BANCO DE ESPAÑA
Eurosistema

22.06.2018

OID: 1.3.6.1.4.1.19484.2.4.1

Time-stamping Authority of Banco de España

Time-Stamp Policies and Practices

This document describes the Time-Stamp Policies and Practices regulating the time-stamp tokens issued by the Banco de España Time-Stamping Authority.

Control Sheet

Title	Time Stamping Policies and Practices
Author	Information Systems Department
Version	1.3
Date	22.06.2018

Change Log

Version	Date	Reason for the change
1.0	25.05.2010	Initial Version
1.1	11.05.2015	Update due to the renewal of the Certification Authorities
1.2	18.12.2017	Update due to the definition of the new proprietary extensions bdeIssuerName and bdeIssuerVAT
1.3	22.06.2018	Update due to the new VAT identification number assigned to Banco de España.

TABLE OF CONTENTS

1 Introduction

1.1 Overview

This document describes the Time-Stamp Policy (TSP) and the Time-Stamp Practices Statement (TSPS) which governs the functioning and operations of the Time-Stamping Authority (hereinafter TSABDE) of Banco de España (hereinafter TSABDE).

The Time-Stamping Service forms part of Banco de España's PKI Certification Services, acting under the provisions of article 2.2[1] of Law 59/2003, of 19 December, the Electronic Signature Act.

The electronic signature provides added security to data, enabling the signatory's identity to be guaranteed and data not to be modified once signed. Time-stamp tokens use electronic signatures, incorporating the time obtained from an accurate and reliable source, to guarantee when a particular action or piece of data existed or was produced.

This TSP and TSPS is applied to all those involved with the TSA of Banco de España (TSABDE), including its service subscribers and relying parties, amongst others. In particular, it includes all the services aimed at managing and operating time-stamping services, and the necessary considerations for application and use of said services and of the time stamps provided by the TSABDE. Consequently, all the parties involved must be aware of the content of this TSP and TSPS and adapt their activities to the stipulations therein.

From the point of view of standards and best practices that the ETSI and IETF working parties have been developing, a Time-Stamping Policy (TSP) is the set of rules that define the applicability or use of a time-stamp token in a community of users, systems or particular class of applications having a series of security requirements in common. On the other hand, a Time-Stamping Practices Statement (TSPS) establishes the specific conditions and circumstances (practices) that a TSA uses to issue time stamps.

Given that TSABDE shares technological infrastructures, procedures, processes, security controls, persons in charge and organisation with the PKI of Banco de España (PKIBDE), in what is applicable, these TSP and TSPS reference, detail and complete the provisions of the PKIBDE "Certification Practices Statement" (DPC).

This document has been drawn up generally in accordance with the ETSI TS 102 023 technical specification, *Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities*[2], both in its content and structure, although in err of consistency and coherence with the Certification Policies and Practices of the Banco de España Public Key Infrastructure (PKIBDE) the order of this document has been amended so that:

- The chapters on References, Definitions and Acronyms are at the beginning of the document, in the introduction.
- The chapter on Obligations and Liabilities is at the end of the document.

[1] This corresponds to the definition given in article 3.10 of Regulation (EU) No 910/2014.

[2] This technical specification has been adopted by the IETF as RFC 3628 *Policy Requirements for Time-Stamping Authorities (TSAs).*

Hence, in order to give the document a uniform structure and facilitate its reading and analysis, all the sections established in ETSI TS 102 023 have been included. Where nothing has been established for any section the phrase "No stipulation" will appear.

In addition to the headings established in ETSI TS 102 023, the chapters have been extended to include additional information of relevance for TSABDE time-stamp subscribers and relying parties. Likewise, a new chapter devoted to Personal Data Protection has been added to comply with Spanish legislation on this issue.

This document assumes that the reader is aware of the concepts of PKI, certificate, electronic signature, TSA, time-stamping services and time stamp.

1.2 Document Name and Identification

Document name	Banco de España Time-Stamping Authority Policies and Practices (TSABDE)
Document version	1.2
Document status	Approved
Date of issue	18.12.2017
Expiry date	Not applicable
OID (Object Identifier)	1.3.6.1.4.1.19484.2.4.1
Document location	http://pki.bde.es/politicas
Related CPS	Certification Practice Statement of the Banco de España's PKI OID 1.3.6.1.4.1.19484.2.2.1

1.3 Participant entities and persons

The entities and persons taking part in this document are:

- Banco de España, as owner of TSABDE.
- The Policy Management Authority.
- The CSP issuer of the TSABDE certificate.
- Subscribers of time stamps issued by TSABDE
- Relying parties of time stamps issued by TSABDE

1.3.1 Policy Management Authority

The Policies Management Authority (PAA) is the organisation set up within Banco de España responsible for approving the Time-Stamp Policies and Practices, as well as approving any modifications to the aforementioned documents.

In particular, the TSABDE PAA is the same organisation as the PKIBDE PAA, its role and function being defined in the PKIBDE Certification Practices Statement.

The PAA is responsible for analysing the full or partial audit reports drawn up on TSABDE and, when necessary, for establishing the corrective actions to be taken.

1.3.2 The CSP issuer of the TSABDE certificate

The CSP issuer of the TSABDE certificate is the PKI of Banco de España, PKIBDE.

1.3.3 Subscribers

Subscribers are defined and described in chapter 3.

1.3.4 Relying Parties

Relying parties are defined and described in chapter 3.

1.3.5 Other affected parties

TSABDE Administrators: People within Banco de España that have Banco de España TSA administration and configuration privileges.

1.4 Management of policies and practices

1.4.1 Banco de España, as owner of TSABDE.

This TSP and TSPS belongs to Banco de España:

Name	Banco de España		
E-mail address	pkibde@bde.es		
Address	C/Alcalá, 48. 28014 - Madrid (Spain)		
Telephone No.	+34913385000	**Fax**	+34915310059

1.4.2 Contact Person

This TSP and TSPS is administered by the Banco de España PKI Policy Management Authority (PAA), belonging to the Information Systems Department:

Name	Information Systems Department Banco de España PKI Policy Administration Authority		
E-mail address	pkibde@bde.es		
Address	C/Alcalá, 522. 28027 - Madrid (Spain)		
Telephone No.	+34913386666	**Fax**	+34913386870

1.4.3 Approval procedures for this TSP and TSPS

The Banco de España Executive Commission is responsible for approving these Time-Stamp Policies and Practices, although it has authorised the PKIBDE Policy Administration Authority, belonging to the Information Systems Department to perform and publish the necessary updates of said documents, issuing periodic reports on this matter.

1.5 References

The following documents have contents relevant for the implementation and/or application of these Time-Stamp Policies and Practices:

- 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

Likewise, the following basic legislation, applicable in this area, has been considered:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the international market and repealing Directive 1999/93/EC.
- Spanish Law 59/2003, of 19 December, the Electronic Signature Act (Spanish Official Gazette, 20 December).
- Spanish Organic Law 15/1999, of 13 December 1999, the Personal Data Protection Act (Official State Gazette, 15 December).
- Royal Decree 1720/2007, of 21 December, which passes the Regulations for implementing Organic Law 15/1999, of 13 December, the Personal data Protection Act
- Royal Legislative Decree 1/1996, of 12 April, approving the Revised Intellectual Property Act (Official State Gazette, 22 April).
- Banco de España Circular 2/2005, of 25 February, on automated electronic files containing personal data managed by Banco de España (Official State Gazette, 22 March).

1.6 Definitions and Acronyms

1.6.1 Definitions

Within the scope of these Time-Stamp Policies and Practices, the following definitions will be used:

Authentication: procedure for verifying the identity of a TSABDE time-stamping services subscriber.

Time-Stamping Authority (TSA): a reliable authority that issues time stamps.

Electronic Certificate: a document signed electronically by a certification services provider, which links signature verification data to a signatory and confirms their identity. This is the definition contained in Law 59/2003, which this document extends to cases in which the signature verification data is linked to a computer component.

Public Key and Private Key: the asymmetric cryptography on which the PKI is based employs a key pair in which what is enciphered with one of these can only be deciphered by the other, and vice versa. One of these keys is "public" and includes the electronic certificate, whilst the other is

"private" and is only known by the certificate subscriber and, when appropriate, by the Keys Archive.

Session Key: key established to encipher communication between two entities. The key is established specifically for each communication, or session, and its utility expires upon termination of the session.

Time-Stamping Practices Statement (TSPS): a statement of the practices the Time-Stamping Authority uses for issuing time-stamp tokens.

Time-Stamping Policy (TSP): a set of rules which establish the applicability of the time-stamp token and its issue features.

Provider of Certification Services: individual or entity that issues electronic certificates or provides other services related to the electronic signature.

Time-stamp token (TST): a data structure tying certain data to a particular instant in time, providing evidence of their existence prior to that instant.

Subscriber: a person or entity subscribing or having subscribed an agreement to use the time-stamping services provided by TSABDE, and that accepts its terms and conditions.

Relying Parties: a person or entity that decides to trust the TSABDE time-stamping services, and in particular that is the receiver and accepts and relies on a time-stamp token issued by TASBDE.

Coordinated Universal Time (UTC): a time scale based on the second, defined by the International Telecommunications Union Radio Committee (ITU-T) TF.460-5 and which coincides approximately with Greenwich Mean Time (GMT).

Time-Stamp Unit (TSU): set of hardware and software that is managed as a unit and which has unique private active signature key at each moment in time. A TSA may have and maintain several TSUs simultaneously, each one operating with a private key and different certificate.

UTC(k): a time scale generated by the "k" laboratory as defined in the T Circular of the *Bureau International des Poids et Mesures* (BPIM) and which is maintained in keeping with the UTC.

The Banco de España Certification Practices Statement (CPS) also contains the following additional definitions.

1.6.2 Acronyms

PAA: Policy Management Authority

CA: Certification Authority

CRL: Certificate Revocation List

C: (Country). Distinguished Name (DN) attribute of an object within the X.500 directory structure

CN: Common Name Distinguished Name (DN) attribute of an object within the X.500 directory structure

CPS: Certification Practice Statement

TSPS: Time-Stamping Practices Statement

ETSI: European Telecommunications Standard Institute

FIPS: Federal Information Processing Standard

GMT: Greenwich Mean Time

HSM: Hardware Security Module: Cryptographic security module used to store keys and carry out secure cryptographic operations

IETF: Internet Engineering Task Force (internet standardisation organisation)

O: Organisation. Distinguished Name (DN) attribute of an object within the X.500 directory structure

OCSP: Online Certificate Status Protocol: This protocol enables online verification of the validity of an electronic certificate.

OID: Object Identifier

OU: Organisational Unit. Distinguished Name (DN) attribute of an object within the X.500 directory structure.

CP: Certificate Policy

PKI: Public Key Infrastructure

PKIBDE: The Banco de España PKI

PCS: Certification Services Provider

TSP: Time-Stamping Policy

RFC: Request For Comments (Standard issued by the IETF)

TSA Time-stamping Authority

TSABDE: The Banco de España TSA

TST: Time-Stamp Token

TSU: Time-Stamping Unit

UTC: Coordinated Universal Time

2 Scope

This document defines the requirements and policies, together with the operating and management practices of the Banco de España Time-Stamping Authority (TSABDE).

This document may therefore be consulted by the subscribers of its services and parties relying of time-stamp tokens, in order to enhance their confidence in the time-stamping services provided by TSABDE.

Likewise, it may also be used by third entities and independent bodies to verify and certify that TSABDE complies with the policies and practices described herein, whereby it may be considered a reliable TSA.

Alternatively, given that TSABDE shares technological infrastructures, procedures, processes, security controls, persons in charge and organisation with the PKI of Banco de España (PKIBDE), in what is applicable, this reference document details and completes the provisions of the PKIBDE "Certification Practices Statement" (CPS).

TSABDE employs public key cryptography, X509 certificates and reliable time sources to provide reliable time-stamp tokens compliant with the applicable standards. .

Lastly, this document neither defines nor specifies the mechanisms or protocols for validating the time-stamp tokens issued.

3 General concepts

3.1 Time-Stamping Services

The time-stamping services provided by TSABDE are structured into two parts:

- Time-stamp token generation and issue: this comprises the technical and organisational components that issue time-stamp tokens (TSTs)
- Time-stamp token management service: the technical and organisational components that supervise and control that the operations for issuing time-stamp tokens are performed properly, including their time synchronisation with a reliable UTC reference source.

Time-stamping services are provided as per the applicable legislation and standards, described in section *1.5 References* of this document.

3.2 Time-stamping Authority of Banco de España (TSABDE)

The Time-Stamping Authority of Banco de España (TSABDE) is responsible for correctly rendering the services described in section 3.1 in accordance with the Policies and Practices set forth in this document, to generate confidence among its users (subscribers and relying parties).

TSABDE is charged with operating one or several Time-Stamping Units (TSUs) which will create and sign the time-stamp tokens (TST) on behalf of the TSABDE.

Each TSU must have its own private key, which must be associated to a unique electronic certificate issued by PKIBDE. In any event, TSABDE is identified by the electronic signature certificate which each TSU uses to generate and issue time-stamp tokens.

Generally speaking, TSABDE operates within the sphere of Banco de España services, applications and systems or those of others related to them and only issues time-stamp token to end users in said scenarios.

3.3 Subscribers

Subscribers are persons or entities that use the time-stamping services provided by TSABDE and that therefore accept its terms and conditions.

Subscribers are responsible for the use they make of TSABDE services, and must inform relying parties about the correct use of time-stamp tokens and their conditions.

3.4 Relying Parties

Relying parties are persons or entities that decide to trust TSABDE's time-stamping services, and they are, in particular, receivers who accept and trust the time-stamp tokens issued by TSABDE

3.5 TSA Policy and Practices

3.5.1 Objective

The Time-Stamp Policy described in this document aims to define the requirements TSABDE should fulfil to render a reliable time-stamping service, in keeping with the standards indicated in section 1.5, and particularly with ETSI TS 102 023, *Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-stamping Authorities.*

The Time-Stamping Policy sets forth what conditions TSABDE fulfils, whereas the Practices Statement indicates how it fulfils them.

The policy and practices applicable to TSABDE are detailed in sections 4 and 5 of this document, respectively. All the TSABDE policy and practice documents are approved by the PKIBDE Policy Administration Authority.

3.5.2 Specificity level

The Time-Stamping Policy is less specific than the Practices, given that the Practices Statement specifies how TSABDE fulfils the technical, organisational and procedural requirements set forth in the policy.

3.5.3 Approach

This document sets forth the general TSABDE operating rules but it does not include the technical specifications of its infrastructure and communications, organisation structure, operating procedures or security controls and measures. In particular, it does not define the environment in which TSABDE TSUs are working.

The technical and operating details are described in the PKIBDE“Certification Practices Statement” (CPS) and in other internal documents.

4 Time-Stamping Policy

4.1 Overview

This policy defines the set of rules and procedures for reliably generating and issuing time-stamp tokens in compliance with the ETSI TS 102 023 technical standard. The private keys and time-stamp units (TSUs) comply with ETSI TS 101 861 *Time-stamping Profile* and RFC 3161 *Time-stamp Protocol (TSP)* technical specifications.

TSABDE uses specific private keys in each TSU for signing time-stamp tokens, which contain an identification of the applicable time-stamping policy.

Time-stamp tokens (TSTs) are issued with an accuracy of ±1 seconds of UTC.

4.2 Identification

The OID (object identifier) of the Time-Stamping Policy is:

1.3.6.1.4.1.19484.2.4.1

This OID is included as the policy identifier on each time-stamp token TSABDE issues.

4.3 User community and applicability

4.3.1 User community

The user community of time-stamp tokens issued by TSABDE comprises solely its subscribers and their relying parties. All subscribers are automatically considered as relying parties.

All end users of Banco de España services, applications and systems or those related to them are potential subscribers. TSABDE does not provide time-stamping services to the general public outside the scope of its applications and systems.

When subscribers or relying parties request and/or accept time-stamp tokens issued by TSABDE, this automatically implies acceptance of the terms and conditions set forth in these Time-Stamp Policies and Practices.

4.3.2 Time-stamp token applicability

TSABDE establishes no specific restrictions for use of the time-stamp tokens it issues, although it should be understood that the time-stamping services offered by TSABDE have neither been designed nor authorised to be used in high-risk activities or where failproof activity is required, such as those involved in hospital, nuclear, air-traffic control or railway facilities or any other where a failure could involve death, personal injury or serious harm to the environment.

In particular, time-stamp tokens issued in keeping with this policy may be for:

- Enhancing an electronic signature[1], awarding it certainty of the time of issue
- Protecting long-lasting electronic signatures[1]

[1] The aim of time-stamp tokens issued under the Time-Stamp Policies and Practices described in this document is to enhance any electronic signature, irrespective of the legal nature of the same (simple, advanced or recognised signature), in accordance with Law 59/2003, the Electronic Signature Act.

- Providing evidence and reliable proof that certain data existed before a specific moment in time
- Determining the moment at which a transaction was undertaken
- Use in documentation and data archiving systems
- Register and log systems

Time-stamp tokens issued by TSABDE are only valid for use in Banco de España services, applications and systems. Or those related to them.

4.3.3 Constraints and Restrictions in Time-stamp token usage

Any other use not included in the previous point shall be excluded.

4.4 Conformity and audits

TSABDE will include this policy's OID (described in section 4.2) in all the time-stamp tokens it issues to indicate they conform with it.

Likewise, TSABDE will only accept time-stamp token generation requests which include the OID for this policy, or which do not explicitly include any other policy.

The PAA is responsible for assuring that time-stamping services rendered comply with the stipulations included in these Time-Stamping Policies and Practices and for assuring the reliability of the controls and requirements described in this document. To this end, Banco de España will periodically audit TSABDE functioning in accordance with the Audit Plan and guidelines set forth in the PKIBDE CPS.

4.5 Repositories and Publication of Information

4.5.1 Repositories

The TSABDE repository comprises a free-access web service which shall contain the following information:

For the TSABDE signature certificate:
- WEB: http://pki.bde.es/certs

For TSABDE certification chain certificates:
- WEB: http://pki.bde.es/certs

For the **CPS, TSP and TSPS:**

The Time-Stamping Policies and Practices described in this document and the PKIBDE CPS are available for public access at http://pki.bde.es/politicas.

In particular, this page gives access to the following document (X.Y indicates the version):
- PKIBdE_DPC-vX.Y.pdf
- PKIBdE_PST_y_DPST-vX.Y.pdf

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

For notification of relevant facts (e.g.: TSA commitment)

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

4.5.2 Publication Timescale or Frequency

The TSP and the TSPS are published as they are created and again when any modification to them is approved. Modifications are made public on the website referred to in the previous section.

4.5.3 Repository Access Controls

Reading access to the TSP and TSPS is open. However, only TSABDE is authorised to modify, substitute or eliminate information from its repository or website. For this purpose, TSABDE will establish controls that prevent unauthorised individuals from tampering with the information contained in the repositories.

5 BDE TSA Practices

TSABDE has the necessary controls in place to guarantee that time-stamping services are rendered as per the guidelines and requirements set forth in this policies and practices document.

5.1 Practices Statement and Basic Statement

5.1.1 BDE TSA Practices Statement

The procedures, control mechanisms and technical infrastructures described in this chapter are the basis for TSABDE operation. Given that TSABDE shares technological infrastructures, procedures, processes, security controls, supervisors and organisation with the PKI of Banco de España (PKIBDE), the PKIBDE "Certification Practices Statement" (CPS) contains other applicable controls.

In particular, this Time-Stamping Policies and Practices document, together with the PKIBDE CPS regulate the operation and requirements of the TSABDE time-stamping service.

These documents, together with any other relevant information, are available to the public in the repositories described in section 4.5, and under the intellectual property considerations detailed in section 6.4.

The Policy Administration Authority is responsible for maintaining and approving all the policies and practices governing TSABDE functioning.

Likewise, the PAA is responsible for assuring that the policies and practices are correctly implemented and function properly. To this end, TSABDE performs periodic assessments and audits to determine the state of security controls and procedures and carry out the relevant changes, as per the mechanisms and procedures described in the PKIBDE CPS.

Lastly, the TSABDE vulnerabilities analysis is covered under the Banco de España Audit Plan, as indicated in the PKIBDE CPS.

5.1.2 BDE TSA Basic Statement

The TSA Basic Statement describes the fundamental aspects and conditions for use of the time-stamping services, and corresponds with the "TSA Disclosure Statement" defined in standard ETSI TS 102 023. In this case, in order to avoid unnecessary separation of documents, the contents of the aforementioned are included in this document, which therefore acts as the Basic Statement.

The fundamental aspects of the Basic Statement are as follows:

- TSABDE is a service of Banco de España, the contact details of which are included at the beginning of this document in section 1.4
- The availability of the service rendered by TSABDE is described in section 5.3.1 of this document.
- Each time-stamp token issued by TSABDE contains the policy identifier (OID) included in section 4.2 of this document.
- The cryptographic algorithms and the length of the keys admitted and used by TSABDE are compliant with *ETSI TS 101 861 Time-stamping Profile* and are:
    - The following algorithms are admitted for time-stamp token requests:
        Hash: SHA-512, SHA-384, SHA-256, SHA-224, SHA-1, MD5, RIPEMD-160
    - For time-stamp tokens issued:
        Hash: SHA-1
        Signature: sha1WithRSAEncryption, key length at least 2048 bits.
- TSABDE does not set confidence or validity constraints on its time-stamping services beyond those described in section 4 of this document. If it is detected that the cryptographic algorithms used or the key lengths have ceased to be secure, TSABDE will publish this information on its website.
- TSABDE assures the accuracy indicated in the Time-Stamping Policy section 4.1, with respect to reliable UTC time sources defined in section 5.3.4, and guarantees that it will not issue time-stamp tokens with lesser accuracy.
- Generally, TSABDE establishes no specific restrictions for use of the time-stamp tokens it issues, although it should be understood that the time-stamping services offered by TSABDE have neither been designed nor authorised to be used in high-risk activities or where failproof activity is required, such as those involved in hospital, nuclear, air-traffic control or railway facilities or any other where a failure could involve death, personal injury or serious harm to the environment.
- The applicability of the time-stamp tokens issued by TSABDE is described in section 4.3.2 of this document.
- Time-stamp tokens issued by TSABDE are only valid for use in Banco de España services, applications and systems or those related to them.
- The obligations incumbent on subscribers are described in section 6.5.3 of this document.
- The obligations incumbent on relying parties are described in section 6.5.4 of this document.
- TSABDE securely maintains the records corresponding to its operations, in keeping with section 5.5.11 of this document.
- TSABDE operations and functioning, as well as this Time-Stamping Policies and Practices Statement shall be subject to Spanish and European legislation and the specific regulations of Banco de España applicable to them, described in section 5.5.10 of this document.
- TSABDE liabilities and limitations on liabilities are described in section 6.6 of this document.
- All claims between users or third parties and TSABDE shall be notified as per the provisions of section 6.11 of this document. In the event that agreement cannot be reached between the

parties, resolution of any dispute that may arise shall be submitted to the courts and tribunals specified in section.6.11, the parties waiving any other jurisdiction to which they may have a right.

- TSABDE guarantees that the time-stamping services are rendered compliant to the stipulations included in these Time-Stamping Policies and Practices. To this end, Banco de España will periodically audit TSABDE functioning in accordance with the Audit Plan and guidelines set forth in the PKIBDE CPS.
- TSABDE provides its time-stamp tokens to its user community free of charge.

5.2 Key life-cycle management

5.2.1 TSA key generation

The cryptographic keys of the TSUs used in TSABDE services are generated in hardware cryptographic modules (HSM) which are certified with a minimum security level of FIPS 140-2 level 3, EAL4, or similar. These HSM devices are permanently located in a secure physical environment, common to the other PKIBDE infrastructures and systems, as is described in the CPS.

Likewise, these keys are generated under multi-person control[1] with the participation of at least two supervisors from the TSABDE.

The cryptographic algorithm used to generate the signature key is RSA, using a key length of at least 2048 bits. sha256WithRSAEncryption is used to sign Time-stamping Authority certificates. If it is detected that these algorithms or the key lengths have ceased to be secure, TSABDE will replace them with other new ones that are considered secure and it will publish said information on its website.

5.2.2 Protection of the TSU private key

TSABDE takes the necessary measures to assure that TSU private keys are confidential and that their integrity is maintained.

Amongst other measures this includes the use of HSM modules certified to FIPS 140-2 level 3, EAL4 or similar, for generating, storing and safekeeping keys and the generation of time-stamp token signatures. Only TSABDE will have access to the private keys used, which shall furthermore be enciphered for storage.

The private key of the certificates used by TSABDE shall not be stored outside the HSM modules.

Nevertheless, Banco de España has a back-up copy of these HSMs, which are made by Banco de España staff appointed for this purpose, following the guidelines laid down in the PKIBDE CPS. In the event of a disaster, these back-up copies will be retrieved under multi-person control, involving at least two TSABDE supervisors.

The persons performing these tasks are duly qualified to do so and the staff controls applicable are those described in the PKIBDE CPS.

5.2.3 Distribution of the TSU public key

The public key of each TSU is included in its corresponding certificate.

The electronic certificates used at TSABDE will be issued by PKIBDE.

---

[1] Multi-person control: control by more than one person, normally a subgroup 'k' of a total of 'n' people. This guarantees that no one has individual control of the critical activities and, at the same time, it facilitates availability of the necessary people.

The certificate for each TSU, together with its certification chain, will be published in the TSABDE repositories described in section 4.5 of this document.

The profile of the certificate issued for TSABDE complies with standard X509 v3 and RFC 3161, and is described in detail in section 5.4 of this document.

5.2.4 Renewal of TSU keys

TSABDE will renew the signature keys used by its TSUs sufficiently in advance of their expiry.

Likewise, TSU signature keys will also be renewed before conclusion of their validity period, provided that they are considered potentially compromised by TSABDE supervisors, either because the cryptographic algorithm or the key length are considered vulnerable, or for any other reason.

In either case, key renewal will be considered as a new generation of keys, as set forth in section 5.2.1 of this document.

5.2.5 End of the TSU key life cycle

TSU signature keys will be replaced sufficiently in advance of their expiry, as set forth in section 5.2.4 of this document.

The TSUs will reject any attempt to generate time-stamp tokens with a signature key once it has expired.

TSABDE keeps an archive of all its certificates and public keys in the repositories described in section 4.5 of this document. The archiving term will follow the provisions set forth in the PKIBDE CPS for archiving public keys, in order to be able to validate time-stamp tokens issued in the past. The PKIBDE and TSABDE managers are responsible for the control of said register.

The archive has the appropriate means to protect the information it contains against tampering.

5.2.6 Life cycle management of the cryptographic module (HSM) used to generate time-stamp tokens

The life cycles of the HSM modules used are managed as per the guidelines and controls set forth in PKIBDE CPS.

In particular, TSABDE uses commercially available hardware and software cryptographic modules developed by third parties. TSABDE only uses cryptographic modules certified to FIPS 140-2 Level 3, EAL4 or similar standards.

These HSM devices are permanently located in a secure physical environment, common to the other PKIBDE infrastructures and systems, as is described in the CPS.

Prior to their installation, it is verified that they have not been tampered with or modified during transport or delivery and that they work correctly.

Likewise, these HSMs are configured so that their initiation, restoration and administration are performed under multi-person control, with at least two PKIBDE supervisors. Their private keys are activated and deactivated as per the provisions of the PKIBDE CPS. The persons performing these tasks are duly qualified to do so and the staff controls applicable are those described in the CPS.

In the event of a breakdown or disaster, replacement of these HSM modules shall be considered a new installation and all the requirements described in this section shall be applicable.

5.3 Time-stamping

5.3.1 Access to the service

Time-stamp tokens may be requested using the TSP protocol (Time-Stamp Protocol) as per standard RFC 3161.

The address for accessing the service is: http://pkitsa.bde.es, accessible only through the internal Banco de España network.

5.3.2 Service availability

The time-stamping services offered by TSABDE are available continuously, every day of the year.

5.3.3 Time-stamp token

TSABDE takes the necessary technical measures to assure that time-stamp tokens are issued securely and include the correct date/time.

The time-stamp tokens generated are compliant with the standards referred to in section 1.5 of this document and they follow the structure defined in *RFC 3161 Time-stamp Protocol (TSP)*. In particular, each time-stamp token includes at least:

- The identifier of the time-stamp policy, specified in section 4.2
- The representation (hash) of the data set for which the time-stamp token is being provided.
- A unique serial number which can be used to identify the time-stamp token.
- The time expressed in “Zulu” format ("Zulu" time). The clock is synchronised with the secure time sources described in section 5.3.4, and to the accuracy declared in 4.1.
- The electronic signature generated by the TSU, using the private key only for time-stamping.
- The TSU electronic certificate used to sign the stamp, which will serve as identification for said TSU and the TSABDE itself. This certificate will be structured as described in section 5.4 of this document.

TSABDE keeps audit records of all the calibrations with respect to the secure time source and will not issue time-stamp tokens if the accuracy were not within the stipulated tolerances.

5.3.4 Synchronisation of the clock with UTC

TSABDE provides the time instant with the accuracy declared in the Time-Stamping Policy in section 4.1, with respect to a secure source which establishes date and time. More specifically, the clock signal comes from one of these sources:

- The atomic clock in Braunschweig, Germany, (Physikalisch Technische Bundesanstalt), which gives the official time within the Eurosystem. It is encoded and transmitted by radio.
- From the Spanish Royal Navy Institute and Observatory (ROA), which is responsible for maintaining the basic Time Unit, declared for legal purposes as the National Standard for said unit, as well as maintaining and officially disseminating "Coordinated Universal Time" (UTC (ROA)), considered for all effects and purposes to be the basis of legal time throughout national territory. (R. D. 23 October 1992, no. 1308/1992).

TSUs have the necessary technical measures in place to avoid their clocks deviating from their stated accuracy. Furthermore, these clocks are protected and are periodically and automatically recalibrated against the secure time source. They are likewise capable of detecting deviations from the established accuracy and of activating a new calibration.

Alternatively, TSUs are permanently located in a secure physical environment, common to the other PKIBDE infrastructures and systems, as is described in the CPS. Likewise, remote access to the same is protected against unauthorised access.

Lastly, all the events occurring regarding synchronisation and modification of the time of each TSU are recorded, in order to detect and trace deviations with respect to the clock and the stated accuracy, be they accidental or intentional.

5.4 Profile of the TSU certificate signature

5.4.1 Version number

The certificates used by TSABDE use version 3 of the X.509 standard (X.509 v3)

5.4.2 Certificate issuer

The electronic certificates used at TSABDE are issued by PKIBDE.

5.4.3 Name formats and restrictions

The names contained in the certificates are restricted to X.500 distinguished names, which are unique and unambiguous.

The certificates contain the X.500 *Distinguished Name* of the issuer in the *issuer name* field.

The *subject name* field contains the X.500 *Distinguished Name* identifying TSABDE, whose common name will be the following value:

CN=BANCO DE ESPAÑA – TSA *FREE_TEXT*

Where *FREE_TEXT* is a free text that differentiates different certificates generated by one same Time-Stamping Authority that has a number of TSUs.

The rest of the DN attributes shall have the following fixed values:

O=BANCO DE ESPAÑA, C=ES

5.4.4 Certificate profile and extensions

The extensions used are:

- *Subject Key Identifier* Classified as non-critical.
- *Authority Key Identifier* Classified as non-critical.
- *KeyUsage*. Classified as critical.
- *extKeyUsage* Classified as critical.
- *CertificatePolicies*. Classified as non-critical.
- *SubjectAlternativeName*. Classified as non-critical.
- *BasicConstraints*. Classified as critical.
- *CRLDistributionPoint*. Classified as non-critical.
- *Auth. Information Access*. Classified as non-critical.
- *bdeCertType (1.3.6.1.4.1.19484.2.3.6)*. Classified as non-critical.
- *bdeIssuerName* (*1.3.6.1.4.1.19484.2.3.17*). Classified as non-critical.
- *bdeIssuerVAT (1.3.6.1.4.1.19484.2.3.18)*. Classified as non-critical.

The table below shows the profile of TSABDE certificates.

Profile of the PKI TSA certificate

FIELD	CONTENT	CRITICAL extensions
Field X509v1		
1. Version	V3	
2. Serial Number	Random	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA– AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Lifetime	1 year	
6. Subject	CN=BANCO DE ESPAÑA - TSA *FREE_TEXT*[1] O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algorithm: RSA Encryption Key length: 2048 (bit string)	
1. Subject Key Identifier	Resulting from use of the hash SHA-1 function on the TSA public key.	NO
2. Authority Key Identifier		NO
keyIdentifier	Result of using the hash SHA-1 function on the public key of the issuing CA	
3. KeyUsage		YES
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	YES
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1 (CPS)	
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] Free text that differentiates different certificates generated by one same Time-Stamping Authority that has a number of TSUs.

6. Subject Alternate Names	URL Address=http://pkitsa.bde.es	
7. Basic Constraints		YES
Subject Type	End Entity	
Path Length Constraint	Not used	
8. CRLDistributionPoints	(1) Active Directory: 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] (1.3.6.1.4.1.19484.2.3.18)	VATES-Q2802472G	NO

5.5 TSA management and operation

Given that TSABDE shares technological infrastructures, procedures, processes, security controls, supervisors and organisation with the PKI of Banco de España (PKIBDE), in the following sections the provisions of the PKIBDE "Certification Practices Statement" (CPS) will apply.

In those cases in which it is deemed necessary, a description of the corresponding sections of the CPS will be given in which they are laid out in detail.

5.5.1 Security management

TSABDE guarantees that appropriate security levels are in place in its operations in keeping with best practices and applicable standards.

In particular, the aspects concerning security management are shared with PKIBDE and these are described in chapters *5 Physical security controls, installations, management and operating controls*, and *6 Technical security controls in the* PKIBDE CPS.

5.5.2 Asset management and classification

In order to guarantee a suitable level of security in its business processes, Banco de España as the body in charge of the TSABDE keeps an inventory of its information assets and it applies the corresponding security level in each case.

[1] Certificates issued before June 22th 2018 contain the former Banco de España VAT identification number: V28000024.

5.5.3 Security relating to staff

TSABDE applies appropriate practices in the recruitment, hiring, management and termination of its employment relationships with staff.

In particular, aspects relating to staff management are shared with PKIBDE and they are described in sections *5.2 Procedure controls*, and *5.3* PKIBDE CPS staff controls.

5.5.4 Physical and workplace security

TSABDE is located and operates in a secure environment, common to the rest of the PKIBDE infrastructures and systems, as described in the CPS, section *5.1 Physical controls*.

5.5.5 Operations management

TSABDE applies operating controls as per ETSI TS 102 023 and internal policies in place in Banco de España.

5.5.6 Systems access management

TSABDE is located and operates in a secure environment, common to the rest of the PKIBDE infrastructures and systems, whereby it maintains controls on physical and logical access to the installations, hardware, systems and information. These controls are described in chapters *5 Physical security controls, installations, management and operating controls*, and *6 Technical security controls of* the PKIBDE CPS.

5.5.7 Deployment and reliable maintenance of systems

The certificates used for the time-stamping service are generated and managed in a secure environment as per the stipulations in section 5.2 of this document.

Likewise, TSABDE shares the security controls during the systems' life cycle with PKIBDE, as is described in section *6.6 Life cycle security controls* in the PKIBDE CPS. Hence, control procedures are applied to changes to maintain the degree of systems reliability.

5.5.8 TSA service commitment

The way TSABDE manages possible incidents is described in section *5.7 Recovery in the event of a key being compromised or a catastrophe* in the PKIBDE CPS.

TSABDE will not issue time-stamp tokens until corrective actions have been applied and the incident has been resolved. The following incidents are, in particular, identified:

- Compromising of the TSU private key, in which case TSBDE will immediately request the certificate be revoked. The TSU will not issue time-stamp tokens whilst it does not have a valid private key.
- The TSU will not issue time-stamp tokens if its clock is outside the accuracy tolerances with respect to UTC until the time calibration has been restored. In keeping with the provisions of section 5.5.11 of this document, TSABDE keeps audit records, including information about clock synchronisation.
- Other disasters caused by force majeure.

In the event of security being compromised or this being suspected, or the internal clock were to come out of synchronisation, TSABDE will notify its subscribers and relying parties about the incident through the repositories defined in section 4.5 of this document. The information published shall include details which serve to define the time-stamp tokens that have been affected.

5.5.9 Termination of the TSA

If it ceases to provide time-stamping services, TSABDE will ensure that the potential problems to subscribers and relying parties be kept to a minimum and it will maintain the records necessary to provide certain proof of provision of time-stamping services for legal purposes.

In the event of TSABDE terminating or ceasing its activities, it shall notify its subscribers at least two months in advance of said event.

If TSABDE were to decide to transfer the activity to another time-stamping authority, it shall notify its subscribers of the terms of said transfer. For this purpose, TSABDE shall publish a document explaining the transfer terms and conditions and the characteristics of the TSA to which it proposes to transfer the time-stamping service.

TSABDE shall notify its termination of activity and other relevant details by publishing them on its website in the repositories defined in section 4.5 of this document.

In the event of it concluding or ceasing activity, TSABDE shall apply for the TSU certificates to be revoked.

5.5.10 Compliance with legal requirements

TSABDE complies with all legal requirements, both those relating to its time-stamping certification services and to personal data protection (see section 7 of this document). The main regulations applicable are:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the international market and repealing Directive 1999/93/EC.
- European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Spanish Law 59/2003, of 19 December, the Electronic Signature Act.
- Spanish Organic Law 15/1999, of 13 December 1999, the Personal Data Protection Act.
- Royal Decree 1720/2007, of 21 December, which passes the Regulations for implementing Organic Law 15/1999, of 13 December, the Personal Data Protection Act.
- Banco de España Circular 2/2005, of 25 February, on automated electronic files containing personal data managed by Banco de España (Official State Gazette, 22 March).

5.5.11 Register of information concerning the operation of time-stamping services

TSABDE keeps a record of the information on its operations for a period of 15 years. The records are protected to ensure their integrity and confidentiality.

The records are available to subscribers, in what refers to them, and to the authorities so requiring, in compliance with the law.

Amongst others, TSABDE keeps records which include the precise moment in time of:

- Time-stamp token requests and time-stamp tokens issued.
- Events related to TSU administration (certificate management, key management and clock synchronisation).

As regards management procedures, controls and audits on TSABDE records, these are governed by sections *5.4 Security audit procedures* and *5.5 Record archiving* PKIBDE CPS.

5.6 Organisation

TSABDE belongs to Banco de España.

Through the PAA, Banco de España undertakes to engage in the necessary security measures to comply with the standards and laws applicable to time-stamping service, as well as with the policies and practices covered in this document for rendering time-stamping services.

The documents regulating its activity are in the repositories described in section 4.5 of this document.

6 Other Legal and Business Matters

6.1 Fees

6.1.1 Fees for issuing time-stamp tokens

No fees are applied for the issue of time-stamp tokens under this Time-Stamping Policy.

6.1.2 Certificate access fees

Access to certificates used by the TSABDE under this Policy is free of charge and, therefore, no fee is applicable.

6.1.3 Fees for other services, such as policy information

No fee shall be applied for information services on this policy, nor on any additional service that is known at the time of drawing up this document.

6.1.4 Refund policy

Given that there are no fees for this Time-Stamping Policy, no refund policy is required.

6.2 Information Confidentiality

6.2.1 Scope of confidential information

All information not considered by TSABDE as public shall be of a confidential nature. The nature of confidential information is expressly given to:

- The private keys of the TSUs that make up TSABDE.
- The information on operations carried out by TSABDE, including the time-stamp tokens issued.
- The information referring to security, control and audit procedure parameters.
- The information of a personal nature provided by TSABDE subscribers, as per the provisions of the regulations on personal data protection and its implementation rules.

6.2.2 Non-confidential information

The following information is considered public information and, therefore, available to third parties:

- The contents of these Time-Stamping Policies and Practices
- That included in the Certification Practices Statement (CPS) and the PKIBDE Certification Policies.

6.2.3 Duty to maintain professional secrecy

In this respect, the provisions of section *9.2.3 Duty to maintain professional secrecy* in the PKIBDE CPS is applicable.

6.3 Personal Data Protection

In keeping with Spanish legislation on this matter, included in chapter 7 of this document.

6.4 Intellectual Property Rights

In this respect, the provisions of section *9.4 Intellectual property rights* in the PKIBDE CPS.

6.5 Obligations

6.5.1 General obligations incumbent on TSABDE

Banco de España operates TSABDE and assumes responsibility for assuring that the time-stamping services rendered comply with these policies and practices and for fulfilment of the requirements and controls established in section 5 of this document, together with the applicable legal regulations.

It should be noted that the obligations and responsibilities set forth in the PKIBDE CPS are also applicable.

6.5.2 TSABDE obligations towards its subscribers

TSABDE assumes the following obligations towards its subscribers:

1 To operate in accordance with these Time-Stamping Policies and Practices and the PKIBDE Certification Practices Statement

2 To operate based on reliable systems, technologies, soft- and hardware and with suitable staff.

3 To guarantee that the time-stamp tokens issued contain no erroneous or false data.

4 To assure that TSUs keep their clock synchronised and at the stated accuracy with respect to the UTC.

5 To perform internal and external reviews to assure compliance with applicable legislation and internal policies and procedures.

6 To provide uninterrupted access to time-stamping services except in the case of scheduled downtime, loss of time synchronisation and force majeure.

7 In the event of security being compromised or there being a suspicion of this, or the internal clock coming out of synchronisation, to post details of the incident. The information published shall include details which serve to define the time-stamp tokens that have been affected.

8 Any other obligation set forth for PKIBDE in section 9.5 Obligations in the CPS and which were applicable to TSABDE.

6.5.3 Obligations incumbent on subscribers

Subscribers of TSABDE time-stamping services are obliged to:

1 Use suitable software for requesting and obtaining time-stamp tokens.

2 Verify that the time-stamp token has been correctly signed.

3 Verify by CRL query or OCSP protocol that the private key used to generate the time-stamp token has not been compromised.

4 Be aware of and accept the conditions and constraints on the use of time-stamp tokens set forth in this Policy.

5 Limit and use the time-stamp tokens as permitted under this Policy.

6 Not monitor, tamper with or carry out any reverse engineering on the technical implementation (hardware and software) of the time-stamping services.

7 Any other that is applicable by law, under applicable regulations, under the Time-Stamping Policy or the PKIBDE CPS.

6.5.4 Obligations incumbent on relying parties

Third parties that accept and rely on time-stamp tokens issued by TSABDE are obliged to:

1 Verify that the time-stamp token has been correctly signed and that the private key used for signing it was not compromised at the time of verification. During the period that the TSU is valid, relying parties may check the status of the private key by consulting the CRL or by online consultation using OCSP protocol. Once the TSU certificate expires, relying parties may trust the time-stamp token by requesting a new one or directly if, at the time of verification, it is known that:

a The TSU private key has not been compromised at any time, and

b The hash cryptographic function used in the time-stamp token is still considered secure, and

c The cryptographic algorithm and the size of the key used for the electronic signature are still considered secure.

2 Limit reliability of the time-stamp tokens to the accepted uses of the same, in compliance with provisions of this Time-Stamping Policy

3 Be aware of the guarantees and accept the responsibilities applicable in acceptance and use of time-stamp tokens.

4 Notify of any event or anomalous situations concerning the time-stamping service and/or the time-stamp tokens issued and that may be considered cause for their cancellation.

5 Be aware and to take any precaution stipulated by agreement with the Time-Stamping Authority, in order to obtain time-stamping services.

6.6 Liabilities

6.6.1 Liabilities incumbent on TSABDE

TSABDE shall only be held liable in the case of breach of the obligations contained in Law 59/2003, dated 19 December, the Electronic Signature Act and its implementing regulations, in these Time-Stamping Policies and Practices and in the PKIBDE CPS.

6.6.2 PKIBDE liability exemption

TSABDE shall not be held liable concerning the use and applicability of the time-stamp tokens issued for any activity not specified in this Policy.

TSABDE shall not be held responsible for the content of the documents and data to which the time-stamp token issued is applied, and will not be held liable for possible damages in transactions to which it has been applied.

TSABDE does not represent any of the subscribers or relying parties of the time-stamp tokens it issues.

6.6.3 Scope of liability coverage

As specified in section *9.6.3 Scope of liability coverage* of the PKIBDE CPS.

6.7 Loss Limits

As specified in section *9.7 Loss limits* of the PKIBDE CPS.

6.8 Validity Period

6.8.1 Term

As specified in section *9.8.1 Term* of the PKIBDE CPS.

6.8.2 Replacement and repeal of the Time-Stamping Policies and Practices

As specified in section *9.8.2 Replacement and repeal* of the PKIBDE CPS.

6.8.3 Consequences of termination

As specified in section *9.8.3 Consequences of termination* of the PKIBDE CPS.

6.9 Individual notices and communications with participants

As specified in section *9.9 Individual notices and communications with participants* of the PKIBDE CPS.

6.10 Specification amendment procedures

6.10.1 Amendment procedures

The body empowered to make and approve amendments on the TSABDE Time-Stamping Policy and Practices is the Policy Management Authority (PAA). The PAA contact details can be found under point 1.4 Policy and Practices Management.

6.10.2 Notification period and mechanism

In the event that the PAA deems that the changes to the specification may affect the acceptability of time-stamp tokens, subscribers and relying parties will be notified that a change has been made and that they must consult the new Time-Stamping Policy and Practices in the repository indicated.

6.10.3 Circumstances in which the OID must be changed

When, in the opinion of the PAA, the changes to specifications do not affect the acceptability of the time-stamp tokens, the lower version number of the document will be increased as well as the last number of the Object Identifier (OID) that represents it, maintaining the highest version number of the document, as well as the rest of the associated OID. It is not deemed necessary to notify subscribers and relying parties of this type of modification.

Should the PAA deem that the amendments to the specifications could affect the acceptability of the time-stamp tokens, the highest version number of the document shall be changed and its lowest number placed at zero.

The last two numbers of the Object Identifier (OID) representing it will also be modified. Subscribers and relying parties will be notified of this type of modification.

6.11 Disputes and Jurisdiction

As specified in section *9.11 Disputes and jurisdiction* of the PKIBDE CPS.

6.12 Governing Law

In keeping with Spanish and European legislation on this matter, included in chapter 5.5.10 of this document.

6.13 Compliance with Applicable Law

As specified in section *9.13 Compliance with Applicable Law* of the PKIBDE CPS.

6.14 Miscellaneous Provisions

6.14.1 Entire agreement clause

All subscribers of the time-stamping service, by the mere fact of using it, and relying parties, accept all the contents of the latest version of these Time-Stamping Policy and Practices.

6.14.2 Independence

As specified in section *9.14.2 Independence* of the PKIBDE CPS.

6.14.3 Resolution through the courts

No stipulation.

6.15 Other Provisions

No stipulation.

7 Legal regime and personal data protection

The TSABDE Personal Data Protection Policy should include the provisions of Organic Law 15/1999, of 13 December, the Personal Data Protection Act (LOPD) and its implementing regulations, including, of particular importance, Royal Decree 1720/2007, of 21 December, which passes the implementing regulations for Organic Law 15/1999, of 13 December, the Personal Data Protection Act.

Banco de España Circular 2/2005, of 25 February, on automated electronic files containing personal data managed by Banco de España (Official State Gazette, 22 March) and its subsequent updates are also applicable.

Likewise, where applicable, the internal rules and procedures established by Banco de España and designed to guarantee the level of security required by the aforementioned Royal Decree, shall be observed.

Should it be necessary to collect personal data from the subscriber in order to render the time-stamping service, it shall be verified that the latter has been informed and that he expresses his agreement that his personal details be processed, to the purpose for which they are to be used, to the recipients thereof and their inclusion on the file declared for this purpose by PKIBDE.

The parties to which the data belong may exercise their rights to access, rectify, cancel or oppose the holding of said data by writing to the contact address indicated in this document.

Personal data may only be disclosed to third parties, without the consent of the person affected, in the circumstances established in the regulatory legislation on personal data protection.

Lastly, the considerations set forth in Chapter *10 Personal Data Protection* of the PKIBDE CPS.