BANCO DE ESPAÑA
Eurosistema

20.10.2014

OID: 1.3.6.1.4.1.19484.2.2.1.1.4

Banco de España's Public Key Infrastructure

Certification Practice Statement

OVERVIEW This document covers the Certification Practice Statement (CPS) that governs the functioning and operations of Banco de España's Public Key Infrastructure (PKI).

This CPS is applicable to all participants related to Banco de España's PKI hierarchy, including the Certification Authorities (CA), Registration Authorities, Certificate Applicants and Subscribers and Relying Parties, among others.

Control Sheet

Title	Certification Practice Statement
Author	General Secretariat Legal Department Information Systems Department
Version	1.4
Date	20.10.2014

Change Log

Version	**Date**	**Change Reason**
1.0	5.04.2006	Initial Version
1.1	25.10.2006	Inclusion of new proprietary extensions (Section 7.1.2)
1.2	25.05.2010	Document review after electronic time stamping services deployment. Approval process description clarification for CP and CPS renaming Policy Approval Authority by Policy Administration Authority
1.3	07.07.2011	Revision of BdE liabilities
1.4	20.10.2014	Consolidation in a single document of the certificate policies for all the certificates issued for Banco de España's internal users

TABLE OF CONTENTS

CONTENT, RIGHTS AND OBLIGATIONS ESTABLISHED IN THIS CERTIFICATION PRACTICE STATEMENT 13

1 Introduction 13

1.1 Overview 13

1.2 Document Name and Identification 15

1.3 PKI Participants 15

1.3.1 The Policies Administration Authority 15

1.3.2 Certification Authorities 16

1.3.3 Registration Authorities 16

1.3.4 Validation Authority 16

1.3.5 Keys Archive 17

1.3.6 Certificate Subscribers 17

1.3.7 Relying Parties 17

1.3.8 Other affected parties 17

1.4 Certificate Usage 18

1.4.1 Certificate Usage Constraints and Restrictions 18

1.5 Policy Administration 18

1.5.1 The Bank of Spain, as PKIBDE owner 18

1.5.2 Contact Person 18

1.5.3 Establishment of the suitability of a CPS from an External CA as regards the PKIBDE Certificate Policies 19

1.5.4 Approval Procedure for this CPS 19

1.6 Definitions and Acronyms 19

1.6.1 Definitions 19

1.6.2 Acronyms 20

2 Publication and Repository Responsibilities 22

2.1 Repositories 22

2.2 Publication of Certification Data 23

2.3 Publication Timescale or Frequency 23

2.4 Repository Access Controls 23

3 Identification and Authentication (I&A) 24

3.1 Naming 24

3.1.1 Types of names 24

3.1.2 The need for names to be meaningful 24

3.1.3 Rules for interpreting various name formats 24

3.1.4 Uniqueness of names 24

3.1.5 Name dispute resolution procedures 24

3.1.6 Recognition, authentication, and the role of trademarks 24

3.2 Initial Identity Validation 24

3.2.1 Means of proof of possession of the private key 24

3.2.2 Identity authentication for an entity 24

3.2.3 Identity authentication for an individual 24

3.2.4 Non-verified applicant information 25

3.2.5 Validation of authority 25

3.2.6 Criteria for operating with external CAs 25

3.3 Identification and Authentication for Re-key Requests 25

3.3.1 Identification and authentication requirements for routine re-key 25

3.3.2 Identification and authentication requirements for re-key after certificate revocation 26

4 Certificate Life Cycle Operational Requirements 27

4.1 Certificate Application 27

4.1.1 Who can submit a certificate application? 27

4.1.2 Enrolment process and applicants' responsibilities 27

4.2 Certificate Application Processing 27

4.2.1 Performance of identification and authentication procedures 27

4.2.2 Approval or rejection of certificate applications 27

4.2.3 Time limit for processing the certificate applications 27

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 28

4.4 Certificate Acceptance 28

4.4.1 Form of certificate acceptance 28

4.4.2 Publication of the certificate by the CA 28

4.4.3 Notification of certificate issuance by the CA to other Authorities 28

4.5 Key Pair and Certificate Usage 28

4.5.1 Subscribers' use of the private key and certificate 28

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

4.6 Certificate Renewal 29

4.6.1 Circumstances for certificate renewal with no key changeover 29

4.7 Certificate Re-key 29

4.7.1 Circumstances for certificate renewal with key changeover 29

4.7.2 Who may request certificate renewal? 29

4.7.3 Procedures for processing certificate renewal requests with key changeover 29

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 Modification 30

4.8.1 Circumstances for certificate modification 30

4.9 Certificate Revocation and Suspension 30

4.9.1 Circumstances for revocation 30

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 revocation 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 34

4.10.3 Additional features 34

4.11 End of Subscription 34

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 Facility, Management, and Operational 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 36

5.1.7 Waste disposal 36

5.1.8 Offsite backup 36

5.2 Procedural Controls 36

5.2.1 Roles responsible for PKI control and management 36

5.2.2 Number of individuals required to perform each task 37

5.2.3 Identification and authentication of each user 38

5.2.4 Roles that require separation of duties 38

5.3 Personnel Controls 38

5.3.1 Requirements concerning professional qualification, knowledge and experience 38

5.3.2 Background checks and clearance procedures 38

5.3.3 Training requirements 38

5.3.4 Retraining requirements and frequency 38

5.3.5 Frequency and sequence for job rotation 38

5.3.6 Sanctions for unauthorised actions 38

5.3.7 Requirements for third party contracting 39

5.3.8 Documentation supplied to personnel 39

5.4 Audit Logging Procedures 39

5.4.1 Types of events recorded 39

5.4.2 Frequency with which audit logs are processed 40

5.4.3 Period for which audit logs are kept 40

5.4.4 Audit log protection 40

5.4.5 Audit log back up procedures 40

5.4.6 Audit data collection system (internal vs. external) 40

5.4.7 Notification to the subject who caused the event 40

5.4.8 Vulnerability assessment 41

5.5 Records Archival 41

5.5.1 Types of records archived 41

5.5.2 Archive retention period 41

5.5.3 Archive protection 41

5.5.4 Archive backup procedures 41

5.5.5 Requirements for time-stamping records 41

5.5.6 Audit data archive system (internal vs. external) 41

5.5.7 Procedures to obtain and verify archived information 42

5.6 Key Changeover 42

5.7 Compromise and Disaster Recovery 42

5.7.1 Incident and compromise handling procedures 42

5.7.2 Corruption of computing resources, software, and/or data 42

5.7.3 Action procedures in the event of compromise of an Authority's private key 42

5.7.4 Installation following a natural disaster or another type of catastrophe 43

5.8 CA or RA Termination 43

5.8.1 Certification Authority 43

5.8.2 Registration Authority 44

6 Technical Security Controls 45

6.1 Key Pair Generation and Installation 45

6.1.1 Key pair generation 45

6.1.2 Delivery of private keys to subscribers 45

6.1.3 Delivery of the public key to the certificate issuer 45

6.1.4 Delivery of the CA's public key to relying parties 45

6.1.5 Key sizes 45

6.1.6 Public key generation parameters and quality checks 45

6.1.7 Accepted key usage (KeyUsage field in X.509 v3) 45

6.2 Private Key Protection and Cryptographic Module Engineering Controls 46

6.2.1 Cryptographic module standards 46

6.2.2 Private key multi-person (k out of n) control 46

6.2.3 Escrow of private keys 46

6.2.4 Private key backup copy 46

6.2.5 Private key archive 46

6.2.6 Private key transfer into or from a cryptographic module 47

6.2.7 Private key storage in a cryptographic module 47

6.2.8 Private key activation method 47

6.2.9 Private key deactivation method 47

6.2.10 Private key destruction method 47

6.2.11 Cryptographic module classification 47

6.3 Other Aspects of Key Pair Management 47

6.3.1 Public key archive 47

6.3.2 Operational period of certificates and usage periods for key pairs 47

6.4 Activation Data 48

6.4.1 Generation and installation of activation data 48

6.4.2 Activation data protection 48

6.4.3 Other activation data aspects 48

6.5 Computer Security Controls 48

6.5.1 Specific security technical requirements 48

6.5.2 Computer security evaluation 48

6.6 Life Cycle Security Controls 48

6.6.1 System development controls 48

6.6.2 Security management controls 48

6.6.3 Life cycle security controls 49

6.7 Network Security Controls 49

6.8 Timestamping 49

7 Certificate, CRL, and OCSP Profiles 50

7.1 Certificate Profile 50

7.1.1 Version number 50

7.1.2 Certificate extensions 50

7.1.3 Algorithm Object Identifiers (OID) 51

7.1.4 Name formats 51

7.1.5 Name constraints 51

7.1.6 Certificate Policy Object Identifiers (OID) 51

7.1.7 Use of the "PolicyConstraints" extension 51

7.1.8 Syntax and semantics of the “PolicyQualifier 51

7.1.9 Processing semantics for the critical “Certificate Policy” extension 52

7.2 CRL Profile 52

7.2.1 Version number 52

7.2.2 CRL and extensions 52

7.3 OCSP Profile 52

7.3.1 Version number(s) 52

7.3.2 OCSP Extensions 52

8 Compliance Audit and Other Assessment 53

8.1 Frequency or Circumstances of Controls for each Authority 53

8.2 Identity/Qualifications of the Auditor 53

8.3 Relationship between the Assessor and the Entity being Assessed 53

8.4 Aspects Covered by Controls 53

8.5 Actions Taken as a Result of Deficiencies Found 53

8.6 Notification of the Results 54

9 Other Business and Legal Matters 55

9.1 Fees 55

9.1.1 Certificate issuance or renewal fees 55

9.1.2 Certificate access fees 55

9.1.3 Revocation or status information fees 55

9.1.4 Fees for other services, such as policy information 55

9.1.5 Refund policy 55

9.2 Confidentiality of Business Information 55

9.2.1 Scope of confidential information 55

9.2.2 Non-confidential information 55

9.2.3 Duty to maintain professional secrecy 56

9.3 Privacy of Personal Information 56

9.3.1 Personal data protection policy 56

9.3.2 Information considered private 56

9.3.3 Information not classified as private 56

9.3.4 Responsibility to protect personal data 56

9.3.5 Notification of and consent to the use of personal data 56

9.3.6 Disclosure within legal proceedings 56

9.3.7 Other circumstances in which data may be made public 56

9.4 Intellectual Property Rights 56

9.5 Representations and Warranties 57

9.5.1 Obligations of the CA 57

9.5.2 Obligations of the RA 58

9.5.3 Obligations of certificate subscribers 58

9.5.4 Obligations of relying parties 59

9.5.5 Obligations of other participants 59

9.6 Disclaimers of Warranties 59

9.6.1 PKIBDE's liabilities 59

9.6.2 PKIBDE liability exemption 60

9.6.3 Scope of liability coverage 60

9.7 Limitations of Liability 60

9.8 Term and Termination 61

9.8.1 Term 61

9.8.2 CPS substitution and termination 61

9.8.3 Consequences of termination 61

9.9 Individual notices and communications with participants 61

9.10 Amendments 61

9.10.1 Amendment procedures 61

9.10.2 Notification period and mechanism 61

9.10.3 Circumstances in which the OID must be changed 61

9.11 Dispute Resolution Procedures 62

9.12 Governing Law 62

9.13 Compliance with Applicable Law 62

9.14 Miscellaneous Provisions 62

9.14.1 Entire agreement clause 62

9.14.2 Independence 62

9.14.3 Resolution through the courts 63

9.15 Other Provisions 63

10 Personal Data Protection 64

10.1 Data Protection Legal Scheme 64

10.2 File Creation and Registration 64

10.3 Personal Data Protection Act Security Document 65

10.3.1 Aspects covered 65

10.3.2 Duties and obligations of the personnel 65

10.3.3 Personal Data Protection Structure 65

10.3.4 Security level 66

10.3.5 Information systems 66

10.3.6 List of users 66

10.3.7 Incident notification and management. 66

10.3.8 Backup copies and recovery. 66

10.3.9 Access control 67

10.3.10 Temporary files 67

10.3.11 Support media management 67

10.3.12 Use of real data in tests 67

CONTENT, RIGHTS AND OBLIGATIONS ESTABLISHED IN THIS CERTIFICATION PRACTICE STATEMENT

This section provides an overview of the content, rights and obligations established in this Certification Practice Statement (CPS).Its content must be supplemented with the corresponding Certificate Policy (CP), applicable to the certificate requested or being used.
It is recommended that this CPS be read fully, as well as the applicable CPs, in order to understand the purposes, specifications, regulations, rights, obligations and responsibilities governing the provision of the certification service.

- This CPS and the related documentation regulate the entire life-cycle of electronic certificates, from their request to their end of subscription or revocation, as well as the relations that are established between the certificate applicant/subscriber, the Certification Authority and the relying parties. It takes into consideration both the electronic certificates governed by Law 59/2003, dated 19 December, the Electronic Signature Act (Ley de Firma Electrónica) and the computer components electronic certificates, not considered in that Act.
- The Certification Authorities of Banco de España PKI issue different types of certificates for which there are specific Certification Policies (CP). Consequently, when requesting any kind of certificate and in order to request and use them correctly, applicants must be aware of the content of this CPS and, as appropriate, the applicable CP. The stipulations contained in the Certificate Policies shall prevail over the regulations in this CPS.
- The CPS and the CPs set out the scope of liabilities for the different parties involved, as well as their limits as regards possible damages.
- Both the CPS and the rest of the related documentation are available to certificate applicants, subscribers and relying parties on the website http://pki.bde.es.
- Certificate subscribers shall make appropriate use of certificates and shall be solely responsible for any use other than that specified in the CPS and corresponding CP.
- Certificate subscribers shall notify the Certification Authority of any modification or variation in the data provided to obtain the certificate, regardless of whether or not said data is included on the certificate itself.
- Safekeeping of the private key by certificate subscribers is an essential requirement for the security of the system. Therefore, the Certification Authority must immediately be informed of the existence of any of the causes established in the CPS for revocation/suspension of certificate validity, thus enabling suspension/revocation of the compromised certificate to prevent its illegal use by unauthorised third parties.
- Persons who wish to rely on a certificate are responsible for verifying, using the information sources provided, that the certificate and the rest of the certificates in the chain of trust are valid and have not expired or been suspended or revoked.
- The CPS and the CPs set out the scope of liabilities for the different parties involved, as well as their limits as regards possible damages.

For more information, consult the website established for this purpose at http://pki.bde.es or contact the Certification Authority by e-mail at pkibde@bde.es.

1 Introduction

1.1 Overview

This document covers the Certification Practice Statement (CPS) that governs the functioning and operations of the Public Key Infrastructure (hereinafter referred to as PKI) of Banco de España (hereinafter referred to as PKIBDE).

This CPS is applicable to all participants related to Banco de España's PKI hierarchy, including the Certification Authorities (CA), Registration Authorities, Certificate Applicants and Subscribers and Relying Parties, among others.

This CPS, 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.

Furthermore, when drafting its content, European standards have been taken into consideration, among which the most significant are:

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

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

- European Parliament and Council Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures (OJ, 19 January 2000).
- 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 (Spanish Official Gazette, 15 December).
- Spanish Royal Decree 1720/2007, of 21 December, approving Regulations for the development of Spanish Organic Law 15/1999.
- Royal Legislative Decree 1/1996, of 12 April, approving the Revised Intellectual Property Act (Spanish Official Gazette, 22 April).
- Banco de España's Circular 2/2005, of 25 February, on electronic files with personal data managed by Banco de España (Spanish Official Gazette, 22 March) and subsequent updates.

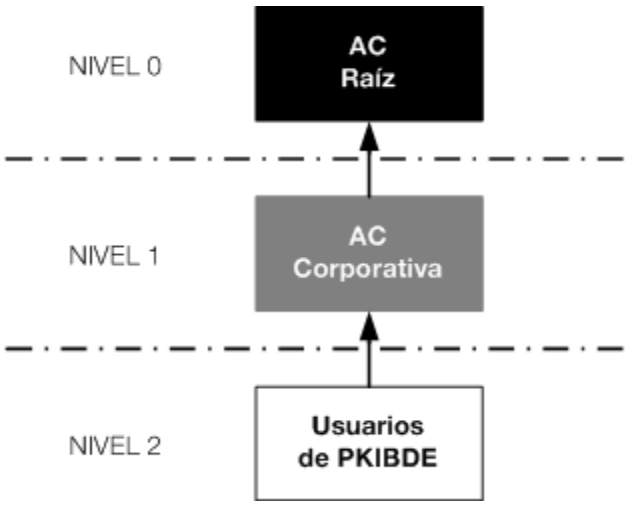
This CPS sets out the services policy, as well as a statement on the level of guarantee provided, by way of description of the technical and organisational measures established to guarantee the PKI's level of security.

The CPS includes all the activities for managing electronic certificates throughout their life cycle, and serves as a guide for the relations between PKIBDE and its users. Consequently, all the parties involved must be aware of the content of the CPS and adapt their activities to the stipulations therein.

Spanish Law 59/2003, of 19 December, the Electronic Signature Act, Section 6, limits the status of electronic signature subscribers to entities and individuals. This notwithstanding, the Certification Practice Statement is applicable both to certificates associated with individuals and, therefore, subject to the aforementioned Act, and to other different categories of certificates that are linked to computer components; that is, corporate systems and services.

This CPS assumes that the reader is conversant with the PKI, certificate and electronic signature concepts. If not, readers are recommended to obtain information on the aforementioned concepts before they continue reading this document.

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



1.2 Document Name and Identification

Document name	Certification Practice Statement of the Bank of Spain's PKI
Document version	1.4
Document status	Approved
Date of issue	20/10/2014
OID (Object Identifier)	1.3.6.1.4.1.19484.2.2.1.1.4
CPS location	http://pki.bde.es/politicas

1.3 PKI Participants

The participating entities and persons are:

- Banco de España, as owner of PKIBDE.
- The Policies Administration 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 The Policies Administration Authority

The Policies Approval Authority (PAA) is the organisation established within Information Systems Department of Banco de España as responsible for administering this CPS and PKIBDE's Certificate Policies.

The PAA is also responsible, in the event of having to evaluate the possibility of an external CA interoperating with PKIBDE, for establishing whether or not the CPS of said CA is suitable for the Certificate Policy in question.

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

1.3.2 Certification Authorities

These are the individuals, policies, procedures and computer systems entrusted with issuing the electronic certificates and assigning them to their subscribers. Additionally, they carry out the renewal or revocation of the aforementioned certificates and generate the public and private keys, when so established under their practices and policies.

The Certification Authorities that make up PKIBDE are:

- **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 08-07-2004 11:34:12 to 08-07-2034 11:34:12
Message Digest (SHA-1)	2B60 DE7D 3337 8BF7 5B67 8B10 77BB F951 6029 D6A8

- **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 29-07-2004 9:03:28 to 29-07-2019 9:03:28
Message Digest (SHA-1)	ABE6 1ED2 5AF6 4253 F77B 322F 6F21 3729 B539 1BDA

1.3.3 Registration Authorities

These are the individuals, policies, procedures and computer systems entrusted with verifying the identity of the electronic signature applicants and, when appropriate, of the attributes associated with them.

The Registration Authorities (RA) identify the certificate applicants pursuant to the rules established in this CPS and the agreement signed with the CA. When the CA is Banco de España, no agreement is required, the relations between both parties will be governed by this CPS and the applicable CP.

The Registration Authorities responsible for dealing with certification applications are defined in the corresponding Certificate Policy for each type of certificate.

The CA may use one or several freely chosen Registration Authorities (RA) to render the certifications services.

1.3.4 Validation Authority

The Validation Authority (VA) is the computer system, together with the corresponding policies and procedures, responsible for verifying the status of the certificates issued by PKIBDE, by way of the *Online Certificate Status Protocol* (OCSP), which determines the current status of an electronic

signature at the request of a Relying Party, without the need to access the Certificate Revocation Lists.
This validation mechanism is supplementary to the publication of the Certificate Revocation Lists (CRL).

1.3.5 Keys Archive

The Certificate Policies may establish the existence of a Keys Archive, which is a computer system that, together with the corresponding policies and procedures, enables the archiving and recovery of the private keys belonging to subscribers of the certificates regulated under said policies. The Keys Archive must guarantee the confidentiality of the private keys and their recovery must require the intervention of at least two people. The CP must regulate the request and processing procedures for key recovery.
Pursuant to Law 59/2003, of 19 December, the Electronic Signature Act, under no circumstances will private keys linked to electronic signature certificates be archived.

1.3.6 Certificate Subscribers

A Certificate Subscriber is any individual or computer component for which a certificate is issued within the PKIBDE environment. Certificate entitlement becomes effective once the certificate has been issued by the CA and accepted by the applicant.
The types of entities that can hold PKIBDE certificates are defined and limited in each Certificate Policy. In general terms, without prejudice to the Certificate Policy in each case, the following chart shows some of the types of PKIBDE subscribers:

Certification Environment	Subscribers
Corporate CA	Banco de España's employees
	Personnel belonging to contracted companies and external collaborators that work in the Bank's facilities
	Internal computer components
	Computer components of external entities
	PKIBDE entities
	Banco de España's Time Stamping Authority (TSABDE)

1.3.7 Relying Parties

Relying parties are individuals or entities other than subscribers that have decided to accept and rely on a certificate issued by PKIBDE
The Certificate Policies corresponding to each type of certificate determine the relying parties for each certificate. It is not the purpose of this CPS to determine these.

1.3.8 Other affected parties

Applicants: individuals, as well as computer component managers, who have applied to PKIBDE for the issue of a certificate.
User Administrators: individuals within Banco de España who process the personal certificate requests and verify that they are obtained correctly.
CA's Remote Administrators: individuals within Banco de España who manage the component certificate requests and have remote CA privileges.

1.4 Certificate Usage

1 Certificates issued by Banco de España may only be used by:

a Individuals or entities that have to deal with Banco de España because of the powers and responsibilities attributed to them under Law 13/1994, of 1 June, which grant them the status of a Central Bank and member of the European System for Central Banks.

b Its employees or contracted personnel, both in the internal and external relations necessary for the internal, inherent or operational running of the institution as for computer applications put at their disposal.

2 Within the scope of the paragraph above, certificates issued by PKIBDE may be used for financial activities, with the constraints established in each case pursuant to Section 7.3 and Section 11, letters h) and i) of the Electronic Signature Act.

The appropriate use of each certificate is established in the Certificate Policies corresponding to each type of certificate. It is not the purpose of this CPS to determine said usage.

1.4.1 Certificate Usage Constraints and Restrictions

The certificates must be used in accordance with the functions and purposes defined in their corresponding CP and may not be used for activities or purposes not included therein.

Likewise, the certificates must be used solely in accordance with the applicable legislation and especially as regards the import and export restrictions prevailing at any time concerning cryptography.

Unless otherwise specified in the CP, the certificates may not be used to act as Registration Authority or Certification Authority, or for signing public key certificates of any kind or Certificate Revocation Lists (CRL).

The certification services provided by PKIBDE have not been designed nor are they authorised for use in high risk activities or those that require fail-safe operations, such as those related to the running of hospital, nuclear or air or rail traffic control facilities, or any other where failure could lead to death, personal injury or serious environmental damage.

The Certificate Policies corresponding to each certificate may establish additional certificate usage constraints or restrictions. It is not the purpose of this CPS to establish said additional constraints and restrictions.

1.5 Policy Administration

1.5.1 The Bank of Spain, as PKIBDE owner

This CPS belongs to the Bank of Spain:

Name	Banco de España		
E-mail address	pkibde@bde.es		
Address	C/Alcalá, 48. 28014 - Madrid (Spain)		
Telephone	+34913385000	**Fax**	+34915310059

1.5.2 Contact Person

This CPS is managed by the Policiy Administration Authority (PAA) for Banco de España's PKI, belonging to the Information Systems Department:

Name	Banco de España's PKI Policy Administration Authority		
E-mail address	pkibde@bde.es		
Address	C/Alcala, 522. 28027 - Madrid (Spain)		
Telephone	+34913386666	**Fax**	+34913386875

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

In the event of having to evaluate the possibility of an external CA interoperating with PKIBDE, the Policy Administration Authority is responsible for determining whether or not the CPS of the external CA is suitable for the Certificate Policy in question. The procedures for establishing suitability are included in the CP that contemplates the possibility of operating with other CAs.

1.5.4 Approval Procedure for this CPS

Banco de España's Executive Board is accountable for approving this CPS, as well as the different Certificate Policies (CP); it has, nevertheless, authorized the Policy Administration Authority (PAA), which belongs to Information Systems Department, to elaborate and publish the needed updates to said documents, informing about them on a periodic basis.

1.6 Definitions and Acronyms

1.6.1 Definitions

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

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

Electronic Certificate: a document signed electronically by a certification services provider, which links signature verification data (public key) 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.

Computer Component (or simply, "component"): refers to any software or hardware device that may use electronic certificates, for its own use, for the purpose of its identification or for exchanging signed or enciphered data with relying parties.

Directory: data repository that is accessed through the LDAP protocol.

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.

Public Key Infrastructure: set of individuals, policies, procedures, and computer systems necessary to provide authentication, encipherment, integrity and nonrepudiation services, by way of public and private key cryptography and electronic certificates.

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 at the top level guarantees the trustworthiness of its subordinate CAs, one of which is the Corporate CA.
Provider of Certification Services: individual or entity that issues electronic certificates or provides other services related to the electronic signature.
Applicants: individuals who apply for a certificate for themselves or for a computer component.
Relying Parties: individuals or entities other than subscribers that decide to accept and rely on a certificate issued by PKIBDE.
Subscribers: individuals or computer components for which an electronic certificate is issued and accepted by said individuals or, in the case of component certificates, by the component manager.

1.6.2 Acronyms

PAA: Policy Adminstration 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
CDP: CRL Distribution Point
CEN: Comité Européen de Normalisation
CN: Common Name Distinguished Name (DN) attribute of an object within the X.500 directory structure
CSR: Certificate Signing Request: set of data that contains the public key and its electronic signature using the companion private key, sent to the Certification Authority for the issue of an electronic signature that contains said public key.
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
PIN: Personal Identification Number: password that protects access to a cryptographic card.
PKCS: Public Key Infrastructure Standards: internationally accepted PKI standards developed by RSA Laboratories
PKI: Public Key Infrastructure
PKIBDE: The Bank of Spain's PKI

PKIX: Work group within the IETF (Internet Engineering Task Group) set up for the purpose of developing PKI and internet specifications.
PCS: Provider of Certification Services.
PUK: PIN UnlocK Code: password used to unblock a cryptographic card that has been blocked after repeatedly and consecutively entering the wrong PIN.
RFC: Request For Comments (Standard issued by the IETF)

2 Publication and Repository Responsibilities

2.1 Repositories

PKIBDE's repository comprises a directory service via Microsoft Active Directory or via LDAP, in both cases for internal use of Banco de España, and a Web service, with free access. They are as follows:

Repository for CRLs of Root CA certificates:

- Active Directory (only for use from Banco de España's internal network):

ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ, CN=SNTPKI01, CN=CDP, CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES ?authorityRevocationList ?base?objectclass=cRLDistributionPoint"

- LDAP (only for use from the Banco de España's internal network):

ldap://pkildap.bde.es/CN=CRL,CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ, CN=Internas, CN=PKI, CN=Configuration, DC=BDE, DC=ES ?authorityRevocationList ?base ?objectclass=cRLDistributionPoint"

- WEB:

http://pki.bde.es/crls/ACraiz.crl

Repository for CRLs of Corporate CA certificates:

- Active Directory (only for use from Banco de España's internal network):

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

- LDAP (only for use from Banco de España's internal network):

ldap://pkildap.bde.es/CN=CRL,CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA, CN=Internas, CN=PKI, CN=Configuration, DC=BDE, DC=ES ?certificateRevocationList ?base ?objectclass=cRLDistributionPoint"

- WEB:

http://pki.bde.es/crls/ACcorporativa.crl

Online validation service that implements the OCSP protocol:

- WEB: http://pkiva.bde.es (only for use from Banco de España's internal network)

For Root CA and Corporate CA certificates:

- WEB: http://pki.bde.es/certs/ACraiz.crt
- WEB: http://pki.bde.es/certs/ACcorporativa.crt

Repository for certificates generated by Root CA:

- Active Directory (only for use from Banco de España's internal network)
- WEB (only for certain certificates): http://pki.bde.es/certs

For CPSs and CPs:

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

From these pages it is possible to access the following documents (X.Y indicates the version):

- PKIBdE_DPC-vX.Y.pdf
- PKIBdE_PC_CertUsuarioInterno-vX.Y.pdf

- PKIBdE_PC_CertComponentes-vX.Y.pdf
- PKIBdE_PC_CertComponentesEntidadesExternas-vX.Y.pdf
- PKIBdE_PC_CertTSA_ vX.Y.pdf
- PKIBdE_PST_y_DPST-vX.Y.pdf

PKIBDE's repository does not contain any information of a confidential nature.

2.2 Publication of Certification Data

It is mandatory for CAs within the PKIBDE trust hierarchy to publish information relating to their practices, their certificates and the current status of said certificates.
This CPS is public and is available on the PKIBDE website referred to in Section 2.1. *Repositories*, in PDF format.
The Certificate Policies are public and are available on the PKIBDE website referred to in Section 2.1. *Repositories*, in PDF format.
The PKIBDE Certificate Revocation Lists (CRLs) are public and are available, in CRL v2 format, in the repository and on the PKIBDE website referred to in Section 2.1. Repositories.
The Certificate Revocation Lists will be signed electronically by the PKIBDE CA that issued them.
The information on certificate status can be consulted by accessing the CRL directly or via the available online validation service that implements the OCSP.

2.3 Publication Timescale or Frequency

The CPS and the CPs 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 Section 2.1 *Repositories*.
The CA will add revoked certificates to the corresponding CRL during the period of time established under point 4.9.7 Issue Frequency of CRLs.

2.4 Repository Access Controls

Reading access to the CPS and CP is open. However, only PKIBDE is authorised to modify, substitute or eliminate information from its repository or website. For this purpose, PKIBDE will establish controls that prevent unauthorised individuals from manipulating the information contained in the repositories.

3 Identification and Authentication (I&A)

3.1 Naming

3.1.1 Types of names

All certificate holders must have a distinguished name pursuant to the X.500 standard.

The procedure for distinguished name assignment is determined in the policy drawn up for this purpose, developed and described in the Certificate Policy corresponding to the certificate in question. This policy must be in line with the general guidelines described in this chapter of the CPS.

3.1.2 The need for names to be meaningful

In all cases, it is recommended that certificate subscribers' distinguished names be meaningful.

In any case, the procedure for making distinguished names meaningful is determined in the policy drawn up for this purpose, developed and described in the Certificate Policy corresponding to the certificate in question.

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

The whole made up of the combination of the distinguished name plus the KeyUsage extension content must be unique and unambiguous.

The Certificate Policies will establish the procedures to guarantee uniqueness.

3.1.5 Name dispute resolution procedures

Any dispute concerning ownership of names will be resolved as stipulated in point 9.11 *Claims and Jurisdiction* in this CPS.

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

In the event that the key pair is generated by the certificate applicant, the possession of the private key, companion of the public key for which the certificate is being requested, shall be proven by sending the certificate signing request (CSR), which shall include the public key signed using the companion private key.

This procedure may be modified with another established in each case in the applicable Certificate Policy.

3.2.2 Identity authentication for an entity

When applicable, each CP will establish the identity authentication procedure for entities.

3.2.3 Identity authentication for an individual

The Certificate Policy applicable to each type of certificate will define the identification procedure for an individual.

It may not be decided that said procedure be less strict than other identification procedures used by Banco de España.
As a general rule, no remote means of identification shall be used, other than electronic signatures with certificates issued by PKIBDE or by other Certification Services Providers accepted by Banco de España.
Each CP will establish the data to be provided by the applicant, determining, among others, the following aspects:

- Types of identity documents valid for identification.
- CA or RA procedures to identify the individual.
- Whether or not in-person identification is required.
- Means of proof of belonging to a specific organisation.

3.2.4 Non-verified applicant information

Each CP will establish which part of the information provided in the application for a certificate shall not necessarily be verified.

3.2.5 Validation of authority

For issuance of computer component certificates, verification of the authority of the person responsible for the application for said certificates will be established in the specific CP.

3.2.6 Criteria for operating with external CAs

Before establishing interoperation with external CAs, their suitability to meet certain requirements must be established. The minimum criteria to consider a CA suitable to interoperate with PKIBDE, which may be extended in each case by the PAA, are:

- The external CA must provide a level of security in the handling of its certificates, and throughout their entire life cycle, equal, at least, to that of PKIBDE. This requirement shall be included in the corresponding CPS and CP and in their fulfilment by the CA.
- It must comply with the ETSI TS 101 456: *Policy requirements for certification authorities issuing qualified certificates* or equivalent.
- It must provide an audit report from an independent Authority of recognised prestige regarding its operations, as a means of verifying the existing level of security. The PAA may waive this requirement for CAs belonging to Public Administrations or the European System of Central Banks.
- It must establish a collaboration agreement that sets out the commitments given as regards the security of the certificates included in the interoperation.

Even when the CA fulfils the aforementioned requirements, the PAA may refuse the application for interoperation without the need to give any justification.
Interoperation may be carried out by way of cross-certification, unilateral certification or by other means.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication requirements for routine re-key

The identification and individual authentication process is defined in the Certificate Policy applicable to each type of certificate.
As a general rule, no remote means of identification/authentication shall be used, other than electronic signatures with certificates issued by PKIBDE.

3.3.2 Identification and authentication requirements for re-key after certificate revocation

The identification and individual authentication processes are defined in the Certificate Policy applicable to each type of certificate, and they must be at least as strict as those applied to the initial certificate application.

As a general rule, no remote means of identification/authentication shall be used, other than electronic signatures with certificates issued by PKIBDE.

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Each Certificate Policy establishes who can apply for a certificate and the information to be supplied in the application. Furthermore, the CP establishes the steps required to carry out this process.

4.1.2 Enrolment process and applicants' responsibilities

In general, the PKIBDE Registration Authority is responsible for establishing the suitability of the type of certificate to the characteristics of the applicants' duties, as established in the Certificate Policy in each case. The Registration Authority may authorise or refuse the certificate application.
Certificate applications, once completed shall be sent by the PKIBDE Registration Authority to the Certification Authority.
As a rule, all applicants who seek a certificate must:

- Complete the certificate application form with all the information requested by PKIBDE to issue said certificates. It should be noted that not all the information requested will appear on the certificate and that said information will be kept confidentially by the Certification Authority, pursuant to the applicable laws on personal data protection.
- Deliver the certificate application, which includes the public key, to the corresponding RA, in the event that the key pair has been generated by the applicant and the certificate is generated directly based on said request. The procedure for delivery will be established in the corresponding CP.

The existence of the application form and, in general, of the enrolment procedure for PKIBDE certificates are defined in the Certificate Policy corresponding to each certificate.

4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

The individual identification process is defined in the Certificate Policy applicable to each type of certificate. The procedure must be as strict as the other identification procedures used by Banco de España.

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. The procedure determining the nature and form of these verifications is established in the corresponding Certificate Policy.
PKIBDE may refuse to issue a certificate to any applicant based exclusively on its own criteria and without leading to any liability whatsoever for any consequences that may arise from said refusal.

4.2.3 Time limit for processing the certificate applications

The PKIBDE 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, when appropriate, and its delivery. In any case, the minimum deadlines for processing certificate applications will be established in the corresponding CPs.

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 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 entry into effect, which may not be more than 15 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.

All stipulations in this section are subject to the different Certificate Policies regarding the issue of certificates covered by said policies.

4.3.2 CA notification to the applicants of certificate issuance

Each CP will establish the manner in which applicants must be informed of the issuance of their certificates.

4.4 Certificate Acceptance

4.4.1 Form of certificate acceptance

Certificate acceptance signifies commencement of the subscribers' obligations in relation to Banco de España's PKI

Certificates that require identification in person shall carry certificate subscribers' explicit acceptance and acknowledgement that they are in agreement with the terms and conditions contained in the terms and conditions acceptance form for the certification services provided by the Banco de España's Certification Authority, which govern the rights and obligations assumed between PKIBDE and subscribers. Likewise it shall also carry express declaration that the subscribers are aware of the existence of this Certification Practice Statement, which sets out the technology and operations of the electronic certificate services provided by PKIBDE.

For online renewals, terms and conditions acceptance may be carried out by way of the electronic signature.

The corresponding CP may detail or extend the manner in which certificates are accepted.

4.4.2 Publication of the certificate by the CA

Publication of certificates in PKIBDE's repository shall be established in each CP.

4.4.3 Notification of certificate issuance by the CA to other Authorities

When a PKIBDE CA issues a certificate pursuant to a certificate application processed through an RA, it shall send a copy of the same to the RA that forwarded the application.

4.5 Key Pair and Certificate Usage

4.5.1 Subscribers' use of the private key and certificate

The responsibilities and constraints relating to the use of key pairs and certificates will be established in the corresponding CP.

Subscribers may only use the private key and the certificate for the uses authorised in the CP and in accordance with the 'Key Usage' and 'Extended Key Usage' fields of the certificate. 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 end-of-life or revocation, subscribers must discontinue the use of the private key.

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

Relying parties may only rely on the certificates as stipulated in the corresponding CP and in accordance with the 'Key Usage' field of the certificate.

Relying parties must successfully perform public key operations as a condition for relying on a certificate and are obliged to check the status of a certificate using the mechanisms established in this CPS and the corresponding CP. Likewise, they accept the obligations regarding the conditions of use set forth in those documents.

4.6 Certificate Renewal

4.6.1 Circumstances for certificate renewal with no key changeover

All certificate renewals covered by this CPS 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 Statement, their content is "no stipulation".

4.7 Certificate Re-key

4.7.1 Circumstances for certificate renewal with key changeover

The certificate renewal procedure shall depend on the Certificate Policy applicable to each type of certificate.

A 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 certificate renewals covered by this CPS shall be carried out with change of keys.

4.7.2 Who may request certificate renewal?

Renewal must be requested by certificate subscribers, although not all certificates include this option. Each Certificate Policy will establish who may request certificate renewal.

4.7.3 Procedures for processing certificate 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 is still valid. If any of the subscriber's data have changed, they must be verified and registered with the agreement of the subscriber.

In general, there are two possible certificate renewal identification and verification scenarios:

- Renewal due to end-of-life of a certificate for internal user: in this case renewal must be requested in person at the places of registration, as established for initial issuance.
- Renewal of a component certificate: all renewals may be carried out remotely, making the request by way of identification using a valid certificate issued by PKIBDE or another CPS accepted by Banco de España, or using any other mechanisms established in the Certificate Policies.

These guidelines are subject to the Certificate Policy applied to each certificate, which shall always prevail over the stipulations in this point.
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

Each CP shall establish the manner in which applicants will be informed that the corresponding certificate has been issued in their name.

4.7.5 Manner of acceptance of certificates with changed keys

Each CP shall establish the manner of acceptance.

4.7.6 Publication of certificates with the new keys by the CA

Each CP shall establish, as appropriate, the procedure for publishing the certificates in the PKIBDE repository.

4.7.7 Notification of certificate issuance by the CA to other Authorities

When a PKIBDE CA issues a certificate pursuant to a certificate application processed through an RA, it shall send a copy of the same to the RA that forwarded the application.

4.8 Certificate Modification

4.8.1 Circumstances for certificate modification

Certificate modification takes place when a new one is issued due to changes in the certificate information not related to its public key or end-of-life of the certificate.
Certificate modification may be due to causes such as:

- Change of name.
- Change of duties within the organisation.
- Reorganisation resulting in a change in the DN.

All certificate modifications carried out within the scope of this CPS 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.

The revocation request process is defined in the Certificate Policy applicable to each type of certificate.
Revocation of a certificate entails its publication on the public-access Certificate Revocation Lists (CRL). Once the period of validity of a revoked certificate has expired, it is removed from the CRL.

Causes for revocation:
Notwithstanding the applicable legislation, a certificate may be revoked in the following cases:
- 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 on the Acceptance Form for the terms and conditions of the certification services provided by Banco de España's Certification Authority, in the associated CP or in this CPS.
- The subscriber ceases to belong to the group, when said membership granted the subscriber the right to hold the certificate.
- PKIBDE ceases its 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 of the subscriber or an authorised third party.
- The certificate of a higher RA or CA in the certificate trust hierarchy is revoked.
- The existence of any other cause specified in this CPS or in the corresponding Certificate Policies established for each type of certificate.

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 subscriber's private key has been compromised, or in the event of any other determining factor that recommends taking such action.
Additionally, certificate subscribers or, in the case of component certificates, component managers may also request revocation of their certificates, which must be carried out in accordance with the conditions specified in point 4.9.3.
The identification policy for revocation requests may be the same as that of the initial registration.
The authentication policy shall accept revocation requests signed electronically by the certificate subscriber, as long as it is done using a valid certificate other than the one for which the revocation is requested.
The different Certificate Policies may establish other identification procedures of a stricter nature.

4.9.3 Procedures for requesting certificate revocation

The revocation request procedure for each type of certificate shall be established in the corresponding Certificate Policy.

In general, notwithstanding the CP:

- Subscribers shall be notified of the revocation of their certificates by e-mail. Following certificate revocation, subscribers must discontinue use of the private key pertaining to said certificate.
- Certificate revocation requests received after the date of expiry will be not be processed.

The information required to request certificate revocation shall be established at the expense of that specified in the corresponding Certificate Policy.

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

Each CP shall establish the maximum time allowed for processing revocation requests. Notwithstanding the aforementioned, it is hereby established that said time shall, as a rule, will be less than 24 hours.

4.9.6 Requirements for revocation verification by relying parties

Revocation verification, whether by directly consulting the CRL or using the OCSP protocol, is mandatory for each use of the certificates by relying parties.

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. Certificate Revocation Lists stored in cache[1] memory, even when not expired, do not guarantee availability of updated revocation data.

Optionally, unless the applicable CP establishes otherwise, the Validation Authority may be used for revocation verification.

When the CP accepts other forms of revocation data publication, the requirements for checking said data will be specified in the CP itself.

4.9.7 CRL issuance frequency

PKIBDE shall publish a new CRL in its repository whenever a revocation occurs. In any case, PKIBDE shall publish a new CRL in its repository at least every 24 hours for Subordinated CAs and at least every 15 years for the Root CA, even when the CRL has not been modified; that is, even when no certificate has been revoked since the previous publication.

4.9.8 Maximum latency between the generation of CRLs and their publication

Each CP will establish the maximum time allowed between generation of the CRLs and their publication in the repository.

4.9.9 Online certificate revocation status checking availability

PKIBDE provides a web server on which it publishes the CRLs for verification of the status of the certificates it issues. Additionally, there is a Validation Authority that, via OCSP protocol, enables certificate status verification.

---

[1]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.

The web addresses for access to the CRLs and the Validation Authority are set out in point 2.1 *Repositories*.

4.9.10 Online revocation checking requirements

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

4.9.11 Other forms of revocation alerts available

Some CPs may accept other forms of revocation alerts, such as CRL Distribution Points (CDP).

4.9.12 Special requirements for the revocation of compromised keys

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

4.9.13 Causes for suspension

Suspension of certificate validity shall be applied (when said operation is included in the corresponding CP), in the following cases, among others:

- Temporary change of any of the certificate subscribers' circumstances that make it advisable to suspend the certificates for the duration of said change. Upon return to the initial situation, the certificate suspension will be lifted. The characteristics of and requirements for the suspension will be established in the corresponding Certificate Policy.
- Notification by certificate subscribers of the possible compromise of their keys. In the event that the suspicion, due to the level of certainty, does not warrant immediate revocation, the certificates of the subscriber in question will be suspended until the possible compromise of the keys has been established. Once the study has been completed, a determination will be made as to whether the certificates are to be revoked or the suspension lifted.
- Legal or administrative decisions that so order.

4.9.14 Who can request the suspension?

Requests may be submitted by the certificate subscriber or the person established by the corresponding CP.

4.9.15 Procedure for requesting certificate suspension

Each CP shall establish the procedure for requesting certificate suspension.

4.9.16 Suspension period limits

Notwithstanding the content of the Certificate Policies, PKIBDE will suspend validity of certificates for a maximum of 1 year, following which the certificates will be revoked, unless certificate suspension has been lifted in advance.

Expiry or request for revocation of a certificate during the period of suspension shall have the same effect as in the case of expiry or request for revocation of non-suspended certificates.

4.10 Certificate Status Services

4.10.1 Operational characteristics

PKIBDE has at least two services that provide information on the status of certificates issued by its CA:

- Publication of Certificate Revocation Lists (CRL). Access to CRLs can be obtained via Active Directory or LDAP (only relying parties located in Banco de España's internal network) and HTTP (all relying parties).
- Online validation service (Validation Authority, VA) that implements the RFC 2560 Online Certificate Status Protocol. Using this protocol, the current status of an electronic certificate can be determined without using the CRLs. An OCSP client sends a certificate status request to the VA, which in turn, after consulting the CRLs it has available, sends a reply regarding the certificate status via HTTP. This service is only available for relying parties located within the Banco de España's internal network.

4.10.2 Service availability

The service, in its two varieties, is available permanently, every day of the year, both for Banco de España's internal relying parties and external relying parties.

4.10.3 Additional features

To use the online validation service, relying parties must have an RFC 2560 compliant OCSP client.

4.11 End of Subscription

Certificate subscription may be ended due to the following causes:

- 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 policies and practices for key registration and recovery shall be identified in each CP that establishes private key escrow.

No private key for any certificate in which the nonrepudiation electronic signature functionality has been authorised shall be escrowed. This can be verified by checking whether or not the 'Key Usage' code is 1 in the 'Nonrepudiation' field.

4.12.2 Session key protection and recovery policies and practices

When appropriate, the corresponding CP will identify the policies and practices for the protection and recovery of session keys.

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

The aspects related to physical security controls are set out in detail in the documentation drawn up for this purpose by the Banco de España's Security Services and Information Systems department. This point establishes the most significant measures taken.

5.1.1 Site location and construction

The building in which the PKIBDE infrastructure is located has access control security measures that permit duly authorised personnel to access the building.

All PKIBDE's critical operations are carried out in physically secure facilities, with specific levels of security for the most critical elements. These systems are separate from other Banco de España's systems, meaning that only authorised personnel may access them.

The PKIBDE Data Processing Centres meet the following physical requirements:

a They are distant from smoke ventilation points to avoid possible damage from fires on other floors.

b Absence of windows to the outside of the building.

c Surveillance cameras in restricted access areas.

d Access control based on card and password.

e Fire protection and prevention systems: detectors, extinguishers, personnel training on what steps to take in the event of fire, etc.

f Transparent partitions that delimit the different zones and enable observation of the rooms from the access passageways, in order to detect intrusions or illicit activity inside.

g Cabling, both for data transmission and telephony, protected against damage and interception.

5.1.2 Physical access

There is a complete system to control physical access by individuals at the entry and exit, comprising various levels of security. All sensitive operations are carried out within a physically secure facility with different levels of security required to access critical machinery and applications.

PKIBDE systems are separated from other Banco de España's systems in such a way that only authorised personnel may access them, guaranteeing the independence of the other computer systems.

Loading and unloading areas are isolated and under permanent surveillance, by human and technical means.

5.1.3 Power and air-conditioning

The rooms in which PKIBDE infrastructure equipment is located have suitable power supply and air-conditioning for the requirements of the equipment installed in them. The infrastructure is protected against power failures or any other electricity supply anomaly. Systems that so require have permanent power supply units as well as a generator.

5.1.4 Water exposure

Appropriate measures have been taken to prevent exposure of the equipment and cables to water.

5.1.5 Fire prevention and protection

The rooms have the suitable means (detectors) to protect their content against fire.

Cabling is installed under a false floor or above a false ceiling and the appropriate means (detectors in the floor and ceilings) have been installed to protect them against fire.

5.1.6 Storage system

PKIBDE has established all the necessary procedures to make backup copies of all its productive infrastructure data.

PKIBDE has organised backup copy plans, the same as those used in the rest of Banco de España's central infrastructure, for all the sensitive data and those considered necessary for activity continuity.

5.1.7 Waste disposal

A waste management policy has been adopted that guarantees destruction of any material that could contain information, as well as a management policy for removable media.

5.1.8 Offsite backup

PKIBDE has backup copies in two of its own premises, which have the necessary security measures in place and are suitably physically separated.

5.2 Procedural Controls

For security reasons, the information related to procedural controls is considered confidential and only part of this is included herein.

PKIBDE endeavours to ensure that all management, related to both operational and administrative procedures, is carried out in a secure manner, pursuant to the guidelines in this document, carrying out periodic audits. (See Chapter 8 *Performing audits and other conformity controls*).

Additionally, duties have been divided to prevent a single person from obtaining control of the entire infrastructure.

5.2.1 Roles responsible for PKI control and management

The following responsibilities are established for control and management of the system:

PKI Administrators. Three different functions are established for PKI administration:

- *HSM Administrators*: A group of 7 Administrators has been established for the HSM of the Root CA and 6 for the Corporate CA, each with a cryptographic card to control access to their functions. To carry out the operations that require the role of Administrator, a total of 2 cards must be inserted in the HSM, of the 7 or 6 established, depending on whether it is the Root CA or the Corporate CA. The HSM Administrators are responsible for carrying out the following operations:

  1 Recovery of cryptographic hardware functionality in the event of HSM failure.

  2 Key recovery in the event of accidental deleting.

  3 Replacement of a set of administrator cards. This operation only needs to be carried out when increasing or reducing the number of administrator cards.

  4 Replacement of a set of operator cards. This operation only needs to be carried out when increasing or reducing the number of operator cards or to replace the existing one due to deterioration

  5 Increase in the number of HSM integrated in the infrastructure.

  6 Given that operation is carried out in FIPS140-2 Level 3 mode, authorisation for the generation of operator and keys sets. This operation is only required during the CA's key generation protocol.

- *HSM Operators*: A group of 5 operators for both the Root and Corporate CAs is established, each with a cryptographic card to control access to their functions. To use the keys protected by

the set of operator cards, two operator cards need to be inserted in the HSM reader. The HSM Operators are responsible for carrying out the following operations:

1 Key activation for their use. This means that each initiation of a CA requires the insertion of the operator cards linked to the keys.

2 Authorisation for application key generation, although this authorisation may also be carried out by an Administrator. This operation is only required during the CA's key generation protocol.

3 Booting of the CA configuration interface and those of the other entities that make up the PKI. Through this interface, the operator can modify the Certificate Policies and define the CA's remote administrators.

Operations carried out by operators are more frequent than those carried out by Administrators, as they must intervene whenever the CA needs to be reconfigured or when one of the processes involved in PKIBDE needs to be rebooted.

- *CA's Remote Administrators*: Once the PKI processes have been initiated by the HSM operators, the administration / management tasks during the life cycle of the certificates issued by the CA will be carried out by the Remote Administrators. These Administrators are responsible for:

1 Issuance of the user certificates in the cases established by the CP.

2 Issuance of component certificates.

3 Certificate revocation and suspension.

4 Suspension of services.

Each CA Remote Administrator must have a certificate to authenticate. Generation of user certificates that enable these Administrators to exchange requests with the CA will be carried out by the HSM operators, via the CA Administration Interface.

Systems Administrator: responsible for the operation of the systems that make up the PKI, the hardware and the base software. The responsibilities of this profile include, among others, administration of the database system, the repository and the operating systems.

Security Co-ordinator: responsible for establishing and verifying all physical and computer security procedures.

Policy Administration Authority: authority responsible for establishing and approving the Certificate Policies.

Audit Administrator: responsible for carrying out and reviewing internal audits of the system.

Backup Administrator: responsible for carrying out and reviewing the backup copies of the system.

User Administrators: responsible for processing personal certificate requests, controlling their correct download by subscribers and subscribers' acceptance of the terms and conditions of use.

5.2.2 Number of individuals required to perform each task

A minimum of two people with sufficient professional capacity are required to perform the tasks of HSM Administration and Operation set out under point 5.2.1 *Roles responsible for PKI control and management*.

5.2.3 Identification and authentication of each user

The HSM Administrators and Operators are identified and authenticated in the HSMs by way of shared secrecy techniques in specific HSM cryptographic cards.

The rest of the PKIBDE authorised users are identified by way of electronic certificates issued by the PKI and authenticated by way of cryptographic cards.

5.2.4 Roles that require separation of duties

Personnel assignment will ensure that the following rules of incompatibility are complied with:

- An HSM Administrator may not be an Audit Administrator.
- A Systems Administrator may not be a Security Co-ordinator or an Audit Administrator.
- A Security Co-ordinator may not be a Systems Administrator, nor a CA Remote Administrator or an Audit Administrator.
- An Audit Administrator may not be an HSM Administrator, nor a Systems Administrator, User Administrator, CA Remote Administrator, or a Security Co-ordinator.

5.3 Personnel Controls

5.3.1 Requirements concerning professional qualification, knowledge and experience

All personnel working in the PKIBDE environment must have sufficient knowledge, experience and training for optimum performance of their assigned duties.

Therefore, Banco de España carries out the personnel selection processes it considers necessary to ensure that the professional profiles of personnel are the most suitable to the features inherent to the tasks to be carried out.

5.3.2 Background checks and clearance procedures

In accordance with personnel selection procedures established by Banco de España.

5.3.3 Training requirements

In accordance with to procedures established by Banco de España.

Specifically, personnel related to PKI operations will receive the necessary training to ensure the correct performance of their duties. The following aspects are included in the training:

- Delivery of a copy of the Certification Practices Statement.
- Awareness programmes for physical, logical, and technical security.
- Operation of the software and hardware corresponding to each specific role.
- Security procedures corresponding to each specific role.
- Operational and administrative procedures for each specific role.
- Procedures for PKI operations recovery in the event of catastrophe.

5.3.4 Retraining requirements and frequency

In accordance with to procedures established by Banco de España.

5.3.5 Frequency and sequence for job rotation

No stipulation.

5.3.6 Sanctions for unauthorised actions

Unauthorised action shall be classified as a work offence, sanctioned pursuant to Banco de España's Labour Regulations and in the Workers' Statute, without prejudice to the liabilities of any other kind that may be incurred.

5.3.7 Requirements for third party contracting

Banco de España's general regulations shall be applied to contracting.

5.3.8 Documentation supplied to personnel

Access will be given to the mandatory security regulations together with this CPS and those contained in the applicable CP.

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

The operations are divided into events, so data on one or more events are logged for each relevant operation. The events recorded include, at least, the following data:

Category: Indicates the importance of the event.

- Information: the events in this category contain data on operations carried out successfully.
- Mark: every time an administration session is initiated or terminated, an event of this category is recorded.
- Alert: indicates that an unusual occurrence was detected during the operation, but it did not cause an operation failure (for example a refused batch request).
- Error: indicates an operation failure due to a predictable error (for example, a batch that was not processed because the RA requested a certificate template for which it was not authorised).
- Fatal Error: indicates that there was an exceptional occurrence during an operation (for example, failure to access a database table).

Date: Date and time of the event.

Author: Distinguished Name of the Authority that generated the event.

Role: Type of Authority that generated the event.

Event Type: Identifies the type of event, differentiating between, among others, cryptographic, user interface or library events.

Event ID: Number that uniquely identifies an event among a group of events of the same type, generated by the same module.

Module: Identifies the module that generated the event. The possible modules are:

- CA.
- RA.
- Information Repository.
- Data storage control libraries.

Level: Number that indicates the level at which the event is located. The events produced by some operations are organised hierarchically, so an event may group other events from a lower level, depending on the complexity of the operation. For level-one events, this field will indicate a value of 1. For second and successive level events, it will indicate the corresponding value. Events to which this characteristic is not applicable will be assigned a value of 0.

Remarks: Textual representation of the event. For some events the description is followed by a list of parameters, the values of which will vary depending on the data on which the operation was carried out.

Some examples of parameters that are included for the description of the "Generated Certificate" event are: the serial number, the distinguished name of the subscriber of the certificate issued and the certificate template applied.

The events registered in the database may be subject to certificate types, specified in the Certificate Policy.

5.4.2 Frequency with which audit logs are processed

Logs are analysed manually when necessary, and there is no established frequency for this process.

5.4.3 Period for which audit logs are kept

The information generated in the audit logs is kept online until it is archived. Once archived, audit logs are kept for at least 5 years.

5.4.4 Audit log protection

Events logged by the PKI are protected by encipherment in such a way that they can only be accessed by the event viewing applications and with the appropriate access controls.
Destruction of an audit archive can only be carried out with the authorisation of PKIBDE's Systems Administrator, Security Co-ordinator and Audit Administrator. Said destruction may be carried out by written recommendation from any of the three Authorities or the audited service's Administrator.

5.4.5 Audit log back up procedures

Backup copies of audit logs are made in accordance with the standard measures established by Banco de España for Central Computer Database backup copies.

5.4.6 Audit data collection system (internal vs. external)

The PKI's system for compiling audit data is a combination of automatic and manual processes carried out by the PKI applications. All the CA, RA and Remote Administrators' logs are stored in PKIBDE internal systems.
All the significant elements in PKIBDE are accumulated in a Database. The security control procedures employed by PKIBDE are based on the construction technology used in the database.
The system's features are as follows:

- It enables verification of database integrity; that is, it detects any possible fraudulent manipulation of the data.
- It ensures nonrepudiation by the authors of operations carried out on the data. This is achieved using electronic signatures.
- It keeps a historical log of data updating; that is, it stores successive versions of each log resulting from the different operations carried out. This makes it possible to log the operations carried out and prevent loss of electronic signatures carried out previously by other users when the data is updated.

The following list is a summary of the possible risks to which a database may be exposed, which can be detected with the integrity tests:

- Fraudulent insertion or alteration of a session log.
- Fraudulent elimination of intermediate sessions.
- Fraudulent insertion, alteration or elimination of a historical log.
- Fraudulent insertion, alteration or elimination of a log query table.

5.4.7 Notification to the subject who caused the event

No automatic notification of audit log file actions to the subject who caused the event has been established.

5.4.8 Vulnerability assessment

Vulnerability assessment is covered by Banco de España's Audit Plan.

5.5 Records Archival

5.5.1 Types of records archived

Each Certificate Authority within in PKIBDE stores, for the established periods, all the information related to the operations carried out with certificates and keeps an events log.

Logged operations include those carried out by the administrators who use the PKIBDE element administration applications, as well as all the data related to the registration process.

The types of data or files archived include, among others:

- Data related to certificate application and registration processes.
- Those specified under point 5.4.1.
- Keys historical archive.

5.5.2 Archive retention period

All the information related to certificates is held for a period of 15 years, which is the legally mandated period for recognised certificates.

For audit logs, point 5.4.3 shall apply, always taking into account any specific particularity of the Certificate Policy for the certificate corresponding to the data involved.

5.5.3 Archive protection

Log Archives are protected by encipherment in such a way that they can only be accessed by the event viewing applications and with the appropriate access controls.

Destruction of a log archive can only be carried out with the authorisation of PKIBDE's Systems Administrator, Security Co-ordinator and Audit Administrator. Said destruction may be carried out by written recommendation from any of the three Authorities or the audited service's Administrator.

5.5.4 Archive backup procedures

Backup copies of log archives are made in accordance with the standard measures established by Banco de España for Central Computer Database backup copies.

5.5.5 Requirements for time-stamping records

The information systems employed by PKIBDE guarantee logging of the time at which the log entries were made. The moment in time in the systems comes from a secure source that establishes the date and time. Specifically, the clock signal comes from:

- The atomic clock in Braunschweig, Germany (Physikalisch Technische Bundesanstalt), which represents the official time within Eurosystem. It is encrypted and transmitted via radio.
- From Real Instituto y Observatorio de la Armada (ROA), which is accountable for maintaining the basic unit of Time, declared with legal effects as National Pattern for said unit, as well as for the maintenance and official broadcast of the scale “Universal Coordinated Time” (UTC(ROA)) to be considered to all intents and purposes as the base for the legal time in all national territory (R.D. 23 October 1992, num. 1308/1992).

5.5.6 Audit data archive system (internal vs. external)

Data collection is internal to the Authority and corresponds to PKIBDE.

5.5.7 Procedures to obtain and verify archived information

Events logged by the PKI are protected by encipherment in such a way that they can only be accessed by the event viewing and management applications.

This verification must be carried out by the Audit Administrator, who must have access to the verification and integrity control tools for the PKI events log.

5.6 Key Changeover

The procedures to provide subscribers and relying parties of the certificates of the former with a new CA public key, in the event of key changeover, are the same as those used to provide the current public key. Consequently, the new key will be published in the PKIBDE repository (see point 2.1)

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

Banco de España has established a Contingency Plan that sets out the actions to be taken, resources to be used and personnel to be employed in the case of a deliberate or accidental event that renders useless or deteriorates the resources or certification services provided by PKIBDE.

The Contingency Plan deals with the following aspects, among others:

- Redundancy of the most critical components.
- Start-up of an alternative backup centre.
- Complete and periodic checks of the backup copy service.

In the event of any compromise of the signature verification data of any Certification Authority, PKIBDE shall inform all PKIBDE certificate subscribers and relying parties known that all the certificates and revocation lists of certificates signed with said data are no longer valid. Service will be re-established as soon as possible.

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

If computing resources, software, and/or data are corrupted or suspected to be corrupted, PKI operations will be halted until the environment's security has been re-established, with the incorporation of new components, the suitability of which can be accredited. At the same time, an audit will be carried out to identify the cause of the corruption and ensure it does not reoccur.

In the event that issued certificates are affected, the users of the same will be notified and new certificates issued.

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

If an Authority's private key is compromised, it will be revoked immediately. The corresponding CRL will then be generated and published and the Authority's activity ceased, carrying out the generation, certification and start-up of a new Authority with the same name as the eliminated one and with a new key pair.

In the event that the Authority affected is a CA, its revoked certificate shall remain accessible in the PKIBDE repository in order to continue verifying the certificates issued whilst it was operational.

The Authorities that make up PKIBDE that are dependent on the affected CA will be informed of the situation and urged to request new certification by the CA with its new key.

All the affected Authorities will be notified that the certificates and revocation data, supplied with CA's compromised key, cease to be valid from the moment of notification, so they must use the CA's new public key to verify data validity.
Certificates signed by the Authorities dependent on the affect CA during the period between key compromise and the corresponding certificate revocation will likewise be revoked, notifying their subscribers of this circumstance and issuing new certificates.

5.7.4 Installation following a natural disaster or another type of catastrophe

The PKIBDE Certification Authority system can be reconstructed in the event of disaster. Carrying out this reconstruction requires:

- A system with hardware, software and a Security Cryptographic Hardware device similar to that which existed prior to the disaster.
- Administrator cards for all the PKIBDE Certification Authorities.
- A backup copy of the system disks prior to the disaster.

With these elements it is possible to reconstruct the system as it was at the time the backup copy was made and, therefore, recover the CA, including its private keys.
Storage, both of the CA Administrator access cards and of the copies of each CA's system disks is carried out in a different place, sufficiently distant and protected in order to avoid, as far as possible, concurrence of simultaneous disasters in the production and recovery element systems.

5.8 CA or RA Termination

5.8.1 Certification Authority

In the event of termination of activities of a CA, PKIBDE will ensure that the potential problems for its certificate subscribers and relying parties are kept to a minimum, as well as ensuring maintenance of the records required to provide certified proof of the certificates for legal purposes.
In the event of termination of the activities of one or all of the CA's, PKIBDE will notify their certificate subscribers and relying parties, by any means that guarantee sending and receipt of said notifications and with a minimum notice of 2 months prior to the termination of activities, that it intends to have the corresponding CA/CAs discontinue its/their activities as certification services provider/s.
In the event the PKIBDE decides to transfer the activity to another Certification Services Provider, it shall notify its certificate subscribers regarding the transfer agreements. For this purpose, PKIBDE shall send a document explaining the transfer terms and conditions and the characteristics of the Provider to which it proposes to transfer certificate management. This notification shall be carried out by any means that guarantee sending and receipt of the notification, at least two months prior to the effective termination of its activities.
PKIBDE shall notify the Ministry of Industry, Trade and Tourism, with the advance notice indicated in the previous paragraph, of the termination of its activities and the destination of the certificates, specifying whether their management is to be transferred and to whom, or whether their validity is to be terminated.
Likewise, it shall report any other relevant circumstance that could prevent activity continuity.
PKIBDE shall send the Ministry of Industry, Trade and Tourism, prior to final termination of its activity, the data related to the certificates for which validity has been terminated, so that it can take custody of them for the purposes established under Section 20.1.f of the Electronic Signature Act.

Once two months have elapsed without any transfer agreement having been drawn up, the certificates will be revoked.

5.8.2 Registration Authority

Once the Registration Authority ceases to carry out its duties, it shall transfer the records it holds to PKIBDE, when the obligation subsists to maintain the information on file; otherwise, it will be destroyed.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Key pairs for internal PKIBDE components, specifically Root CA and Corporate CA, are generated in cryptographic hardware modules with FIPS 140-2 Level 3 certification, installed in their respective systems. The hardware and software systems used are compliant with the CWA 14167-1 and CWA 14167-2 standards.

The key pairs for the rest of the subscribers are generated as stipulated in the applicable Certificate Policy for each certificate.

The hardware and software devices to be used in the generation of keys for each type of certificate issued by PKIBDE are determined by the applicable Certificate Policy.

6.1.2 Delivery of private keys to subscribers

The method used to deliver private keys to their subscribers depends on each certificate and is established in the Certificate Policy corresponding to each certificate.

6.1.3 Delivery of the public key to the certificate issuer

The method used to deliver the public key to the issuer when it is generated by the subscriber will depend on each certificate and will be established in the Certificate Policy corresponding to each certificate.

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

The public key of the Root CA and the Corporate CA are made available to relying parties in the PKIBDE repository (see point 2.1), notwithstanding the possibility of the CP establishing additional mechanisms for the delivery of said keys.

6.1.5 Key sizes

Root CA and Corporate CA key sizes are 2048 bits.

The size of the keys for each type of certificate issued by PKIBDE is defined in the applicable Certificate Policy.

6.1.6 Public key generation parameters and quality checks

Root CA and Corporate CA keys are encoded pursuant to RFC 3280 and PKCS#1. The key generation algorithm is the RSA.

The key generation parameters for each type of certificate issued by PKIBDE are determined in the applicable Certificate Policy.

The procedures and means of checking the quality of the key generation parameters for each type of certificate issued by PKIBDE are determined in the applicable Certificate Policy.

6.1.7 Accepted key usage (KeyUsage field in X.509 v3)

The accepted key usage for each type of certificate issued by PKIBDE is defined in the applicable Certificate Policy.

All certificates issued by PKIBDE contain the *Key Usage* extension defined under the X.509 v3 standard, which is classified as critical. Additional constraints may be established through the *Extended Key Usage* extension.

It should be noted that the efficiency of constraints based on certificate extensions can sometimes depend on the operational characteristics of computer applications that have not been designed by PKIBDE.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards

The modules used to create keys used by Root CA and Corporate CA comply with FIPS 140-2 Level 3 certification.

Start-up of each one of the Certification Authorities, taking into account that a Hardware Security cryptographic Module (HSM) is used, involves the following tasks:

a HSM module status boot up.

b Creation of administration and operator cards.

c Generation of the CA keys.

PKIBDE uses hardware and software cryptographic modules available commercially, developed by third parties. PKIBDE only uses cryptographic modules with FIPS 140-2 Level 3 certification that comply with the following standards:

- FCC: CRFA47, Section 15, Subsection B, Class A
- EC: EN 55022 Class A, EN 55024-1, EN 60950

As regards the cryptographic cards with advanced electronic signature certificates, suitable for secure signature creation devices, they comply with the CC EAL4+ security level, although the equivalent ITSEC E3 or FIPS 140-2 Level 2 certifications are also acceptable.

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

Both the Root CA and Corporate CA private keys are under multi-person control[1]. This is activated by booting the CA software using a minimum combination of operators from the corresponding CA. It is the only method to activate said private key.

Two PKIBDE operators, out of a total of five, are necessary to activate and use PKIBDE's Root CA and Corporate CA private keys.

6.2.3 Escrow of private keys

Escrow of the private keys for the certificates is carried out by their subscribers. PKIBDE encipherment private keys are only escrowed by archiving them.

The private keys of the Certification Authorities that make up PKIBDE are housed in cryptographic hardware devices with FIPS-2 Level 3 certification linked to each of the CAs.

6.2.4 Private key backup copy

The private keys of PKIBDE CAs are archived under the protection of the HSMs belonging to each of them and to which only the administrators and operators of the corresponding CAs have access.

6.2.5 Private key archive

Private keys for signatures of individuals are never archived in order to guarantee nonrepudiation.

[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.

Encipherment private keys are archived and their recovery procedures are established in their CPs.

6.2.6 Private key transfer into or from a cryptographic module

Private keys can only be transferred between cryptographic modules (HSM) and require the intervention of two of the seven administrators.

6.2.7 Private key storage in a cryptographic module

Private keys are generated in the cryptographic module when each PKIBDE Authority that makes use of said modules is created, and they are stored enciphered.

6.2.8 Private key activation method

As stipulated under point 6.2.2 *Private key multi-person control*, the private keys of both the Root CA and the Corporate CA are activated by booting the CA software using a minimum combination of operators of the corresponding CA. It is the only method to activate said private key.

Specifically, two PKIBDE operators are required to activate the private keys of the PKIBDE *Root CA* and *Corporate CA*.

Activation of the keys of the rest of the subscribers is determined in the applicable Certificate Policies.

6.2.9 Private key deactivation method

The System Administrator, with authorisation from two HSM Administrators, can deactivate PKIBDE CA's keys by halting the computer application of the corresponding CA.

6.2.10 Private key destruction method

No stipulation.

6.2.11 Cryptographic module classification

The cryptographic modules used comply with the FIPS 140-2 Level 3 standard.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archive

PKIBDE maintains an archive of all the certificates issued, which include the public keys, for a period of fifteen (15) years. The administrator of each PKIBDE CA is responsible for controlling this register.

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

6.3.2 Operational period of certificates and usage periods for key pairs

PKIBDE's Root CA certificate and key pair are valid for thirty (30) years and those of PKIBDE's Corporate CA for fifteen (15) years.

The active lifetime for the rest of the certificates is established in the Certificate Policy applicable to each one.

6.4 Activation Data

6.4.1 Generation and installation of activation data

To establish a Certification Authority, cryptographic cards must be created to be used for recovery and operational activities. The CA has two operational roles, each of which require their corresponding cryptographic cards:

- The set of *administrator cards*. These cards will be required to recover the HSM status in the event of a disaster or to transfer the keys to another module.
- The set of *operator cards*. These cards are used to protect the CAs keys. There must be a minimum number of operators present and they must indicate the PINs for their respective cards to carry out any operation with the CA, regardless of whether or not it involves the use of the CA keys.

If one or more cards are lost or damaged, or the administrator forgets the PIN or ceases to use it for any reason, the whole set of cards must be regenerated as soon as possible, using all of the security cards.

6.4.2 Activation data protection

Only authorised personnel, in this case the PKI Operators corresponding to each CA, hold cryptographic cards capable of CA activation and know the PINs and passwords to access the activation data.

6.4.3 Other activation data aspects

No stipulation.

6.5 Computer Security Controls

The data related to this section are considered confidential information and are provided only to those who can certify a need to know, such as in the case of external or internal inspection audits.

6.5.1 Specific security technical requirements

The data related to this section are considered confidential information and are provided only to those who can certify a need to know.

6.5.2 Computer security evaluation

PKIBDE permanently evaluates its level of security to identify any possible weaknesses and establish the corresponding corrective measures, through internal and external audits, as well as continuously carrying out security checks.

6.6 Life Cycle Security Controls

The data related to this section are considered confidential information and are provided only to those who can certify a need to know.

6.6.1 System development controls

Security controls are required from the very beginning, both in the acquisition of computer systems and in their development, as they could affect PKIBDE security.

6.6.2 Security management controls

There is a security organisation entrusted with its management.

6.6.3 Life cycle security controls

Security controls exist for the entire life cycle of systems with any impact on PKIBDE's security.

6.7 Network Security Controls

The data related to this section are considered confidential information and are provided only to those who can certify a need to know.

6.8 Timestamping

No stipulation.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version number

PKIBDE supports and uses X.509 Version 3 (X.509 v3) certificates.

7.1.2 Certificate extensions

The certificate extensions used generically are:

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

PKIBDE Certificate Policies may establish variations in the set of extensions used for each type of certificate.

PKIBDE has established a policy for assigning OIDs within its private numbering scale under which the OID for all the proprietary extensions for PKIBDE certificates begin with the prefix 1.3.6.1.4.1.19484.2.3.

PKIBDE has established the following proprietary extensions:

OID	Concept	Description
1.3.6.1.4.1.19484.2.3.1	Name	Name and surnames of the individual who is the certificate subscriber
1.3.6.1.4.1.19484.2.3.2	Surname 1	
1.3.6.1.4.1.19484.2.3.3	Surname 2	
1.3.6.1.4.1.19484.2.3.4	Employee No.	Banco de España's employee or contracted personnel no.
1.3.6.1.4.1.19484.2.3.5	User code	User code in Banco de España's Information Systems
1.3.6.1.4.1.19484.2.3.6	bdeCertType	Identifies the type of certificate
1.3.6.1.4.1.19484.2.3.7	bdeDocIdent	ID document (NIF (Tax No.), Passport No., etc.)
1.3.6.1.4.1.19484.2.3.8	bdeNombEnt	Name of the certificate issuing entity
1.3.6.1.4.1.19484.2.3.9	bdeCIF	Tax no. of the entity
1.3.6.1.4.1.19484.2.3.10	bdeValidTipo	Validation procedure for the certificate application
1.3.6.1.4.1.19484.2.3.11	bdeValidID	Code of the internal AU that validated the application or PCS identifier and type of certificate used to request the certificate
1.3.6.1.4.1.19484.2.3.12	bdeCodBETipo	BDE entity code type

1.3.6.1.4.1.19484.2.3.13	bdeCodBE	BDE entity code
1.3.6.1.4.1.19484.2.3.14	bdeNumDifer	Number used to differentiate two certificates issued for the same external entity
1.3.6.1.4.1.19484.2.3.15	bdeTipoPersona	Identifier used in internal user certificates to differentiate between employees and subcontrators.

7.1.3 Algorithm Object Identifiers (OID)

Cryptographic algorithm object identifiers (OID):
SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)

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.

7.1.6 Certificate Policy Object Identifiers (OID)

To be established in each Certificate Policy.
PKIBDE has established a policy for assignment of OIDs within its private enumeration scale under which the OID for all the PKIBDE Policy Certificates begin with the prefix 1.3.6.1.4.1.19484.2.2

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:

- URL CPS: contains the URL to the CPS and the CP that govern the certificate.
- Notice Reference: Text note that is displayed on the screen, upon request from an application or an individual, when a third party verifies a certificate.

The Notice Reference field will include text with basic information on the certificate and the policies to which it is subject:

> Certificate subject to: Banco de España's Certification Practice Statement.
>

Legally recognised certificates shall include, in the Notice Reference field, a text with basic information on the certificate, its status as a recognised certificate, the policies to which it is subject and the address of Banco de España, as required under Section 11.2 of Law 59/2003, the Electronic Signature Act:

7.1.9 Processing semantics for the critical "Certificate Policy" extension

The extension will be classified as *nonCritical* when used for the purpose of maintaining maximum capability to operate with other CAs of the certificate. This is done following the recommendations for the standard applications for secure e-mail, S/MIME [RFC 2632], and web authentication, SSL/TLS [RFC 2246]. The fact that the extension is not critical does not prevent the applications from using the information contained in said extension.

7.2 CRL Profile

7.2.1 Version number

PKIBDE supports and uses X.509 version 2 (v2) CRLs.

7.2.2 CRL and extensions

No stipulation.

7.3 OCSP Profile

7.3.1 Version number(s)

The profile is defined in RFC 2560.

7.3.2 OCSP Extensions

The Validation Authority supports signed requests and the NONCE extension.

8 Compliance Audit and Other Assessment

8.1 Frequency or Circumstances of Controls for each Authority

PKIBDE will be audited regularly, in accordance with Banco de España's Audits Plan. This guarantees that its functioning and operations are in accordance with the stipulations included in this CPS and the CPs.

At least one audit every two years will be carried out, pursuant to the Security Measures Regulations (RD 1720/2007, dated 21 December) for intermediate level files.

8.2 Identity/Qualifications of the Auditor

Audits may be entrusted to external audit firms or the Internal Audit Department, depending on the availability of personnel qualified in the specific aspects to be audited and the stipulations of the Audits Plan.

All teams or the person designated to carry out a security audit on PKIBDE must fulfil the following requirements:

- Appropriate training and experience in PKI, security, cryptographic technology and audit procedures.
- Independence at the organisational level from the PKIBDE Authority.

8.3 Relationship between the Assessor and the Entity being Assessed

Regardless of the purpose of the audit, the external auditor and the audited party (PKIBDE) shall not have any kind of relationship that could derive in a conflict of interests. In the case of internal auditors, these may not have any operational relationship with the area being audited.

8.4 Aspects Covered by Controls

The audit shall determine whether or not the PKIBDE services are in accordance with this CPS and the applicable CPs. It shall also determine whether and to what degree there is a risk of the operations failing to conform to what is established in said documents.

The scope of the audit activities shall include, at least:

- Security and privacy policy
- Physical security
- Technological evaluation
- Management of the CA's services
- Personnel selection
- Applicable CPS and CPs
- Contracts

8.5 Actions Taken as a Result of Deficiencies Found

Corrective measures shall be taken upon identification of deficiencies found as a result of the audit. The Policy Administration Authority (PAA), in collaboration with the auditor, shall be responsible for establishing them.

In the event of observing serious deficiencies, the Policy Administration Authority may make, among others, the following decisions: temporary suspension of operations until the deficiencies

are corrected, revocation of certificates issued to the assessed entity, changes in the personnel involved, invocation of the liabilities policy and more frequent overall audits.

8.6 Notification of the Results

The audit team shall notify the results of the audit to the PKIBDE Policy Administration Authority (PAA), the PKIBDE Security Manager, as well as the PKIBDE administrators and those of the Authority in which incidents were detected.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The fees for the issuance and renewal of each certificate are specified in the applicable Certificate Policy.

9.1.2 Certificate access fees

The fees for certificate access are specified in the applicable Certificate Policy.

9.1.3 Revocation or status information fees

The fees for access to the information on the status or revocation of each certificate are specified in the applicable Certificate Policy

9.1.4 Fees for other services, such as policy information

No fees shall be applied for supplying information on this CPS or the Certificate Policies managed by PKIBDE or for any other additional service that may be known at the time of drawing up this document.

This provision may be modified by the Certificate Policy applicable in each case.

9.1.5 Refund policy

Should any Certificate Policy specify any fee applicable for certification or revocation services provided by PKIBDE for the type of certificate it defines, the corresponding refund policy must be established.

9.2 Confidentiality of Business Information

Notwithstanding Section 6 of Royal Legislative Decree 1298/1986, dated 26 June, concerning Banco de España's duty to maintain the confidentiality of data and information it obtains in the course of its activities, the following confidentiality scheme is set up for data related to PKIBDE:

9.2.1 Scope of confidential information

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

- The private keys of the Certification Authorities that make up PKIBDE.
- The private keys that PKIBDE holds in escrow.
- The information related to operations carried out by PKIBDE.
- The information referring to security, control and audit procedure parameters.
- Personal data provided by certificate subscribers to PKIBDE during the registration process, pursuant to that established in the personal data protection laws and their implementation regulations.

9.2.2 Non-confidential information

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

- The content of this Certification Policy Statement.
- The information contained in applicable Certificate Policies.
- The certificates issued by PKIBDE.
- The list of certificates suspended or revoked.

9.2.3 Duty to maintain professional secrecy

Banco de España's employees who take part in any activities inherent to or derived from PKIBDE are committed to maintaining professional secrecy and, therefore, are subject to the regulatory laws applicable thereto, contained mainly in the Banco de España's Internal Regulations, approved by Resolution of the Governing Council dated 28 March 2000 and in the internal agreement regulations.

Likewise, contracted personnel that take part in any PKIBDE activities or operations are subject to the duty of professional secrecy within the framework of their contractual obligations with Banco de España.

9.3 Privacy of Personal Information

9.3.1 Personal data protection policy

Pursuant to applicable Spanish legislation, set forth in Chapter 10, point 10.1 and following.

9.3.2 Information considered private

All data corresponding to individuals is subject to the personal data protection laws.

9.3.3 Information not classified as private

Each CP shall establish the personal data to be included in the certificates and the public-access, certificate and CRL repositories. Acceptance by subscribers of the certificates issued in their name constitutes their consent to publication.

9.3.4 Responsibility to protect personal data

This responsibility is regulated in Chapter 10.

9.3.5 Notification of and consent to the use of personal data

Each CP shall establish the mechanisms to notify subscribers and, when appropriate, obtain their consent for the use of personal data.

9.3.6 Disclosure within legal proceedings

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.

9.3.7 Other circumstances in which data may be made public

These possible circumstances are regulated in Chapter 10.

9.4 Intellectual Property Rights

In the terms established under Royal Legislative Decree 1/1996, dated 12 April, approving the Revised Text of the Intellectual Property Act (Texto Refundido de la Ley de Propiedad Intelectual), Banco de España is the exclusive owner of all rights related to the electronic certificates issued by PKIBDE for individuals and computer components; the certificate revocation lists; the content of this Certification Practice Statement and the Certificate Policies. Furthermore, Banco de España is the holder of the rights related to any other electronic or any other kind of document, protocol, computer program and hardware, file, directory, database and consultation service that may be generated or used in the area of the PKIBDE's activities.

The object identifiers (OIDs) used are the property of Banco de España and have been registered with the Internet Assigned Number Authority (IANA) under the iso.org.dod.internet.private.enterprise 1.3.6.1.4.1-IANA-Registered Private Enterprises section, having been assigned the number **1.3.6.1.4.1.19484** (BANCO DE ESPAÑA). This may be consulted and verified at http://www.iana.org/assignments/enterprise-numbers

Unless express agreement is obtained from Banco de España, no OID assigned to Banco de España may be used, partially or fully, except for the specific uses included in the Certificate or Directory.

9.5 Representations and Warranties

9.5.1 Obligations of the CA

The CAs that operate within the PKIBDE hierarchy must ensure that all the obligations established under this point are included, as applicable, in the Certificate Policies. Each CA shall be responsible for fulfilment of its obligations, as stipulated in this CPS, even when part of its activities is subcontracted. Likewise, each CA shall provide its services in a manner consistent with the CPS.

The CAs that operate within the PKIBDE hierarchy have the following obligations:

CAO.1	To carry out their operations in accordance with this CPS.
CAO.2	To protect the private keys.
CAO.3	To issue certificates in accordance with the applicable Certificate Policy.
CAO.4	Following receipt of a valid certificate application, to issue certificates in accordance with the X.509 v3 standard and the requirements of the application.
CAO.5	To issue certificates that are in accordance with the information known at the time of their issue, and free from data recording errors.
CAO.6	To publish the certificates, when necessary, to interoperate with other users or computer systems that so require.
CAO.7	To revoke the certificates in the terms of point *4.4 Certificate Revocation and Suspension* and publish revoked certificates in the CRL and in the directory and web services referred to under point *4.9.7 Issue Frequency of CRLs*
CAO.8	To publish this CPS and the applicable CPs on the website referred to under point *2.1 Repositories*.
CAO.9	To notify changes to this CPS and the CPs as established under point 9*.10.2 Notification Period and Mechanism*
CAO.10	To conserve the terms and conditions acceptance documents for the certification services of Banco de España's certification authority that have been signed, on paper or electronically, by the certificate applicants in which they acknowledge that they have understood their obligations and rights, consent to the use of their personal data by the CA and confirm that the information provided is correct.
CAO.11	To guarantee the availability of the CRLs, pursuant to point 4.9.9 in this CPS.
CAO.12	In the event that the CA revokes a certificate, to notify this to the certificate users in accordance with the applicable Certificate Policy.

CAO.13	To collaborate with the PKIBDE authorities in validating re-keying.
CAO.14	To operate in accordance with the applicable legislation. Specifically with: - European Parliament and Council Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures (OJ,19 January 2000). - 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 (Spanish Official Gazette, 15 December).
CAO.15	To protect the keys in its custody, if any.
CAO.16	Not to store, under any circumstances, the signature creation data, the private key, of the subscribers of certificates issued for the purpose of using them for electronic signature *(key usage = nonrepudiation)*, whether acknowledged or not.
CAO.17	In the event of ceasing its activity, to report this at least two months in advance to the subscribers of certificates issued by them and to the Ministry of Industry, Trade and Tourism, as stipulated under point 5.8.1.
CAO.18	To keep a record of all the information and documentation related to a recognised certificate for a period of fifteen years.

9.5.2 Obligations of the RA

The RAs operating in Banco de España's PKIBDE shall fulfil the following obligations:

RAO.1	To identify Subscribers and/or Applicants and the organisations they represent correctly, in accordance with the procedures established in this CPS and Certificate Policies specific to each type of certificate, employing any legally approved means.
RAO.2	To formalise the issue of the Certificates to the Subscribers in the terms and conditions established in the Certificate Policies.
RAO.3	To store in a secure manner and for a reasonable period of time the documentation provided in the certificate issue process and in its suspension/revocation process.
RAO.4	To carry out any duties that may correspond, through the personnel necessary in each case, as established in this CPS.

9.5.3 Obligations of certificate subscribers

The subscribers of certificates issued under this CPS shall have the following obligations:

CSO.1	Provide accurate, full and truthful information regarding the data requested by those entrusted with their verification in order to carry out the registration process.
CSO.2	To inform PKIBDE management of any modification to said data.
CSO.3	To understand and accept the terms and conditions of use of the certificates and, specifically, those contained in this CPS and the applicable CPs, as well as any modifications thereto.
CSO.4	To restrict and condition the use of the certificates to the scope of their labour relationship with the Bank of Spain and pursuant to that permitted under the corresponding Certificate Policy and this CPS.

CSO.5	To take the necessary care and measures to guarantee the safekeeping of their cryptographic card, preventing its loss, disclosure, modification or unauthorised use.
CSO.6	The process to obtain the certificates requires the personal selection of a control PIN for the cryptographic card and activation of the private keys and a PUK for unlocking. The holder is responsible for keeping the PIN and PUK numbers secret.
CSO.7	To immediately request the revocation of a certificate upon detecting any inaccuracy in the information contained therein or upon becoming aware of or suspecting any compromise of the private key corresponding to the public key contained in the certificate due, among other causes, to: loss, theft, potential compromise, knowledge by third parties of the PIN and/or PUK.
CSO.8	Not monitor, manipulate or carry out any reverse engineering on the technical implementation (hardware and software) of the certification services.
CSO.9	Not to transfer or delegate to third parties their obligations pertaining to a certificate assigned to them.
CSO.10	Any other obligation derived under law, this CPS or the Certificate Policies.

9.5.4 Obligations of relying parties

Third parties who accept and rely on certificates issued by PKIBDE shall have the following obligations:

RPO.1	To limit reliability on the certificates to the uses that they allow, pursuant to the certificate extensions and the corresponding Certificate Policy.
RPO.2	To verify the validity of the certificates upon receipt of the documents signed electronically by checking that the certificate is valid and has not expired or been suspended or revoked.
RPO.3	To assume the responsibility for correct verification of the electronic signatures.
RPO.4	To assume responsibility for checking the validity as well as the revocation or suspension status of the certificates they accept and rely on.
RPO.5	To be aware of the guarantees and responsibilities derived from acceptance of the certificates on which they rely and accept that they are subject to them.
RPO.6	To notify any anomalous event or circumstance pertaining to the certificate, which could be considered cause for its revocation.

9.5.5 Obligations of other participants

OPO.1	The Repository Service shall maintain the information on revoked certificates accessible by subscribers and relying parties, in CRL format.

9.6 Disclaimers of Warranties

9.6.1 PKIBDE's liabilities

PKIBDE shall 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 implementation regulations, in this CPS and in the specific Certificate Policies.

Particularly, PKIBDE as certification service provider will be liable in case of damages to the signer or bona fide third parties in case of lack or delay while including certificates in the revocation information service.

Banco de España's PKI shall only accept liability for damages caused by undue use of a certificate when said certificate and its associated Certificate Policy state, in a manner clearly recognisable by third parties, a limitation as to its possible use or as to the value of valid transactions that may be carried out using it.

Banco de España's PKI, as Provider of Certification Services, does not accept liability for the content of documents signed using its certificates, nor for any other use of its certificates, such as message or communication encipherment processes.

Banco de España's PKI does not represent, in any way whatsoever, the users nor relying parties of the certificate it issues.

9.6.2 PKIBDE liability exemption

PKIBDE assumes no liability in the event of losses or damages:

LIAB.1	Related to services it provides, in the event of war, natural disaster or any other kind of accidental or force majeure circumstances: public disorder, transport strike, loss of power and/or telephone service, computer viruses, deficiencies in telecommunication services or compromise in the asymmetric keys derived from an unforeseeable technological hazard.
LIAB.2	Incurred during the period between certificate application and delivery to the user.
LIAB.3	Caused by certificate usage that exceeds the limitations established in the same, the corresponding Certificate Policy and this CPS.
LIAB.4	Caused by misuse of the information contained in the certificate.
LIAB.5	Caused by improper or fraudulent use of certificates or the CRLs issued by PKIBDE
LIAB.6	Banco de España's PKI shall not hold itself liable in any way whatsoever for the use of certificates issued by its CAs and the private/public key pair linked to subscribers for any activity not specified in the CPS or in the corresponding Certificate Policies.
LIAB.7	Banco de España's PKI, as Provider of Certification Services, shall not be liable for the content of documents signed using its certificates, nor for any other use of its certificates, such as message or communication encipherment processes.

9.6.3 Scope of liability coverage

Pursuant to Section 20.2, Law 59/2003, dated 19 December, Banco de España has taken out civil liability insurance coverage in the amount of €3,000,000 to cover any risks of liability for damages that may be caused by the use of recognised certificates issued by PKIBDE.

9.7 Limitations of Liability

Except as stipulated in the provisions of this CPS, PKIBDE assumes no other commitment, gives no other guarantee, and shall accept no other liability regarding certificate subscribers or relying parties.

9.8 Term and Termination

9.8.1 Term

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

This CPS 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 Root CA keys, at which time it is mandatory to draw up a new version.

9.8.2 CPS substitution and termination

This CPS shall be substituted for 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 CPS is terminated, it will be withdrawn from the PKIBDE public repository, though it will be held for 15 years.

9.8.3 Consequences of termination

The obligations and constraints established under this CPS, 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

All notifications, demands, applications or any other type of communication required in the practices described in this CPS shall be carried out by electronic message or in writing, by registered post, addressed to any of the addresses contained in point 1.5 Policy Administration. Electronic notifications shall be effective upon receipt by the recipients to which they are addressed.

9.10 Amendments

9.10.1 Amendment procedures

The Authority empowered to carry out and approve amendments to PKIBDE's CPS and CPs is the Policy Administration Authority (PAA). The PAA's contact data can be found under point 1.5 Policy Administration in this CPS.

9.10.2 Notification period and mechanism

Should the PAA deem that the amendments to the specifications could affect the acceptability of the certificates for specific purposes, it shall notify the users of certificates corresponding to the amended CP or CPS that an amendment has been carried out and that they should consult the new CPS in the established repository.

9.10.3 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 certificates, 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 considered necessary to notify this type of modification to users of the certificates corresponding to the CP or CPS modified.

Should the PAA deem that the amendments to the specifications could affect the acceptability of the certificates for specific purposes, 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) that represents it will also be modified. This type of modification will be notified to the users of the certificates corresponding to the CP or CPS modified.

9.11 Dispute Resolution Procedures

All disputes between users and PKIBDE shall be notified by the disputing party to Banco de España's Policy Administration Authority (PAA), endeavouring to resolve said disputes between the parties themselves.

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 of the city of Madrid, the parties waiving any other jurisdiction to which they may have a right.

9.12 Governing Law

The operations and functioning of PKIBDE, as well as this Certification Practice Statement and the applicable Certificate Policy for each type of certificate shall be subject to the regulations applicable to them and, specifically:

- European Parliament and Council Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures (OJ,January 2000).
- 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 (Spanish Official Gazette, 15 December).
- Spanish Royal Decree 1720/2007, of 21 December, approving the Regulations for the development of the Spanish Organic Law 15/1999.
- Banco de España's Circular 2/2005, of 25 February, on electronic files with personal data managed by Banco de España (Spanish Official Gazette, 22 March), and its subsequent updates.

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.

9.13 Compliance with Applicable Law

The Policy Administration Authority is responsible for ensuring compliance with the applicable legislation stated under the previous point.

9.14 Miscellaneous Provisions

9.14.1 Entire agreement clause

All the relying parties accept the content of the latest version of this CPS and the applicable CPs in their entirety.

9.14.2 Independence

Should any of the provisions of this CPS 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 CPS 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

Organic Law 15/1999, dated 13 December, the Personal Data Protection Act and its executive legislation are applicable to this Certification Practice Statement, including Royal Decree 1720/2007, date 21 December. The files shall be held by a public entity and their creation, modification or elimination shall be carried out by way of Banco de España's Circular published in the Spanish Official Gazette.

Furthermore, Banco de España's Internal Circular 3/2002 regarding Automated Personal Data Protection and its implementation regulations shall be applicable together with its subsequent updates.

Notwithstanding their other obligations, the Registration Authorities set up in PKIBDE shall verify that all certificate applicants give their consent to the use of their personal data and are informed of the purpose for which they shall be used and their inclusion in a file declared for said purpose by PKIBDE.

When said data are not collected directly from the affected parties, PKIBDE or its representative shall notify them, within the three months following registration of the data and in an express, precise and unequivocal manner, of the content of the previous point.

The parties to which the data pertain may exercise their rights to access, rectify, cancel or oppose the holding of said data by writing to the address set out in the following point of this CPS.

The data contained in the secure Certificate Directory are considered personal data pursuant to the Personal Data Protection Act (Ley Orgánica de Protección de Datos de Carácter Personal, LOPD) and any other supplementary legislation and, for this reason, PKIBDE shall not give third parties access to them.

However, for the proper fulfilment of the certification services, PKIBDE makes the lists of revoked certificates (that do not contain personal data) available to relying parties. The relying party, as assignee of this information, may only use it in accordance with said purposes.

10.2 File Creation and Registration

The creation and registration data for Banco de España's "Electronic Certificates" file are:

- Creation: Banco de España's Circular 2/2005, dated 25 February (Official Spanish Gazette published 22 March)
- Registration number in the General Data Protection Registry: 2051360139

The name of the file, its manager and the area entrusted with dealing with petitions to exercise rights are:

File Name:	Electronic Certificates
File Manager:	Banco de España
Public Support Service:	Information Systems Department

10.3 Personal Data Protection Act Security Document

10.3.1 Aspects covered

This CPS, as stated in point 1.1, has been drawn up in accordance with the specifications of RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" from the Internet Engineering Task Force (IETF) for this kind of document.

Notwithstanding the above, and taking into account Law 59/2003, dated 19 December, the Electronic Signature Act, which considers the CPS as a security document pursuant to the personal data protection legislation, it is mandatory to add this section to include all the requirements established in Royal Decree 1720/2007, dated 21 December, approving the regulations for the development of the Spanish Organic Law 15/1999 dated 13 December, concerning personal data protection.

For this purpose, the following aspects are covered:

- Basic structure of personal data.
- Applicable level of security.
- Information systems that support the file.
- List of users.
- Incident notification and management.
- Backup copies and recovery.
- Access control
- Temporary files.
- Support media management
- Use of real data in tests

The rest of the aspects that must be considered in a Security Document have already been included in previous chapters of this CPS.

Furthermore, in that which is not contrary to this CPS, Banco de España's Internal Circular 3/2002 regarding Automated Personal Data Protection and its implementation regulations shall be applicable, as well as its subsequent updates.

The purpose of the Security Document is to preserve the personal data processed by PKIBDE and, therefore, it affects all resources (persons, equipment, communications, software, procedures, etc.) involved in the data processing.

10.3.2 Duties and obligations of the personnel

This CPS, and any of its future versions, are or will be known by all persons who access the personal data processed by PKIBDE, and it is mandatory to fulfil all the duties and obligations established therein.

10.3.3 Personal Data Protection Structure

The following table shows certificate subscribers' data processed by PKIBDE, employing the denominations used on the form for reporting files to the Spanish Data Protection Agency:

DATA PROCESSED
Identification data
D.N.I./N.I.F. (ID DOC./TAX NO.)
Name and surnames
E-mail address
Personal registration no.
Electronic signature
Employment data
Others: Company

10.3.4 Security level

The personal data processed require a basic level of security, without prejudice to providing a higher level of security, given the special circumstances of security required for a PKI and the level of security established in this CPS.

10.3.5 Information systems

Within the information structure established by PKIBDE, there are three subsystems with some implications for personal data processing. A brief list and description is given of these below:

- **Certificate management subsystem**: This is responsible for creating the certificates in accordance with the X.509v3 standard, where the keys generated by the keys subsystem and other identification data defined in the corresponding CP are entered.
- **Registration Authority subsystem**: This is responsible for identifying the certificate applicant for the subsequent issue of the certificate by PKIBDE.
- **Publication subsystem**: This is responsible for managing publication of the certificate revocation lists (CRL) and the certificates directory.

10.3.6 List of users

The Security Co-ordinator keeps a list of users with access to the personal data processed by the PKI, with indication of roles and access levels. Said list of users is of a confidential nature for security reasons and, therefore, access to it requires a reasoned request made to the Security Co-ordinator.

This list does not include users with access to electronic certificates for the purpose of using them to send enciphered information nor users with access to the CRLs.

10.3.7 Incident notification and management.

The internal procedures of the Information Systems Department associated with incident management ensure that all incidents are registered and documented, carrying out their monitoring. Information is registered regarding: date, time, type of incident, person reporting the incident, person to whom resolution of the incident is assigned, documentation on its cause and the effects.

10.3.8 Backup copies and recovery.

Backup up copies are made daily pursuant to the applicable Banco de España's central computer regulations.

Data recovery is carried out with authorisation from the file manager:

a Incidents in the computer system: These are reported to the computer system's manager, who will obtain authorisation from the owner through the procedure established for this purpose.
b Incidents in the computer system infrastructure: The procedures followed are those established in the Information System Department's backup plans for each contingency.

10.3.9 Access control

Authorisation for access to information systems shall be based exclusively on a need-to-know basis for the work to be carried out. User and element administrators shall be responsible always for validating this need before granting access to data.
Likewise, all the elements that enable access to personal data shall be given restricted use classification.

10.3.10 Temporary files

The software used to generate an electronic certificate under the X.509v3 generates temporary files, audit registration files, which are duly safeguarded, given the need for traceability of the facility for the activity of providing certification services in fulfilment of Law 59/2003, dated 19 December, the Electronic Signature Act.

10.3.11 Support media management

The internal support media are correctly identified by their barcodes or include their corresponding identification label.
The support media are located in the computer rooms. Access to these rooms is restricted, with permanent authorisation being validated by the Information Systems Manager, whilst provisional access to these rooms may only be authorised by the Operations Manager or the Head of Operations.
Any removal of support media from Banco de España's premises must be authorised by the PKI Administrator. The Information Systems Department keeps a hardcopy log of all incoming/outgoing support media.
Any support media that had contained personal data shall be erased using physical deletion or a similar procedure. This process shall be carried out whenever support media that are to be sent outside are reused; in other cases, support media handling does not occur, as management is carried out directly by the robots that handle the cartridges.
Before authorisation is given to send support media with data outside for maintenance operations, they shall be physically erased and degaussed. Sending support media outside only occurs in the case of disks.

10.3.12 Use of real data in tests

Real personal data shall not be used to carry out tests, unless the same levels of security as those established in this CPS are ensured.
The test procedures used by the Information Systems Department ensure fulfilment of the security level required for the use of real data in tests.