BANCO DE ESPAÑA
Eurosistema

18.12.2017

OID: 1.3.6.1.4.1.19484.2.4.1

Autoridad de Sellado de Tiempo del Banco de España

Políticas y Prácticas de Sellado de Tiempo

Este documento recoge la declaración de Políticas y Prácticas de Sellado de Tiempo que regula los sellos de tiempo emitidos por la Autoridad de Sellado de Tiempo del Banco de España.

Hoja de Control

Título	Políticas y Prácticas de Sellado de Tiempo
Autor	Departamento de Sistemas de Información
Versión	1.2
Fecha	18.12.2017

Registro de Cambios

Versión	Fecha	Motivo del cambio
1.0	25.05.2010	Primera versión
1.1	11.05.2015	Actualización con motivo de la renovación de las Autoridades de Certificación
1.2	18/12/2017	Actualización con objeto de definir las nuevas extensiones propietarias bdelssuerName y bdelssuerVAT

ÍNDICE

1 Introducción

1.1 Resumen

Este documento recoge la Política de Sellado de Tiempo (PST) y la Declaración de Prácticas de Sellado de Tiempo (DPST) que rige el funcionamiento y operaciones de la Autoridad de Sellado de Tiempo (en adelante TSA) del Banco de España (desde ahora TSABDE).

El servicio de Sellado de Tiempo se enmarca dentro de los Servicios de Certificación de la PKI del Banco de España, actuando al amparo de lo dispuesto en el artículo 2.2[1] de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

La firma electrónica proporciona una seguridad añadida a los datos permitiendo garantizar la identidad del firmante y la no modificación de los datos una vez firmado. Los sellos de tiempo usan firmas electrónicas, incorporando el tiempo obtenido desde una fuente precisa y confiable, para garantizar cuándo existía o se produjo una determinada transacción o dato.

Esta PST y DPST se aplica a todos los intervinientes relacionados con la TSA del Banco de España (TSABDE), incluyendo los Suscriptores de sus servicios y Terceros Aceptantes, entre otros. En particular, incluye todas las actividades encaminadas a la gestión y operación de los servicios de sellado, y las consideraciones necesarias para la aplicabilidad y utilización de dichos servicios y de los sellos de tiempo proporcionados por TSABDE. En consecuencia, todas las partes involucradas tienen la obligación de conocer esta PST y DPST y ajustar su actividad a lo dispuesto en la misma.

Desde el punto de vista de los estándares y buenas prácticas que han desarrollado los grupos de trabajo del ETSI e IETF, una Política de Sellado de Tiempo (PST) es el conjunto de reglas que definen la aplicabilidad o uso de un sello de tiempo en una comunidad de usuarios, sistemas o clase particular de aplicaciones que tengan en común una serie de requisitos de seguridad. Por otro lado, una Declaración de Prácticas de Sellado de Tiempo (DPST) establece las condiciones y circunstancias específicas (prácticas) que una TSA utiliza para la emisión de sellos de tiempo.

Puesto que TSABDE comparte infraestructuras tecnológicas, procedimientos, procesos, controles de seguridad, responsables y organización, con la PKI del Banco de España (PKIBDE), en aquellos aspectos que sean de aplicación, estas PST y DPST referencian, detallan y completan lo estipulado en la "Declaración de Prácticas de Certificación" (DPC) de PKIBDE.

Este documento se ha elaborado en líneas generales de acuerdo con la especificación técnica ETSI TS 102 023, *Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities*[2], tanto en su contenido como en su estructura, si bien por homogeneidad y coherencia con la documentación de Políticas y Prácticas de Certificación de la Infraestructura de Clave Pública del Banco de España (PKIBDE) se ha modificado el orden de este documento para que:

- Los capítulos de Referencias y de Definiciones y Acrónimos están al principio del documento y dentro de la Introducción
- El capítulo de Obligaciones y Responsabilidades esté al final del documento.

---

[1] Se corresponde a la definición recogida en el artículo 3.10 del Reglamento (UE) Nº 910/2014

[2] Esta especificación técnica ha sido adoptada por el IETF como la RFC 3628 *Policy Requirements for Time-Stamping Authorities (TSAs).*

En este sentido, a fin de dotar de un carácter uniforme al documento y facilitar su lectura y análisis, se incluyen todas las secciones establecidas en la ETSI TS 102 023. Cuando no se haya previsto nada en alguna sección aparecerá la frase "No estipulado".

Adicionalmente a los epígrafes establecidos en la ETSI TS 102 023, los capítulos se han extendido para incorporar información adicional de relevancia para los suscriptores de TSABDE y terceros aceptantes de sus sellos de tiempo. Del mismo modo, se ha incluido un nuevo capítulo dedicado a la Protección de Datos de Carácter Personal para dar cumplimiento a la legislación española en la materia.

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

1.2 Nombre del documento e identificación

Nombre del documento	Políticas y Prácticas de Sellado de Tiempo de la Autoridad de Sellado de Tiempo del Banco de España (TSABDE)
Versión del documento	1.2
Estado del documento	Aprobado
Fecha de emisión	18.12.2017
Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.19484.2.4.1
Ubicación del documento	http://pki.bde.es/politicas
DPC Relacionada	Declaración de Practicas de Certificación de la PKI del Banco de España OID 1.3.6.1.4.1.19484.2.2.1

1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes en este documento son:

- El Banco de España como titular de TSABDE.
- La Autoridad de Administración de Políticas.
- El PSC emisor del certificado de TSABDE
- Los Suscriptores de los sellos de tiempo emitidos por TSABDE
- Los Terceros Aceptantes de los sellos de tiempo emitidos por TSABDE.

1.3.1 Autoridad de Administración de Políticas

La Autoridad de Administración de Políticas (AAP) es la organización establecida dentro del Banco de España responsable de la aprobación de las presentes Políticas y Prácticas de Sellado de Tiempos, así como de la aprobación de las modificaciones en dichos documentos.

En particular, la AAP de TSABDE es la misma organización que la AAP de la PKIBDE, cuyo rol y función están definidos en la Declaración de Prácticas de Certificación de PKIBDE.

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

1.3.2 PSC emisor del certificado de TSABDE

El PSC emisor del certificado de TSABDE es la PKI del Banco de España, PKIBDE.

1.3.3 Suscriptores

La definición y descripción de Suscriptores está recogida en el capítulo 3.

1.3.4 Terceros aceptantes

La definición y descripción de Terceros aceptantes está recogida en el capítulo 3.

1.3.5 Otros afectados

Administradores de TSABDE: personas que dentro del Banco de España tienen privilegios de administración y configuración de la TSA del Banco de España.

1.4 Administración de las políticas y prácticas

1.4.1 El Banco de España como titular de TSABDE

Esta PST y DPST 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

1.4.2 Persona de contacto

Esta PST y DPST 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

1.4.3 Procedimientos de Aprobación de esta PST y DPST

La Comisión Ejecutiva del Banco de España es la responsable de la aprobación de las presentes Políticas y Prácticas de Sellado de Tiempo, 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.

1.5 Referencias

El contenido de los siguientes documentos es relevante para el desarrollo y/o aplicación de las presentes Políticas y Prácticas de Sellado de tiempo:

- ETSI TS 101 456, Policy Requirements for Certification Authorities Issuing Qualified Certificates.
- ETSI TS 101 733, Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)
- ETSI TS 101 861, Time-stamping Profile.
- ETSI TS 101 903, XML Advanced Electronic Signatures (XAdES)
- ETSI TS 102 023, Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities.
- ETSI TS 102 042, Policy Requirements for certification authorities issuing public key certificates.
- ETSI TS 102 176.1, Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash Functions and Asymmetric Algorithms.
- RFC 3161, Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).
- RFC 3628, Policy Requirements for Time-Stamping Authorities (TSAs)
- ISO/IEC 18014-1, Time-stamping services — Part 1: Framework

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, de 13 de diciembre, de protección de datos de carácter personal
- 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

1.6 Definiciones y Acrónimos

1.6.1 Definiciones

En el ámbito de estas Políticas y Prácticas de Sellado de Tiempo se emplearán estas definiciones:

Autenticación: procedimiento de comprobación de la identidad de un suscriptor de servicios de sellos de tiempo de TSABDE.

Autoridad de Sellado de Tiempo (TSA): autoridad de confianza que emite los sellos de tiempo.

Certificado electrónico: un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su

identidad. Esta es la definición de la Ley 59/2003 que en este documento se extiende a los casos en que la vinculación de los datos de verificación de firma se hace a un componente informático.

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

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

Declaración de Prácticas de Sellado de Tiempo (DPST): declaración de las prácticas que la Autoridad de Sellado de Tiempo emplea para la emisión de sellos de tiempo.

Política de Sellado de Tiempo (PST): conjunto de reglas que establecen la aplicabilidad del sello de tiempo y sus características de emisión.

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

Sello de Tiempo (time-stamp token ó TST): estructura de datos que ligan unos datos determinados a un instante de tiempo particular, proporcionando evidencia de su existencia con anterioridad a ese instante.

Suscriptor: persona o entidad que suscribe o tiene suscrito un acuerdo de utilización de los servicios de sellado de tiempo proporcionados por TSABDE, y que acepta sus términos y condiciones

Tercero Aceptante: persona o entidad que decide confiar en los servicios de sellado de tiempo de TSABDE, y en particular que es receptora, acepta y confía en un Sello de Tiempo emitido por TSABDE.

Tiempo Universal Coordinado (UTC): escala de tiempo, basada en el segundo, definida por el Comité de Radio de la Unión Internacional de Telecomunicaciones (ITU-T) TF.460-5 y que coincide aproximadamente con el Tiempo Medio de Greenwich (GMT).

Unidad de Sellado de Tiempo (time-stamp unit ó TSU): conjunto de hardware y software que se gestiona como una unidad y que tiene una única clave privada de firma activa en cada momento. Una TSA puede disponer y mantener varias TSUs de forma simultánea, cada una operando con una clave privada y certificado distinto.

UTC(k): escalada de tiempo generada por el laboratorio "k" de la forma definida en la Circular T del *Bureau International des Poids et Mesures* (BPIM) y que se mantiene de acuerdo con el UTC.

En la Declaración de Prácticas de Certificación (DPC) del Banco de España se pueden encontrar definiciones adicionales.

1.6.2 Acrónimos

AAP: Autoridad de Administración de Políticas

AC: Autoridad de Certificación

CRL: Certificate Revocation List (Lista de Certificados Revocados)

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

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

DPC: Declaración de Prácticas de Certificación

DPST: Declaración de Prácticas de Sellado de Tiempo

ETSI: European Telecommunications Standard Institute

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

GMT: Greenwich Mean Time

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)

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

PKI: Public Key Infrastructure (Infraestructura de Clave Pública)

PKIBDE: PKI del Banco de España

PSC: Prestador de Servicios de Certificación

PST: Política de Sellado de Tiempo

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

TSA: Time-stamping Authority (Autoridad de Sellado de Tiempo)

TSABDE: TSA del Banco de España

TST: Time-stamping Token (Sello de Tiempo)

TSU: Time-stamping Unit (Unidad de Sellado de Tiempo)

UTC: Coordinated Universal Time (Tiempo Universal Coordinado)

2 Alcance

Este documento define los requisitos y políticas, así como las prácticas operativas y de gestión de la Autoridad de Sellado de Tiempo del Banco de España (TSABDE).

En este sentido, este documento podrá ser consultado por los suscriptores de sus servicios, y por terceros aceptantes de los sellos de tiempo, para que puedan establecer su confianza en los servicios de sellado de tiempo proporcionados por TSABDE.

Del mismo modo, podrá ser utilizado también por terceras entidades y organismos independientes como base para comprobar y certificar que TSABDE es conforme a las políticas y prácticas recogidas en este documento, de tal forma que pueda considerarse como una TSA confiable.

Por otra parte, puesto que TSABDE comparte infraestructuras tecnológicas, procedimientos, procesos, controles de seguridad, responsables y organización, con la PKI del Banco de España (PKIBDE), en aquellos aspectos que sean de aplicación, este documento referencia, detalla y completa lo estipulado en la "Declaración de Prácticas de Certificación" (DPC) de PKIBDE.

TSABDE emplea criptografía de clave pública, certificados X509 y fuentes fiables de tiempo para proporcionar sellos de tiempo fiables y conformes a los estándares de aplicación.

Por último, este documento no define ni especifica los mecanismos y protocolos para la validación de los sellos de tiempo emitidos.

3 Conceptos generales

3.1 Servicios de Sellado de Tiempo

Los servicios de sellado de tiempo que proporciona TSABDE se estructuran en dos partes:

- Generación y emisión de los sellos de tiempo: comprende los componentes técnicos y organizativos que emiten los sellos de tiempo (TST)
- Gestión del servicio de sellado de tiempo: los componentes técnicos y organizativos que supervisan y controlan que la operativa de la emisión de sellos de tiempo se realice de forma adecuada, incluyendo la sincronización temporal con la fuente fiable de referencia UTC

Los servicios de sellado de tiempo se prestan de acuerdo con la legislación y estándares de aplicación recogidos en el apartado *1.5 Referencias* de este documento.

3.2 Autoridad de Sellado de Tiempo del Banco de España (TSABDE)

La Autoridad de Sellado de Tiempo del Banco de España (TSABDE) es la responsable de la correcta prestación de los servicios recogidos en el apartado 3.1 conforme a las Políticas y Prácticas establecidas en este documento, para generar confianza a sus usuarios (suscriptores y terceros aceptantes)

TSABDE tiene la responsabilidad de operar una o varias Unidades de Sellado de Tiempo (TSU) las cuales crearán y firmarán los sellos de tiempo (TST) en nombre de TSABDE.

Cada TSU ha de tener su propia clave privada, la cual tendrá asociado un certificado electrónico único emitido por PKIBDE. En cualquier caso, TSABDE queda identificada por el certificado electrónico de firma que utilice cada TSU para la generación y emisión de los sellos de tiempo.

Con carácter general, TSABDE opera en el ámbito de los servicios, aplicaciones y sistemas del Banco de España, u otros relacionados con ellos, y sólo emite sellos de tiempo a los usuarios finales en dichos escenarios.

3.3 Suscriptores

Los suscriptores son personas o entidades que utilizan los servicios de sellado de tiempo proporcionados por TSABDE y que, por lo tanto, acepta sus términos y condiciones.

Los suscriptores son responsables del uso que hagan de los servicios de TSABDE, y han de informar a los Terceros Aceptantes del uso correcto de los sellos de tiempo y de sus condiciones.

3.4 Terceros aceptantes

Los terceros aceptantes son las personas o entidades que deciden confiar en los servicios de sellado de tiempo de TSABDE, y en particular que son receptores, aceptan y confían en los Sellos de Tiempo emitidos por TSABDE

3.5 Política y Prácticas de la TSA

3.5.1 Objetivo

La Política de Sellado de Tiempo recogida en este documento tiene como objetivo definir los requisitos a cumplir por TSABDE para la prestación de un servicio de sellado de tiempo de confianza, de acuerdo con los estándares señalados en el apartado 1.5, y especialmente con ETSI TS 102 023, *Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities.*

La Política de Sellado de Tiempo establece qué condiciones cumple TSABDE, mientras que la Declaración de Prácticas establece cómo las cumple.

La política y las prácticas que son de aplicación a TSABDE están detalladas en los apartados 4 y 5 de este documento, respectivamente. Todos los documentos de prácticas y políticas de TSABDE son aprobados por la Autoridad de Administración de Políticas de PKIBDE.

3.5.2 Nivel de especificidad

La Política de Sellado de tiempo es menos específica que las Prácticas, dado que la Declaración de Prácticas especifica cómo TSABDE cumple los requerimientos técnicos, organizativos y procedimentales establecidos en la política.

3.5.3 Enfoque

Este documento establece las reglas generales para la operación de TSABDE, pero no recoge especificaciones técnicas detalladas de su infraestructura y comunicaciones, estructura de la organización, procedimientos operativos o medidas y controles de seguridad. En particular, no define el entorno en el que las TSU de TSABDE están funcionando.

Los detalles técnicos y operativos están recogidos en la "Declaración de Prácticas de Certificación" (DPC) de PKIBDE, y en documentos adicionales de carácter interno.

4 Política de Sellado de Tiempo

4.1 Resumen

Esta Política define el conjunto de reglas y procedimientos para la generación y emisión confiable de sellos de tiempo, de acuerdo con la especificación técnica ETSI TS 102 023. Las claves privadas y las unidades de sellado de tiempo (TSU) cumplen con las especificaciones técnicas de ETSI TS 101 861 *Time-stamping Profile*, y de RFC 3161 *Time-stamp Protocol (TSP)*

TSABDE emplea claves privadas específicas en cada TSU para la firma de los sellos de tiempo, los cuales contienen una identificación de la política de sellado de aplicación.

Los Sellos de Tiempo (TST) se emiten con una precisión ±1 segundos de UTC.

4.2 Identificación

El OID (object identifier) de esta Política de Sellado de Tiempo es:

1.3.6.1.4.1.19484.2.4.1

Este OID se incluye como identificador de la política en cada sello de tiempo emitido por TSABDE.

4.3 Comunidad de usuarios y aplicabilidad

4.3.1 Comunidad de usuarios

La comunidad de usuarios de los sellos de tiempo emitidos por TSABDE incluye únicamente a sus suscriptores y a sus terceros aceptantes. Todos los suscriptores son considerados de forma automática como terceros aceptantes.

Son suscriptores potenciales todos los usuarios finales de los servicios, aplicaciones y sistemas del Banco de España, o relacionados con ellos. TSABDE no proporciona servicios de sellado de tiempo al público en general fuera del ámbito de sus aplicaciones y sistemas.

La solicitud y/o utilización de un sello de tiempo emitido por TSABDE por parte de un suscriptor o tercero aceptante implica automáticamente la aceptación de las cláusulas y condiciones establecidas en estas Políticas y Prácticas de Sellado de Tiempo.

4.3.2 Aplicabilidad de los sellos de tiempo

TSABDE no establece restricciones específicas para el uso de los sellos de tiempo que emite, si bien se ha de entender que los servicios de sellado de tiempo que ofrece TSABDE 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.

En particular, los sellos de tiempo emitidos de acuerdo con esta política pueden ser usados para:

- Reforzar una firma electrónica[1], dotándola de una certeza temporal
- Proteger las firmas electrónicas de larga duración[2]
- Proporcionar una evidencia y prueba confiable de que determinados datos existían antes de un momento temporal concreto
- Determinar el momento de realización de una transacción
- Utilización en sistemas de archivo de documentación y datos
- Sistemas de registro y logs

Los sellos de tiempo emitidos por TSABDE sólo son válidos para su uso en los servicios, aplicaciones y sistemas del Banco de España, o relacionados con ellos.

4.3.3 Limitaciones y restricciones en el uso de los sellos de tiempo

Cualquier uso no incluido en el apartado anterior queda excluido.

4.4 Conformidad y auditorías

TSABDE incluirá el OID de esta Política (descrito en el apartado 4.2) en todos los sellos de tiempo que emita para indicar su conformidad con ella.

Asimismo, TSABDE sólo aceptará las peticiones de generación de un sello de tiempo que incluyan el OID de esta Política, o que no incluyan ninguna política de forma explícita.

La AAP es responsable de que la prestación de los servicios de sellado de tiempo sea conforme con las estipulaciones incluidas en estas Políticas y Prácticas de Sellado de Tiempo, y asegura la fiabilidad de los controles y requisitos descritos en este documento. En este sentido, el Banco de España llevará a cabo auditorías periódicas del funcionamiento de TSABDE, de acuerdo con el Plan de Auditorías y directrices establecidas en la DPC de PKIBDE.

4.5 Repositorios y publicación de información

4.5.1 Repositorios

El repositorio de TSABDE está compuesto por un servicio Web, con acceso libre, que contendrá la información siguiente:

Para el certificado de firma de TSABDE:
- WEB: http://pki.bde.es/certs

Para los certificados de la cadena de certificación de TSABDE:
- WEB: http://pki.bde.es/certs

[1] El objetivo de los sellos de tiempo emitidos bajo las Políticas y Prácticas de Sellado de Tiempo recogidas en este documento pretenden reforzar cualquier firma electrónica, independientemente del carácter legal de la misma (firma simple, avanzada o reconocida), según la Ley 59/2003 de Firma Electrónica.

[2] ETSI TS 101 733 Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES) y ETSI TS 101 903, XML Advanced Electronic Signatures (XAdES)

Para la DPC, la PST y las DPST:

Las Políticas y Prácticas de Sellado de Tiempo recogidas en este documento, y la DPC de PKIBDE, son de acceso público en http://pki.bde.es/politicas.

En particular, desde la página se accede al documento siguiente (X.Y indica la versión):

- PKIBdE_DPC-VX.Y.pdf
- PKIBdE_PST_y_DPST-VX.Y.pdf

Para la notificación de hechos relevantes (ej: compromiso de TSA)

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

4.5.2 Temporalidad o frecuencia de publicación

La PST y las DPST 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 anterior.

4.5.3 Controles de acceso a los repositorios

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

5 Prácticas de TSABDE

TSABDE tiene implantados los controles necesarios para garantizar que la prestación de los servicios de sellado de tiempo se realiza según las directrices y requisitos establecidos en este documento de políticas y prácticas.

5.1 Declaración de Prácticas y Declaración básica

5.1.1 Declaración de Prácticas de TSABDE

Los procedimientos, mecanismos de control e infraestructuras técnicas que se describen en este capítulo, son la base del funcionamiento de TSABDE. Puesto que TSABDE comparte infraestructuras tecnológicas, procedimientos, procesos, controles de seguridad, responsables y organización, con la PKI del Banco de España (PKIBDE), en la "Declaración de Prácticas de Certificación" (DPC) de PKIBDE se encuentran descritos otros controles de aplicación.

En particular, el presente documento de Políticas y Prácticas de Sellado de Tiempo conjuntamente con la DPC de PKIBDE regulan la operación y requisitos de los servicios de sellado de tiempo de TSABDE.

Estos documentos, así como cualquier otra información de relevancia, están disponibles al público en los repositorios descritos en el apartado 4.5, y bajo las consideraciones de propiedad intelectual recogidas en el apartado 6.4.

La Autoridad de Administración de Políticas es la responsable de mantener y aprobar todas las políticas y prácticas que rigen el funcionamiento de TSABDE.

Por otra parte, la AAP es la responsable de la correcta implantación y funcionamiento de las políticas y prácticas. En este sentido, TSABDE efectúa evaluaciones y auditorías periódicas para determinar el estado de los controles y procedimientos de seguridad y efectuar los cambios pertinentes, según los mecanismos y procedimientos descritos en la DPC de PKIBDE.

Por último, el análisis de vulnerabilidades de TSABDE queda cubierto con el Plan de Auditoría del Banco de España, según se establece en la DPC de PKIBDE.

5.1.2 Declaración Básica de TSABDE

La Declaración Básica de la TSA recoge las condiciones y aspectos fundamentales de uso de los servicios de sellado de tiempo, y se corresponde con la "TSA Disclosure Statement" definida en el estándar ETSI TS 102 023. En este caso, para evitar una innecesaria disgregación de documentos, se integra su contenido en el de este documento, la cual actúa, por tanto, como Declaración Básica.

Los aspectos fundamentales de la Declaración Básica son los siguientes:

- TSABDE es un servicio del Banco de España, cuyos datos de contacto se encuentran al principio de este documento en el apartado 1.4
- La disponibilidad del servicio prestado por TSABDE está descrito en el apartado 5.3.1 del presente documento.
- Cada sello de tiempo emitido por TSABDE contiene el identificador de política (OID) incluido en el apartado 4.2 de este documento.
- Los algoritmos criptográficos y la longitud de las claves soportadas y utilizadas por TSABDE cumplen con *ETSI TS 101 861 Time-stamping Profile* y son:
    - Para la peticiones de sellos de tiempo, se soportan los algoritmos siguientes:
        Hash: SHA-512, SHA-384, SHA-256, SHA-224, SHA-1, MD5, RIPEMD-160
    - Para los sellos de tiempo emitidos:
        Hash: SHA-1
        Firma: sha1WithRSAEncryption, longitud de clave de al menos 2048 bits.
- TSABDE no establece limitaciones de confianza y validez en sus servicios de sellado de tiempo adicionales a las recogidas en el apartado 4 de este documento. Si se determinara que los algoritmos criptográficos empleados o la longitud de claves han dejado de ser seguros, TSABDE publicará dicha información en su página web.
- TSABDE asegura la precisión establecida en la Política de Sellado del apartado 4.1, con respecto a las fuentes de tiempo UTC de confianza definidas en el apartado 5.3.4, y garantiza que no emitirá sellos de tiempo con una menor precisión.
- Con carácter general, TSABDE no establece restricciones específicas para el uso de los sellos de tiempo que emite, si bien se ha de entender que los servicios de sellado de tiempo que ofrece TSABDE 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.
- La aplicabilidad de los sellos de tiempo emitidos por TSABDE está descrita en el apartado 4.3.2 del presente documento.
- Los sellos de tiempo emitidos por TSABDE sólo son válidos para su uso en los servicios, aplicaciones y sistemas del Banco de España, o relacionados con ellos.
- Las obligaciones de los suscriptores están descritas en el apartado 6.5.3 del presente documento.
- Las obligaciones de los terceros aceptantes están descritas en el apartado 6.5.4 del presente documento.
- TSABDE mantiene de forma segura los registros correspondientes a sus operaciones, de acuerdo con el apartado 5.5.11 del presente documento.
- Las operaciones y funcionamiento de TSABDE, así como la presente Declaración de Políticas y Prácticas de Sellado de Tiempo estarán sujetas a la legislación española y europea, y a la

normativa específica del Banco de España que les sea aplicable, recogida en el apartado 5.5.10 del presente documento.

- Las responsabilidades y limitaciones de responsabilidad de TSABDE están descritas en el apartado 6.6 del presente documento.
- Todas las reclamaciones entre usuarios o terceros y TSABDE deberán ser comunicadas conforme a lo establecido en el apartado 6.11 del presente documento. 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 especificados en dicho apartado 6.11, con renuncia a cualquier otro fuero que pudiera corresponderles.
- TSABDE garantiza que la prestación de los servicios de sellado de tiempo es conforme con las estipulaciones incluidas en estas Políticas y Prácticas de Sellado de Tiempo. En este sentido, el Banco de España llevará a cabo auditorías periódicas del funcionamiento de TSABDE, de acuerdo con el Plan de Auditorías y directrices establecidas en la DPC de PKIBDE.
- TSABDE proporciona sus sellos de tiempo a su comunidad de usuarios de forma gratuita.

5.2 Gestión del ciclo de vida de las claves

5.2.1 Generación de la clave de la TSA

Las claves criptográficas de las TSUs utilizadas en los servicios de TSABDE se generan en módulos criptográficos hardware (HSM) que están certificados con un nivel de seguridad mínimo FIPS 140-2 nivel 3, EAL4 o similar. Estos dispositivos HSM están permanentemente ubicados en un entorno físico seguro, común al resto de infraestructuras y sistemas de PKIBDE, según se describe en la DPC.

Asimismo, estas claves se generan bajo un control multipersona[1] con la participación de, al menos, dos responsables de TSABDE.

El algoritmo criptográfico utilizado para la generación de la clave de firma es RSA, utilizando una longitud de clave de al menos 2048 bits. Para la firma de los certificados de Autoridad de Sellado de Tiempo se usa sha256WithRSAEncryption. Si se determinara que estos algoritmos o la longitud de la clave han dejado de ser seguros, TSABDE los sustituirá por otros nuevos que sean considerados seguros, y publicará dicha información en su página web.

5.2.2 Protección de la clave privada de la TSU

TSABDE adopta las medidas necesarias para garantizar que las claves privadas de las TSUs sean confidenciales y mantengan su integridad.

Esto incluye, entre otras medidas, el uso de módulos HSMs certificados FIPS 140-2 de nivel 3, EAL4 o similar, para la generación, almacenamiento y custodia de las claves, y la generación de las firmas de los sellos de tiempo. Sólo TSABDE tendrá acceso a las claves privadas utilizadas, las cuales además se almacenarán cifradas.

No se efectuará el archivo de la clave privada de los certificados utilizados por TSABDE fuera de los módulos HSMs.

No obstante, el Banco de España dispone de una copia de seguridad de estos HSMs, las cuales son realizadas por el personal del Banco de España designado a tal efecto siguiendo las directrices detalladas en la DPC de PKIBDE. En caso de desastre, la recuperación a partir de estas copias de seguridad se realiza bajo un control multipersona con la participación de, al menos, dos responsables de TSABDE.

Las personas que realizan todas estas tareas están debidamente cualificadas para ello, y son de aplicación los controles de personal detallados en la DPC de PKIBDE.

5.2.3 Distribución de la clave pública de la TSU

La clave pública de cada TSU está incluida en su certificado correspondiente.

Los certificados electrónicos utilizados en TSABDE serán emitidos por PKIBDE.

El certificado de cada TSU, así como su cadena de certificación, se publicarán en los repositorios de TSABDE descritos en el apartado 4.5 de este documento.

---

[1] 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.

El perfil del certificado emitido para TSABDE cumple con el estándar X509 v3 y la RFC 3161, y se encuentra detallado en el apartado 5.4 del presente documento.

5.2.4 Renovación de las claves de las TSU

TSABDE renovará las claves de firma utilizadas por sus TSUs con la suficiente antelación a su caducidad.

Asimismo, las claves de firma de las TSU también se renovarán antes del fin de su periodo de validez siempre que sean consideradas potencialmente comprometidas por los responsables de TSABDE, bien porque se considere que el algoritmo criptográfico o la longitud de clave se consideran vulnerables, bien por cualquier otro motivo.

En ambos casos, la renovación de las claves se considerará como una nueva generación de claves, según se establece en el apartado 5.2.1 del presente documento.

5.2.5 Final del ciclo de vida de las claves de la TSU

Las claves de firma de las TSUs se sustituirán con antelación a su caducidad, según se establece en el apartado 5.2.4 del presente documento.

Las TSUs rechazarán cualquier intento de generar sellos de tiempo con una clave de firma una vez haya caducado.

TSABDE mantiene un archivo con todos sus certificados y claves públicas, en los repositorios descritos en el apartado 4.5 de este documento. El plazo de archivo seguirá las directrices establecidas en la DPC de PKIBDE para el archivo de las claves públicas, con el objetivo de poder validar los sellos de tiempo emitidos en el pasado. El control de dicho registro está a cargo de los Administradores de PKIBDE y de TSABDE

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

5.2.6 Gestión del ciclo de vida del modulo criptográfico (HSM) empleado para generar los sellos de tiempo

La gestión del ciclo de vida de los módulos HSMs utilizados se realiza conforme a las directrices y controles establecidos en la DPC de PKIBDE.

En particular, TSABDE utiliza módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros. TSABDE únicamente utiliza módulos criptográficos con certificación FIPS 140-2 Nivel 3, EAL4 o similar.

Estos dispositivos HSM están permanentemente ubicados en un entorno físico seguro, común al resto de infraestructuras y sistemas de PKIBDE, según se describe en la DPC.

Con anterioridad a su instalación se verifica que en su transporte y entrega no ha sido manipulado ni modificado, y que funciona correctamente.

Asimismo estos HSMs se configuran para que su inicialización, restauración y administración tenga un control multipersona con la participación de, al menos, dos responsables de PKIBDE. La activación y desactivación de sus claves privadas se realiza de forma análoga a lo establecido en la DPC de PKIBDE. Las personas que realizan todas estas tareas están debidamente cualificadas para ello, y son de aplicación los controles de personal detallados en la DPC.

En caso de avería o desastre, la sustitución de estos módulos HSMs se considerará como una nueva instalación, y serán de aplicación todos los requisitos descritos en este apartado.

5.3 Sellado de tiempo

5.3.1 Acceso al servicio

Los sellos de tiempo se pueden solicitar mediante el protocolo TSP (Time-Stamp Protocol) de acuerdo con lo establecido en la RFC 3161.

La dirección de acceso al servicio es http://pkitsa.bde.es, accesible únicamente desde la red interna del Banco de España.

5.3.2 Disponibilidad del servicio

Los servicios de sellado de tiempo ofrecidos por TSABDE está disponible de forma ininterrumpida todos los días del año.

5.3.3 Sello de tiempo

TSABDE adopta las medidas técnicas necesarias para garantizar que los sellos de tiempo se emiten de forma segura e incluyen la fecha/hora correcta.

Los sellos de tiempo generados son conformes con los estándares referenciados en el apartado 1.5 de este documento, y siguen la estructura definida en la *RFC 3161 Time-stamp Protocol (TSP)*. En particular cada sello de tiempo incluye, al menos:

- El identificador de la política de sellado de tiempo, especificado en el apartado 4.2
- La representación (hash) del conjunto de datos al que se le está proporcionando el sello de tiempo.
- Un número de serie único que puede ser utilizado para identificar el sello de tiempo.
- El tiempo, expresado en formato “Zulu” ("Zulu" time). El reloj está sincronizado con la fuente de tiempos segura descrita en el apartado 5.3.4, y con la precisión declarada en 4.1.
- La firma electrónica generada por la TSU, usando la clave privada utilizada sólo para el sellado de tiempo.
- El certificado electrónico de la TSU utilizado para la firma del sello, el cual servirá como identificación de dicha TSU y de la propia TSABDE. Este certificado tendrá la estructura descrita en el apartado 5.4 del presente documento.

TSABDE mantiene registros de auditoría de todas las calibraciones respecto a la fuente de tiempo segura, y no emitirá sellos de tiempo si la precisión está fuera del margen establecido.

5.3.4 Sincronización del reloj con UTC

TSABDE proporciona el instante de tiempo con la precisión declarada en la Política de Sellado de Tiempo del apartado 4.1, con respecto a 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).

Las TSU tienen establecidas las medidas técnicas necesarias para evitar que sus relojes sufran desviaciones dentro de la precisión declarada. Además, estos relojes están protegidos y se recalibran periódicamente y de forma automática respecto a la fuente de tiempos segura.

Asimismo son capaces de detectar las desviaciones respecto a la precisión establecida y activar una nueva calibración.

Por otra parte, las TSU están permanentemente ubicadas en un entorno físico seguro, común al resto de infraestructuras y sistemas de PKIBDE, según se describe en la DPC. Del mismo modo, el acceso remoto a las mismas está protegido frente a accesos no autorizados.

Por último, se registran todos los eventos generados relativos a la sincronización y modificación de la hora de cada TSU, con el objetivo de detectar y trazar las desviaciones con respecto al reloj y a la precisión declarada, ya sea de forma accidental o intencionada.

5.4 Perfil del Certificado de firma de la TSU

5.4.1 Número de versión

Los certificados utilizados por TSABDE utilizan el estándar X.509 versión 3 (X.509 v3)

5.4.2 Emisor del certificado

Los certificados electrónicos utilizados en TSABDE son emitidos por PKIBDE.

5.4.3 Formatos y restricciones de los nombres

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

Los certificados contienen el *Distinguished Name* X.500 del emisor en el campo *issuer name.*

El campo *subject name* contiene el *Distinguished Name* X.500 que identifica a TSABDE, cuyo nombre común tendrá el siguiente valor:

CN=BANCO DE ESPAÑA – TSA *TEXTO_LIBRE*

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

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

O=BANCO DE ESPAÑA, C=ES

5.4.4 Perfil y extensiones del certificado

Las extensiones utilizadas son:

- *Subject Key Identifier*. Calificada como no crítica.
- *Authority Key Identifier*. Calificada como no crítica.
- *KeyUsage*. Calificada como crítica.
- *extKeyUsage*. Calificada como crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *SubjectAlternativeName*. Calificada como no crítica.
- *BasicConstraints*. Calificada como crítica.
- *CRLDistributionPoint*. 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.
- *bdeIssuerName* (*1.3.6.1.4.1.19484.2.3.17*). Calificada como no crítica.
- *bdeIssuerVAT (1.3.6.1.4.1.19484.2.3.18)*. Calificada como no crítica.

A continuación se recoge el perfil de los certificados de TSABDE.

Perfil de certificado de TSA de la PKI

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

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

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

5.5 Gestión y operación de la TSA

Puesto que TSABDE comparte infraestructuras tecnológicas, procedimientos, procesos, controles de seguridad, responsables y organización, con la PKI del Banco de España (PKIBDE), en los apartados siguientes es de aplicación lo estipulado en la "Declaración de Prácticas de Certificación" (DPC) de PKIBDE.

En aquellos casos que se estime necesario, se describirán los apartados correspondientes de la DPC donde se detallan

5.5.1 Gestión de la seguridad

TSABDE asegura el mantenimiento de un nivel apropiado de seguridad en sus operaciones de acuerdo con las mejores prácticas y los estándares de aplicación.

En particular, los aspectos relativos a la gestión de la seguridad son compartidos con PKIBDE y se encuentran descritos en los capítulos *5 Controles de seguridad física, instalaciones, gestión y operacionales*, y *6 Controles de seguridad técnica* de la DPC de PKIBDE.

5.5.2 Gestión y clasificación de activos

Para garantizar el adecuado nivel de seguridad de sus procesos de negocio, el Banco de España como responsable de TSABDE, mantiene un inventario de sus activos de información y les aplica el nivel de seguridad pertinente en cada caso.

5.5.3 Seguridad ligada al personal

TSABDE mantiene unas prácticas apropiadas en la selección, contratación, gestión y finalización de la relación de personal.

En particular, los aspectos relativos a la gestión del personal son compartidos con PKIBDE y se encuentran descritos en los apartados *5.2 Controles de procedimiento*, y *5.3 Controles de personal* de la DPC de PKIBDE.

5.5.4 Seguridad física y del entorno

TSABDE está ubicada y opera en un entorno seguro, común al resto de infraestructuras y sistemas de PKIBDE, según se describe en el apartado *5.1 Controles físicos* de la DPC.

5.5.5 Gestión de las operaciones

TSABDE mantiene controles operacionales de acuerdo con ETSI TS 102 023 y con las políticas internas del propio Banco de España.

5.5.6 Gestión de acceso a los sistemas

TSABDE está ubicada y opera en un entorno seguro, común al resto de infraestructuras y sistemas de PKIBDE, para el que mantiene controles de acceso físico y lógico a las instalaciones, hardware, sistemas e información. En los capítulos *5 Controles de seguridad física, instalaciones, gestión y operacionales,* y *6 Controles de seguridad técnica* de la DPC de PKIBDE se describen estos controles.

5.5.7 Despliegue y mantenimiento confiable de los sistemas

Los certificados utilizados para el servicio de sellado de tiempo se generan y gestionan en un entorno seguro de acuerdo con lo establecido en el apartado 5.2 del presente documento.

Del mismo modo, TSABDE comparte con PKIBDE los controles de seguridad durante el ciclo de vida de los sistemas, según se describe en el apartado *6.6 Controles de seguridad del ciclo de vida* de la DPC de PKIBDE. En este sentido, se aplican procedimientos de control de cambios para mantener el grado de confiabilidad de los sistemas

5.5.8 Compromiso de los servicios de la TSA

La gestión que realiza TSABDE ante posibles incidentes está descrita en el apartado *5.7 Recuperación en caso de compromiso de una clave o catástrofe* de la DPC de PKIBDE.

TSABDE no emitirá sellos de tiempo hasta que haya aplicado las acciones correctoras y se haya solventado el incidente. En particular, se identifican los siguientes incidentes:

- Compromiso de la clave privada de la TSU, en cuyo caso TSBDE solicitará de inmediato la revocación del certificado. La TSU no emitirá sellos de tiempo mientras no disponga de una clave privada válida.
- La TSU no emitirá sellos de tiempo si su reloj está fuera de la precisión establecida respecto a UTC hasta que no se restaure la calibración temporal. De acuerdo con lo establecido en el apartado 5.5.11 de este documento, TSABDE mantiene registros de auditoría, incluyendo información sobre la sincronización de los relojes.
- Otros desastres ocasionados por causa de fuerza mayor

En caso de que se produjera un compromiso, hubiera sospecha del mismo, o haya pérdida de la sincronización del reloj interno, TSABDE comunicará los detalles del incidente a sus suscriptores y terceros aceptantes a través de su web en los repositorios definidos en el apartado 4.5 de este

documento. Entre la información a publicar se deberán aportar datos que sirvan para determinar los sellos de tiempo que se han visto afectados.

5.5.9 Finalización de la TSA

En el caso de cesar la actividad de prestación de servicios de sellado de tiempo, TSABDE se asegurará de que los potenciales problemas para los suscriptores y los terceros aceptantes sean los mínimos, así como el mantenimiento de los registros requeridos para proporcionar prueba cierta de la prestación del servicio de sellado de tiempo a efectos legales.

En caso de finalización o cese de actividad de los servicios de TSABDE, ésta notificará tal hecho a sus suscriptores con un plazo mínimo de antelación de 2 meses al citado cese.

En el supuesto de que TSABDE decidiera transferir la actividad a otra Autoridad de Sellado de Tiempo, comunicará a sus suscriptores los acuerdos de transferencia. A tal efecto TSABDE publicará un documento explicativo de las condiciones de transferencia y de las características de la TSA al que se propone la transferencia del servicio de sellado de tiempo.

TSABDE realizará la comunicación del cese de actividad y otros detalles relativos mediante la publicación a través de su web en los repositorios definidos en el apartado 4.5 de este documento.

En caso de finalización o cese de la actividad, TSABDE solicitará la revocación de los certificados de las TSU.

5.5.10 Cumplimiento de los requisitos legales

TSABDE cumple con todos los requerimiento legales, tanto relacionados con los servicios de certificación y sellado de tiempo, como con la protección de datos de carácter personal (ver apartado 7 del presente documento). Las principales normativas de aplicación son:

- 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.
- DIRECTIVA 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- 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.
- 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

5.5.11 Registro de información referente a la operación de los servicios de sellado de tiempo

TSABDE mantiene registro de toda la información relevante de sus operaciones por un periodo de 15 años. Los registros se protegen para garantizar su integridad y confidencialidad.

Los registros están a disposición de los suscriptores, en lo que se refiera a ellos, y de las autoridades que los requieran conforme a la ley.

Entre otros, TSABDE mantiene registros, que incluyen el instante temporal preciso, de:

- Peticiones de sellado de tiempo y sellos de tiempo emitidos.
- Eventos relacionados con la administración de la TSU (gestión de certificados, gestión de claves y sincronización de relojes).

En lo concerniente a los procedimientos de gestión, controles y auditoría relativos a los registros de TSABDE, son de aplicación los apartados *5.4 Procedimientos de auditoría de seguridad* y *5.5 Archivo de registros* de la DPC de PKIBDE.

5.6 Organización

TSABDE es propiedad del Banco de España.

El Banco de España, a través de la AAP, se responsabiliza de adoptar las medidas de seguridad necesarias para cumplir con los estándares y leyes de aplicación al servicio de sellado de tiempo, así como con las políticas y prácticas recogidas en el presente documento para la prestación de los servicios de sellado de tiempo.

Los documentos reguladores de su actividad se encuentran en los repositorios descritos en el apartado 4.5 del presente documento.

6 Otras cuestiones legales y de actividad

6.1 Tarifas

6.1.1 Tarifas de emisión de sellos de tiempo

No se aplica ninguna tarifa sobre la emisión de sellos de tiempo bajo el amparo de la presente Política de Sellado de Tiempo.

6.1.2 Tarifas de acceso a los certificados

El acceso a los certificados utilizados por TSABDE es gratuito y por tanto no hay ninguna tarifa de aplicación sobre el mismo.

6.1.3 Tarifas de otros servicios tales como información de políticas

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

6.1.4 Política de reembolso

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

6.2 Confidencialidad de la información

6.2.1 Ámbito de la información confidencial

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

- Las claves privadas de las TSU que componen TSABDE.
- La información relativa a las operaciones que lleve a cabo TSABDE, incluyendo los sellos de tiempo emitidos.
- La información referida a los parámetros de seguridad, control y procedimientos de auditoría.
- La información de carácter personal proporcionada por los suscriptores a TSABDE, de conformidad con lo dispuesto en la normativa sobre protección de datos de carácter personal y reglas de desarrollo.

6.2.2 Información no confidencial

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

- La contenida en las presentes Políticas y Prácticas de Sellado de Tiempo
- La incluida en la Declaración de Practicas de Certificación (DPC) y las Políticas de certificación de PKIBDE.

6.2.3 Deber de secreto profesional

Es de aplicación lo especificado en el apartado *9.2.3 Deber de secreto profesional* de la DPC de PKIBDE.

6.3 Protección de la información personal

De acuerdo con la legislación española al respecto, se recoge dentro del capítulo 7 del presente documento.

6.4 Derechos de propiedad Intelectual

Es de aplicación lo especificado en el apartado *9.4 Derechos de propiedad Intelectual* de la DPC de PKIBDE.

6.5 Obligaciones

6.5.1 Obligaciones generales de TSABDE

El Banco de España opera TSABDE y asume la responsabilidad de que los servicios de sellado de tiempo prestados son conformes a lo especificado en estas políticas y prácticas, y del cumplimiento de los requerimientos y controles establecidos en el apartado 5 de este documento, así como de las regulaciones legales de aplicación.

Cabe destacar que también son de aplicación las obligaciones y responsabilidades establecidas en la DPC de PKIBDE.

6.5.2 Obligaciones de TSABDE respecto a sus suscriptores

TSABDE asume las siguientes obligaciones con respecto a sus suscriptores:

1 Operar de acuerdo a estas Políticas y Prácticas de Sellado de Tiempo y a la Declaración de Prácticas de Certificación de PKIBDE

2 Operar sobre la base de sistemas, tecnologías, equipamiento software y hardware confiables, y con el personal adecuado

3 Garantizar que los sellos de tiempo emitidos no contienen ningún dato erróneo o falso

4 Asegurar que las TSU mantienen su reloj sincronizado y con la precisión declarada con respecto al tiempo UTC

5 Llevar a cabo revisiones internas y externas para asegurar el cumplimiento de la legislación de aplicación y las políticas y procedimientos internos

6 Proporcionar acceso ininterrumpido a los servicios de sellado de tiempo excepto en caso de interrupciones programadas, pérdidas de la sincronización temporal o causas de fuerza mayor

7 En caso de que se produjera un compromiso, hubiera sospecha del mismo, o haya pérdida de la sincronización del reloj interno, comunicar los detalles del incidente. Entre la información a publicar se deberán aportar datos que sirvan para determinar los sellos de tiempo que se han visto afectados

8 Cualquier otra obligación establecida para PKIBDE en el apartado 9.5 Obligaciones de la DPC y que fuera de aplicación para TSABDE

6.5.3 Obligaciones de los suscriptores

Es obligación de los suscriptores de los servicios de sellado de tiempo de TSABDE:

1 Utilizar software adecuado para la solicitud y obtención de sellos de tiempo

2 Verificar que el sello de tiempo ha sido firmado correctamente

3 Verificar, mediante consulta de CRL o protocolo OCSP, que la clave privada empleada para generar el sello de tiempo no ha sido comprometida

4 Conocer y aceptar las condiciones y limitaciones de utilización de los sellos de tiempo establecidas en esta Política

5 Limitar y adecuar el uso de los sellos de tiempo a lo permitido por esta Política

6 No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica (hardware y software) de los servicios de sellado de tiempo

7 Cualquier otra que se derive de la ley, la normativa aplicable, de las Política de Sellado de tiempo, o de la DPC de PKIBDE

6.5.4 Obligaciones de los Terceros Aceptantes

Es obligación de las terceras partes que acepten y confíen en los sellos de tiempo emitidos por TSABDE:

1 Verificar que el sello de tiempo ha sido firmado correctamente y que la clave privada utilizada para su firma no estaba comprometida en el momento de la verificación. Durante el periodo de validez del certificado de la TSU, el estado de la clave privada puede verificarse consultando la CRL o mediante consulta on-line por protocolo OCSP. Una vez que caduque el certificado de la TSU el tercero aceptante podrá confiar en el sello de tiempo mediante la solicitud de uno nuevo, o bien directamente si en el momento de la verificación se conoce que:

- **a** La clave privada de la TSU no ha sido comprometida en ningún momento, y
- **b** La función criptográfica hash utilizada en el sello de tiempo se considera todavía segura, y
- **c** El algoritmo criptográfico y el tamaño de la clave utilizado para la firma electrónica se considera todavía seguro

2 Limitar la fiabilidad de los sellos de tiempo a los usos permitidos de los mismos, en conformidad con lo expresado en esta Política de Sellado de Tiempo

3 Tener conocimiento de las garantías y aceptar las responsabilidades aplicables en la aceptación y uso de los sellos de tiempo

4 Notificar cualquier hecho o situación anómala relativa al servicio de sellado, y/o a los sellos de tiempo emitidos, y que pueda ser considerado como causa de revocación del mismo

5 Tener conocimiento y asumir cualquier otra precaución que tuviera establecida mediante acuerdo con la Autoridad de Sellado de Tiempo, para la obtención de servicios de sellado de tiempo

6.6 Responsabilidades

6.6.1 Responsabilidades de TSABDE

TSABDE sólo 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 las presentes Políticas y Prácticas de Sellado de Tiempo, y en la DPC de PKIBDE.

6.6.2 Exención de responsabilidades de PKIBDE

TSABDE no asumirá responsabilidad alguna en relación al uso y aplicabilidad de los sellos de tiempo emitidos para cualquier actividad no especificada en la presente Política.

TSABDE no se responsabiliza del contenido de los documentos y datos a los que se aplique el sello de tiempo que emita, y no responde de posibles daños y perjuicios en transacciones a las que se haya aplicado.

TSABDE no representa en forma alguna a los suscriptores ni a terceras partes aceptantes de los sellos de tiempo que emite.

6.6.3 Alcance de la cobertura

Según lo especificado en el apartado *9.6.3 Alcance de la cobertura* de la DPC de PKIBDE.

6.7 Limitaciones de pérdidas

Según lo especificado en el apartado *9.7 Limitaciones de pérdidas* de la DPC de PKIBDE.

6.8 Periodo de validez

6.8.1 Plazo

Es de aplicación lo especificado en el apartado *9.8.1 Plazo* de la DPC de PKIBDE.

6.8.2 Sustitución y derogación de las Políticas y Prácticas de Sellado de Tiempo

Según lo especificado en el apartado *9.8.2 Sustitución y derogación* de la DPC de PKIBDE.

6.8.3 Efectos de la finalización

Según lo especificado en el apartado *9.8.3 Efectos de la finalización* de la DPC de PKIBDE.

6.9 Notificaciones individuales y comunicaciones con los participantes

Según lo especificado en el apartado *9.9 Notificaciones individuales y comunicaciones con los participantes* de la DPC de PKIBDE.

6.10 Procedimientos de cambios en las especificaciones

6.10.1 Procedimiento para los cambios

La Autoridad con atribuciones para realizar y aprobar cambios sobre la Política y las Prácticas de Sellado de Tiempo de TSABDE es la Autoridad de Administración de Políticas (AAP). Los datos de contacto de la AAP se encuentran en el apartado 1.4 Administración de las políticas y prácticas.

6.10.2 Periodo y mecanismo de notificación

En el caso de que la AAP juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los sellos de tiempo se comunicará a los suscriptores y terceros aceptantes que se ha efectuado un cambio y que deben consultar las nuevas Políticas y Prácticas de Sellado de Tiempo en el repositorio establecido.

6.10.3 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 sellos de tiempo 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 suscriptores y terceros aceptantes.

En el caso de que la AAP juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los sellos de tiempo 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 suscriptores y terceros aceptantes de los sellos de tiempo.

6.11 Reclamaciones y jurisdicción

Según lo especificado en el apartado *9.11 Reclamaciones y jurisdicción* de la DPC de PKIBDE.

6.12 Normativa aplicable

De acuerdo con la legislación española y europea al respecto, se recoge dentro del apartado 5.5.10 del presente documento.

6.13 Cumplimiento de la normativa aplicable

Según lo especificado en el apartado *9.13 Cumplimiento de la normativa aplicable* de la DPC de PKIBDE.

6.14 Estipulaciones diversas

6.14.1 Cláusula de aceptación completa

Todos los Subscriptores del servicio de sellado de tiempo, por el mero hecho de utilizarlo, así como los Terceros Aceptantes, asumen en su totalidad el contenido de la última versión de estas Políticas y Prácticas de Sellado de Tiempo.

6.14.2 Independencia

Según lo especificado en el apartado *9.14.2 Independencia* de la DPC de PKIBDE.

6.14.3 Resolución por la vía judicial

No estipulado.

6.15 Otras estipulaciones

No estipulado.

7 Régimen jurídico y protección de datos de carácter personal

Es de aplicación a la Política de Protección de Datos de Carácter Personal de TSABDE lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal (LOPD) 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, de 13 de diciembre, de protección de datos de carácter personal.

También es de aplicación la 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.

En el caso de que para la prestación del servicio de sellado de tiempo sea necesario recabar datos personales del suscriptor, se verificará que éste es informado y presta su consentimiento al tratamiento de sus datos personales, a la finalidad que se les va a dar, a los destinatarios de los mismos y su inclusión en el fichero declarado al efecto por PKIBDE.

El titular de los datos podrá ejercer los derechos de acceso, rectificación, cancelación y oposición, dirigiéndose a la dirección de contacto señalada en este documento.

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.

Por último, son también de aplicación las consideraciones establecidas en el capítulo *10 Protección de datos de carácter personal* de la DPC de PKIBDE.