BANCO DE ESPAÑA
Eurosistema

11.05.2015

OID: 1.3.6.1.4.1.19484.2.2.9

The Banco de España's Public Key Infrastructure

Policy Certificate for internal use component certificates

OVERVIEW This document sets out the Certificate Policy (CP) governing the internal-use component certificates issued by the Corporate Certification Authority of the Banco de España's Public Key Infrastructure (PKI).

Control Sheet

Title	Policy Certificate for internal use component certificates
Author	Information Systems Department
Version	1.2
Date	11.05.2015

Change Log

Version	Date	Reason for the change
1.0	5.04.2006	Initial Version
1.1	25.05.2010	Review following introduction of electronic dating services Renaming of the Policy Approval Authority to Policy Management Authority
1.2	11.05.2015	Update due to the renewal of the Certification Authorities

TABLE OF CONTENTS

1 Introduction 13

1.1 Overview 13

1.2 Document Name and Identification 14

1.3 PKI Participants 14

1.3.1 Policy Management Authority 14

1.3.2 Certification Authorities 14~~15~~

1.3.3 Registration Authorities 17~~15~~

1.3.4 Validation Authority 17~~15~~

1.3.5 Keys Archive 17~~16~~

1.3.6 Certificate Subscribers 18~~16~~

1.3.7 Relying Parties 18~~16~~

1.3.8 Other affected parties 18~~16~~

1.4 Certificate Usage 18~~16~~

1.4.1 Appropriate certificate use 18~~16~~

1.4.2 Certificate Usage Constraints and Restrictions 19~~17~~

1.5 Policy Administration 19~~17~~

1.5.1 Banco de España, as PKIBDE owner 19~~17~~

1.5.2 Contact Person 19~~17~~

1.5.3 Establishment of the suitability of a CPS from an External CA as regards PKIBDE Certificate Policies 19~~18~~

1.5.4 Approval Procedures for this CP19~~18~~

1.6 Definitions and Acronyms 20~~18~~

1.6.1 Definitions 20~~18~~

1.6.2 Acronyms 20~~19~~

2 Repositories and Publication of Information 22~~20~~

2.1 Repositories 22~~20~~

2.2 Publication of Certification Data 22~~20~~

2.3 Publication Timescale or Frequency 2220

2.4 Repository Access Controls 2220

3 Identification and Authentication of Certificate Subscribers 2321

3.1 Naming 2321

3.1.1 Types of names 2321

3.1.2 The need for names to be meaningful 2321

3.1.3 Rules for interpreting various name formats 2321

3.1.4 Uniqueness of names 2321

3.1.5 Name dispute resolution procedures 2321

3.1.6 Recognition, authentication, and the role of trademarks 2422

3.2 Initial Identity Validation 2422

3.2.1 Means of proof of possession of the private key 2422

3.2.2 Identity authentication for an entity 2422

3.2.3 Identity authentication for an individual 2422

3.2.4 Non-verified applicant information 2422

3.2.5 Validation of authority 2422

3.2.6 Criteria for operating with external CAs 2422

3.3 Identification and Authentication for Re-key Requests 2422

3.3.1 Identification and authentication requirements for routine re-key 2422

3.3.2 Identification and authentication requirements for re-key after certificate revocation 2422

4 Certificate Life Cycle Operational Requirements 2523

4.1 Certificate Application 2523

4.1.1 Who can submit a certificate application? 2523

4.1.2 Enrolment process and applicants' responsibilities 2523

4.2 Certificate Application Processing 2624

4.2.1 Performance of identification and authentication procedures 2624

4.2.2 Approval or rejection of certificate applications 2624

4.2.3 Time limit for processing the certificate applications 2624

4.3 Certificate Issuance 2724

4.3.1 Actions performed by the CA during the issuance of the certificate 2724

4.3.2 CA notification to the applicants of certificate issuance 2725

4.4 Certificate Acceptance 2725

4.4.1 Form of certificate acceptance 2725

4.4.2 Publication of the certificate by the CA 2725

4.4.3 Notification of certificate issuance by the CA to other Authorities 2725

4.5 Key Pair and Certificate Usage 2725

4.5.1 Subscribers' use of the private key and certificate 2725

4.5.2 Relying parties' use of the public key and the certificate 2826

4.6 Certificate Renewal with no Key Changeover 2826

4.6.1 Circumstances for certificate renewal with no key changeover 2826

4.7 Certificate Renewal with Key Changeover 2826

4.7.1 Circumstances for certificate renewal with key changeover 2826

4.7.2 Who may request certificate renewal? 2826

4.7.3 Procedures for processing certificate renewal requests with key changeover 2826

4.7.4 Notification of the new certificate issuance to the subscriber 2926

4.7.5 Manner of acceptance of certificates with changed keys 2927

4.7.6 Publication of certificates with the new keys by the CA 2927

4.7.7 Notification of certificate issuance by the CA to other Authorities 2927

4.8 Certificate Modification 2927

4.8.1 Circumstances for certificate modification 2927

4.9 Certificate Revocation and Suspension 2927

4.9.1 Circumstances for revocation 2927

4.9.2 Who can request revocation? 3028

4.9.3 Procedures for requesting certificate revocation 3028

4.9.4 Revocation request grace period 3028

4.9.5 Time limit for the CA to process the revocation request 3028

4.9.6 Requirements for revocation verification by relying parties 3028

4.9.7 CRL issuance frequency 3028

4.9.8 Maximum latency between the generation of CRLs and their publication 3028

4.9.9 Online certificate revocation status checking availability 3129

4.9.10 Online revocation checking requirements 3129

4.9.11 Other forms of revocation alerts available 3129

4.9.12 Special requirements for the renewal of compromised keys 3129

4.9.13 Causes for suspension 3129

4.9.14 Who can request the suspension? 3129

4.9.15 Procedure for requesting certificate suspension 3129

4.9.16 Suspension period limits 3129

4.10 Certificate status services 3129

4.10.1 Operational characteristics 3129

4.10.2 Service availability 3129

4.10.3 Additional features 3129

4.11 End of Subscription 3129

4.12 Key Escrow and Recovery3230

4.12.1 Key escrow and recovery practices and policies 3230

4.12.2 Session key protection and recovery policies and practices 3230

5 Management, Operational, and Physical Controls 3331

5.1 Physical Security Controls 3331

5.1.1 Site location and construction 3331

5.1.2 Physical access 3331

5.1.3 Power and air-conditioning 3331

5.1.4 Water exposure 3331

5.1.5 Fire prevention and protection 3331

5.1.6 Storage system 3331

5.1.7 Waste disposal 3331

5.1.8 Offsite backup 3331

5.2 Procedural controls 3331

5.2.1 Roles responsible for PKI control and management 3331

5.2.2 Number of individuals required to perform each task 3331

5.2.3 Identification and authentication of each user 3331

5.2.4 Roles that require separation of duties 3331

5.3 Personnel Security Control 3331

5.3.1 Requirements concerning professional qualification, knowledge and experience 3331

5.3.2 Background checks and clearance procedures 3331

5.3.3 Training requirements 3432

5.3.4 Retraining requirements and frequency 3432

5.3.5 Frequency and sequence for job rotation 3432

5.3.6 Sanctions for unauthorised actions 3432

5.3.7 Requirements for third party contracting 3432

5.3.8 Documentation supplied to personnel 3432

5.4 Security Audit Procedures 3432

5.4.1 Types of events recorded 3432

5.4.2 Frequency with which audit logs are processed 3432

5.4.3 Period for which audit logs are kept 3432

5.4.4 Audit log protection 3432

5.4.5 Audit log back up procedures 3432

5.4.6 Audit data collection system (internal vs. external) 3432

5.4.7 Notification to the subject who caused the event 3432

5.4.8 Vulnerability assessment 3432

5.5 Records Archive 3432

5.5.1 Types of records archived 3432

5.5.2 Archive retention period 3533

5.5.3 Archive protection 3533

5.5.4 Archive backup procedures 3533

5.5.5 Requirements for time-stamping records 3533

5.5.6 Audit data archive system (internal vs. external) 3533

5.5.7 Procedures to obtain and verify archived information 3533

5.6 CA Key Changeover 3533

5.7 Compromised Key and Disaster Recovery 3533

5.7.1 Incident and compromise handling procedures 3533

5.7.2 Corruption of computing resources, software, and/or data 3533

5.7.3 Action procedures in the event of compromise of an Authority's private key 3533

5.7.4 Installation following a natural disaster or another type of catastrophe 3533

5.8 CA or RA Termination 3533

5.8.1 Certification Authority 3533

5.8.2 Registration Authority 3533

6 Technical Security Controls 3634

6.1 Key pair generation and installation 3634

6.1.1 Key pair generation 3634

6.1.2 Delivery of private keys to subscribers 3634

6.1.3 Delivery of the public key to the certificate issuer 3634

6.1.4 Delivery of the CA's public key to relying parties 3634

6.1.5 Key sizes 3634

6.1.6 Public key generation parameters and quality checks 3634

6.1.7 Key usage purposes (KeyUsage field in X.509 v3) 3634

6.2 Private Key Protection and Cryptographic Module Engineering Controls 3735

6.2.1 Cryptographic module standards 3735

6.2.2 Private key multi-person (k out of n) control 3735

6.2.3 Escrow of private keys 3735

6.2.4 Private key backup copy 3735

6.2.5 Private key archive 3836

6.2.6 Private key transfer into or from a cryptographic module 3836

6.2.7 Private key storage in a cryptographic module 3836

6.2.8 Private key activation method 3836

6.2.9 Private key deactivation method 38~~36~~

6.2.10 Private key destruction method 38~~36~~

6.2.11 Cryptographic module classification 38~~36~~

6.3 Other Aspects of Key Pair Management 38~~36~~

6.3.1 Public key archive 38~~36~~

6.3.2 Operational period of certificates and usage periods for key pairs 38~~36~~

6.4 Activation Data 38~~36~~

6.4.1 Generation and installation of activation data 38~~36~~

6.4.2 Activation data protection 38~~36~~

6.4.3 Other activation data aspects 38~~36~~

6.5 Computer Security Controls 39~~37~~

6.5.1 Specific security technical requirements 39~~37~~

6.5.2 Computer security evaluation 39~~37~~

6.6 Life cycle security controls 39~~37~~

6.6.1 System development controls 39~~37~~

6.6.2 Security management controls 39~~37~~

6.6.3 Life cycle security controls 39~~37~~

6.7 Network Security Controls 39~~37~~

6.8 Time-stamping 39~~37~~

7 Certificate, CRL and OCSP Profiles 40~~38~~

7.1 Certificate Profile 40~~38~~

7.1.1 Version number 40~~38~~

7.1.2 Certificate extensions 40~~38~~

7.1.3 Algorithm Object Identifiers (OID) 50~~49~~

7.1.4 Name formats 50~~49~~

7.1.5 Name constraints 50~~49~~

7.1.6 Certificate Policy Object Identifiers (OID) 50~~49~~

7.1.7 Use of the "PolicyConstraints" extension 50~~49~~

7.1.8 Syntax and semantics of the “PolicyQualifier 50

7.1.9 Processing semantics for the critical "CertificatePolicy" extension 5150

7.2 CRL Profile 5150

7.2.1 Version number 5150

7.2.2 CRL and extensions 5150

7.3 OCSP Profile 5150

7.3.1 Version number(s) 5150

7.3.2 OCSP Extensions 5150

8 Compliance Audits and Other Controls 5251

8.1 Frequency or Circumstances of Controls for each Authority 5251

8.2 Identity/Qualifications of the Auditor 5251

8.3 Relationship between the Assessor and the Entity being Assessed 5251

8.4 Aspects Covered by Controls 5251

8.5 Actions Taken as a Result of Deficiencies Found 5251

8.6 Notification of the Results 5251

9 Other Legal and Business Matters 5352

9.1 Fees 5352

9.1.1 Certificate issuance or renewal fees 5352

9.1.2 Certificate access fees 5352

9.1.3 Revocation or status information fees 5352

9.1.4 Fees for other services, such as policy information 5352

9.1.5 Refund policy 5352

9.2 Information Confidentiality 5352

9.2.1 Scope of confidential information 5352

9.2.2 Non-confidential information 5352

9.2.3 Duty to maintain professional secrecy 5352

9.3 Personal Data Protection 5352

9.3.1 Personal data protection policy 5352

9.3.2 Information considered private 5352

9.3.3 Information not classified as private 5352

9.3.4 Responsibility to protect personal data 5352

9.3.5 Notification of and consent to the use of personal data 5352

9.3.6 Disclosure within legal proceedings 5453

9.3.7 Other circumstances in which data may be made public 5453

9.4 Intellectual Property Rights 5453

9.5 Obligations 5453

9.5.1 Obligations of the CA 5453

9.5.2 Obligations of the RA 5453

9.5.3 Obligations of certificate subscribers 5453

9.5.4 Obligations of relying parties 5453

9.5.5 Obligations of other participants 5453

9.6 Liabilities 5453

9.6.1 PKIBDE's liabilities 5453

9.6.2 PKIBDE liability exemption 5453

9.6.3 Scope of liability coverage 5453

9.7 Loss Limits 5453

9.8 Validity Period 5453

9.8.1 Term 5453

9.8.2 CP substitution and termination 5554

9.8.3 Consequences of termination 5554

9.9 Individual notices and communications with participants 5554

9.10 Specification Amendment Procedures 5554

9.10.1 Amendment procedures 5554

9.10.2 Notification period and mechanism 5554

9.10.3 Circumstances in which the OID must be changed 5554

9.11 Disputes and Jurisdiction 5554

9.12 Governing Law 5554

9.13 Compliance with Applicable Law 5554

9.14 Miscellaneous Provisions 5554

9.14.1 Entire agreement clause 55~~54~~

9.14.2 Independence 56~~55~~

9.14.3 Resolution through the courts 56~~55~~

9.15 Other Provisions 56~~55~~

10 Personal Data Protection 57~~56~~

10.1 Data Protection Legal Scheme 57~~56~~

10.2 File Creation and Registration 57~~56~~

10.3 Personal Data Protection Act Security Document 57~~56~~

1 Introduction

1.1 Overview

This document sets out the Certificate Policy (CP) governing the internal-use component certificates issued by the Corporate Certification Authority of the Banco de España's Public Key Infrastructure (hereinafter, PKIBDE).

This Certificate Policy regulates all the internal-use component certificates issued by PKIBDE, and specifically:

- Web certificates for use with SSL (Secure Socket Layer) / TLS (Transport Layer Security) protocol.
- Authentication and signature certificates for components.
- Encipherment certificates for components.
- Generic certificates for components.
- Code signature certificates.
- Domain controller certificates.

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

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

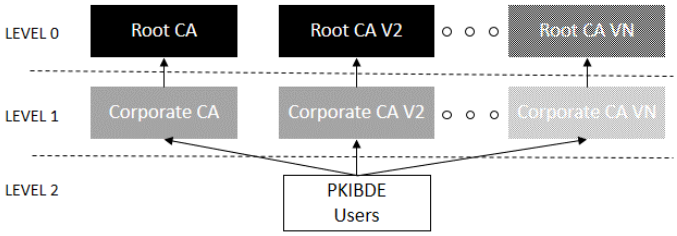
This CP, with the exception of section 9, which contains a slight variation, has been structured in accordance with the guidelines of the PKIX work group in the IETF (Internet Engineering Task Force) in its reference document RFC 3647 (approved in November 2003) "Internet X.509 Public Key Infrastructure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

The CP includes all the activities for managing internal-use component certificates throughout their life cycle, and serves as a guide for the relations between Corporate CA and its users. Consequently, all the parties involved must be aware of the content of the CP and adapt their activities to the stipulations therein.

This CP assumes that the reader is 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 the Banco de España's PKI is as follows[1]:

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



1.2 Document Name and Identification

Document name	Policy Certificate (CP) for internal-use component certificates
Document version	1.2
Document status	Approved
Date of issue	11.05.2015
OID (Object Identifier)	1.3.6.1.4.1.19484.2.2.9
CPS location	http://pki.bde.es/politicas
Related CPS	Certification Practice Statement of the Banco de España's PKI OID 1.3.6.1.4.1.19484.2.2.1

1.3 PKI Participants

The participating entities and persons are:

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

1.3.1 Policy Management Authority

The Policy Management Authority is defined in accordance with the PKIBDE Certification Practice Statement.

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 currently make up PKIBDE are:

1.3.2.1 Root Certification Authorities

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

Distinguished Name	CN= BANCO DE ESPAÑA – AC RAIZ , O=BANCO DE ESPAÑA, C=ES
Serial Number	F16D 7586 5D7C CF92 41AD A17A CD9A 3DE2
Distinguished Name of Issuer	CN= BANCO DE ESPAÑA – AC RAIZ , O=BANCO DE ESPAÑA, C=ES
Validity Period	From 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
Cryptographic algorithms	SHA-1 / RSA 2048

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

  - With SHA-1 algorithm[2]:

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

  - With SHA-256 algorithm:

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

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

- With SHA-512 algorithm:

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

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

1.3.2.2 Intermediate Certification Authorities

- **Corporate CA**: Certification Authority subordinate to the Root CA. Its duty is to issue certificates for PKIBDE users. This CP refers to the component certificates issued by the same for external entities. 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 29-07-2004 9:03:28
Message Digest (SHA-1)	ABE6 1ED2 5AF6 4253 F77B 322F 6F21 3729 B539 1BDA
Cryptographic algorithms	SHA-1 / RSA 2048

- **Corporate CA V2**: Certification Authority subordinate to the Root CA. It is responsible for issuing certificates for PKIBDE users. Certification Authority subordinate to the Root CA. It is responsible for issuing certificates for PKIBDE users:
  - With SHA-1[3] algorithm:

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

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

- With SHA-256 algorithm:

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

- With SHA-512 algorithm:

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

Corporate CA V2 has been issued to replace Banco de España's Corporate CA, as a result of the update of the cryptographic upgrade of the algorithms and key lengths used according to international recommendations.
Both intermediate CAs are valid until their expiration date or revocation. However the Corporate CA will cease providing end entity certificate issuance since the entry into Service of Corporate CA V2, and it will be remain alive only to enable revocation of certificates previously issued by it.

1.3.3 Registration Authorities

The Registration Authorities are defined in accordance with the PKIBDE Certification Practice Statement.
Issue of internal-use component certificates shall be carried out using the Corporate Registration Authority, where administrators with the Registration Officer for Components role will access using their authentication certificates issued by the Corporate CA for the internal-use component certificates management.

1.3.4 Validation Authority

The Validation Authority is defined in accordance with the PKIBDE Certification Practice Statement.

1.3.5 Keys Archive

The Keys Archive, defined in the PKIBDE Certification Practice Statement, is not applicable in this Certificate Policy.

1.3.6 Certificate Subscribers

The Certificate Subscribers are defined in accordance with the PKIBDE Certification Practice Statement.

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

Certification Environment	Subscribers
Corporate CA	Internal-use components (Corporate Services and Systems)

Despite being component certificates, there must be a person responsible for each one. The type of individuals who can act as component managers are set out in the following chart:

Certificate type	Manager
Web certificates for use with SSL/TLS protocol	Web server manager
Authentication and signature certificates for internal-use components	Component manager
Generic certificates for internal-use components	Component manager
Code signature certificates	Project development manager
Domain controller certificate	Active Directory manager

1.3.7 Relying Parties

Relying parties are those that make use of the certificates to identify components (servers, applications, code, etc.) for which a certificate has been issued or to exchange encrypted information with them.

1.3.8 Other affected parties

Applicants: individuals who have requested issuance of a PKIBDE certificate for a component.

CA's Remote Administrators: individuals within the Banco de España who manage the component certificate requests and have remote CA privileges.

1.4 Certificate Usage

1.4.1 Appropriate certificate use

The certificates regulated under this CP shall be used to authenticate components and the encipherment of communications within the Banco de España's Information Systems environment.

The following chart offers details on the appropriate uses, depending on the type of component certificate:

Certificate type	Appropriate Usage
Web certificates for use with SSL/TLS protocol	Authentication of web servers with respect to their clients and establishment of communications using

	the SSL protocol
Authentication and signature certificates for internal-use components	Authentication of components with respect to other components or individuals and transaction signatures
Generic certificates for internal-use components	Authentication of components and encipherment of communications
Code signature certificates	Code signature to guarantee authentication and integrity
Domain controller certificate	Authentication of the domain controller with respect to the 'smartcard logon' client

1.4.2 Certificate Usage Constraints and Restrictions

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

1.5 Policy Administration

1.5.1 Banco de España, as PKIBDE owner

This CP belongs to Banco de España:

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

1.5.2 Contact Person

This CP is managed by the Policy Management Authority (PMA) of the Banco de España PKI:

Name	Information Systems Department Banco de España PKI Policy Management Authority		
E-mail address	pkibde@bde.es		
Address	C/Alcalá, 522. 28027 - Madrid (Spain)		
Telephone No.	+34913386666	**Fax**	+34913386875

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

As specified in PKIBDE's CPS.

1.5.4 Approval Procedures for this CP

As specified in PKIBDE's CPS.

1.6 Definitions and Acronyms

1.6.1 Definitions

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

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

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.

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 Management Authority

CA: Certification Authority

RA: Registration Authority

VA: Validation Authority

CRL: Certificate Revocation List

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

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 Banco de España PKI

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

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 Repositories and Publication of Information

2.1 Repositories

As specified in PKIBDE's CPS.

2.2 Publication of Certification Data

As specified in PKIBDE's CPS.

2.3 Publication Timescale or Frequency

As specified in PKIBDE's CPS.

2.4 Repository Access Controls

As specified in PKIBDE's CPS.

3 Identification and Authentication of Certificate Subscribers

3.1 Naming

3.1.1 Types of names

The certificates issued by PKIBDE contain the Distinguished Name (or DN) X.500 of the issuer and that of the certificate subject in the fields issuer name and subject name, respectively.
The attribute CN (Common Name) of the DN must include a reference to a specific component, which is the certificate subscriber. On the other hand, the DN will indicate that it is a component through the organisational unit (OU), distinguishing the type of component through the CN.
The CNs, depending on the type of component certificate, will be:

Certificate type	CN
Web certificates for use with SSL (Secure Socket Layer) protocol	CN=<host name>
Authentication and signature certificates for internal-use components	CN=[A/F] Code_Component Description
Generic certificates for internal-use components	CN=[G] Code_Component Description
Signature certificates for internal-use code	CN=[F] Code_Component Description
Domain controller certificate	CN=<Controller DNS Name>

The PS (Pseudonym) attribute may be optionally used for the Generic certificates for internal-use components.

The rest of the attributes of the DN, except in the Domain Controller Certificate, which have no additional attributes, will have the following fixed values:

OU=COMPONENTES, O=BANCO DE ESPAÑA, C=ES

3.1.2 The need for names to be meaningful

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

3.1.3 Rules for interpreting various name formats

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

3.1.4 Uniqueness of names

Certificate DNs may not be repeated. The use of the component's unique code guarantees the uniqueness of the DN.

3.1.5 Name dispute resolution procedures

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

3.1.6 Recognition, authentication, and the role of trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Means of proof of possession of the private key

When the component certificate key pairs are generated by the Corporate CA, this point is not applicable.

In the event that the key pair is generated by the component, the possession of the private key, companion of the public key for which the certificate generation is being requested, shall be proven by sending the certification request, which shall include the public key signed using the companion private key.

3.2.2 Identity authentication for an entity

There is no provision for issuance of internal-use component certificates to entities outside the Banco de España and, therefore, no identification procedure for these needs to be established.

3.2.3 Identity authentication for an individual

In general, authentication of individuals within the framework of this policy shall be carried out remotely, either by signed e-mail or using an authentication certificate.

3.2.4 Non-verified applicant information

All the information stated in the previous section must be verified.

3.2.5 Validation of authority

There is no provision for issuance of internal-use component certificates to entities outside the Banco de España and, therefore, no verification of the authority procedure needs to be established.

3.2.6 Criteria for operating with external CAs

As specified in PKIBDE's CPS.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and authentication requirements for routine re-key

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

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

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

4 Certificate Life Cycle Operational Requirements

This chapter contains the operational requirements for the life cycle of component certificates issued by the Corporate CA. Although these certificates will be stored in the computer components themselves or in the cryptographic hardware that supports them, it is not the purpose of this Certificate Policy to regulate the management of said elements.
On the other hand, in this chapter some illustrations will be provided for better understanding. In the event of any difference or discrepancy between the text and the illustrations, the text will prevail in all cases, given the necessary synthetic nature of the illustrations.

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Applications for a component certificate must be carried out by the designated manager of that component; it is possible for a component to have more than one designated manager. The following chart shows the types of component managers:

Certificate type	Manager
Web certificates for use with SSL/TLS protocol	Web server manager
Authentication and signature certificates for internal-use components	Component manager
Generic certificates for internal-use components	Component manager
Code signature certificates	Project development manager
Domain controller certificate	Active Directory manager

Application for a certificate does not mean it will be obtained if the applicant does not fulfil the requirements established in the CPS or in this CP for component certificates. The PKI Administrator may request that the applicant provide the documentation it deems appropriate.

4.1.2 Enrolment process and applicants' responsibilities

There are two types of processes, depending on whether the key pair is generated by the component or the Corporate CA:

1 The authorised applicant (responsible for the component) sends his request either by a signed mail to the Registration Officer for Components role, or electronically by any means authorized for that purpose by Banco de España. There are two types of request:

- **a** Request that includes the public key and data in PKCS#10 format for the CA to generate the certificate.
- **b** Request in which only the request is included and the CA must generate the key pair.

2 The Registration Officer for Componets, using the Registration Authority, reviews the request and, if appropriate, processes it, launching the certificate issuing process.

3 The CA issues the certificate and makes it available to the RA, allowing the download to the Registration Officer for Components and telematics systems authorized for that purpose by Banco de España.

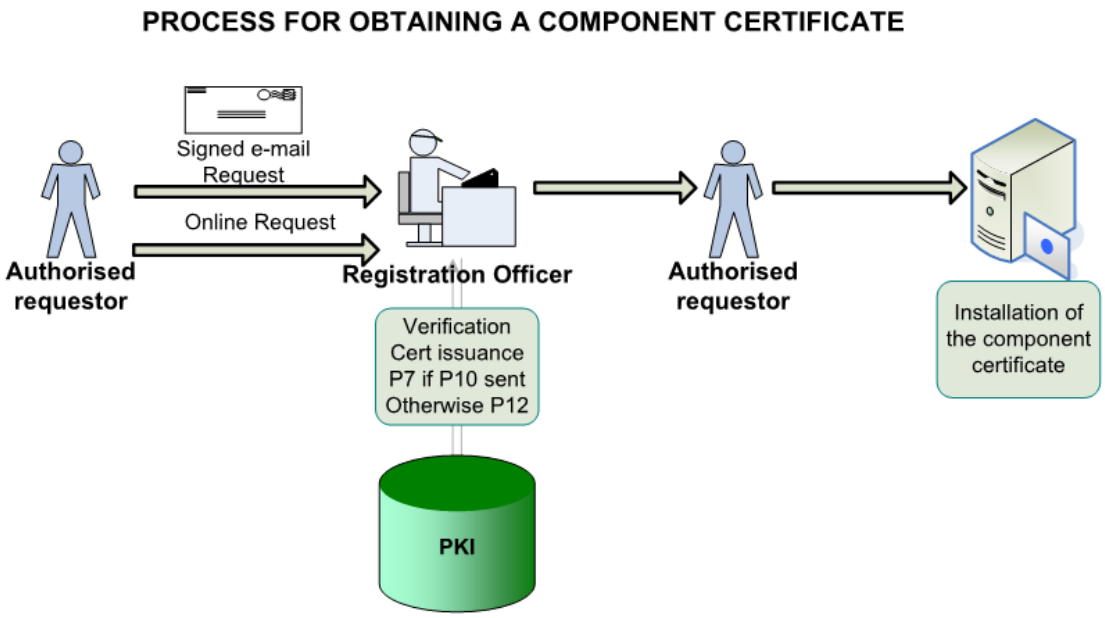
4 The Registration Officer for Components, if the certificate request was received by signed email, sends the applicant the certificate and the protection password by signed and encrypted e-mail. There are two possibilities:

a Applicants send a PKCS#10 with the generated key pair data, in which case they are sent the certificate in PKCS#7 format.

b Applicants do not send anything, in which case they are sent the certificate in PKCS#12 format.

The responsibilities of applicants not contained in this section are included in the PKIBDE Certificate Practice Statement (CPS).

The following illustration offers a summary of the process for obtaining a component certificate.



4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

Identification and authentication are always carried out electronically, with verification of the data supplied corresponding to the RA's Registration Officer for Components.

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.

4.2.3 Time limit for processing the certificate applications

The PKIBDE Corporate CA shall not be held liable for any delays that may arise in the period between application for the certificate, publication in the PKIBDE repository and its delivery. As far as possible, the Corporate CA will process requests within 24 hours.

4.3 Certificate Issuance

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

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

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

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

4.3.2 CA notification to the applicants of certificate issuance

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

4.4 Certificate Acceptance

4.4.1 Form of certificate acceptance

Applicants must confirm acceptance of the component certificate and its terms and conditions by signing the document established for that purpose.

4.4.2 Publication of the certificate by the CA

The component certificate will be published in the PKIBDE repository.

4.4.3 Notification of certificate issuance by the CA to other Authorities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Subscribers' use of the private key and certificate

Subscribers may only use the private key and the certificate for the uses authorised in this 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.

The component certificates regulated by this CP may be used only to provide the following security services:

Certificate type	Appropriate Usage
Web certificates for use with SSL/TLS protocol	Authentication of web servers with respect to their clients and establishment of communications using the SSL protocol
Authentication and signature certificates for internal-use components	Authentication of components with respect to other components or individuals and transaction signatures
Generic certificates for internal-use components	Authentication of components and encipherment of communications
Code signature certificates	Code signature to guarantee authentication and integrity

Domain controller certificate	Authentication of the domain controller with respect to the 'smartcard logon' client

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

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

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

4.6 Certificate Renewal with no Key Changeover

4.6.1 Circumstances for certificate renewal with no key changeover

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

4.7 Certificate Renewal with Key Changeover

4.7.1 Circumstances for certificate renewal with key changeover

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

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

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

4.7.2 Who may request certificate renewal?

Renewals must be requested by the certificate subscriber component manager.

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 component manager.

Identification and authentication for component certificate renewal are the same as for its initial issue.

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

In any case, certificate renewal is subject to:

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

The renewal process is the same as that of the initial issue and, therefore, is not described again.

4.7.4 Notification of the new certificate issuance to the subscriber

They are notified by e-mail.

4.7.5 Manner of acceptance of certificates with changed keys

Applicants must confirm acceptance of the component certificate and its terms and conditions by signing the document established for that purpose.

4.7.6 Publication of certificates with the new keys by the CA

The component certificate will be published in the PKIBDE repository.

4.7.7 Notification of certificate issuance by the CA to other Authorities

No stipulation.

4.8 Certificate Modification

4.8.1 Circumstances for certificate modification

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

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

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

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

Revocation of a certificate entails its publication on the public-access Certificate Revocation Lists (CRL). 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 in the CPS or in this CP.
- The component ceases to be in service.
- 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 component manager or an authorised third party.
- The certificate of a higher RA or CA in the certificate trust hierarchy is revoked.
- Any of the other causes specified in this CP or in the CPS.

The main effect of revocation as regards the certificate is the immediate and early termination of its term of validity, with which the certificate becomes invalid. Revocation shall not affect the underlying obligations created or notified by this CP, 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.

Likewise, component managers may also request revocation of their certificates, which they must do in accordance with the conditions established under point 4.9.3.

4.9.3 Procedures for requesting certificate revocation

Requests for revocation shall be carried out by the component manager in a similar manner as that described under point 4.1.2 for the issue request. They shall always be dealt with by the RA's Registration Officer for Components.

Apart from this ordinary procedure, PKI Operators and Administrators may immediately revoke any certificate upon becoming aware of the existence of any of the causes for revocation.

4.9.4 Revocation request grace period

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

4.9.5 Time limit for the CA to process the revocation request

Requests for revocation of component certificates are processed immediately.

4.9.6 Requirements for revocation verification by relying parties

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

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

For component certificates, the ordinary validity verification procedure for a certificate shall be carried out with Banco de España's Validation Authority, which shall indicate, through the OCSP protocol, the status of the certificate.

4.9.7 CRL issuance frequency

As specified in PKIBDE's CPS.

4.9.8 Maximum latency between the generation of CRLs and their publication

The maximum time allowed between generation of the CRLs and their publication in the repository is 6 hours.

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

4.9.9 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.

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

No stipulation.

4.9.12 Special requirements for the renewal of compromised keys

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

4.9.13 Causes for suspension

There is no provision for the suspension of internal-use component certificates.

4.9.14 Who can request the suspension?

No stipulation.

4.9.15 Procedure for requesting certificate suspension

No stipulation.

4.9.16 Suspension period limits

No stipulation.

4.10 Certificate status services

4.10.1 Operational characteristics

As specified in PKIBDE's CPS.

4.10.2 Service availability

As specified in PKIBDE's CPS.

4.10.3 Additional features

As specified in PKIBDE's CPS.

4.11 End of Subscription

Certificate subscription may be ended due to the following causes:

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

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

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery practices and policies

The private key for internal-use component certificates is not archived.

4.12.2 Session key protection and recovery policies and practices

No stipulation.

5 Management, Operational, and Physical Controls

5.1 Physical Security Controls

5.1.1 Site location and construction

As specified in PKIBDE's CPS.

5.1.2 Physical access

As specified in PKIBDE's CPS.

5.1.3 Power and air-conditioning

As specified in PKIBDE's CPS.

5.1.4 Water exposure

As specified in PKIBDE's CPS.

5.1.5 Fire prevention and protection

As specified in PKIBDE's CPS.

5.1.6 Storage system

As specified in PKIBDE's CPS.

5.1.7 Waste disposal

As specified in PKIBDE's CPS.

5.1.8 Offsite backup

As specified in PKIBDE's CPS.

5.2 Procedural controls

5.2.1 Roles responsible for PKI control and management

As specified in PKIBDE's CPS.

5.2.2 Number of individuals required to perform each task

As specified in PKIBDE's CPS.

5.2.3 Identification and authentication of each user

As specified in PKIBDE's CPS.

5.2.4 Roles that require separation of duties

As specified in PKIBDE's CPS.

5.3 Personnel Security Control

5.3.1 Requirements concerning professional qualification, knowledge and experience

As specified in PKIBDE's CPS.

5.3.2 Background checks and clearance procedures

As specified in PKIBDE's CPS.

5.3.3 Training requirements
As specified in PKIBDE's CPS.

5.3.4 Retraining requirements and frequency
As specified in PKIBDE's CPS.

5.3.5 Frequency and sequence for job rotation
As specified in PKIBDE's CPS.

5.3.6 Sanctions for unauthorised actions
As specified in PKIBDE's CPS.

5.3.7 Requirements for third party contracting
As specified in PKIBDE's CPS.

5.3.8 Documentation supplied to personnel
As specified in PKIBDE's CPS.

5.4 Security Audit Procedures
5.4.1 Types of events recorded
As specified in PKIBDE's CPS.

5.4.2 Frequency with which audit logs are processed
As specified in PKIBDE's CPS.

5.4.3 Period for which audit logs are kept
As specified in PKIBDE's CPS.

5.4.4 Audit log protection
As specified in PKIBDE's CPS.

5.4.5 Audit log back up procedures
As specified in PKIBDE's CPS.

5.4.6 Audit data collection system (internal vs. external)
As specified in PKIBDE's CPS.

5.4.7 Notification to the subject who caused the event
As specified in PKIBDE's CPS.

5.4.8 Vulnerability assessment
As specified in PKIBDE's CPS.

5.5 Records Archive
5.5.1 Types of records archived
As specified in PKIBDE's CPS.

5.5.2 Archive retention period
As specified in PKIBDE's CPS.

5.5.3 Archive protection
As specified in PKIBDE's CPS.

5.5.4 Archive backup procedures
As specified in PKIBDE's CPS.

5.5.5 Requirements for time-stamping records
As specified in PKIBDE's CPS.

5.5.6 Audit data archive system (internal vs. external)
As specified in PKIBDE's CPS.

5.5.7 Procedures to obtain and verify archived information
As specified in PKIBDE's CPS.

5.6 CA Key Changeover
As specified in PKIBDE's CPS.

5.7 Compromised Key and Disaster Recovery
5.7.1 Incident and compromise handling procedures
As specified in PKIBDE's CPS.

5.7.2 Corruption of computing resources, software, and/or data
As specified in PKIBDE's CPS.

5.7.3 Action procedures in the event of compromise of an Authority's private key
As specified in PKIBDE's CPS.

5.7.4 Installation following a natural disaster or another type of catastrophe
As specified in PKIBDE's CPS.

5.8 CA or RA Termination
5.8.1 Certification Authority
As specified in PKIBDE's CPS.

5.8.2 Registration Authority
No stipulation.

6 Technical Security Controls

Technical security controls for PKIBDE internal components, and specifically for Root CA and Corporate CA in the certificate issuing and signing processes are detailed in the CPS of the PKIBDE.
This paragraph describes the technical security controls for issuing certificates under this CP

6.1 Key pair generation and installation

6.1.1 Key pair generation

If it is the PKIBDE Corporate CA that generates the keys for component certificates, these will be created in cryptographic hardware modules with FIPS 140-2 Level 3 certification, installed in the CA. However, this policy does stipulate that it is mandatory for these pairs of keys to be generated by PKIBDE.

6.1.2 Delivery of private keys to subscribers

In the case of delivery of the private key when generated by the CA, the delivery will be carried out by signed e-mail to the component manager, attaching a file in PKCS#12 format.

6.1.3 Delivery of the public key to the certificate issuer

When the key pair has been generated by the component, the public key will be provided by way of a file in PKCS#10 format, attaching the request, which will constitute the certificate signing request (CSR).
When the key pair has been generated by the Corporate CA, no delivery is necessary.

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

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

6.1.5 Key sizes

The minimum size of the component certificate keys is 2048 bits.

6.1.6 Public key generation parameters and quality checks

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

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

The keys defined in this policy and, therefore, the accompanying certificates, shall be used for the component operations that require authentication, electronic signature or encipherment with respect to the Banco de España's information systems.
For this purpose, the 'Key Usage' and 'Extended Key Usage' fields of the certificate include the following uses:

Certificate type	Key Usage	Extended Key Usage
Web server certificates for use of SSL/TLS protocol	digitalSignature. keyEncipherment. keyAgreement	Serverauth AnyExtendedKeyUsage
Authentication and signature certificates for components	digitalSignature. keyEncipherment. keyAgreement	EmailProtection anyExtendedKeyUsage
Generic certificates for components	digitalSignature. dataEncipherment. keyEncipherment. keyAgreement	emailProtection anyExtendedKeyUsage
Code signature certificates	digitalSignature.	codeSigning anyExtendedKeyUsage
Domain controller certificate	digitalSignature. keyEncipherment	Serverauth clientAuth

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards

The module used for the creation of keys used by PKIBDE's Corporate CA has FIPS 140-2 Level 3 certification.

Start-up of each one of the Certification Authorities, taking into account that a 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.

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

The private key, both for the Root CA and the Subordinate CA, is under multi-person control; it can be activated by running the CA software through a combination of CA operators.

It is the only method to activate said private key.

No multi-person control has been set to access the private keys of certificates issued under this CP.

6.2.3 Escrow of private keys

The private keys of component certificates are housed on the components themselves or in additional devices, and access to operations should be protected by a PIN.

6.2.4 Private key backup copy

Given that this CP does not stipulate that it is mandatory for the component certificate key pairs to be generated by the PKIBDE CA, neither does it dictate any procedure for making back-up copies of these key, although this is highly recommendable.

6.2.5 Private key archive

The Corporate CA, once it has finalised the component certificate issuing process, keeps a copy of its private key, in cases in which it has generated it.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private key storage in a cryptographic module

If the PKIBDE CA generates private keys, these will be stored in the Corporate AC cryptographic module, but they are not subsequently conserved.

6.2.8 Private key activation method

In cases in which the private key is generated by the CA, a PKCS#12 file protected by a password is provided.

In cases in which it is generated by the component, once the certificate has been obtained, it will be activated in accordance with the specifications for the component in question.

6.2.9 Private key deactivation method

Deactivation occurs once an established period of time has elapsed since the PIN was entered, or through specific mechanisms in each component.

6.2.10 Private key destruction method

As specified in PKIBDE's CPS.

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

As specified in PKIBDE's CPS.

6.3.2 Operational period of certificates and usage periods for key pairs

Component certificates are valid for a 4-year usage period, although at the time of issue, the CA may set different periods.

6.4 Activation Data

6.4.1 Generation and installation of activation data

As specified in PKIBDE's CPS.

6.4.2 Activation data protection

As specified in PKIBDE's CPS.

6.4.3 Other activation data aspects

As specified in PKIBDE's CPS.

6.5 Computer Security Controls

6.5.1 Specific security technical requirements

As specified in PKIBDE's CPS.

6.5.2 Computer security evaluation

As specified in PKIBDE's CPS.

6.6 Life cycle security controls

6.6.1 System development controls

As specified in PKIBDE's CPS.

6.6.2 Security management controls

As specified in PKIBDE's CPS.

6.6.3 Life cycle security controls

As specified in PKIBDE's CPS.

6.7 Network Security Controls

As specified in PKIBDE's CPS.

6.8 Time-stamping

As specified in PKIBDE's CPS.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version number

Component certificates for internal use issued by the Corporate CA use the X.509 version 3 (X.509 v3) standard.

7.1.2 Certificate extensions

The certificate extensions used generically are:

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

Below are the profiles for the types of component certificates issued by PKIBDE for internal use:

7.1.2.1 Secure Server Certificate (SSL/TLS)

Secure Server Certificate (SSL/TLS)		
FIELD	**CONTENT**	**CRITICAL extensions**
Field X509v1		
1. Version	V3	
2. Serial Number	Random	
3. Signature Algorithm	sha1withRsaSignature / sha256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Lifetime	4 years	
6. Subject	CN=<host name>, OU=COMPONENTES, O=BANCO DE ESPAÑA, C=ES	
7. Subject Public Key Info	Algorithm: RSA Encryption Minimum key length: 2048 (big string)	
X509v3 extensions		
1. Subject Key Identifier	Derived from using the SHA-1 hash on the subject's public key.	NO
2. Authority Key Identifier		NO
keyIdentifier	Derived from using the SHA-1 hash on the issuing CA's public key: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		YES
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	serverAuth, anyExtendedKeyUsage	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. © 2015 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.9	
Notice Reference	Certificado de componente informático para uso interno sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. Subject Alternate Names	DNSName=<FQDN> E-mail address pursuant to RFC 822 (optional) IPAddress	NO
7. Basic Constraints		YES
Subject Type	End Entity	
Path Length Constraint	Not used	
8. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributi	NO

Secure Server Certificate (SSL/TLS)		
FIELD	**CONTENT**	**CRITICAL extensions**
	onPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	
9. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
10. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	SERVIDOR_SSL	

7.1.2.2 Authentication/signature certificate for internal-use components

Authentication/signature certificate for internal-use components		
FIELD	**CONTENT**	**CRITICAL extensions**
Field X509v1		
1. Version	V3	
2. Serial Number	Random	
3. Signature Algorithm	SHA-256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Lifetime	4 years	
6. Subject	CN=[A/F] Code_Component Description OU=COMPONENTES O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algorithm: RSA Encryption Minimum Key Length: 2048(big string)	
X509v3 extensions		
1. Subject Key Identifier	Derived from using the SHA-1 hash on the subject's public key.	NO
2. Authority Key Identifier		NO
keyIdentifier	Derived from using the SHA-1 hash on the issuing CA's public key: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		YES
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	emailProtection, anyExtendedKeyUsage	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. © 2015 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.9	
Notice Reference	Certificado de componente informático para uso interno sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. Subject Alternate Names	E-mail address pursuant to RFC 822 (optional)	NO
7. Basic Constraints		YES
Subject Type	End Entity	
Path Length Constraint	Not used	
8. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE	NO

Authentication/signature certificate for internal-use components		
FIELD	**CONTENT**	**CRITICAL extensions**
	,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	
9. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
10. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	FIRMA_COMPONENTES	

7.1.2.3 Generic certificate for internal-use components

Generic certificate for internal-use components		
FIELD	**CONTENT**	**CRITICAL extensions**
Field X509v1		
1. Version	V3	
2. Serial Number	Random	
3. Signature Algorithm	sha1withRsaSignature / sha256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Lifetime	4 years	
6. Subject	CN=[G] Code_Component Description PS=Código_usuario (campo opcional) OU=COMPONENTES O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algorithm: RSA Encryption Minimum Key Length: 2048 (big string)	
X509v3 extensions		
1. Subject Key Identifier	Derived from using the SHA-1 hash on the subject's public key.	NO
2. Authority Key Identifier		NO
keyIdentifier	Derived from using the SHA-1 hash on the issuing CA's public key: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		YES
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	1	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	clientAuth, emailProtection, anyExtendedKeyUsage	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. © 2015 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.9	
Notice Reference	Certificado de componente informático para uso interno sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. Subject Alternate Names	E-mail address pursuant to RFC 822 (optional)	NO
7. Basic Constraints		YES
Subject Type	End Entity	
Path Length Constraint	Not used	
8. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Publi	NO

Generic certificate for internal-use components		
FIELD	**CONTENT**	**CRITICAL extensions**
	c%20Key%20Services,CN=Services,CN=Configuration,DC=BDE ,DC=ES?certificateRevocationList?base?objectclass=cRLDistrib utionPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	
9. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
10. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	GENERICA_COMPONENTES	

7.1.2.4 Code signature certificate

Code signature certificate		
FIELD	**CONTENT**	**CRITICAL extensions**
Field X509v1		
1. Version	V3	
2. Serial Number	Random	
3. Signature Algorithm	sha256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Lifetime	4 years	
6. Subject	CN=[F] Code_Component Description OU=COMPONENTES O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algorithm: RSA Encryption Minimum Key Length: 2048(big string)	
X509v3 extensions		
1. Subject Key Identifier	Derived from using the SHA-1 hash on the subject's public key.	NO
2. Authority Key Identifier		NO
keyIdentifier	Derived from using the SHA-1 hash on the issuing CA's public key: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		YES
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	codeSigning, anyExtendedKeyUsage	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. © 2015 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.9	
Notice Reference	Certificado de componente informático para uso interno sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. Basic Constraints		YES
Subject Type	End Entity	
Path Length Constraint	Not used	
7. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO

Code signature certificate		
FIELD	**CONTENT**	**CRITICAL extensions**
	(2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	
8. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
9. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	FIRMA_CODIGO	

7.1.2.5 Domain controller certificate

7.1.2.6

Domain controller certificate		
FIELD	**CONTENT**	**CRITICAL extensions**
Field X509v1		
1. Version	V3	
2. Serial Number	Random	
3. Signature Algorithm	sha256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Lifetime	4 years	
6. Subject	CN=<Domain Controller DNS Name>	
7. Subject Public Key Info	Algorithm: RSA Encryption Minimum Key Length: 2048 (big string)	
X509v3 extensions		
1. Subject Key Identifier	Derived from using the SHA-1 hash on the subject's public key.	NO
2. Authority Key Identifier		NO
keyIdentifier	Derived from using the SHA-1 hash on the issuing CA's public key: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		YES
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	clientAuth, serverAuth	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. © 2015 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.9	
Notice Reference	Certificado de componente informático para uso interno sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. Subject Alternate Names	Other Name: 1.3.6.1.4.1.311.25.1=<Controller GUID> DNS Name=<Controller DNS Name>	NO
7. Basic Constraints		YES
Subject Type	End Entity	
Path Length Constraint	Not used	
8. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl	NO

Domain controller certificate		
FIELD	**CONTENT**	**CRITICAL extensions**
	(3) HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	
9. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
10. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	CONTROLADOR_DOMINIO	

7.1.3 Algorithm Object Identifiers (OID)

Cryptographic algorithm object identifiers (OID):

- SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
- SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- SHA-512 with RSA Encryption (1.2.840.113549.1.1.13)

7.1.4 Name formats

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

7.1.5 Name constraints

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

The PS (Pseudonym) attribute may be optionally used for the Generic certificates for internal-use components.

The CN (Common Name) attributes of the DN will be what distinguish one DN from another. The rest of the attributes of the DN, except in the Domain Controller Certificate, which have no additional attributes, will have the following fixed values:

OU=COMPONENTE, O=BANCO DE ESPAÑA, C=ES

7.1.6 Certificate Policy Object Identifiers (OID)

The OID of this CP is 1.3.6.1.4.1.19484.2.2.9. An X.Y format extension is added to indicate the version.

7.1.7 Use of the "PolicyConstraints" extension

No stipulation.

7.1.8 Syntax and semantics of the "PolicyQualifier

The Certificate Policies extension contains the following Policy Qualifiers:

- URL CPS: contains the URL to the CPS and to 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 content for certificates regulated under this policy can be seen in point 7.1.2 Certificate extensions.

7.1.9 Processing semantics for the critical "CertificatePolicy" extension

No stipulation.

7.2 CRL Profile

7.2.1 Version number

As specified in PKIBDE's CPS.

7.2.2 CRL and extensions

As specified in PKIBDE's CPS.

7.3 OCSP Profile

7.3.1 Version number(s)

As specified in PKIBDE's CPS.

7.3.2 OCSP Extensions

As specified in PKIBDE's CPS.

8 Compliance Audits and Other Controls

8.1 Frequency or Circumstances of Controls for each Authority
As specified in PKIBDE's CPS.

8.2 Identity/Qualifications of the Auditor
As specified in PKIBDE's CPS.

8.3 Relationship between the Assessor and the Entity being Assessed
As specified in PKIBDE's CPS.

8.4 Aspects Covered by Controls
As specified in PKIBDE's CPS.

8.5 Actions Taken as a Result of Deficiencies Found
As specified in PKIBDE's CPS.

8.6 Notification of the Results
As specified in PKIBDE's CPS.

9 Other Legal and Business Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

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

9.1.3 Revocation or status information fees

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

9.1.4 Fees for other services, such as policy information

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

9.1.5 Refund policy

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

9.2 Information Confidentiality

9.2.1 Scope of confidential information

As specified in PKIBDE's CPS.

9.2.2 Non-confidential information

As specified in PKIBDE's CPS.

9.2.3 Duty to maintain professional secrecy

As specified in PKIBDE's CPS.

9.3 Personal Data Protection

9.3.1 Personal data protection policy

As specified in PKIBDE's CPS.

9.3.2 Information considered private

As specified in PKIBDE's CPS.

9.3.3 Information not classified as private

As specified in PKIBDE's CPS.

9.3.4 Responsibility to protect personal data

As specified in PKIBDE's CPS.

9.3.5 Notification of and consent to the use of personal data

As specified in PKIBDE's CPS.

9.3.6 Disclosure within legal proceedings

As specified in PKIBDE's CPS.

9.3.7 Other circumstances in which data may be made public

As specified in PKIBDE's CPS.

9.4 Intellectual Property Rights

As specified in PKIBDE's CPS.

9.5 Obligations

9.5.1 Obligations of the CA

As specified in PKIBDE's CPS.

The services provided by the CA in the context of this CP are the services of issuance, renewal and revocation of component certificates.

9.5.2 Obligations of the RA

As specified in PKIBDE's CPS.

9.5.3 Obligations of certificate subscribers

As specified in PKIBDE's CPS.

9.5.4 Obligations of relying parties

As specified in PKIBDE's CPS.

9.5.5 Obligations of other participants

As specified in PKIBDE's CPS.

9.6 Liabilities

9.6.1 PKIBDE's liabilities

As specified in PKIBDE's CPS.

9.6.2 PKIBDE liability exemption

As specified in PKIBDE's CPS.

9.6.3 Scope of liability coverage

As specified in PKIBDE's CPS.

9.7 Loss Limits

As specified in PKIBDE's CPS.

9.8 Validity Period

9.8.1 Term

This CP shall enter into force from the moment it is approved by the PAA and published in the PKIBDE repository.

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

9.8.2 CP substitution and termination

This CP shall always be substituted by a new version, regardless of the importance of the changes carried out therein, meaning that it will always be applicable in its entirety.
When the CP is terminated, it will be withdrawn from the PKIBDE public repository, although it will be held for 15 years.

9.8.3 Consequences of termination

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

9.9 Individual notices and communications with participants

As specified in PKIBDE's CPS.

9.10 Specification Amendment Procedures

9.10.1 Amendment procedures

As specified in PKIBDE's CPS.

9.10.2 Notification period and mechanism

As specified in PKIBDE's CPS.

9.10.3 Circumstances in which the OID must be changed

As specified in PKIBDE's CPS.

9.11 Disputes and Jurisdiction

As specified in PKIBDE's CPS.

9.12 Governing Law

As specified in PKIBDE's CPS.

9.13 Compliance with Applicable Law

As specified in PKIBDE's CPS.

9.14 Miscellaneous Provisions

9.14.1 Entire agreement clause

As specified in PKIBDE's CPS.

9.14.2 Independence

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

9.14.3 Resolution through the courts

No stipulation.

9.15 Other Provisions

No stipulation.

10 Personal Data Protection

10.1 Data Protection Legal Scheme

As specified in PKIBDE's CPS.

10.2 File Creation and Registration

As specified in PKIBDE's CPS.

10.3 Personal Data Protection Act Security Document

As specified in PKIBDE's CPS.