BANCO DE ESPAÑA
Eurosistema

11.05.2015

OID: 1.3.6.1.4.1.19484.2.2.11

Banco de España Public Key Infrastructure

Certificate Policy for Time-stamping Authority Certificates

This document contains the Certificate Policy (CP) that regulates the certificates issued by the Corporate CA for the Banco de España Time-Stamping Authority

---

Control Sheet

Title	Certificate Policy for Time-Stamping Authority Certificates
Author	Information Systems Department
Version	1.1
Date	11.05.2015

Change Log

Version	Date	Reason for the change
1.0	21.05.2010	Initial Version
1.1	11.05.2015	Update due to the renewal of the Certification Authorities

TABLE OF CONTENTS

1 Introduction 14

1.1 Overview 14

1.2 Document Name and Identification 15

1.3 PKI Participants 15

1.3.1 Policy Management Authority 15

1.3.2 Certification Authorities 16

1.3.3 Registration Authorities 18

1.3.4 Validation Authority 18

1.3.5 Keys Archive 18

1.3.6 Certificate Subscribers 18

1.3.7 Relying Parties 19

1.3.8 Other affected parties 19

1.4 Certificate Usage 19

1.4.1 Appropriate certificate use 19

1.4.2 Certificate Usage Constraints and Restrictions 20

1.5 Policy Administration 20

1.5.1 Banco de España, as owner of PKIBDE.20

1.5.2 Contact Person 20

1.5.3 Establishment of the suitability of a CPS from an External CA as regards PKIBDE Certificate Policies of PKIBDE 20

1.5.4 Approval Procedures for this CP20

1.6 Definitions and Acronyms 20

1.6.1 Definitions 20

1.6.2 Acronyms 22

2 Repositories and Publication of Information 24

2.1 Repositories 24

2.2 Publication of Certification Data 24

2.3 Publication Timescale or Frequency 24

2.4 Repository Access Controls 24

3 Identification and Authentication of Certificate Subscribers 25

3.1 Naming 25

3.1.1 Types of names 25

3.1.2 The need for names to be meaningful 25

3.1.3 Rules for interpreting various name formats 25

3.1.4 Uniqueness of names 25

3.1.5 Name dispute resolution procedures 25

3.1.6 Recognition, authentication, and the role of trademarks 26

3.2 Initial Identity Validation 26

3.2.1 Means of proof of possession of the private key 26

3.2.2 Identity authentication for a legal person 26

3.2.3 Identity authentication for a natural person 26

3.2.4 Non-verified applicant information 26

3.2.5 Validation of authority 26

3.2.6 Criteria for operating with external CAs 26

3.3 Identification and Authentication in Key Renewal Requests 26

3.3.1 Identification and authentication requirements for routine key renewal 26

3.3.2 Identification and authentication requirements for key renewal after certificate revocation 26

4 Certificate Life Cycle Operating Requirements 27

4.1 Certificate Application 27

4.1.1 Who can submit a certificate application? 27

4.1.2 Registration of applications for certificates and applicants' responsibilities 27

4.2 Certificate Application Processing 28

4.2.1 Performance of identification and authentication procedures 28

4.2.2 Approval or rejection of certificate applications 28

4.2.3 Time limit for processing the certificate applications 28

4.3 Certificate Issuance 28

4.3.1 Actions performed by the CA during the issuance of the certificate 28

4.3.2 CA notification to the applicants of certificate issuance 29

4.4 Certificate Acceptance 29

4.4.1 Form of certificate acceptance 29

4.4.2 Publication of the certificate by the CA 29

4.4.3 Notification of certificate issuance by the CA to other Authorities 29

4.5 Key Pair and Certificate Usage 29

4.5.1 Subscribers' use of the private key and certificate 29

4.5.2 Relying parties' use of the public key and the certificate 29

4.6 Certificate Renewal with no Key Changeover 29

4.6.1 Circumstances for certificate renewal with no key changeover 29

4.7 Certificate Renewal with Key Changeover 29

4.7.1 Circumstances for certificate renewal with key changeover 29

4.7.2 Who may request certificate renewal? 30

4.7.3 Procedures for processing renewal requests with key changeover 30

4.7.4 Notification of the new certificate issuance to the subscriber 30

4.7.5 Manner of acceptance of certificates with changed keys 30

4.7.6 Publication of certificates with the new keys by the CA 30

4.7.7 Notification of certificate issuance by the CA to other Authorities 30

4.8 Certificate Amendment 30

4.8.1 Circumstances for certificate amendment 30

4.9 Certificate Revocation and Suspension 31

4.9.1 Circumstances for revocation 31

4.9.2 Who can request revocation? 31

4.9.3 Procedures for requesting certificate revocation 32

4.9.4 Revocation request grace period 32

4.9.5 Time limit for the CA to process the revocation request 32

4.9.6 Requirements for revocation verification by relying parties 32

4.9.7 CRL issuance frequency 32

4.9.8 Maximum latency between the generation of CRLs and their publication 32

4.9.9 Online certificate revocation status checking availability 32

4.9.10 Online revocation checking requirements 33

4.9.11 Other forms of revocation alerts available 33

4.9.12 Special requirements for the renewal of compromised keys 33

4.9.13 Causes for suspension 33

4.9.14 Who can request the suspension? 33

4.9.15 Procedure for requesting certificate suspension 33

4.9.16 Suspension period limits 33

4.10 Certificate Status Services 33

4.10.1 Operational characteristics 33

4.10.2 Service availability 33

4.10.3 Additional features 33

4.11 End of Subscription 33

4.12 Key Escrow and Recovery 34

4.12.1 Key escrow and recovery practices and policies 34

4.12.2 Session key protection and recovery policies and practices 34

5 Management, Operating, Installations and Physical Controls 35

5.1 Physical Security Controls 35

5.1.1 Site location and construction 35

5.1.2 Physical access 35

5.1.3 Power and air-conditioning 35

5.1.4 Water exposure 35

5.1.5 Fire prevention and protection 35

5.1.6 Storage system 35

5.1.7 Waste disposal 35

5.1.8 Offsite backup 35

5.2 Procedural Controls 35

5.2.1 Roles responsible for PKI control and management 35

5.2.2 Number of individuals required to perform each task 35

5.2.3 Identification and authentication of each user 35

5.2.4 Roles that require separation of duties 35

5.3 Personnel Security Control 36

5.3.1 Requirements concerning professional qualification, knowledge and experience 36

5.3.2 Background checks and clearance procedures 36

5.3.3 Training requirements 36

5.3.4 Retraining requirements and frequency 36

5.3.5 Frequency and sequence for job rotation 36

5.3.6 Sanctions for unauthorised actions 36

5.3.7 Requirements for third party contracting 36

5.3.8 Documentation supplied to personnel 36

5.4 Security Audit Procedures 36

5.4.1 Types of events recorded 36

5.4.2 Frequency with which audit logs are processed 36

5.4.3 Period for which audit logs are kept 36

5.4.4 Audit log protection 36

5.4.5 Audit log back up procedures 36

5.4.6 Audit data collection system (internal vs. external) 37

5.4.7 Notification to the subject who caused the event 37

5.4.8 Vulnerability assessment 37

5.5 Records Archive 37

5.5.1 Types of events archived 37

5.5.2 Archive retention period 37

5.5.3 Archive protection 37

5.5.4 Archive backup procedures 37

5.5.5 Requirements for time-stamping records 37

5.5.6 Audit data archive system (internal vs. external) 37

5.5.7 Procedures to obtain and verify archived information 37

5.6 CA Key Changeover 37

5.7 Compromised Key and Disaster Recovery 37

5.7.1 Incident and compromise handling procedures 37

5.7.2 Corruption of computing resources, software, and/or data 37

5.7.3 Action procedures in the event of compromise of an Authority's private key 38

5.7.4 Installation following a natural disaster or other type of catastrophe 38

5.8 CA or RA Termination 38

5.8.1 Certification Authority 38

5.8.2 Registration Authority 38

6 Technical Security Controls 39

6.1 Key pair generation and installation 39

6.1.1 Key pair generation 39

6.1.2 Delivery of private keys to subscribers 39

6.1.3 Delivery of the public key to the certificate issuer 39

6.1.4 Delivery of the CA's public key to relying parties 39

6.1.5 Key sizes 39

6.1.6 Public key generation parameters and quality checks 39

6.1.7 Key usage purposes (KeyUsage field in X.509 v3) 39

6.2 Private Key Protection and Cryptographic Module Engineering Controls 40

6.2.1 Cryptographic module standards 40

6.2.2 Private key multi-person (k out of n) control 40

6.2.3 Escrow of private keys 40

6.2.4 Private key backup copy 40

6.2.5 Private key archive 40

6.2.6 Private key transfer into or from a cryptographic module 40

6.2.7 Private key storage in a cryptographic module 40

6.2.8 Private key activation method 40

6.2.9 Private key deactivation method 40

6.2.10 Private key destruction method 41

6.2.11 Cryptographic module classification 41

6.3 Other Aspects of Key Pair Management 41

6.3.1 Public key archive 41

6.3.2 Operational period of certificates and usage periods for key pairs 41

6.4 Activation Data 41

6.4.1 Generation and installation of activation data 41

6.4.2 Activation data protection 41

6.4.3 Other activation data aspects 41

6.5 Computer Security Controls 41

6.5.1 Specific security technical requirements 41

6.5.2 Computer security evaluation 41

6.6 Life Cycle Security Controls 41

6.6.1 System development controls 41

6.6.2 Security management controls 41

6.6.3 Life cycle security controls 42

6.7 Network Security Controls42

6.8 Time-Stamping 42

7 Certificate, CRL and OCSP Profiles 43

7.1 Certificate Profile 43

7.1.1 Version number 43

7.1.2 Certificate extensions 43

7.1.3 Algorithm Object Identifiers (OID) 46

7.1.4 Name formats 46

7.1.5 Name constraints 46

7.1.6 Certificate Policy Object Identifiers (OID) 46

7.1.7 Use of the "PolicyConstraints" extension46

7.1.8 Syntax and semantics of the “PolicyQualifier 46

7.1.9 Processing semantics for the critical “CertificatePolicy” extension 46

7.2 CRL Profile 46

7.2.1 Version number 46

7.2.2 CRL and extensions 47

7.3 OCSP Profile 47

7.3.1 Version number(s) 47

7.3.2 OCSP Extensions 47

8 Compliance Audit and Other Controls 48

8.1 Frequency or Circumstances of Controls for each Authority 48

8.2 Identity/Qualifications of the Auditor 48

8.3 Relationship between the Assessor and the Entity being Assessed 48

8.4 Aspects Covered by Controls 48

8.5 Actions taken as a result of deficiencies found 48

8.6 Notification of the results 48

9 Other business and legal matters 49

9.1 Fees 49

9.1.1 Certificate issuance or renewal fees 49

9.1.2 Certificate access fees 49

9.1.3 Revocation or status information fees 49

9.1.4 Fees for other services, such as policy information 49

9.1.5 Refund policy 49

9.2 Information Confidentiality 49

9.2.1 Scope of confidential information 49

9.2.2 Non-confidential information 49

9.2.3 Duty to maintain professional secrecy 49

9.3 Personal Data Protection 49

9.3.1 Personal data protection policy 49

9.3.2 Information considered private 49

9.3.3 Information not classified as private 50

9.3.4 Responsibility to protect personal data 50

9.3.5 Notification of and consent to the use of personal data 50

9.3.6 Disclosure within legal proceedings 50

9.3.7 Other circumstances in which data may be made public 50

9.4 Intellectual Property Rights 50

9.5 Obligations 50

9.5.1 Obligations of the CA 50

9.5.2 Obligations of the RA 50

9.5.3 Obligations incumbent on certificate subscribers 50

9.5.4 Obligations incumbent on relying parties 50

9.5.5 Obligations incumbent on other participants 51

9.6 Liabilities 51

9.6.1 PKIBDE's liabilities 51

9.6.2 PKIBDE liability exemption 51

9.6.3 Scope of liability coverage 51

9.7 Loss Limits 51

9.8 Validity Period 51

9.8.1 Term 51

9.8.2 CP substitution and termination 51

9.8.3 Consequences of termination 52

9.9 Individual notices and communications with participants 52

9.10 Specification amendment procedures 52

9.10.1 Amendment procedures 52

9.10.2 Notification period and mechanism 52

9.10.3 Circumstances in which the OID must be changed 52

9.11 Disputes and Jurisdiction 52

9.12 Governing Law 52

9.13 Compliance with applicable law 52

9.14 Miscellaneous provisions 52

9.14.1 Entire agreement clause 52

9.14.2 Independence 52

9.14.3 Resolution through the courts 52

9.15 Other Provisions 53

10 Personal Data Protection 54

10.1 Data Protection Legal Scheme 54

10.2 File Creation and Registration 54

10.3 Personal Data Protection Act Security Document 54

1 Introduction

1.1 Overview

This document sets out the Certificate Policy (CP) governing the certificates issued by the Time-Stamping Authority (hereinafter, TSA) by the Banco de España Public Key Infrastructure (hereinafter, PKIBDE). In particular, this CP governs the certificates issued by the Banco de España Time-Stamping Authority, TSABDE.

From the perspective of the X.509 v3 standard, a CP is a set of rules that define the applicability or use of a certificate within a community of users, systems or specific class of applications that have a series of security requirements in common.

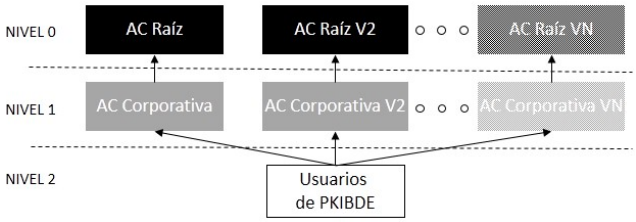
This CP details and completes the "Certification Practice Statement" (CPS) of the Banco de España's PKI (PKIBDE), containing the rules by which the use of the certificates defined in this policy are governed, as well as the scope of application and the technical characteristics of this type of certificate.

This CP, with the exception of section 9, which contains a slight variation, has been structured in accordance with the guidelines of the PKIX work group in the IETF (Internet Engineering Task Force) in its reference document RFC 3647 (approved in November 2003) "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*". In order to give the document a uniform structure and facilitate its reading and analysis, all the sections established in RFC 3647 have been included. Where nothing has been established for any section the phrase “No stipulation” will appear. Additionally, apart from the headings established in RFC 3647, a new chapter has been included that deals with personal data protection in order to comply with Spanish legislation on this matter.

The CP includes all the activities aimed at managing Time-Stamping Authority certificates during their life cycle. Consequently, all the parties involved must be aware of the content of the CP and adapt their activities to the stipulations therein.

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

The general architecture, in hierarchic terms, of the Banco de España's PKI is as follows[1]:



1.2 Document Name and Identification

Document name	Certificate Policy (CP) for PKIBDE Time-Stamping Certificates
Document version	1.1
Document status	Approved
Date of issue	11.05.2015
Expiry date	Not applicable
OID (Object Identifier)	1.3.6.1.4.1.19484.2.2.11
CPS 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 PKI Participants

The participating entities and persons are:

- Banco de España, as owner of PKIBDE.
- The Policy Management Authority.
- The Certification Authorities.
- The Registration Authorities.
- The Validation Authorities.
- The Keys Archive.
- The Applicants and Subscribers of the certificates issued by PKIBDE.
- The Relying Parties of the certificates issued by PKIBDE.

1.3.1 Policy Management Authority

The Policy Management Authority is defined in accordance with the PKIBDE Certification Practice Statement (hereinafter, CPS).

[1] Sequent renewals of the Certification Authorities, either Root or Corporate, will be indicated by a version number, as shown in the drawning.

1.3.2 Certification Authorities

Certification Authorities are defined as per the PKIBDE CPS.

The Certification Authorities that currently make up PKIBDE are:

1.3.2.1 Root Certification Authorities

- **Root CA**: First-level Certification Authority. This CA only issues certificates for itself and its Subordinate CAs. It will only be in operation whilst carrying out the operations for which it is established. Its most significant data are:

Distinguished name	CN=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Serial number	F16D 7586 5D7C CF92 41AD A17A CD9A 3DE2
Distinguished Name of Issuer	CN=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Validity period	From 2004-07-08 11:34:12 to 2034-07-08 11:34:12
Message digest (SHA-1)	2B60 DE7D 3337 8BF7 5B67 8B10 77BB F951 6029 D6A8
Cryptographic algorithms	SHA-1 / RSA 2048

- **Root CA V2**: First-level Certification Authority. This CA only issues certificates for itself and its Subordinate CAs. It will only be in operation whilst carrying out the operations for which it is established. Three valid certificate have been issued for this CA, using the same key pair:

  - With SHA-1 algorithm[2]:

Distinguished name	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Serial number	25B4 07F6 4A5C F9F1 5547 7951 2040 982B
Distinguished Name of Issuer	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Validity period	From 2015-05-04 12:42:33 to 2045-05-04 12:42:33
Message digest (SHA-1)	A84A 2C75 2746 B21B 567F 8B07 EC2A FCB9 7551 046A
Cryptographic algorithms	SHA-1 / RSA 4096

  - With SHA-256 algorithm:

Distinguished name	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Serial number	4554 22D4 E876 1BFC 5547 4D19 4E85 6E37
Distinguished Name of Issuer	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Validity period	From 2015-05-04 12:42:33 to 2045-05-04 12:42:33
Message digest (SHA-1)	ACBC CB74 406A 5588 EB88 2F5F 5994 9DDC B831 7986
Cryptographic algorithms	SHA-256 / RSA 4096

[2] This certificate will be only used in systems that do no support higher algorithms

- With SHA-512 algorithm:

Distinguished name	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Serial number	19D8 C7AA 668C 3E0F 5547 7970 D573 00FC
Distinguished Name of Issuer	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Validity period	From 2015-05-04 12:42:33 to 2045-05-04 12:42:33
Message digest (SHA-1)	2AD9 E9BF FCDD B5D4 46C9 7A3A D4BB 6DCE A3B1 219C
Cryptographic algorithms	SHA-512 / RSA 4096

Root CA V2 has been issued to replace Banco de España's Root CA, as a result of the update of the cryptographic upgrade of the algorithms and key lengths used according to international recommendations. Both Root CAs are valid until their expiration date.

1.3.2.2 Intermediate Certification Authorities

- **Corporate CA**: Certification Authority subordinate to the Root CA. It is responsible for issuing certificates for PKIBDE users. Its most significant data are:

Distinguished name	CN=BANCO DE ESPAÑA-AC CORPORATIVA, O=BANCO DE ESPAÑA, C=ES
Serial number	366A 524D A5E4 4AF8 4108 A140 9B9B 76EB
Distinguished Name of Issuer	CN=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Validity period	From 2004-07-29 9:03:28 to 2019-07-29 9:03:28
Message digest (SHA-1)	ABE6 1ED2 5AF6 4253 F77B 322F 6F21 3729 B539 1BDA
Cryptographic algorithms	SHA-1 / RSA 2048

- **Corporate CA V2**: Certification Authority subordinate to the Root CA. It is responsible for issuing certificates for PKIBDE users. Certification Authority subordinate to the Root CA. It is responsible for issuing certificates for PKIBDE users:

- With SHA-1[3] algorithm:

Distinguished name	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Serial number	5F8B 48ED 492D 5236 5547 7730 704F 397F
Distinguished Name of Issuer	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Validity period	From 2015-05-04 18:00:00 to 2030-05-04 18:00:00
Message digest (SHA-1)	4832 0271 9F45 67EB 42E4 4A13 04DE D1F7 7B7B 7EE9
Cryptographic algorithms	SHA-1 / RSA 4096

[3] This certificate will be only used in systems that do no support higher algorithms

- With SHA-256 algorithm:

Distinguished name	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Serial number	18D8 765B E681 86C6 5547 76F5 9227 2480
Distinguished Name of Issuer	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Validity period	From 2015-05-04 18:00:00 to 2030-05-04 18:00:00
Message digest (SHA-1)	A8F0 5CAC 9C65 18C0 8FF6 3F82 C338 DE46 D8B9 3E38
Cryptographic algorithms	SHA-256 / RSA 4096

- With SHA-512 algorithm:

Distinguished name	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Serial number	293F 0A37 5B54 D2D2 5547 7749 5728 B9B6
Distinguished Name of Issuer	CN= BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Validity period	From 2015-05-04 18:00:00 to 2030-05-04 18:00:00
Message digest (SHA-1)	B3CF 4285 869F 6C07 45B1 D69C 8EC2 7683 6953 DE5E
Cryptographic algorithms	SHA-512 / RSA 4096

Corporate CA V2 has been issued to replace Banco de España's Corporate CA, as a result of the update of the cryptographic upgrade of the algorithms and key lengths used according to international recommendations.

Both intermediate CAs are valid until their expiration date or revocation. However the Corporate CA will cease providing end entity certificate issuance since the entry into Service of Corporate CA V2, and it will be remain alive only to enable revocation of certificates previously issued by it.

1.3.3 Registration Authorities

The Registration Authorities are defined in accordance with the PKIBDE Certification Practice Statement.

TSA Certificates will be issued by the PKIBDE Administrators, which shall act as Registration Authorities to verify applicants' details and to generate certification/repeal requests, directly using the Corporate CA administration.

1.3.4 Validation Authority

Validation Authority is defined as per the PKIBDE CPS.

1.3.5 Keys Archive

The Keys Archive defined in the CPS is not applicable in this certificate policy.

1.3.6 Certificate Subscribers

Certificate subscribers are defined as per the PKIBDE CPS.

The type of entities that can be subscribers of the certificates referred to in this CP are limited to those shown in the following chart:

Certification Environment	Subscribers
Corporate CA	Time-Stamping Authority

It should be recalled that these Time-Stamping Authorities may be internal (e.g. TSABDE) or external to Banco de España. In both cases, there shall be a supervisor for each TSA. The type of individuals who can act as component managers are set out in the following chart:

Certificate type	Manager
Time-Stamping Authority Certificates	Time-Stamping Authority Supervisor

1.3.7 Relying Parties

Relying parties are defined as per the PKIBDE CPS. In particular, they shall be those who recognise and make use of the Time-Stamp Tokens issued by a TSA, whose certificate has been issued by PKIBDE under this CP.

1.3.8 Other affected parties

Applicants: They are the Time-Stamping Authority Supervisors.

CA Administrator: Individuals within Banco de España who manage the TSA certificate requests and have CA administration privileges.

1.4 Certificate Usage

1.4.1 Appropriate certificate use

The Time-Stamping Authority owning the certificate shall have a "Time-Stamping Policy" in place, compliant with acknowledged best practices for rendering time-stamping services.

It shall likewise have an updated "Time-Stamping Policies and Practices" document that describes said policy, which is accessible to the public and free of charge, which indicates its supervisors and describes its obligations and liabilities, the processes and procedures for managing and operating the TSA, key life cycles, security mechanisms, etc.

The following table shows appropriate usage of certificates in greater detail:

Certificate type	Appropriate Usage
Time-Stamping Authority Certificates	Rendering of time-stamping services (compliant with the "TSA Time-Stamping Policies and Practices" of the TSA)

1.4.2 Certificate Usage Constraints and Restrictions

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

1.5 Policy Administration

1.5.1 Banco de España, as owner of PKIBDE.

This CP 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

1.5.2 Contact Person

This CP is managed by the PKIBDE Policy Management Authority (PMA).

Name	Information Systems Department Banco de España PKI Policy Management Authority		
E-mail address	pkibde@bde.es		
Address	C/Alcalá, 522. 28027 - Madrid (Spain)		
Telephone No.	+34913386610	**Fax**	+34913386870

1.5.3 Establishment of the suitability of a CPS from an External CA as regards PKIBDE Certificate Policies of PKIBDE

As specified in PKIBDE's CPS.

1.5.4 Approval Procedures for this CP

As specified in PKIBDE's CPS.

1.6 Definitions and Acronyms

1.6.1 Definitions

Within the scope of this CP the following terms are used:

Authentication: the process of verifying the identity of an applicant or subscriber of a PKIBDE certificate.

Time-Stamping Authority (TSA): authority that issues time-stamp tokens.

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 uses 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.

Directory: information repository that follows the ITU-T X.500 standard.

Identification: the process of establishing the identity of an applicant or subscriber of a PKIBDE certificate.

User Identifier: a set of characters that are used to uniquely identify the user of a system.

Trust Hierarchy: set of certification authorities that maintain a relationship of trust by which a CA of a higher level guarantees the trustworthiness of one or several lower level CAs. In the case of PKIBDE, the hierarchy has two levels, the Root CA on the higher level guarantees the reliability of its subordinate CAs.

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

Applicants: person who requests a certificate for themselves, for a legal person or for a Time-Stamping Authority.

Relying Parties: individuals or entities other than subscribers that decide to accept and rely on a certificate issued by PKIBDE.

Subscribers: person, computer component or entity (e.g.: Time-Stamping Authority) for which an electronic certificate is issued by the latter or by its applicant.

UTC (Coordinated Universal Time): a time-zone of reference with respect to which all the other time-zones in the world are calculated. Defined in ITU-R Recommendation TF.460-5

UTC(k): time-scale performed by the “k” laboratory and maintained in accordance with UTC, in order to attain a tolerance margin of +-100 ns with respect to it (Recommendation TF.536-1)

Subscriber: an entity requesting TSA services and which has explicitly or implicitly accepted its terms and conditions.

Time-stamping policy: set of rules governing the applicability of the time-stamp token for a particular community and/or its application with some common security requirements.

TSA Practices Statement: a statement of the practices that a TSA performs in issuing time-stamp tokens.

Time-stamp token: a document signed electronically by the TSA which ties the representation of a piece of data to a specific time, thus establishing that said piece of data existed prior to said moment.

TSA System: a set of IT products and other components organised to support the provision of time-stamp services.

Time-Stamp Unit: a set of hard- and software that have a single active time-stamp token signature key at a given moment.

1.6.2 Acronyms

PAA: Policy Management Authority

CA: Certification Authority

RA: Registration Authority

VA: Validation Authority

CRL: Certificate Revocation List

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

CEN: Comité Européen de Normalisation

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

CWA: CEN Workshop Agreement

DN: Distinguished Name. Unique identification of an entry within the X.500 directory structure

CPS: Certification Practice Statement

ETSI: European Telecommunications Standard Institute

FIPS: Federal Information Processing Standard

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)

LDAP: Lightweight Directory Access Protocol

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

PKCS: Public Key Infrastructure Standards: Internationally accepted PKI standards developed by RSA Laboratories.

PKI: Public Key Infrastructure

PKIBDE: Banco de España PKI

PKIX: Work group within the IETF (Internet Engineering Task Group) set up for the purpose of developing PKI and internet specifications.

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

TSA Time-Stamping Authority

TSU: Time-stamping Unit

UTC: Coordinated Universal Time

2 Repositories and Publication of Information

2.1 Repositories

As specified in PKIBDE's CPS.

2.2 Publication of Certification Data

As specified in PKIBDE's CPS.

2.3 Publication Timescale or Frequency

As specified in PKIBDE's CPS.

2.4 Repository Access Controls

As specified in PKIBDE's CPS.

3 Identification and Authentication of Certificate Subscribers

3.1 Naming

3.1.1 Types of names

The certificates issued by PKIBDE contain *the Distinguished Name* (or DN) X.500 of the issuer and that of the certificate subject in the fields *issuer name* and *subject name*, respectively.

The CN (*Common Name*) attribute of the DN will refer to the code assigned to the Time-Stamping Authority owner of the certificate.

If there is more than one TSU for one same Time-Stamping Authority, the CN shall conclude with a numerical code that solely identifies each TSU.

The component certificate's CN will be as follows:

Certificate type	CN
Time-Stamping Authority Certificates	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

3.1.2 The need for names to be meaningful

In all cases the distinguished name of the certificates must be meaningful and are subject to the rules established in the previous point in this respect.

3.1.3 Rules for interpreting various name formats

The rule applied by PKIBDE for the interpretation of the distinguished names for subscribers of the certificates it issues is the ISO/IEC 9595 (X.500) Distinguished Name (DN) standard.

3.1.4 Uniqueness of names

Certificate DNs may not be repeated.

Should more than one certificate be issued for one same TSA because it has several TSUs, these certificates shall be differentiated by a distinctive number at the end of the corresponding CN.

There cannot be more than one certificate for one same TSU, given for a particular TSA.

3.1.5 Name dispute resolution procedures

Any dispute concerning ownership of names shall be resolved as stipulated in point *9.13 Claims and Jurisdiction* in this document.

3.1.6 Recognition, authentication, and the role of trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Means of proof of possession of the private key

Possession of the private key, companion of the public key for which the TSA supervisor requests a certificate be generated, shall be proven by sending the certification request, which shall include the public key signed using the companion private key.

3.2.2 Identity authentication for a legal person

Certificates from Time-Stamping Authorities are not electronic certificates for legal persons as defined in Section 7, Law 59/2003, dated 19 December, the Electronic Signature Act.

3.2.3 Identity authentication for a natural person

Under this policy, the identity of natural persons shall be authenticated by the electronic signature on the application using a natural person certificate issued by a CSP recognised by Banco de España for these purposes or by PKIBDE. Validation of the identity of the natural person will have been carried out in accordance with the procedures established by the PCS or by PKIBDE.

3.2.4 Non-verified applicant information

Ownership of the domain names or e-mail addresses will not be verified, if it is necessary to include them in the certificate.

3.2.5 Validation of authority

The applicant shall have to be the supervisor of the Banco de España TSA.

3.2.6 Criteria for operating with external CAs

As specified in PKIBDE's CPS.

3.3 Identification and Authentication in Key Renewal Requests

3.3.1 Identification and authentication requirements for routine key renewal

The individual identification process shall be the same as in the initial validation.

3.3.2 Identification and authentication requirements for key renewal after certificate revocation

The individual identification process shall be the same as in the initial validation.

4 Certificate Life Cycle Operating Requirements

This chapter contains the operating requirements for the life cycle of Time-Stamping Authority certificates issued by the Corporate CA.

Although these certificates should be stored on cryptographic support hardware, this Certificate Policy does not undertake to regulate the management of said elements.

On the other hand, in this chapter some illustrations will be provided for better understanding. In the event of any difference or discrepancy between the text and the illustrations, the text will prevail in all cases, given the necessary synthetic nature of the illustrations.

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

The request for a Time-Stamping Authority Certificate must be submitted by the TSA supervisor using a natural person certificate. Said supervisor must have the necessary powers of attorney accrediting them as such.

Application for a certificate does not mean it will be obtained if the applicant does not fulfil the requirements established for TSA certificates in the CPS or in this CP.

4.1.2 Registration of applications for certificates and applicants' responsibilities

1 The application shall be sent by e-mail to Banco de España. The electronic signature may be made either on the document itself or on the application document, or alternatively on the e-mail used to send the request, by one of the natural person certificates of the TSA supervisor issued by a CSP recognised by Banco de España for these purposes or by the PKIBDE.

As regards content, the application must include the certificate signing request (CSR) with the associated public key, as well as the information necessary for the CA to generate the certificate.

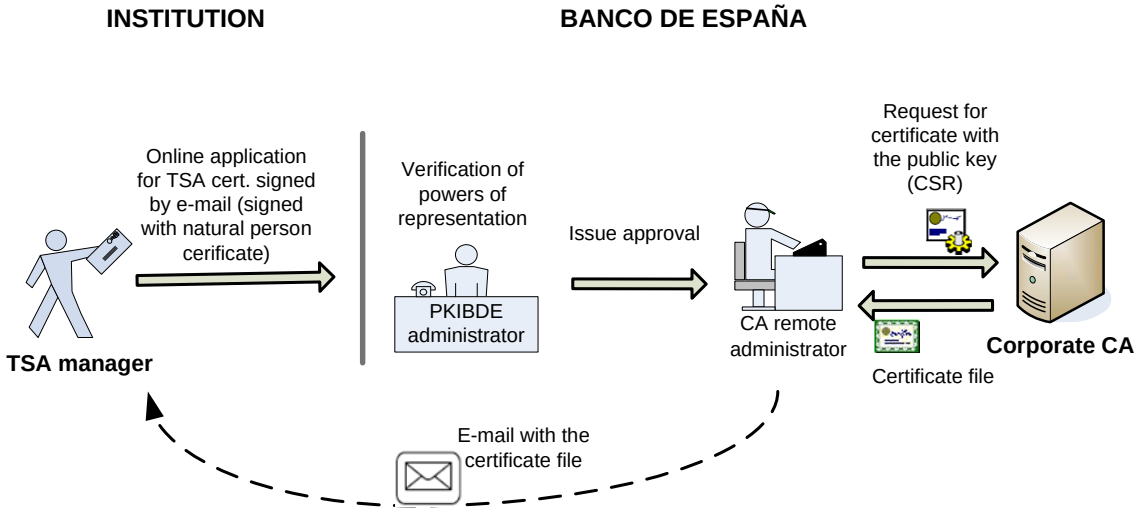
2 The PKIBDE manager or supervisor shall verify the applicant's powers of attorney, already available in Banco de España, as a prerequisite for approving issue of the certificate.

3 A remote CA administrator will receive the e-mail message with the go-ahead, verify the electronic signature and perform the necessary checks on the data and information the applicant has provided. If everything is correct, the remote administrator will connect to request the certificate be issued using a certificate request (CSR) with the public key.

4 The CA issues the certificate and the remote administrator subsequently downloads the corresponding file.

5 Banco de España sends the applicant the certificate by e-mail.

The following illustration offers a summary of the process described:



4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

The PKIBDE manager or supervisor will identify and authenticate the applicant by validating the electronic signature on the application or on the e-mail used to send it.

4.2.2 Approval or rejection of certificate applications

Certificates will be issued once PKIBDE has completed the verifications necessary to validate the certificate application.

For these purposes, PKIBDE or its managers and supervisors can collect the documentation they consider necessary from the applicant.

4.2.3 Time limit for processing the certificate applications

The PKIBDE Corporate CA shall not be held liable for any delays that may arise in the period between application for the certificate, publication in the PKIBDE repository and its delivery. The Corporate CA will process the requests as quickly as possible.

4.3 Certificate Issuance

4.3.1 Actions performed by the CA during the issuance of the certificate

Issuance of the certificate signifies final approval of the application by the CA.

When the PKIBDE Corporate CA issues a certificate pursuant to a certificate application, it will make the notifications established under point 4.3.2. of this chapter.

All certificates will become effective upon issue, unless the certificate indicates a later date and time of coming into force, which may not be more than 15 calendar days following issue. The period of validity is subject to possible early, temporary or permanent termination in the event of circumstances that give cause to the suspension or revocation of the certificate.

4.3.2 CA notification to the applicants of certificate issuance

Applicants will be advised of the issuance of the certificate via e-mail.

4.4 Certificate Acceptance

4.4.1 Form of certificate acceptance

Application for the certificate carries the applicants' implicit acceptance of the CPS and the CP, as well as of the certificate.

4.4.2 Publication of the certificate by the CA

The Time-Stamping Authority Certificate will be published in the PKIBDE repository.

4.4.3 Notification of certificate issuance by the CA to other Authorities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Subscribers' use of the private key and certificate

Subscribers may only use the private key and the certificate for the uses authorised under this CP and pursuant to the provisions in the 'Key Usage' and 'Extended Key Usage' fields of the certificate, and with the stipulations of its "Time-Stamping Policies and Practices". Likewise, subscribers may only use the key pair and the certificate once they have accepted the terms and conditions of use established in the CPS and CP, and only for that which is stipulated therein.

Following certificate expiry or revocation, subscribers must cease to use the private key.

4.5.2 Relying parties' use of the public key and the certificate

Relying parties should only trust certificates for the purposes set forth in this CP, the TSA "Time-Stamping Policies and Practices" and in accordance with the 'Key Usage' field on the certificate.

To trust the certificate, relying parties must successfully complete public key transactions, and take responsibility for verifying the certificate status using the means set forth by the CPS and in this CP. They are likewise bound to the conditions of use established in these documents.

4.6 Certificate Renewal with no Key Changeover

4.6.1 Circumstances for certificate renewal with no key changeover

All certificate renewals covered by this CP shall be carried out with change of keys. Consequently, the remaining points in section 4.6 (4.6.2 to 4.6.7) established in RFC 3647 are not included and, therefore, for the purposes of this CP, their content is "no stipulation".

4.7 Certificate Renewal with Key Changeover

4.7.1 Circumstances for certificate renewal with key changeover

A TSA certificate may be renewed for the following reasons, among others:

- Expiry of the validity period.
- Modification of the data contained in the certificate.
- When the keys are compromised or are no longer fully reliable.
- Change of format.

All renewals, regardless of their cause, shall be carried out with a change of keys.

4.7.2 Who may request certificate renewal?

Renewal must be requested by the TSA supervisor.

4.7.3 Procedures for processing renewal requests with key changeover

During the renewal process, the CA will check that the information used to verify the identity and attributes of the subscriber are still valid. If any of the subscriber's data have changed, they must be verified and registered with the agreement of the TSA supervisor.

The requirements for renewal will be the same as those for initial certificate issue.

If any of the conditions established in this CP have changed, the TSA supervisor must be made aware of this and agree to it.

In any case, certificate renewal is subject to:

- The request being made in due time and manner, following the instructions and regulations established by PKIBDE specifically for this purpose.
- The CA not having certain knowledge of the existence of any cause for the revocation / suspension of the certificate.
- The request for the renewal of the provision of services being for the same type of certificate as the one initially issued.

4.7.4 Notification of the new certificate issuance to the subscriber

The TSA supervisor will be notified by e-mail.

4.7.5 Manner of acceptance of certificates with changed keys

Renewal of the certificate entails the applicants' implicit acceptance of the CPS and the CP, as well as of the certificate.

4.7.6 Publication of certificates with the new keys by the CA

The TSA certificate will be published in the PKIBDE repository.

4.7.7 Notification of certificate issuance by the CA to other Authorities

No stipulation.

4.8 Certificate Amendment

4.8.1 Circumstances for certificate amendment

All certificate amendments carried out within the scope of this CP will be treated as certificate renewals and, therefore, the previous points in this respect shall be applicable.

Consequently, the remaining points in section 4.8 (4.8.2 to 4.8.7) established in RFC 3647 are not included, meaning that, for the purpose of this Statement, they are not regulated.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

Certificate revocation is the action that renders a certificate invalid prior to its expiry date. Certificate revocation produces the discontinuance of the certificate's validity, rendering it permanently inoperative as regards its inherent uses and, therefore, discontinuance of the provision of certification services. Revocation of a certificate prevents its legitimate use by the subscriber.

Revocation of a certificate entails its publication on the public-access Certificate Revocation Lists (CRL).

Causes for revocation:

- Loss, disclosure, modification or any other circumstance that compromises the subscriber's private key or when suspicion of such compromise exists.
- Deliberate misuse of keys and certificates, or failure to observe or infringement of the operational requirements contained in the CPS or in this CP.
- TSA ceasing to perform its functions, a circumstance that entitled it to hold the certificate.
- Ceasing of PKIBDE activity.
- Defective issue of a certificate due to:
    1. Failure to comply with the material requirements for certificate issuance.
    2. Reasonable belief that basic information related to the certificate is or could be false.
    3. The existence of a data entry error or any other processing error.
- The key pair generated by the subscriber has been found to be "weak".
- The information contained in a certificate or used for the application becomes inaccurate.
- By order given from the TSA supervisor or an authorised third party or natural person applicant representing a legal person.
- The certificate of a higher CA in the certificate trust hierarchy is revoked.
- Any of the other causes specified in this CP or in the CPS.

The main effect of revocation as regards the certificate is the immediate and early termination of its term of validity, with which the certificate becomes invalid. Revocation shall not affect the underlying obligations created or notified by this CPS, nor shall its effects be retroactive.

4.9.2 Who can request revocation?

PKIBDE or any of the Authorities that comprise the former may, of their own accord, request the revocation of a certificate if they become aware or suspect that the TSA's private key has been compromised, or in the event of any other factor that recommends taking such action.

Likewise, the TSA supervisor may also request revocation of their certificates, which they must do in accordance with the conditions set forth in section 4.9.3.

4.9.3 Procedures for requesting certificate revocation

Requests for revocation shall be carried out by the TSA supervisor in a similar manner as that described in section 4.1.2 for the issue request. They shall always be processed by the PKIBDE manager or supervisor.

Apart from this ordinary procedure, PKIBDE operators and managers may immediately revoke any certificate upon becoming aware of the existence of any of the causes for revocation.

4.9.4 Revocation request grace period

Revocation shall be carried out immediately following the processing of each request that is verified as valid. Therefore, the process will not include a grace period during which the revocation request may be cancelled.

4.9.5 Time limit for the CA to process the revocation request

Requests for revocation of TSA certificates must be processed as quickly as possible, and in no case may said processing take more than 24 hours.

4.9.6 Requirements for revocation verification by relying parties

Verification of revocations is mandatory for each use made of a TSA certificate.

Relying parties must check the validity of the CRL prior to each use and download the new CRL from the PKIBDE repository when the one they hold expires. CRLs stored in cache[4] memory, even when not expired, do not guarantee availability of updated revocation data.

Alternatively, a PKIBDE Validation Authority can be used (if available as per the provisions set forth in section 2.1 of this CP) to verify online the certificate revocation status.

4.9.7 CRL issuance frequency

As specified in PKIBDE's CPS.

4.9.8 Maximum latency between the generation of CRLs and their publication

The maximum time allowed between generation of the CRLs and their publication in the repository is 1 hour.

4.9.9 Online certificate revocation status checking availability

Alternatively, PKIBDE has an online system (Validation Authority) for verifying the status of a certificate.

The web addresses for accessing the CRLs and the Validation Authority, together with their features and usage constraints, are given in section *2.1 Repository*.

[4]Cache memory: memory that stores the necessary data for the system to operate faster, as it does not have to obtain this data from the source for every operation. Its use could entail the risk of operating with outdated data.

4.9.10 Online revocation checking requirements

When using the Validation Authority, relying parties must have software capable of operating with the OCSP protocol compliant with RFC 3161 to obtain the certificate information.

4.9.11 Other forms of revocation alerts available

No stipulation.

4.9.12 Special requirements for the renewal of compromised keys

There are no variations to the aforementioned clauses for revocation due to private key compromise.

4.9.13 Causes for suspension

There is no provision for the suspension of TSA certificates.

4.9.14 Who can request the suspension?

No stipulation.

4.9.15 Procedure for requesting certificate suspension

No stipulation.

4.9.16 Suspension period limits

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational characteristics

As specified in PKIBDE's CPS.

4.10.2 Service availability

As specified in PKIBDE's CPS.

4.10.3 Additional features

As specified in PKIBDE's CPS.

4.11 End of Subscription

Certificate subscription may be ended due to the following causes:

- Early certificate revocation due to any of the causes established in point 4.9.1.
- Expiry of the certificate.

If certificate renewal is not requested, the end of the subscription will terminate the relationship between the subscriber and the CA.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery practices and policies

The private key for certificates used by TSA is not archived.

4.12.2 Session key protection and recovery policies and practices

No stipulation.

5 Management, Operating, Installations and Physical Controls

5.1 Physical Security Controls

5.1.1 Site location and construction

As specified in PKIBDE's CPS.

5.1.2 Physical access

As specified in PKIBDE's CPS.

5.1.3 Power and air-conditioning

As specified in PKIBDE's CPS.

5.1.4 Water exposure

As specified in PKIBDE's CPS.

5.1.5 Fire prevention and protection

As specified in PKIBDE's CPS.

5.1.6 Storage system

As specified in PKIBDE's CPS.

5.1.7 Waste disposal

As specified in PKIBDE's CPS.

5.1.8 Offsite backup

As specified in PKIBDE's CPS.

5.2 Procedural Controls

5.2.1 Roles responsible for PKI control and management

As specified in PKIBDE's CPS.

5.2.2 Number of individuals required to perform each task

As specified in PKIBDE's CPS.

5.2.3 Identification and authentication of each user

As specified in PKIBDE's CPS.

5.2.4 Roles that require separation of duties

As specified in PKIBDE's CPS.

5.3 Personnel Security Control

5.3.1 Requirements concerning professional qualification, knowledge and experience

As specified in PKIBDE's CPS.

5.3.2 Background checks and clearance procedures

As specified in PKIBDE's CPS.

5.3.3 Training requirements

As specified in PKIBDE's CPS.

5.3.4 Retraining requirements and frequency

As specified in PKIBDE's CPS.

5.3.5 Frequency and sequence for job rotation

As specified in PKIBDE's CPS.

5.3.6 Sanctions for unauthorised actions

As specified in PKIBDE's CPS.

5.3.7 Requirements for third party contracting

As specified in PKIBDE's CPS.

5.3.8 Documentation supplied to personnel

As specified in PKIBDE's CPS.

5.4 Security Audit Procedures

5.4.1 Types of events recorded

As specified in PKIBDE's CPS.

5.4.2 Frequency with which audit logs are processed

As specified in PKIBDE's CPS.

5.4.3 Period for which audit logs are kept

As specified in PKIBDE's CPS.

5.4.4 Audit log protection

As specified in PKIBDE's CPS.

5.4.5 Audit log back up procedures

As specified in PKIBDE's CPS.

5.4.6 Audit data collection system (internal vs. external)

As specified in PKIBDE's CPS.

5.4.7 Notification to the subject who caused the event

As specified in PKIBDE's CPS.

5.4.8 Vulnerability assessment

As specified in PKIBDE's CPS.

5.5 Records Archive

5.5.1 Types of events archived

As specified in PKIBDE's CPS.

5.5.2 Archive retention period

As specified in PKIBDE's CPS.

5.5.3 Archive protection

As specified in PKIBDE's CPS.

5.5.4 Archive backup procedures

As specified in PKIBDE's CPS.

5.5.5 Requirements for time-stamping records

As specified in PKIBDE's CPS.

5.5.6 Audit data archive system (internal vs. external)

As specified in PKIBDE's CPS.

5.5.7 Procedures to obtain and verify archived information

As specified in PKIBDE's CPS.

5.6 CA Key Changeover

As specified in PKIBDE's CPS.

5.7 Compromised Key and Disaster Recovery

5.7.1 Incident and compromise handling procedures

As specified in PKIBDE's CPS.

5.7.2 Corruption of computing resources, software, and/or data

As specified in PKIBDE's CPS.

5.7.3 Action procedures in the event of compromise of an Authority's private key

As specified in PKIBDE's CPS.

5.7.4 Installation following a natural disaster or other type of catastrophe

As specified in PKIBDE's CPS.

5.8 CA or RA Termination

5.8.1 Certification Authority

As specified in PKIBDE's CPS.

5.8.2 Registration Authority

As specified in PKIBDE's CPS.

6 Technical Security Controls

Technical security controls for PKIBDE internal components, and specifically for Root CA and Corporate CA in the TSA certificate issuing and signing processes, are detailed in the Certification Practices Statement (CPS) of the PKIBDE.

This section describes the technical security controls to be fulfilled by a Time-Stamping Authority holding a certificate issued under this CP.

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key generation for Time-Stamping Authority certificates must be carried out by the TSA itself using cryptographic hardware modules holding FIPS 140-2 Level 3 or similar, and pursuant to the provisions in its Time-Stamping Policies and Practices.

6.1.2 Delivery of private keys to subscribers

Not applicable, given that private keys must always be generated by the TSA.

6.1.3 Delivery of the public key to the certificate issuer

The public key is delivered using a file in PKCS#10 format attached to the certificate request application (CSR).

6.1.4 Delivery of the CA's public key to relying parties

The Corporate CA's public key is included in the CA's certificate. The Corporate CA's certificate is not included in the subscriber's certificate. The Corporate CA's certificate must be obtained from the repository, specifying in this document where it is available for certificate subscribers and relying parties to carry out any type of verification.

6.1.5 Key sizes

The minimum size for TSA certificate keys is 2048 bits.

6.1.6 Public key generation parameters and quality checks

TSA public keys are encoded pursuant to RFC 5280 and PKCS#1. The key generation algorithm is the RSA.

6.1.7 Key usage purposes (KeyUsage field in X.509 v3)

The keys defined by this policy and by extension the certificates associated to them, will be used to render time-stamping services and, in particular, for issuing time-stamp tokens by the TSA holding the certificate.

For this purpose, the '*Key Usage*' and '*Extended Key Usage*' fields of the certificate include the following uses:

Certificate type	Key Usage	Extended Key Usage
TSA Certificate	digitalSignature. nonRepudiation	TimeStamping

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards

As the TSA specifies in its Time-Stamping Policies and Practices.

In particular, it must have a security level equivalent to or higher than FIPS 140-2 level 3.

6.2.2 Private key multi-person (k out of n) control

As the TSA specifies in its Time-Stamping Policies and Practices.

6.2.3 Escrow of private keys

As the TSA specifies in its Time-Stamping Policies and Practices.

In particular, the private keys for TSA certificates must be housed in cryptographic hardware devices certified to FIPS-2 level 3 equivalent or above, and only accessible by the TSA.

6.2.4 Private key backup copy

As the TSA specifies in its Time-Stamping Policies and Practices.

6.2.5 Private key archive

This CP prohibits archiving the TSA private key anywhere other than in a cryptographic module.

6.2.6 Private key transfer into or from a cryptographic module

As the TSA specifies in its Time-Stamping Policies and Practices.

6.2.7 Private key storage in a cryptographic module

As the TSA specifies in its Time-Stamping Policies and Practices.

In particular, private keys must be generated in a cryptographic module at the time each of the Time-Stamp Units (TSU) making up the TSA are created and they must be stored in enciphered format.

6.2.8 Private key activation method

The TSA will activate the private key associated with the certificate issued under this CP pursuant to TSA specifications in its Time-Stamping Policies and Practices.

6.2.9 Private key deactivation method

The TSA will deactivate the private key associated with the certificate issued under this CP pursuant to TSA specifications in its Time-Stamping Policies and Practices.

6.2.10 Private key destruction method

As the TSA specifies in its Time-Stamping Policies and Practices.

6.2.11 Cryptographic module classification

The TSA cryptographic module must hold certification equivalent to or higher than FIPS-2 level 3. The specification details must be included in the Time-Stamping Policies and Practices.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archive

As specified in PKIBDE's CPS.

6.3.2 Operational period of certificates and usage periods for key pairs

TSA certificates and their associated key pair have a lifetime of 8 years, although the Corporate CA may establish a shorter period at the time of their issue.

6.4 Activation Data

6.4.1 Generation and installation of activation data

As the TSA specifies in its Time-Stamping Policies and Practices.

6.4.2 Activation data protection

As the TSA specifies in its Time-Stamping Policies and Practices.

6.4.3 Other activation data aspects

As the TSA specifies in its Time-Stamping Policies and Practices.

6.5 Computer Security Controls

6.5.1 Specific security technical requirements

As the TSA specifies in its Time-Stamping Policies and Practices.

6.5.2 Computer security evaluation

As the TSA specifies in its Time-Stamping Policies and Practices.

6.6 Life Cycle Security Controls

6.6.1 System development controls

As the TSA specifies in its Time-Stamping Policies and Practices.

6.6.2 Security management controls

As the TSA specifies in its Time-Stamping Policies and Practices.

6.6.3 Life cycle security controls

As the TSA specifies in its Time-Stamping Policies and Practices.

6.7 Network Security Controls

As the TSA specifies in its Time-Stamping Policies and Practices.

6.8 Time-Stamping

The certificates issued under this CP may be used by the holder TSA for rendering time-stamping services, as it has specified in its Time-Stamping Policies and Practices.

Hence, said TSA must guarantee the security of the time included on the time-stamp tokens it issues, by periodically synchronising them with a reliable time source.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version number

Time-Stamping Authority (TSA) certificates issued by the Corporate CA use the X.509 version 3 (X.509 v3) standard.

7.1.2 Certificate extensions

The certificate extensions used generically 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.
- *BasicConstraint*. Classified as critical.
- *CRLDistributionPoint*. Classified as non-critical.
- *Auth. Information Access*. Classified as non-critical.
- *Subject Alternate Name*. Classified as non-critical.
- *bdeCertType (1.3.6.1.4.1.19484.2.3.6)*. Classified as non-critical.

The table below shows the profile of the Time-Stamping Authority certificates issued by PKIBDE.

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: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
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

7.1.3 Algorithm Object Identifiers (OID)

Cryptographic algorithm object identifiers (OID):
- SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
- SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- SHA-512 with RSA Encryption (1.2.840.113549.1.1.13)

7.1.4 Name formats

Certificates issued by PKIBDE contain the X.500 *Distinguished Name* of the certificate issuer and that of the subject in the *issuer name* and *subject name* fields, respectively.

7.1.5 Name constraints

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

The CN *(Common Name*) attribute of the DN will be what distinguishes one DN from another. The rest of the attributes will have the following fixed values:

O=BANCO DE ESPAÑA, C=ES

7.1.6 Certificate Policy Object Identifiers (OID)

The OID of this CP is 1.3.6.1.4.1.19484.2.2.11 An X.Y format extension is added to indicate the version.

7.1.7 Use of the "PolicyConstraints" extension

No stipulation.

7.1.8 Syntax and semantics of the "PolicyQualifier

The Certificate Policies extension contains the following Policy Qualifiers:
- Element with identifier '1.3.6.1.4.1.19484.2.2.1', which corresponds with the CPS. It includes the qualifiers: 'URL CPS' with the web address to access the CPS and this CP; 'Notice Reference' with a text note on the applicable CPS.
- Element with identifier '1.3.6.1.4.1.19484.2.2.11', which corresponds with this CP. It includes the 'Notice Reference' qualifier, with a text note on this CP.

The content for certificates regulated under this policy can be seen in point *7.1.2 Certificate extensions*.

7.1.9 Processing semantics for the critical "CertificatePolicy" extension

No stipulation.

7.2 CRL Profile

7.2.1 Version number

As specified in PKIBDE's CPS.

7.2.2 CRL and extensions

As specified in PKIBDE's CPS.

7.3 OCSP Profile

7.3.1 Version number(s)

As specified in PKIBDE's CPS.

7.3.2 OCSP Extensions

As specified in PKIBDE's CPS.

8 Compliance Audit and Other Controls

8.1 Frequency or Circumstances of Controls for each Authority

As specified in PKIBDE's CPS.

8.2 Identity/Qualifications of the Auditor

As specified in PKIBDE's CPS.

8.3 Relationship between the Assessor and the Entity being Assessed

As specified in PKIBDE's CPS.

8.4 Aspects Covered by Controls

As specified in PKIBDE's CPS.

8.5 Actions taken as a result of deficiencies found

As specified in PKIBDE's CPS.

8.6 Notification of the results

As specified in PKIBDE's CPS.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No fees are applied for the issue or revocation of certificates under this Certificate Policy.

9.1.2 Certificate access fees

Access to certificates issued under this Policy is free of charge and, therefore, no fee is applicable to them.

9.1.3 Revocation or status information fees

Access to information on the status or revocation of the certificates is open and free of charge and, therefore, no fees are applicable.

9.1.4 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.

9.1.5 Refund policy

Given that there are no fees for this Certificate Policy, no refund policy is required.

9.2 Information Confidentiality

9.2.1 Scope of confidential information

As specified in PKIBDE's CPS.

9.2.2 Non-confidential information

As specified in PKIBDE's CPS.

9.2.3 Duty to maintain professional secrecy

As specified in PKIBDE's CPS.

9.3 Personal Data Protection

9.3.1 Personal data protection policy

As specified in PKIBDE's CPS.

9.3.2 Information considered private

As specified in PKIBDE's CPS.

9.3.3 Information not classified as private

As specified in PKIBDE's CPS.

9.3.4 Responsibility to protect personal data

As specified in PKIBDE's CPS.

9.3.5 Notification of and consent to the use of personal data

As specified in PKIBDE's CPS.

9.3.6 Disclosure within legal proceedings

As specified in PKIBDE's CPS.

9.3.7 Other circumstances in which data may be made public

As specified in PKIBDE's CPS.

9.4 Intellectual Property Rights

As specified in PKIBDE's CPS.

9.5 Obligations

9.5.1 Obligations of the CA

As specified in PKIBDE's CPS.

9.5.2 Obligations of the RA

As specified in PKIBDE's CPS.

9.5.3 Obligations incumbent on certificate subscribers

The specifications of the PKIBDE CPS notwithstanding, the Time-Stamping Authorities holding certificates under this CP shall also have the following obligations:

- To have a "Time-Stamping Policy" in place that complies with acknowledged best practice for the provision of time-stamping services.
- To have an updated "Time-Stamping Policies and Practices" document that describes said policy, which is accessible to the public and free of charge, which indicates its supervisors and describes its obligations and liabilities, the processes and procedures for managing and operating the TSA, key life cycles, security mechanisms, etc.
- To guarantee compliance with all the considerations and to render time-stamping services as per the requirements and procedures described in said "Time-Stamping Policies and Practices" document.
- To adhere to any additional recommendation or obligation indicated by Banco de España for rendering time-stamping services in this CP.

9.5.4 Obligations incumbent on relying parties

The specifications of the PKIBDE CPS notwithstanding, the parties relying on time-stamping services provided using certificates under this CP shall also have the following obligations:

- To be aware and accept any constraint in the use of time-stamp tokens signed with certificates issued under this CP, indicated by the corresponding “Time-Stamping Policies and Practices”.
- To be aware and to take any precaution stipulated by agreement with the Time-Stamping Authority, in order to obtain time-stamping services.

9.5.5 Obligations incumbent on other participants

As specified in PKIBDE's CPS.

9.6 Liabilities

9.6.1 PKIBDE's liabilities

As specified in PKIBDE's CPS.

9.6.2 PKIBDE liability exemption

As specified in PKIBDE's CPS.

Likewise, PKIBDE as certification services provider, shall not be held liable for the time-stamping services offered using its certificates and, in particular, for the content, reliability or accuracy of the time included on the time-stamp tokens signed and issued with its certificates.

Furthermore, neither will it be liable for any damages that may be forthcoming from the time-stamping services provider, caused by a breach of the obligations and liabilities contained in the “Time-Stamping Policies and Practices” or in this CP.

9.6.3 Scope of liability coverage

As specified in PKIBDE's CPS.

9.7 Loss Limits

As specified in PKIBDE's CPS.

9.8 Validity Period

9.8.1 Term

This CPS shall come into force from the moment it is published in the PKIBDE repository.

This CP shall remain valid until such time as it is expressly terminated due to the issue of a new version, or upon re-key of the Corporate CA keys, at which time it is mandatory to issue a new version.

9.8.2 CP substitution and termination

This CP shall always be substituted by a new version, regardless of the importance of the changes carried out therein, meaning that it will always be applicable in its entirety.

When the CP is terminated, it will be withdrawn from the PKIBDE public repository; however, it will be held for 15 years.

9.8.3 Consequences of termination

The obligations and constraints established under this CP, referring to audits, confidential information, PKIBDE obligations and liabilities that came into being whilst it was in force shall continue to prevail following its substitution or termination with a new version in all terms which are not contrary to said new version.

9.9 Individual notices and communications with participants

As specified in PKIBDE's CPS.

9.10 Specification amendment procedures

9.10.1 Amendment procedures

As specified in PKIBDE's CPS.

9.10.2 Notification period and mechanism

As specified in PKIBDE's CPS.

9.10.3 Circumstances in which the OID must be changed

As specified in PKIBDE's CPS.

9.11 Disputes and Jurisdiction

As specified in PKIBDE's CPS.

9.12 Governing Law

As specified in PKIBDE's CPS.

9.13 Compliance with applicable law

As specified in PKIBDE's CPS.

9.14 Miscellaneous provisions

9.14.1 Entire agreement clause

As specified in PKIBDE's CPS.

9.14.2 Independence

Should any of the provisions of this CP be declared invalid, null or legally unenforceable, it shall be deemed as not included, unless said provisions were essential in such a way that excluding them from the CP would render the latter without legal effect.

9.14.3 Resolution through the courts

No stipulation.

9.15 Other Provisions

No stipulation.

10 Personal Data Protection

10.1 Data Protection Legal Scheme

As specified in PKIBDE's CPS.

10.2 File Creation and Registration

As specified in PKIBDE's CPS.

10.3 Personal Data Protection Act Security Document

As specified in PKIBDE's CPS.