apartado 5.4.3, siempre atendiendo a cualquier particularidad especificada en la Política de Certificación del Certificado correspondiente a los datos involucrados.

5.5.3 Protección del archivo

Los Archivos de registro están protegidos mediante cifrado, de forma que nadie, salvo las propias aplicaciones de visualización, con su debido control de accesos, pueda acceder a ellos.

La destrucción de un archivo de Registro solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Coordinador de Seguridad y el Administrador de Auditorías de PKIBDE. Tal destrucción se puede iniciar por la recomendación escrita de cualquiera de estas tres Autoridades o del administrador del servicio auditado.

5.5.4 Procedimientos de copia de respaldo del archivo

Las copias de respaldo de los Archivos de registros se realizan según las medidas estándar establecidas por el Banco de España para las copias de respaldo de las Bases de Datos de los Ordenadores Centrales.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Los sistemas de información empleados por PKIBDE garantizan el registro del tiempo en los que se realizan. El instante de tiempo de los sistemas proviene de una fuente segura que constata la fecha y hora. En concreto, la señal de reloj proviene de alguna de estas fuentes:

- Del reloj atómico de Braunschweig, Alemania, (Physikalisch Technische Bundesanstalt), que representa la hora oficial dentro del Eurosistema. Es codificada y transmitida vía radio.

- Del Real Instituto y Observatorio de la Armada (ROA), que es el responsable del mantenimiento de la unidad básica de Tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como del mantenimiento y difusión oficial de la escala "Tiempo Universal Coordinado" (UTC(ROA)), considerada a todos los efectos como la base de la hora legal en todo el territorio nacional (R. D. 23 octubre 1992, núm. 1308/1992).

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

El sistema de recogida de información es interno a la Autoridad y corresponde a la PKIBDE.

5.5.7 Procedimientos para obtener y verificar información archivada

Los eventos registrados por la PKI están protegidos mediante cifrado, de forma que nadie salvo las propias aplicaciones de visualización y gestión de eventos pueda acceder a ellos.

Esta verificación debe ser llevada a cabo por el Administrador de Auditoría que debe tener acceso a las herramientas de verificación y control de integridad del registro de eventos de la PKI.

5.6 Cambio de claves de una AC

Los procedimientos para proporcionar, en caso de cambio de claves, una nueva clave pública de AC a los titulares y terceros aceptantes de los certificados de la misma son los mismos que para proporcionar la clave pública en vigor. En consecuencia, la nueva clave se publicará en el repositorio de PKIBDE (ver apartado 2.1)

5.7 Recuperación en caso de compromiso de una clave o catástrofe

5.7.1 Procedimientos de gestión de incidentes y compromisos

El Banco de España tiene establecido un Plan de Contingencia que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por PKIBDE.

El Plan de Contingencia contempla, entre otros aspectos, los siguientes:

- La redundancia de los componentes más críticos.
- La puesta en marcha de un centro de respaldo alternativo.
- El chequeo completo y periódico de los servicios de copia de respaldo.

En el caso de que se produjera un compromiso de los datos de verificación de firma de alguna Autoridad de Certificación, PKIBDE informará a todos los titulares de certificados de PKIBDE y terceros aceptantes conocidos que todos los certificados y listas de revocación de certificados firmados con estos datos ya no son válidos. Tan pronto como sea posible se procederá al restablecimiento del servicio.

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

Si los recursos hardware, software, y/o datos se alteran o se sospecha que han sido alterados se detendrá el funcionamiento de la PKI hasta que se restablezca la seguridad del entorno con la incorporación de nuevos componentes cuya adecuación pueda acreditarse. De forma simultánea se realizará una auditoría para identificar la causa de la alteración y asegurar su no reproducción.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los usuarios de los mismos y se procederá a una nueva certificación.

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

En el caso de compromiso de la clave privada de una Autoridad se procederá a su revocación inmediata. Seguidamente, se generará y publicará la correspondiente CRL, cesando el funcionamiento de actividad de la Autoridad y se procederá a la generación, certificación y puesta en marcha de una nueva Autoridad con un nuevo par de claves y con la misma denominación que la eliminada pero modificando el identificador de versión.

En el caso de que la Autoridad afectada sea una AC, el certificado revocado de la misma permanecerá accesible en el repositorio de PKIBDE con objeto de continuar verificando los certificados emitidos durante su periodo de funcionamiento.

Las Autoridades componentes de PKIBDE dependientes de la AC afectada serán informadas del hecho y conminadas a solicitar una nueva certificación por la AC con su nueva clave.

Se notificará a todas las Autoridades afectadas que los certificados y la información sobre su revocación, suministrada con la clave comprometida de la AC, deja de ser válida desde el momento de la notificación, debiendo utilizar para verificar la validez de la información la nueva clave pública de la AC.

Los certificados firmados por Autoridades dependientes de la AC afectada en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, serán a su vez revocados, informados sus titulares de tal hecho y se procederá a la emisión de nuevos certificados.

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

El sistema de Autoridades de Certificación de PKIBDE puede ser reconstruido en caso de desastre. Para llevar a cabo esta reconstrucción es necesario contar con:

- Un sistema con hardware, software y dispositivo Hardware Criptográfico de Seguridad similar al existente con anterioridad al desastre.
- Las tarjetas de administrador de todas las Autoridades de Certificación de PKIBDE.
- Una copia de respaldo de los discos del sistema anterior al desastre.

Con estos elementos es posible reconstruir el sistema tal y como estaba en el momento de la copia de respaldo realizada y, por lo tanto, recuperar la AC, incluidas sus claves privadas.

El almacenado, tanto de las tarjetas de acceso de los administradores de las ACs como de las copias de los discos de sistema de cada AC, se lleva a cabo en un lugar diferente, lo suficientemente alejado y protegido como para dificultar al máximo la concurrencia de catástrofes simultáneas en los sistemas en producción y en los elementos de recuperación.

5.8 Cese de una AC o AR

5.8.1 Autoridad de Certificación

En el caso de cesar la actividad de una de las AC, PKIBDE se asegurará de que los potenciales problemas para los titulares de sus certificados y los terceros aceptantes sean los mínimos, así como el mantenimiento de los registros requeridos para proporcionar prueba cierta de la certificación a efectos legales.

En caso de cese de la actividad de una o de todas sus ACs, PKIBDE comunicará a los titulares de sus certificados, por cualquier medio que garantice el envío y la recepción de la notificación y con un plazo mínimo de antelación de 2 meses al citado cese de actividad, su intención de que la/s AC correspondientes cesen en la actividad como prestadores de servicios de certificación.

En el supuesto de que PKIBDE decidiera transferir la actividad a otro Prestador de Servicios de Certificación, comunicará al titular de sus certificados los acuerdos de transferencia. A tal efecto PKIBDE enviará un documento explicativo de las condiciones de transferencia y de las características del Prestador al que se propone la transferencia de la gestión de los certificados. Esta comunicación se realizará por cualquier medio que garantice el envío y la recepción de la notificación, con una antelación mínima de 2 meses al cese efectivo de su actividad.

PKIBDE comunicará al Ministerio de Industria, Comercio y Turismo, con la antelación indicada en el anterior apartado, el cese de su actividad y el destino que vaya a dar a los certificados especificando si va a transferir la gestión y a quién o si se extinguirá su vigencia.

Igualmente, comunicará cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad.

PKIBDE remitirá al Ministerio de Industria, Comercio y Turismo con carácter previo al cese definitivo de su actividad la información relativa a los certificados cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a los efectos previstos en el artículo 20.1.f de la Ley de Firma electrónica.

Transcurrido el plazo de dos meses, sin que exista acuerdo de transferencia, los certificados serán revocados.

5.8.2 Autoridad de Registro

Una vez que la Autoridad de Registro cese en el ejercicio de las funciones, transferirá los registros que mantenga a PKIBDE, mientras exista la obligación de mantener archivada la información, y de no ser así, ésta será destruida.

6 Controles de seguridad técnica

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

Los pares de claves para los componentes internos de PKIBDE, concretamente AC Raíz y AC Corporativa, se generan en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3 que tienen instalados en sus respectivos sistemas. Los sistemas de hardware y software que se emplean son conformes a las normas CWA 14167-1 y CWA 14167-2.

Los pares de claves para el resto de titulares se generan en función de lo estipulado en la Política de Certificación aplicable a cada certificado.

Los dispositivos hardware o software a utilizar en la generación de claves para cada tipo de certificado emitido por PKIBDE vienen definidos por la Política de Certificación que le sea de aplicación.

6.1.2 Entrega de la clave privada al titular

El método de entrega de la clave privada a sus titulares depende de cada certificado y será establecido en la Política de Certificación correspondiente a cada certificado.

6.1.3 Entrega de la clave pública al emisor del certificado

El método de entrega de la clave pública al emisor en los casos en que la genere el Titular dependerá de cada certificado y será establecido en la Política de Certificación correspondiente.

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

Las claves públicas de las AC Raíz y de AC Corporativa están a disposición de los terceros aceptantes en el Repositorio de PKIBDE (ver apartado 2.1) sin perjuicio de que una PC pueda establecer mecanismos adicionales de entrega de dichas claves.

6.1.5 Tamaño de las claves

El tamaño de las claves de la AC Raíz y de la AC Corporativa es de 2048 bits.

A partir de la versión 2 de las AC Raíz y AC Corporativa, el tamaño de clave es de 4096 bits. Versiones sucesivas podrán ver aumentado el tamaño de clave de las AC de acuerdo a las recomendaciones internacionales existentes en el momento de su creación.

El tamaño de las claves para cada tipo de certificado emitido por PKIBDE viene definido por la Política de Certificación que le sea de aplicación.

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

La clave pública de la AC Raíz y de la AC Corporativa está codificada de acuerdo con RFC 5280 y PKCS#1. El algoritmo de generación de claves es el RSA.

Los parámetros de generación de claves para cada tipo de certificado emitido por PKIBDE vienen definidos en la Política de Certificación que le sea de aplicación.

Los procedimientos y medios de comprobación de la calidad de los parámetros de generación de claves para cada tipo de certificado emitido por PKIBDE vienen definidos por la Política de Certificación que le sea de aplicación.

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

Los usos admitidos de la clave para cada tipo de certificado emitido por PKIBDE vienen definidos por la Política de Certificación que le sea de aplicación.

Todos los certificados emitidos por PKIBDE contienen la extensión *Key Usage* definida por el estándar X.509 v3, la cual se califica como crítica. Asimismo, pueden establecerse limitaciones adicionales mediante la extensión *Extended Key Usage*.

Ha de tenerse en cuenta que la eficacia de las limitaciones basadas en extensiones de los certificados depende, en ocasiones, de la operatividad de aplicaciones informáticas que no han sido fabricadas ni controladas por PKIBDE.

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

6.2.1 Estándares para los módulos criptográficos

Los módulos utilizados para la creación de claves utilizadas por las AC Raíz y AC Corporativa de PKIBDE cumplan con la certificación FIPS 140-2 de nivel 3.

La puesta en marcha de cada una de las Autoridades de Certificación, teniendo en cuenta 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.

PKIBDE utiliza módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros. PKIBDE únicamente utiliza módulos criptográficos con certificación FIPS 140-2 Nivel 3 que cumplan las siguientes normas:

- FCC: CRFA47, Parte 15, Subparte B, Clase A
- CE: EN 55022 Clase A, EN 55024-1, EN 60950

En cuanto a las tarjetas criptográficas con certificados para firma electrónica avanzada, 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

Las claves privadas, tanto de las AC Raíz como AC Corporativa, se encuentran bajo control multipersona[7]. Se activan mediante la inicialización del software de AC por medio de la combinación mínima de operadores de las AC correspondientes. Éste es el único método de activación de dicha clave privada.

Son necesarios dos operadores de PKIBDE, de un total de cinco, para activar y usar las claves privadas de las AC Raíz o de las AC Corporativa de PKIBDE.

6.2.3 Custodia de la clave privada

La custodia de las claves privadas de los certificados la realizan los propios titulares de las mismas. En el caso de las claves privadas de cifrado PKIBDE efectúa sólo su archivo.

Las claves privadas de las Autoridades de Certificación que componen PKIBDE se encuentran alojadas en dispositivos de hardware criptográfico con certificación FIPS-2 de nivel 3 asociadas a cada una de las ACs.

6.2.4 Copia de seguridad de la clave privada

Las claves privadas de las ACs de PKIBDE están archivadas bajo la protección de los HSM que cada una de ellas posee y a los que sólo ellas y los administradores y operadores de la correspondiente AC tienen acceso.

[7] Control multipersona: control por más de una persona, normalmente por un subconjunto 'k' de un total de 'n' personas. De esta forma, se garantiza que nadie tenga el control de forma individual de las actuaciones críticas a la vez que se facilita la disponibilidad de las personas necesarias.

6.2.5 Archivo de la clave privada

Las claves privadas de firma de personas nunca serán archivadas para garantizar el no repudio.

Las claves privadas de cifrado son archivadas, debiéndose establecer en su PC el procedimiento de recuperación.

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

La transferencia de la clave privada sólo se puede hacer entre módulos criptográficos (HSM) y requiere de la intervención de dos de los siete administradores.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas se generan en el módulo criptográfico en el momento de la creación de cada una de las Autoridades de PKIBDE que hacen uso de dichos módulos y se guardan cifradas.

6.2.8 Método de activación de la clave privada

Tal y como se estipula en el apartado 6.2.2 *Control multipersona de la clave privada*, las claves privadas tanto de las AC Raíz como las AC Corporativa, se activan mediante la inicialización del software de AC por medio de la combinación mínima de operadores de la AC correspondiente. Éste es el único método de activación de dicha clave privada.

Concretamente, son necesarios dos Operadores de PKIBDE para activar las claves privadas de las *AC Raíz* y las *AC Corporativa* de PKIBDE.

En el caso de las claves del resto de titulares, la activación de éstas viene definida por la Política de Certificación que les sea de aplicación.

6.2.9 Método de desactivación de la clave privada

El Administrador de Sistemas con autorización de dos Administradores del HSM puede proceder a la desactivación de la clave de las Autoridades de Certificación de PKIBDE mediante la parada de la aplicación informática de la AC correspondiente.

6.2.10 Método de destrucción de la clave privada

No estipulado

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

PKIBDE mantiene un archivo de todos los certificados, los cuales incluyen las claves públicas, emitidos por un periodo de quince (15) años. El control de dicho registro está a cargo de los Administradores de cada una de las ACs de PKIBDE.

El archivo dispone de medios de protección frente a las manipulaciones que pretendan efectuarse sobre la información contenida.

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

Los certificados y pares de claves de AC Raíz de PKIBDE tienen una validez de treinta (30) años y los de AC Corporativa de PKIBDE de quince (15) años.

El periodo de validez del resto de certificados vendrá establecido por la Política de Certificación aplicable a cada uno.

6.4 Datos de activación

6.4.1 Datos de activación de las claves privadas de las Autoridades de Certificación

Las claves privadas de las AC Raíz y Corporativas se encuentran protegidas mediante hardware criptográfico que cumple la normativa FIPS140-2 Nivel 3.

El acceso al hardware criptográfico se controla por medio de dos conjuntos de tarjetas, a su vez protegidas con un PIN.

Se distingue entre dos tipos de tarjeta:

- El conjunto de *tarjetas de administrador*. Estas tarjetas serán necesarias para que dos administradores puedan recuperar el estado del HSM si ocurre algún desastre o si se desea trasladar las claves a otro módulo. El uso de cada tarjeta se encuentra protegido por un PIN diferente.

- El conjunto de *tarjetas de operador*. Estas tarjetas se utilizarán para proteger el acceso a las claves de las AC. Debe haber un mínimo de dos operadores presentes y deben indicar el PIN de sus tarjetas respectivas para realizar cualquier operación con la AC, implique o no el uso de las claves de la AC.

6.4.1.1 Generación e instalación de los datos de activación

La generación de las claves privadas de las AC se protocoliza en forma de una ceremonia de claves que se desarrolla siguiendo un guión prestablecido y con la participación de testigos y responsables que dan fe de la corrección en el procedimiento seguido, lo que permite:

- Garantizar que la clave privada queda guardada convenientemente y que no se generan copias indebidas de la misma. Esto implica:
    - Almacenamiento de las claves utilizando hardware criptográfico (HSM) que cumple la normativa FIPS 140-2 Nivel III
    - Protección de las claves criptográficas almacenadas por el HSM de la CA Raíz, mediante dos conjuntos de tarjetas criptográficas, que son generadas durante la ceremonia de claves, durante la cual el receptor de la tarjeta establece el PIN de protección de la misma:
        - Administradores: Los administradores del HSM tendrán el control sobre la configuración, administración y recuperación de los HSM. Se creará un conjunto de 7 tarjetas criptográficas, de las cuales 2 serán necesarias para realizar las labores de administración ("K de N" = "2 de 7").
        - Operadores: Los operadores del HSM administran la creación, borrado y acceso del conjunto de claves de servicios, almacenadas en el HSM. Se creará un conjunto de 5 tarjetas criptográficas, de las cuales 2 serán necesarias para realizar las labores de operación ("K de N" = "2 de 5").
    - Protección de las credenciales de los roles de administrador de la PKI, de forma que los procesos de administración de PKIBDE sean conformes al perfil de protección CWA-14167-1.
- Auditabilidad del proceso.

Si una o más tarjetas se pierden o dañan, o el administrador olvida su PIN o dejan de ser utilizables por alguna razón, deberá volverse a generar todo el conjunto de tarjetas tan pronto como sea posible utilizando la totalidad de tarjetas de seguridad. El proceso de regeneración del conjunto de tarjetas correspondiente será protocolizado de modo que se mantenga la trazabilidad iniciada con la Ceremonia de Claves.

6.4.1.2 Protección de los datos de activación

Cada una de las tarjetas criptográficas que conforman los conjuntos que protegen las claves del HSM de la CA Raíz así como el juego de tarjetas que contienen las credenciales de los roles de administración, se encuentran protegidas por un PIN que sólo sus titulares conocen.

Adicionalmente cada tarjeta se encuentra dentro de un sobre de seguridad cuyo número de serie es conocido. Por último y con el fin de garantizar su disponibilidad, estos sobres han sido distribuidos en distintas ubicaciones de las instalaciones del Prestador, donde se almacenan dentro de dispositivos de seguridad físicos.

6.4.1.3 Otros aspectos de los datos de activación

El Prestador realizará auditorías periódicas de periodicidad no superior a un trimestre con el objetivo de verificar que el acceso a los datos de activación no ha sido vulnerado.

6.5 Controles de seguridad informática

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos, como en el caso de auditorías externas o internas e inspecciones.

6.5.1 Requerimientos técnicos de seguridad específicos

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

6.5.2 Evaluación de la seguridad informática

PKIBDE evalúa de forma permanente su nivel de seguridad de cara a identificar posibles debilidades y establecer las correspondientes acciones correctoras mediante auditorías externas e internas, así con la realización continua de controles de seguridad.

6.6 Controles de seguridad del ciclo de vida

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

6.6.1 Controles de desarrollo de sistemas

Los requisitos de seguridad son exigibles, desde su inicio, tanto en la adquisición de sistemas informáticos como en el desarrollo de los mismos ya que puedan tener algún impacto sobre la seguridad de PKIBDE.

6.6.2 Controles de gestión de seguridad

Existe una organización de seguridad encargada de su gestión.

6.6.3 Controles de seguridad del ciclo de vida

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas con algún impacto en la seguridad de PKIBDE.

6.7 Controles de seguridad de la red

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

6.8 Sellado de tiempo

No estipulado.

7 Perfiles de los Certificados, CRL y OCSP

7.1 Perfil de certificado

7.1.1 Número de versión

PKIBDE soporta y utiliza certificados 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.
- *BasicConstraints*. Calificada como crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *SubjectAlternativeName*. Calificada como no crítica.
- *CRLDistributionPoint*. Calificada como no crítica.
- *Subject Key Identifier*. Calificada como no crítica.
- *Authority Key Identifier*. Calificada como no crítica.
- *extKeyUsage*. Calificada como no crítica.
- *Auth. Information Access*. Calificada como no crítica.
- *bdeCertType (1.3.6.1.4.1.19484.2.3.6)*. Calificada como no crítica.

Las Políticas de Certificación de PKIBDE pueden establecer variaciones en conjunto de las extensiones utilizadas por cada tipo de certificado.

PKIBDE tiene definida una política de asignación de OID's dentro de su rango privado de numeración por la cual el OID de todas las Extensiones propietarias de Certificados de PKIBDE comienzan con el prefijo 1.3.6.1.4.1.19484.2.3.

PKIBDE tiene definidas las siguientes extensiones propietarias:

OID	Concepto	Descripción
1.3.6.1.4.1.19484.2.3.1	Nombre	Nombre y apellidos de la persona física titular del Certificado
1.3.6.1.4.1.19484.2.3.2	Apellido 1	
1.3.6.1.4.1.19484.2.3.3	Apellido 2	
1.3.6.1.4.1.19484.2.3.4	Nº de empleado	Nº de empleado o contratado en el Banco de España
1.3.6.1.4.1.19484.2.3.5	Código de usuario	Código de usuario en los sistemas de información del Banco de España
1.3.6.1.4.1.19484.2.3.6	bdeCertType	Identifica el tipo de certificado
1.3.6.1.4.1.19484.2.3.7	bdeDocIdent	Documento de identificación (NIF, Nº Pasaporte,…)
1.3.6.1.4.1.19484.2.3.8	bdeNombEnt	Nombre de entidad para la que se emite el certificado
1.3.6.1.4.1.19484.2.3.9	bdeCIF	Código de identificación fiscal de la entidad
1.3.6.1.4.1.19484.2.3.10	bdeValidTipo	Procedimiento de validación de la solicitud de certificado

1.3.6.1.4.1.19484.2.3.11	bdeValidID	Código de UA interna que ha validado la solicitud o identificador de PSC y tipo de certificado utilizado para solicitar el certificado
1.3.6.1.4.1.19484.2.3.12	bdeCodBETipo	Tipo de código de BDE de la entidad
1.3.6.1.4.1.19484.2.3.13	bdeCodBE	Código de BDE de la entidad
1.3.6.1.4.1.19484.2.3.14	bdeNumDifer	Nº utilizado para diferenciar los certificados emitidos a una misma entidad externa
1.3.6.1.4.1.19484.2.3.15	bdeTipoPersona	Identificador que distingue si el titular de un certificado usuario interno es subcontratado o no.

7.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
- SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- SHA-512 with RSA Encryption (1.2.840.113549.1.1.13)

7.1.4 Formatos de nombres

Los certificados emitidos por PKIBDE contienen el distinguished name X.500 del emisor y del titular 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.

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

A definir en cada Política de Certificación.

PKIBDE tiene definida una política de asignación de OID's dentro de su rango privado de numeración por la cual el OID de todas las Políticas de Certificación de PKIBDE comienzan con el prefijo 1.3.6.1.4.1.19484.2.2

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

En el campo Notice Reference se incluirá un texto con información básica sobre el certificado y las políticas a que está sujeto:

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)

En el caso del que el certificado tenga el carácter legal de reconocido, dentro del mismo se incluirá en el campo Notice Reference un texto con información básica sobre el certificado, su carácter de reconocido, las políticas a que está sujeto y el domicilio del Banco de España, tal como exige el artículo 11.2 de la Ley 59/2003 de Firma Electrónica:

Certificado Reconocido según la legislación vigente. Uso sujeto a la DPC del Banco de España.

© 2015 Banco de España. Todos los derechos reservados. (C/Alcalá 48, 28014 Madrid-España)

7.1.9 Tratamiento semántico para la extensión crítica "Certificate Policy"

La extensión será calificada como *nonCritical* cuando se emplee con el objeto de mantener la máxima capacidad de poder operar con otras AC del certificado. Esto se hace siguiendo las recomendaciones para aplicaciones estándar de correo electrónico seguro S/MIME [RFC 2632] y autenticación web SSL/TLS [RFC 2246]. El hecho de que la extensión no sea crítica no impide que las aplicaciones utilicen la información contenida en la citada extensión.

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

Las extensiones utilizadas en las listas de revocación son:

- *CRLNumber*. Calificada como no crítica.
- *AuthorityKeyIdentifier*. Calificada como no crítica.
- *IssuingDistributionPoint*. Calificada como no crítica.

7.3 Perfil de OCSP

7.3.1 Número(s) de versión

El perfil es el definido en la RFC 6960. Es también compatible con RFC 5019.

7.3.2 Extensiones OCSP

La Autoridad de Validación soporta peticiones firmadas y la extensión NONCE.

8 Auditorías de cumplimiento y otros controles

8.1 Frecuencia o circunstancias de los controles para cada Autoridad

Se llevará a cabo una auditoría sobre PKIBDE de forma regular, de acuerdo con el Plan de Auditorías del Banco de España. Con ello se garantiza la adecuación de su funcionamiento y operativa con las estipulaciones incluidas en esta DPC y las PC.

Como mínimo se realizarán auditorías cada dos años, de acuerdo con lo que establece el Reglamento de Medidas de Seguridad (RD 1720/2007, de 21 de diciembre) para los ficheros de nivel medio.

8.2 Identificación/cualificación del auditor

La realización de las auditorías podrá ser encargada a empresas auditoras externas o al Departamento de Auditoría Interna en función de la disponibilidad de personal cualificado en los aspectos concretos a auditar y de lo que establezca el Plan de Auditorías.

Todo equipo o persona designada para realizar una auditoría de seguridad sobre PKIBDE deberá cumplir los siguientes requisitos:

- Adecuada capacitación y experiencia en PKI, seguridad, tecnologías criptográficas y procesos de auditoría.
- Independencia a nivel organizativo de la autoridad de PKIBDE.

8.3 Relación entre el auditor y la Autoridad auditada

Al margen de la función de auditoría, el auditor externo y la parte auditada (PKIBDE) no deberán tener relación alguna que pueda derivar en un conflicto de intereses. En el caso de los auditores internos, estos no podrán tener relación funcional con el área objeto de la auditoría

8.4 Aspectos cubiertos por los controles

La auditoría determinará la adecuación de los servicios de PKIBDE con esta DPC y las PC's aplicables. También determinará los riesgos del incumplimiento de la adecuación con la operativa definida por esos documentos.

El ámbito de actividad de una auditoría incluirá, al menos a:

- Política de seguridad y privacidad
- Seguridad física
- Evaluación tecnológica
- Administración de los servicios de la AC
- Selección de personal
- DPC y PC's competentes
- Contratos

8.5 Acciones a tomar como resultado de la detección de deficiencias

La identificación de deficiencias detectadas como resultado de la auditoría dará lugar a la adopción de medidas correctivas. La Autoridad de Administración de Políticas (AAP), en colaboración con el auditor, será la responsable de la determinación de las mismas.

En el caso de observarse deficiencias graves la Autoridad de Administración de Políticas podrá adoptar, entre otras, las siguientes decisiones: suspensión temporal de las operaciones hasta que las deficiencias se corrijan, revocación del certificado de la Autoridad, cambios en el personal implicado, invocación de la política de responsabilidades y auditorías globales más frecuentes.

8.6 Comunicación de resultados

El equipo auditor comunicará los resultados de la auditoría a la Autoridad de Administración de Políticas de PKIBDE (AAP), al Gestor de Seguridad de PKIBDE, así como a los administradores de PKIBDE y de la Autoridad en la que se detecten incidencias.

9 Otras cuestiones legales y de actividad

9.1 Tarifas

9.1.1 Tarifas de emisión de certificado o renovación

Las tarifas de emisión y renovación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

9.1.2 Tarifas de acceso a los certificados

Las tarifas de acceso a los certificados se especifican en la Política de Certificación que les sea de aplicación.

9.1.3 Tarifas de acceso a la información de estado o revocación

Las tarifas de acceso a la información de estado o revocación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

9.1.4 Tarifas de otros servicios tales como información de políticas

No se aplicará ninguna tarifa por el servicio de información sobre esta DPC, ni las políticas de certificación administradas por PKIBDE, ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la elaboración del presente documento.

Esta disposición podrá ser modificada por la Política de Certificación aplicable en cada caso.

9.1.5 Política de reembolso

En el caso de que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte de PKIBDE para el tipo de certificados que defina, será obligado determinar la política de reembolso correspondiente.

9.2 Confidencialidad de la información

Con independencia de lo establecido en el artículo 6 del Real Decreto-Legislativo 1298/1986, de 26 de junio, sobre el deber de confidencialidad de los datos e informaciones de las que disponga el Banco de España en el ejercicio de sus funciones, se establece el siguiente régimen de confidencialidad de los datos relativos a la PKIBDE:

9.2.1 Ámbito de la información confidencial

Toda información que no sea considerada por PKIBDE como pública revestirá el carácter de confidencial. Se declara expresamente como información confidencial:

- Las claves privadas de las Autoridades que componen PKIBDE.
- Las claves privadas de titulares que PKIBDE mantenga en custodia.
- La información relativa a las operaciones que lleve a cabo PKIBDE.
- La información referida a los parámetros de seguridad, control y procedimientos de auditoría.
- La información de carácter personal proporcionada por los titulares de certificados a PKIBDE durante el proceso de registro, de conformidad con lo dispuesto en la normativa sobre protección de datos de carácter personal y reglas de desarrollo.

9.2.2 Información no confidencial

Se considera información pública y por lo tanto accesible por terceros:

- La contenida en la presente Declaración de Prácticas de Certificación.
- La incluida en las Políticas de certificación que le sean de aplicación.
- Los certificados emitidos por PKIBDE.

- La lista de los certificados suspendidos o revocados.

9.2.3 Deber de secreto profesional

Los empleados del Banco de España que participen en cualesquiera tareas propias o derivadas de la PKIBDE están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa reguladora que les es aplicable recogida fundamentalmente en el Reglamento Interno del Banco de España, aprobado por Resolución del Consejo de Gobierno, de 28 de marzo de 2000 y en la normativa convencional interna.

Asimismo el personal contratado que participe en cualquier actividad u operación de PKBIDE estará sujeto al deber de secreto en el marco de las obligaciones contractuales contraídas con el Banco de España.

9.3 Protección de la información personal

9.3.1 Política de protección de datos de carácter personal

De acuerdo con la legislación española al respecto, se recoge dentro del capítulo 10, apartado 10.1 y siguientes.

9.3.2 Información tratada como privada

Todos los datos correspondientes a las personas físicas están sujetos a la normativa sobre protección de datos de carácter personal.

9.3.3 Información no calificada como privada

En cada PC se establecerá qué datos personales se incluirán en los certificados y en los repositorios de acceso público, certificados y CRL. La aceptación por el titular afectado de la emisión del certificado emitido a su nombre equivale al consentimiento dado para su publicación.

9.3.4 Responsabilidad de la protección de los datos de carácter personal

Esta responsabilidad se regula en el capítulo 10.

9.3.5 Comunicación y consentimiento para usar datos de carácter personal

En cada PC se establecerán los mecanismos por los que se comunicará y obtendrá, en su caso, el consentimiento del titular afectado para el tratamiento de los datos de carácter personal.

9.3.6 Revelación en el marco de un proceso judicial

Los datos de carácter personal solo podrán ser comunicados a terceros, sin consentimiento del afectado, en los supuestos contemplados en la legislación reguladora de protección de datos de carácter personal.

9.3.7 Otras circunstancias de publicación de información

Estas posibles circunstancias se regulan en el capítulo 10.

9.4 Derechos de propiedad Intelectual

En los términos establecidos en el Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, el Banco de España es titular en

exclusiva de todos los derechos relativos a los Certificados electrónicos emitidos por PKIBDE para personas físicas y componentes informáticos; a las listas de revocación de certificados; al contenido de la presente Declaración de Prácticas de Certificación y a las Políticas de Certificación. Asimismo, el Banco de España es titular de los derechos relativos a cualquier otro documento electrónico o de otro tipo, protocolos, programas de ordenador y hardware, archivos, directorios, bases de datos y servicios de consultas que sean generados y utilizados en el ámbito de actuación de la misma PKIBDE.

Los identificadores de objeto (OIDs) utilizados son propiedad del Banco de España y han sido registrados en Internet Assigned Number Authority (IANA) bajo la rama iso.org.dod.internet.private.enterprise 1.3.6.1.4.1-IANA-Registered Private Enterprises), habiéndose asignado el número **1.3.6.1.4.1.19484** (BANCO DE ESPAÑA). Esto puede ser consultado y comprobado en http://www.iana.org/assignments/enterprise-numbers

Queda prohibido, salvo acuerdo expreso con el Banco de España, el uso total o parcial de cualquiera de los OID asignados al Banco de España salvo para los usos específicos con que se incluyeron en el Certificado o en el Directorio.

9.5 Obligaciones

9.5.1 Obligaciones de la AC

Las ACs que operan bajo la jerarquía de PKIBDE deben asegurarse de que todas las obligaciones establecidas en este apartado se recogen, según sea aplicable, en las políticas de certificación. Cada AC es responsable del cumplimiento de sus obligaciones, según se prescriben en esta DPC, incluso aunque parte de su actividad sea realizada mediante contratación externa. Asimismo, cada AC proporcionará sus servicios de forma consistente con esta DPC.

Las ACs que operan bajo la jerarquía de PKIBDE tienen las siguientes obligaciones:

OAC.1	Realizar sus operaciones en conformidad con esta DPC.
OAC.2	Proteger sus claves privadas.
OAC.3	Emitir certificados en conformidad con las Políticas de Certificación que les sean de aplicación.
OAC.4	Tras la recepción de una solicitud válida de certificado, emitir certificados conformes con el estándar X.509 v3 y con los requerimientos de la solicitud.
OAC.5	Emitir certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
OAC.6	Publicar los certificados cuando sea necesario para interactuar con otros usuarios o sistemas informáticos que así lo requieran.
OAC.7	Revocar los certificados en los términos de la sección *4.4 Suspensión y Revocación de Certificados* y publicar los certificados revocados en la CRL en el servicio de directorio y servicio Web referidos en el apartado *2.1 Repositorio,* con la frecuencia estipulada en el punto *4.9.7 Frecuencia de emisión de CRLs*
OAC.8	Publicar esta DPC y las PC aplicables en el sitio web referido en el apartado *2.1 Repositorio*.
OAC.9	Comunicar los cambios de esta DPC y de las PC de acuerdo con lo establecido en el apartado 9*.10.2 Periodo y mecanismo de Notificación*
OAC.10	Conservar los documentos de aceptación de condiciones de los servicios de certificación de la autoridad de certificación del Banco de España firmados, en papel o electrónicamente, con los solicitantes de certificados en los que estos se dan por enterados de sus obligaciones y derechos, consienten en el tratamiento de sus datos personales por la AC y confirman que la información proporcionada es correcta.
OAC.11	Garantizar la disponibilidad de las CRLs de acuerdo con las disposiciones de la sección 4.9.9 de la presente DPC.
OAC.12	En el caso que la AC proceda a la revocación de un certificado, notificarlo a los usuarios de certificados en conformidad con las Políticas de certificación que les sean de aplicación.
OAC.13	Colaborar con las auditorías dirigidas por PKIBDE para validar la renovación de las propias claves.

OAC.14	Operar de acuerdo con la legislación aplicable. En concreto con: - La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (DOUE de 19 de enero de 2000) - La Ley 59/2003, de 19 de diciembre, de Firma Electrónica (BOE de 20) - La L. O. 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal (BOE de 15)
OAC.15	Proteger, en caso de haberlas, las claves bajo su custodia.
OAC.16	No almacenar en ningún caso los datos de creación de firma, clave privada, de los titulares de certificados emitidos con el propósito de utilizarse para firma electrónica *(key usage = non repudiation)*, sean reconocidos o no
OAC.17	En el caso de cesar en su actividad, deberá comunicarlo con una antelación mínima de dos meses, a los titulares de los certificados por ellas emitidos y al Ministerio de Industria, Comercio y Turismo tal como se recoge en el epígrafe 5.8.1.
OAC.18	Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años.

9.5.2 Obligaciones de la AR

Las ARs operativas en la PKI del Banco de España deben cumplir las siguientes obligaciones:

OAR.1	Identificar correctamente al Titular y/o Solicitante y a la organización que represente, conforme a los procedimientos que se establecen en esta DPC y en las Políticas de Certificación específicas para cada tipo de certificado, utilizando cualquiera de los medios admitidos en derecho.
OAR.2	Formalizar la expedición de Certificados con el Titular en los términos y condiciones que establezcan las Políticas de Certificación
OAR.3	Almacenar de forma segura y por un periodo razonable la documentación aportada en el proceso de emisión del certificado y en el proceso de suspensión/revocación del mismo.
OAR.4	Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta DPC.

9.5.3 Obligaciones de los titulares de los certificados

Es obligación de los titulares de los certificados emitidos bajo la presente DPC:

OTC.1	Suministrar información exacta, completa y veraz con relación a los datos que los encargados de su verificación les soliciten para realizar el proceso de registro.
OTC.2	Informar a los responsables de PKIBDE de cualquier modificación de esta información.
OTC.3	Conocer y aceptar las condiciones de utilización de los certificados, en particular las contenidas en esta DPC y en las PC que sean de aplicación, así como las modificaciones de las mismas.
OTC.4	Limitar y adecuar el uso del certificado al ámbito de las relaciones laborales que le unen al Banco de España y de acuerdo con lo permitido por la Política de Certificación pertinente y la presente DPC.
OTC.5	Poner el cuidado y medios necesarios para garantizar la custodia de su tarjeta criptográfica, evitando su pérdida, divulgación, modificación o uso no autorizado.
OTC.6	El proceso de obtención de los certificados exige la elección personal de un PIN de control de la tarjeta criptográfica y de activación de las claves privadas y un PUK de desbloqueo. Es responsabilidad del titular mantener bajo su exclusivo conocimiento el valor del PIN y el del PUK.
OTC.7	Solicitar inmediatamente la revocación de un certificado en el caso de detección de inexactitudes en la información contenida en el mismo o tener conocimiento o sospecha del compromiso de la clave privada correspondiente a la clave pública contenida en el certificado, entre otras causas por: pérdida, robo, compromiso potencial, conocimiento por terceros del PIN y/o PUK.
OTC.8	No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica (hardware y software) de los servicios de certificación.

OTC.9	No transferir ni delegar a un tercero sus responsabilidades sobre un certificado que le haya sido asignado.
OTC.10	Cualquier otra que se derive de la ley, de esta DPC o de las Políticas de Certificación.

9.5.4 Obligaciones de los terceros aceptantes

Es obligación de los terceros que acepten y confíen en los certificados emitidos por PKIBDE:

OTA.1	Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la Política de Certificación pertinente.
OTA.2	Verificar la validez de los certificados en el momento de la recepción de los documentos firmados electrónicamente mediante la comprobación de que el certificado es válido y no ha caducado o ha sido suspendido o revocado.
OTA.3	Asumir su responsabilidad en la correcta verificación de las firmas electrónicas
OTA.4	Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados que acepta y en que confía.
OTA.5	Tener conocimiento de las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y aceptar sujetarse a las mismas.
OTA.6	Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

9.5.5 Obligaciones de otros participantes

OOP.1	El Servicio de Repositorio ha de mantener accesible para los Titulares y Terceros Aceptantes la información de los certificados que han sido revocados, en formato CRL.

9.6 Responsabilidades

9.6.1 Responsabilidad de PKIBDE

PKIBDE solo responderá en el caso de incumplimiento de las obligaciones contenidas en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y normativa de desarrollo, en la presente DPC y en las Políticas de Certificación específicas.

De manera particular, PKIBDE como prestador de servicios de certificación responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.

La PKI del Banco de España sólo responderá de los daños y perjuicios causados por el uso indebido del certificado, cuando se haya consignado en él o en su Política de Certificación asociada, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

La PKI del Banco de España, en tanto que Prestador de Servicios de Certificación, no se responsabiliza del contenido de los documentos firmados con sus certificados, ni de cualquier otro uso de sus certificados, como pueden ser procesos de cifrado de mensajes o comunicaciones.

La PKI del Banco de España no representa en forma alguna a los usuarios ni a terceras partes aceptantes de los certificados que emite.

9.6.2 Exención de responsabilidad de PKIBDE

PKIBDE no asume ninguna responsabilidad en caso de pérdida o perjuicio:

RESP.1	De los servicios que presta, en caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible.
RESP.2	Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario
RESP.3	Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos, la Política de Certificación pertinente y esta DPC.
RESP.4	Ocasionados por el mal uso de la información contenida en el certificado.
RESP.5	Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por PKIBDE
RESP.6	La PKI del Banco de España no asumirá responsabilidad alguna en relación al uso de los Certificados emitidos por sus ACs y el par de claves privada/pública asociado a sus titulares para cualquier actividad no especificada en la DPC o en las Políticas de Certificación correspondientes
RESP.7	La PKI del Banco de España, en tanto que Prestador de Servicios de Certificación, no será responsable del contenido de los documentos firmados con sus certificados ni de cualquier otro uso de sus certificados, como pueden ser procesos de cifrado o comunicaciones.

9.6.3 Alcance de la cobertura

De acuerdo con lo establecido en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre, el Banco de España ha constituido un seguro de responsabilidad civil por importe de 3.000.000 de euros para hacer frente al riesgo de responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados reconocidos que expida PKIBDE.

9.7 Limitaciones de pérdidas

A excepción de lo establecido por las disposiciones de la presente DPC, PKIBDE no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros aceptantes.

9.8 Periodo de validez

9.8.1 Plazo

Esta DPC entra en vigor desde el momento de su publicación en el repositorio de PKIBDE.

Esta DPC estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la AC Raíz, momento en que obligatoriamente se dictará una nueva versión.

9.8.2 Sustitución y derogación de la DPC

Esta DPC será 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 DPC 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 DPC, 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

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta DPC se realizará mediante mensaje electrónico o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto 1.5 Administración de las Políticas. Las comunicaciones electrónicas producirán sus efectos una vez que las reciba el destinatario al que van dirigidas.

9.10 Procedimientos de cambios en las especificaciones

9.10.1 Procedimiento para los cambios

La Autoridad con atribuciones para realizar y aprobar cambios sobre la DPC y las PCs de PKIBDE es la Autoridad de Administración de Políticas (AAP). Los datos de contacto de la AAP se encuentran en el apartado 1.5 Administración de las Políticas de esta DPC.

9.10.2 Periodo y procedimiento de notificación

En el caso de que la AAP juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se comunicará a los usuarios de los certificados correspondientes a la PC o DPC modificada que se ha efectuado un cambio y que deben consultar la nueva DPC en el repositorio establecido.

9.10.3 Circunstancias en las que el OID debe ser cambiado

En los casos en que, a juicio de la AAP, los cambios de las especificaciones no afecten a la aceptabilidad de los certificados se procederá al incremento del número menor de versión del documento y el último número de Identificador de Objeto (OID) que lo representa, manteniendo el número mayor de la versión del documento, así como el resto de su OID asociado. No se considera necesario comunicar este tipo de modificaciones a los usuarios de los certificados correspondientes a la PC o DPC modificada.

En el caso de que la AAP juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma. También se modificarán los dos últimos números del Identificador de Objeto (OID) que lo representa. Este tipo de modificaciones se comunicará a los usuarios de los certificados correspondientes a la PC o DPC modificada.

9.11 Reclamaciones y jurisdicción

Todas reclamaciones entre usuarios y PKIBDE deberán ser comunicadas por la parte en disputa a la Autoridad de Administración de Políticas (AAP) del Banco de España, con el fin de intentar resolverlo entre las mismas partes.

En el caso de que no se llegue a un acuerdo entre las partes, la resolución de cualquier conflicto que pudiera surgir se someterá a los juzgados y tribunales de la ciudad de Madrid con renuncia a cualquier otro fuero que pudiera corresponderles.

9.12 Normativa aplicable

Las operaciones y funcionamiento de PKIBDE, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación que sean de aplicación para cada tipo de certificado, estarán sujetas a la normativa que les sea aplicable y en especial a:

- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica (BOE de 20)
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE de 15)
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba Reglamento de desarrollo de la Ley Orgánica 15/1999
- Circular del Banco de España 2/2005, de 25 de febrero,, sobre ficheros automatizados con datos de carácter personal gestionados por el Banco de España (BOE de 22 de marzo), y sus posteriores actualizaciones

De igual manera, habrán de observarse las normas y procedimientos internos dictados por el Banco de España encaminadas a garantizar el nivel de seguridad exigido por el Real Decreto citado en los casos en que sean de aplicación.

9.13 Cumplimiento de la normativa aplicable

Es responsabilidad de la Autoridad de Administración de Políticas velar por el cumplimiento de la legislación aplicable recogida en el apartado anterior.

9.14 Estipulaciones diversas

9.14.1 Cláusula de aceptación completa

Todos los Terceros Aceptantes asumen en su totalidad el contenido de la última versión de esta DPC y de las PC que sean de aplicación.

9.14.2 Independencia

En el caso de que una o más estipulaciones de esta DPC 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 DPC 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

Es de aplicación a la presente Declaración de Prácticas de Certificación lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal y su normativa de desarrollo, entre la que cabe destacar el Real Decreto 1720/2007, de 21 de diciembre. Los ficheros serán de titularidad pública y su creación, modificación o supresión se realizará mediante Circular del Banco de España publicada en el Boletín Oficial del Estado.

Asimismo, será de cumplimiento lo establecido en la Circular Interna 3/2002 del Banco de España sobre Protección de Datos Automatizados de Carácter Personal y sus normas de desarrollo, y sus posteriores actualizaciones.

Sin menoscabo de otras obligaciones las Autoridades de Registro que se constituyan en PKIBDE verificarán que el solicitante de un certificado presta su consentimiento al tratamiento de sus datos personales y es informado sobre la finalidad que se les va a dar y su inclusión en el fichero declarado al efecto por PKIBDE.

En los casos en que los datos no hayan sido recabados directamente de los interesados, el PKIBDE o su representante informarán de forma expresa, precisa e inequívoca a estos, dentro de los tres meses siguientes al momento del registro de los datos, de lo recogido en el párrafo anterior.

El titular de los datos podrá ejercer los derechos de acceso, rectificación, cancelación y oposición, dirigiéndose para ello a la dirección señalada en el siguiente apartado de la presente DPC.

Los datos contenidos en el Directorio seguro de Certificados tienen la consideración de datos de carácter personal a efectos de lo dispuesto en la LOPD y demás normativa complementaria, y por este motivo, PKIBDE no permitirá el acceso de terceros a los mismos.

No obstante, PKIBDE pone a disposición de los Terceros Aceptantes las listas de revocación de certificados (que no contienen datos personales) para el cumplimiento diligente de los servicios de certificación. El Tercero Aceptante como cesionario de esta información únicamente podrá utilizarla de acuerdo con esas finalidades.

10.2 Creación del fichero e inscripción registral

Los datos de creación e inscripción del fichero “Certificados Electrónicos” del Banco de España son:

- Creación: Circular 2/2005, del Banco de España, de 25 de febrero, (BOE de 22 de marzo)
- Nº de inscripción en el Registro General de Protección de Datos: 2051360139

Asimismo, el nombre del fichero, su responsable y el área encargada de atender las peticiones de ejercicio de derechos son:

Nombre del Fichero:	Certificados Electrónicos
Responsable del Fichero:	Banco de España
Servicio de Atención al Público:	Departamento de Sistemas de Información

10.3 Documento de seguridad LOPD

10.3.1 Aspectos cubiertos

La presente DPC, tal como se señala en el punto 1.1, se ha hecho de acuerdo a la especificación RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" del Internet Engineering Task Force (IETF) para este tipo de documentos.

No obstante lo anterior y teniendo en cuenta lo dispuesto en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, que considera la DPC como documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de carácter personal, resulta obligado añadir el presente apartado con objeto de recoger todos los requisitos contemplados en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

A tal fin se tratan los siguientes aspectos:

- Estructura básica de datos de carácter personal.
- Nivel de seguridad aplicable.
- Sistemas de información que soportan el fichero
- Relación de usuarios
- Notificación y Gestión de Incidencias
- Copias de respaldo y recuperación
- Control de Accesos
- Ficheros Temporales
- Gestión de Soportes
- Utilización de datos reales en pruebas

El resto de aspectos que debe recoger un Documento de Seguridad han sido ya incluidos en capítulos anteriores de la presente DPC.

Asimismo, en lo que no se oponga a la presente DPC, es de aplicación la Circular Interna 3/2002, de 1 de marzo, por la que se regula la Protección de Datos de Carácter Personal en el Banco de España, y sus normas de desarrollo, así como sus posteriores actualizaciones.

El objeto del Documento de Seguridad es preservar los datos de carácter personal procesados por PKIBDE, por lo que afecta a todos aquellos recursos (personas, equipos, comunicaciones, software, procedimientos) implicados en el tratamiento de los datos.

10.3.2 Funciones y obligaciones del personal

Esta DPC, así como futuras versiones de la misma, son conocidas por todas las personas que accedan a los datos de carácter personal gestionados por PKIBDE, siendo de obligado cumplimiento todas las funciones y obligaciones que establece.

10.3.3 Estructura de datos de carácter personal

En la siguiente tabla se recogen los datos, utilizando las denominaciones utilizadas en el formulario de notificación de ficheros a la Agencia Española de Protección de Datos, de los titulares de certificados tratados por PKIBDE:

DATOS TRATADOS
Datos de carácter identificativo
D.N.I./N.I.F.
Nombre y apellidos
Dirección electrónica
Nº registro personal
Firma electrónica
Datos de detalles de empleo
Otros: Empresa

10.3.4 Nivel de seguridad

Los datos de carácter personal tratados exigen el nivel de seguridad básico, sin perjuicio de que dadas las especiales características de seguridad que ha de tener una PKI y el nivel de seguridad que establece esta DPC, se proporciona un nivel de seguridad superior.

10.3.5 Sistemas de información

Dentro de la estructura de sistemas de información que constituye PKIBDE se pueden distinguir tres subsistemas con alguna implicación en el tratamiento de datos de carácter personal. A continuación se relacionan y describen de forma sintética:

- **Subsistema de gestión de certificados**: Se encarga de la creación de los certificados conforme al estándar X.509v3, donde se introducen las claves generadas por el subsistema de generación de claves y otros datos identificativos que se definen en la correspondiente PC.

- **Subsistema de Autoridad de Registro**: Se encarga de la identificación del solicitante del certificado para proceder a la emisión posterior del certificado por PKIBDE.

- **Subsistema de publicación**: Se encarga de la gestión de la publicación de las listas de revocación de certificados (CRL) y del directorio de certificados.

10.3.6 Relación de usuarios

El Coordinador de Seguridad mantiene una relación de los usuarios con acceso a los datos de carácter personal tratados por la PKI en la que se indica su rol y nivel de acceso. Dicha relación de usuarios tiene carácter confidencial por motivos de seguridad, por lo que será precisa una petición motivada al Coordinador de Seguridad para tener acceso a la misma.

No se incluyen en esa relación los usuarios con acceso a los certificados electrónicos a efectos de hacer uso de los mismos para el envío de información cifrada ni los usuarios con acceso a las CRL.

10.3.7 Notificación y gestión de incidencias

Los procedimientos internos del Departamento de Sistemas de Información asociados a la gestión de problemas aseguran que todas las incidencias se registran y documentan, realizándose un seguimiento de las mismas. Se registra información relativa a: fecha, hora, tipo de incidencia, persona que comunica la misma, persona a quien se asigna la resolución de la incidencia, documentación sobre la causa y sus efectos.

10.3.8 Copias de respaldo y recuperación

Las copias de respaldo se realizan de forma diaria conforme a la normativa en vigor del Banco de España para ordenadores centrales.

Las recuperaciones de datos se hacen con la autorización del responsable del fichero:

a Incidencias en el sistema informático: Se comunica al responsable informático del sistema, quien deberá obtener la autorización del propietario mediante los procedimientos establecidos al efecto.

b Incidencias en la infraestructura del sistema informático: Se siguen los procedimientos establecidos en los planes de respaldo del Departamento de Sistemas de Información para cada contingencia.

10.3.9 Control de accesos

Las autorizaciones de acceso a los sistemas de información estarán basadas exclusivamente en el principio de necesidad para el trabajo. Los administradores de usuarios y de elementos se encargarán de validar siempre esta necesidad antes de conceder el acceso a los datos.

Asimismo, todos los elementos que permitan acceder a datos personales estarán catalogados como de uso restringido.

10.3.10 Ficheros temporales

El software utilizado para generar un certificado electrónico conforme al estándar X.509v3 genera ficheros temporales, ficheros de registros de auditoría, que son debidamente custodiados ante la necesidad de trazabilidad de la instalación por la actividad de prestador de servicios de certificación en cumplimiento de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica 59/2003.

10.3.11 Gestión de soportes

Los soportes internos están correctamente identificados por su código de barras o incluyen su correspondiente etiqueta identificativa.

Los soportes están ubicados en las salas de ordenadores. El acceso a estas salas está restringido, las autorizaciones permanentes son validadas por el Jefe del Departamento de Sistemas de Información y el acceso provisional solo podrá ser autorizado por el Jefe de Explotación o el Jefe de Operación.

Toda salida de soportes fuera de los locales del Banco de España deberá ser autorizada por el Administrador de la PKI. El Departamento de Sistemas de Información mantiene un registro en papel de la entrada/salida de soportes.

Los soportes que hubieran contenido datos personales se borrarán utilizando un borrado físico o procedimiento similar. Este proceso se realiza siempre que se reutilizan soportes que van a ser enviados al exterior; en otros casos no existe manipulación de soportes, ya que la gestión es realizada directamente por los robots que gestionan cartuchos.

Antes de autorizar la salida de soportes que contengan datos personales para operaciones de mantenimiento, se procederá a su borrado físico o a su desmagnetización. La salida de soportes por mantenimiento solo se daría en el caso de discos.

10.3.12 Utilización de datos reales en pruebas

No se utilizarán datos personales reales para la realización de pruebas, salvo que se aseguren los mismos niveles de seguridad que establece la presente DCP.

Los procedimientos de pruebas utilizados en el Departamento de Sistemas de Información aseguran el cumplimiento del nivel de seguridad requerido para la utilización de datos reales en pruebas.