BANCO DE ESPAÑA
Eurosistema

11.05.2015

OID: 1.3.6.1.4.1.19484.2.2.2

Infraestructura de Clave Pública del Banco de España

Declaración Básica: características y requerimientos de la PKI

RESUMEN Este texto constituye únicamente un extracto de las características y requerimientos de la PKI del Banco de España, los cuales se describen de forma completa en la Declaración de Prácticas de Certificación (DPC) y en las correspondientes Políticas de Certificación (PC) aplicables al certificado que se esté solicitando o con el que se esté operando.

Es recomendable la lectura de la DPC, así como de las PC que sean de aplicación, con el fin de tener una idea clara de los objetivos, especificaciones, normas, derechos, obligaciones y responsabilidades que rigen la prestación del servicio de certificación.

Esta Declaración Básica ha sido elaborada conforme a la especificación técnica "ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates", en concreto a lo que se recomienda en su anexo B para el "PKI Disclosure Statement".

Hoja de Control

Título	Declaración Básica: características y requerimientos de la PKI
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	Revisión de la primera versión
1.2	25.05.2010	Revisión tras implantación de servicios de fechado electrónico Renombrado de la Autoridad de Aprobación de Políticas a Autoridad de Administración de Políticas
1.3	07.07.2011	Modificaciones tras revisión de política de certificación para certificados de firma electrónica
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

1 Glosario

AC: Autoridad de Certificación.
AAP: Autoridad de Administración de Políticas del Banco de España.
CRL: Lista de Revocación de Certificados.
DPC: Declaración de Prácticas de Certificación.
LDAP: Lightweight Directory Access Protocol (protocolo de acceso a servicios de directorio).
PC: Política de Certificación.
PIN: Contraseña con la que se protege el uso de la tarjeta criptográfica.
PKI: Infraestructura de Clave Pública.
PUK: Contraseña para el desbloqueo de la tarjeta, si ésta se ha bloqueado por repetida introducción de un PIN incorrecto.

2 Datos de contacto de la AC

Esta PKI está administrada por la Autoridad de Administración de Políticas (AAP) de la PKI del Banco de España.

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

3 Tipos de certificado, procedimientos de validación y uso

La PKI del Banco de España emite los siguientes tipos de certificados para usuarios internos:

- **Certificados personales**. Es un paquete de certificados almacenado en un mismo dispositivo criptográfico (típicamente una tarjeta criptográfica) destinado al uso general de cualquier usuario interno de Banco de España. Está compuesto por los siguientes certificados:
  - Certificado de autenticación, para la autenticación del titular frente a los sistemas de información de Banco de España.
  - Certificado de firma electrónica, para la firma electrónica de correos electrónicos, ficheros y transacciones informáticas.
  - Certificado de cifrado (obsoleto[1]) o bien certificado de cifrado recuperable en software, para el cifrado de correo electrónico, ficheros y transacciones.

- **Certificados de administrador**. Es un certificado almacenado en un dispositivo criptográfico (típicamente una tarjeta criptográfica) que se utiliza para la autenticación del titular con una cuenta de administrador frente a los sistemas de información del Banco de España.

- **Certificados provisionales personales**. Es un paquete de certificados almacenado en un dispositivo criptográfico (típicamente una tarjeta criptográfica) que se utiliza en el caso de olvido del dispositivo criptográfico en el que se encuentran los certificados personales habituales del titular.

[1] Este tipo de certificados ya no es emitido por la AC Corporativa, aunque es posible recuperar del Archivo de Claves el correspondiente par de claves de certificados antiguos

Los certificados provisionales personales tienen una fecha de caducidad máxima de 7 días, aunque el Administrador de Usuarios podrá elegir un período inferior en el momento de la solicitud. Está compuesto por los siguientes certificados:

- Certificado de autenticación, para la autenticación del titular frente a los sistemas de información.
- Certificado de firma electrónica, para la firma electrónica de correos electrónicos, ficheros y transacciones informáticas.

- **Certificados provisionales de administrador**. Es un certificado almacenado en un dispositivo criptográfico (típicamente una tarjeta criptográfica) que se utiliza en el caso de olvido del dispositivo criptográfico en el que se encuentra el certificado de administrador habitual del titular. Los certificados provisionales de administrador tienen una fecha de caducidad máxima de 7 días, aunque el Administrador de Usuarios podrá elegir un período inferior en el momento de la solicitud.

Los certificados se emiten para los empleados del Banco de España y para personal ajeno que por su relación con el Banco precise interactuar con los sistemas de información del Banco de España. Todos los certificados personales se utilizarán desde tarjetas criptográficas, con la única excepción de los certificados de cifrado recuperables en software, que pueden ser utilizados en dispositivos móviles. Está prohibido a sus titulares exportar sus claves privadas fuera de las tarjetas.

La comprobación del estado de los certificados puede realizarse mediante consulta de la última CRL en:

- LDAP: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
- WEB: http://pki.bde.es/crls/ACcorporativav2.crl
- WEB: http://pki.redbde.es/crls/ACcorporativav2.crl

4 Limitaciones

Limitaciones en la fiabilidad

Los certificados deben emplearse para las funciones y finalidades establecidas en su correspondiente Política de Certificación.

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.

Salvo que la correspondiente PC autorice otros usos, los certificados emitidos por la PKI del Banco de España sólo son válidos para su uso en relación al propio Banco (autenticación en sus sistemas, firma y cifrado de correo a o desde el Banco, firma y cifrado de información del Banco).

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.

Conservación de la información

La información de registro y de gestión de los certificados se conservará durante 15 años.

5 Obligaciones de los titulares

Es obligación de los Titulares de los certificados emitidos por la PKI del Banco de España:

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.

2 Informar a los responsables de la PKI de cualquier modificación de esta información.

3 Conocer y aceptar las condiciones de utilización de los certificados, en particular las contenidas en la DPC y PCs que sean de aplicación, así como las modificaciones de las mismas.

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 DPC.

5 Poner el cuidado y medios necesarios para garantizar la custodia de su tarjeta, evitando su pérdida, divulgación, modificación o uso no autorizado.

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.

7 Solicitar inmediatamente la revocación de un certificado en caso de detección de inexactitudes en la información contenida en los mismos o de tener conocimiento o sospecha de pérdida de la fiabilidad 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.

8 No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica (hardware y software) de los servicios de certificación.

9 No transferir ni delegar a un tercero las responsabilidades sobre un certificado que le haya sido asignado.

10 Cualquier otra que se derive de la normativa aplicable, de la DPC o de las Políticas de Certificación.

6 Obligaciones de los terceros aceptantes

Es obligación de los terceros que acepten y confíen en los certificados emitidos por la PKI del Banco de España:

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.

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 existe y no ha caducado o ha sido suspendido o revocado.

3 Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.

4 Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados que acepta y en que confía.

5 Tener conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

6 Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

7 Limitación de responsabilidades

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 DPC y en las Políticas de Certificación específicas.

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.

8 Acuerdos, Declaración de Prácticas de Certificación y Políticas de Certificación aplicables

Todos los acuerdos**,** Declaración de Prácticas de Certificación y Políticas de Certificación aplicables se encuentran en la página web establecida al efecto: http://pki.bde.es.

En particular, cabe destacar los siguientes documentos:

Nombre Documento	Nombre Fichero	URL
Declaración de Prácticas de Certificación	PKIBdE_DPC-vX.Y.pdf	http://pki.bde.es/politicas
Política Certificación para certificados de usuario interno	PKIBdE_PC_CertUsuarioInterno-vX.Y.pdf	http://pki.bde.es/politicas
Política de Certificación para certificados personales de autenticación para dispositivos móviles	PKIBdE_PC_CertAutenticacionMovil-vX.Y.pdf	http://pki.bde.es/politicas
Política de Certificación para certificados de componente de uso interno	PKIBdE_PC_CertComponentes-vX.Y.pdf	http://pki.bde.es/politicas
Política de Certificación para certificados de componente de entidades externas	PKIBdE_PC_CertComponentesEntidadesExternas-vX.Y.pdf	http://pki.bde.es/politicas
Política de Certificación para Certificados de Autoridad de Sellado de Tiempo	PKIBdE_PC_CertTSA_vX.Y.pdf	http://pki.bde.es/politicas
Autoridad de Sellado de Tiempo del Banco de España Políticas y Prácticas de Sellado de Tiempo	PKIBdE_PST_y_DPST-vX.Y.pdf	http://pki.bde.es/politicas

X.Y indica la versión en vigor en cada momento

9 Protección de datos de carácter personal

Es de aplicación 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, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999. 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.
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, 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 de contacto señalada en este documento.
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 certificados revocados (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 Gratuidad de la prestación de los servicios de certificación

La obtención y uso de los certificados de usuario interno emitidos por la PKI del Banco de España son gratuitos.

11 Normativa aplicable

Las operaciones y funcionamiento de la PKI del Banco de España, así como la 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:

- 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).
- 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 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).

De igual manera, habrán de observarse las normas y procedimientos internos dictados por el Banco de España encaminados a garantizar el nivel de seguridad exigido por el Real Decreto 1720/2007.

12 Reclamaciones y jurisdicción competente

Todas las reclamaciones entre usuarios o terceros y PKIBDE deberán ser comunicadas a la AAP del Banco de España, con el fin de intentar resolverlo entre las mismas partes.
En el caso de que no se llegara 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.

13 Auditorias, certificaciones y estándares de seguridad de la AC y los repositorios

Auditorías

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 garantizará la adecuación de su funcionamiento y operativa con las estipulaciones incluidas en la 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.

Estándares

Los certificados personales de firma electrónica emitidos por la PKI del Banco de España cumple todos los requisitos técnicos y organizativos establecidos para los certificados reconocidos en:

- Ley 59/2003, de 19 de diciembre, de Firma Electrónica (BOE de 20).
- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.