BANCO DE ESPAÑA
Eurosistema

21.05.2010

OID: 1.3.6.1.4.1.19484.2.2.6.1.2

Banco de España's Public Key Infrastructure

Certificate Policy for Authentication Certificates

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

Control Sheet

Title	Certificate Policy for Authentication Certificates
Author	General Secretariat Legal Department Information Systems Department
Version	1.2
Date	21.05.2010

Change Log

Version	**Date**	**Change Reason**
1.0	5.04.2006	Initial Version
1.1	25.10.2006	Modification of Certificate Profile Elimination of Suspension Process
1.2	21.05.2010	Document review after electronic time stamping services deployment. Rename of Policy Administration Authority by Policy Administration Authority

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 The Policy Administration Authority 14

1.3.2 Certification Authorities 14

1.3.3 Registration Authorities 15

1.3.4 Validation Authority 15

1.3.5 Keys Archive 15

1.3.6 Certificate Subscribers 15

1.3.7 Relying Parties 15

1.3.8 Other affected parties 15

1.4 Certificate Usage 16

1.4.1 Appropriate certificate use 16

1.4.2 Certificate Usage Constraints and Restrictions 16

1.5 Policy Administration 16

1.5.1 Banco de España, as PKIBDE owner 16

1.5.2 Contact Person 16

1.5.3 Establishment of the suitability of a CPS from an External CA as regards the PKIBDE Certificate Policies 16

1.5.4 Approval Procedure for this CP 16

1.6 Definitions and Acronyms 17

1.6.1 Definitions 17

1.6.2 Acronyms 17

2 Publication and Repository Responsibilities 18

2.1 Repositories 18

2.2 Publication of Certification Data 18

2.3 Publication Timescale or Frequency 18

2.4 Repository Access Controls 18

3 Identification and Authentication (I&A) 19

3.1 Naming 19

3.1.1 Types of names 19

3.1.2 The need for names to be meaningful 19

3.1.3 Rules for interpreting various name formats 19

3.1.4 Uniqueness of names 19

3.1.5 Name dispute resolution procedures 19

3.1.6 Recognition, authentication, and the role of trademarks 19

3.2 Initial Identity Validation 19

3.2.1 Means of proof of possession of the private key 19

3.2.2 Identity authentication for an entity 19

3.2.3 Identity authentication for an individual 20

3.2.4 Non-verified applicant information 20

3.2.5 Validation of authority 20

3.2.6 Criteria for operating with external CAs 20

3.3 Identification and Authentication for Re-key Requests 20

3.3.1 Identification and authentication requirements for routine re-key 20

3.3.2 Identification and authentication requirements for re-key after certificate revocation 20

4 Certificate Life-Cycle Operational Requirements 21

4.1 Certificate Application 21

4.1.1 Who can submit a certificate application? 21

4.1.2 Enrolment process and applicants' responsibilities 21

4.2 Certificate Application Processing 22

4.2.1 Performance of identification and authentication procedures 22

4.2.2 Approval or rejection of certificate applications 22

4.2.3 Time limit for processing the certificate applications 23

4.3 Certificate Issuance 23

4.3.1 Actions performed by the CA during the issuance of the certificate 23

4.3.2 CA notification to the applicants of certificate issuance 23

4.4 Certificate Acceptance 23

4.4.1 Form of certificate acceptance 23

4.4.2 Publication of the certificate by the CA 23

4.4.3 Notification of certificate issuance by the CA to other Authorities 23

4.5 Key Pair and Certificate Usage 23

4.5.1 Subscribers' use of the private key and certificate 23

4.5.2 Relying parties' use of the public key and the certificate 24

4.6 Certificate Renewal 24

4.6.1 Circumstances for certificate renewal with no key changeover 24

4.7 Certificate Re-key 24

4.7.1 Circumstances for certificate renewal with key changeover 24

4.7.2 Who may request certificate renewal? 24

4.7.3 Procedures for processing certificate renewal requests with key changeover 24

4.7.4 Notification of the new certificate issuance to the subscriber 25

4.7.5 Manner of acceptance of certificates with changed keys 26

4.7.6 Publication of certificates with the new keys by the CA 26

4.7.7 Notification of certificate issuance by the CA to other Authorities 26

4.8 Certificate Modification 26

4.8.1 Circumstances for certificate modification 26

4.9 Certificate Revocation and Suspension 26

4.9.1 Circumstances for revocation 26

4.9.2 Who can request revocation? 27

4.9.3 Procedures for requesting certificate revocation 27

4.9.4 Revocation request grace period 27

4.9.5 Time limit for the CA to process the revocation request 27

4.9.6 Requirements for revocation verification by relying parties 27

4.9.7 CRL issuance frequency 27

4.9.8 Maximum latency between the generation of CRLs and their publication 28

4.9.9 Online certificate revocation status checking availability 28

4.9.10 Online revocation checking requirements 28

4.9.11 Other forms of revocation alerts available 28

4.9.12 Special requirements for the revocation of compromised keys 28

4.9.13 Causes for suspension 28

4.9.14 Who can request the suspension? 28

4.9.15 Procedure for requesting certificate suspension 28

4.9.16 Suspension period limits 28

4.10 Certificate Status Services 28

4.10.1 Operational characteristics 28

4.10.2 Service availability 28

4.10.3 Additional features 28

4.11 End of Subscription 29

4.12 Key Escrow and Recovery 29

4.12.1 Key escrow and recovery practices and policies 29

4.12.2 Session key protection and recovery policies and practices 29

5 Facility, Management, and Operational Controls 30

5.1 Physical Security Controls 30

5.1.1 Site location and construction 30

5.1.2 Physical access 30

5.1.3 Power and air-conditioning 30

5.1.4 Water exposure 30

5.1.5 Fire prevention and protection 30

5.1.6 Storage system 30

5.1.7 Waste disposal 30

5.1.8 Offsite backup 30

5.2 Procedural Controls 30

5.2.1 Roles responsible for PKI control and management 30

5.2.2 Number of individuals required to perform each task 30

5.2.3 Identification and authentication of each user 30

5.2.4 Roles that require separation of duties 30

5.3 Personnel Controls 30

5.3.1 Requirements concerning professional qualification, knowledge and experience 30

5.3.2 Background checks and clearance procedures 30

5.3.3 Training requirements 30

5.3.4 Retraining requirements and frequency 30

5.3.5 Frequency and sequence for job rotation 31

5.3.6 Sanctions for unauthorised actions 31

5.3.7 Requirements for third party contracting 31

5.3.8 Documentation supplied to personnel 31

5.4 Audit Logging Procedures 31

5.4.1 Types of events recorded 31

5.4.2 Frequency with which audit logs are processed 31

5.4.3 Period for which audit logs are kept 31

5.4.4 Audit log protection 31

5.4.5 Audit log back up procedures 31

5.4.6 Audit data collection system (internal vs. external) 31

5.4.7 Notification to the subject who caused the event 31

5.4.8 Vulnerability assessment 31

5.5 Records Archival 31

5.5.1 Types of records archived 31

5.5.2 Archive retention period 31

5.5.3 Archive protection 31

5.5.4 Archive backup procedures 31

5.5.5 Requirements for time-stamping records 31

5.5.6 Audit data archive system (internal vs. external) 32

5.5.7 Procedures to obtain and verify archived information 32

5.6 Key Changeover 32

5.7 Compromise and Disaster Recovery 32

5.7.1 Incident and compromise handling procedures 32

5.7.2 Corruption of computing resources, software, and/or data 32

5.7.3 Action procedures in the event of compromise of an Authority's private key 32

5.7.4 Installation following a natural disaster or another type of catastrophe 32

5.8 CA or RA Termination 32

5.8.1 Certification Authority 32

5.8.2 Registration Authority 32

6 Technical Security Controls 33

6.1 Key Pair Generation and Installation 33

6.1.1 Key pair generation 33

6.1.2 Delivery of private keys to subscribers 33

6.1.3 Delivery of the public key to the certificate issuer 33

6.1.4 Delivery of the CA's public key to relying parties 33

6.1.5 Key sizes 33

6.1.6 Public key generation parameters and quality checks 33

6.1.7 Key usage purposes (KeyUsage field in X.509 v3) 33

6.2 Private Key Protection and Cryptographic Module Engineering Controls 34

6.2.1 Cryptographic module standards 34

6.2.2 Private key multi-person (k out of n) control 34

6.2.3 Escrow of private keys 34

6.2.4 Private key backup copy 34

6.2.5 Private key archive 34

6.2.6 Private key transfer into or from a cryptographic module 35

6.2.7 Private key storage in a cryptographic module 35

6.2.8 Private key activation method 35

6.2.9 Private key deactivation method 35

6.2.10 Private key destruction method 35

6.2.11 Cryptographic module classification 35

6.3 Other Aspects of Key Pair Management 35

6.3.1 Public key archive 35

6.3.2 Operational period of certificates and usage periods for key pairs 35

6.4 Activation Data 35

6.4.1 Generation and installation of activation data 35

6.4.2 Activation data protection 35

6.4.3 Other activation data aspects 35

6.5 Computer Security Controls 35

6.5.1 Specific security technical requirements 35

6.5.2 Computer security evaluation 35

6.6 Life Cycle Security Controls 36

6.6.1 System development controls 36

6.6.2 Security management controls 36

6.6.3 Life cycle security controls 36

6.7 Network Security Controls 36

6.8 Timestamping 36

7 Certificate, CRL, and OCSP Profiles 37

7.1 Certificate Profile 37

7.1.1 Version number 37

7.1.2 Certificate extensions 37

7.1.3 Algorithm Object Identifiers (OID) 39

7.1.4 Name formats 39

7.1.5 Name constraints 39

7.1.6 Certificate Policy Object Identifiers (OID) 39

7.1.7 Use of the "PolicyConstraints" extension 39

7.1.8 Syntax and semantics of the “PolicyQualifier 39

7.1.9 Processing semantics for the critical “CertificatePolicy” extension 40

7.2 CRL Profile 40

7.2.1 Version number 40

7.2.2 CRL and extensions 40

7.3 OCSP Profile 40

7.3.1 Version number(s) 40

7.3.2 OCSP Extensions 40

8 Compliance Audit and Other Assessment 41

8.1 Frequency or Circumstances of Controls for each Authority 41

8.2 Identity/Qualifications of the Auditor 41

8.3 Relationship between the Assessor and the Entity being Assessed 41

8.4 Aspects Covered by Controls 41

8.5 Actions Taken as a Result of Deficiencies Found 41

8.6 Notification of the Results 41

9 Other Business and Legal Matters 42

9.1 Fees 42

9.1.1 Certificate issuance or renewal fees 42

9.1.2 Certificate access fees 42

9.1.3 Revocation or status information fees 42

9.1.4 Fees for other services, such as policy information 42

9.1.5 Refund policy 42

9.2 Confidentiality of Business Information 42

9.2.1 Scope of confidential information 42

9.2.2 Non-confidential information 42

9.2.3 Duty to maintain professional secrecy 42

9.3 Privacy of Personal Information 42

9.3.1 Personal data protection policy 42

9.3.2 Information considered private 42

9.3.3 Information not classified as private 42

9.3.4 Responsibility to protect personal data 42

9.3.5 Notification of and consent to the use of personal data 42

9.3.6 Disclosure within legal proceedings 42

9.3.7 Other circumstances in which data may be made public 42

9.4 Intellectual Property Rights 43

9.5 Representations and Warranties 43

9.5.1 Obligations of the CA 43

9.5.2 Obligations of the RA 43

9.5.3 Obligations of certificate subscribers 43

9.5.4 Obligations of relying parties 43

9.5.5 Obligations of other participants 43

9.6 Disclaimers of Warranties 43

9.6.1 PKIBDE's liabilities 43

9.6.2 PKIBDE liability exemption 43

9.6.3 Scope of liability coverage 43

9.7 Limitations of Liability 43

9.8 Term and Termination 43

9.8.1 Term 43

9.8.2 CP substitution and termination 43

9.8.3 Consequences of termination 44

9.9 Individual notices and communications with participants 44

9.10 Amendments 44

9.10.1 Amendment procedures 44

9.10.2 Notification period and mechanism 44

9.10.3 Circumstances in which the OID must be changed 44

9.11 Dispute Resolution Procedures 44

9.12 Governing Law 44

9.13 Compliance with Applicable Law 44

9.14 Miscellaneous Provisions 44

9.14.1 Entire agreement clause 44

9.14.2 Independence 44

9.14.3 Resolution through the courts 44

9.15 Other Provisions 44

10 Personal Data Protection 45

10.1 Data Protection Legal Scheme 45

10.2 File Creation and Registration 45

10.3 Personal Data Protection Act Security Document 45

1 Introduction

1.1 Overview

This document sets out the Certificate Policy (CP) governing the personal authentication certificates issued by the Corporate Certification Authority of the Public Key Infrastructure (hereinafter, PKI) of Banco de España (hereinafter, PKIBDE).

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.

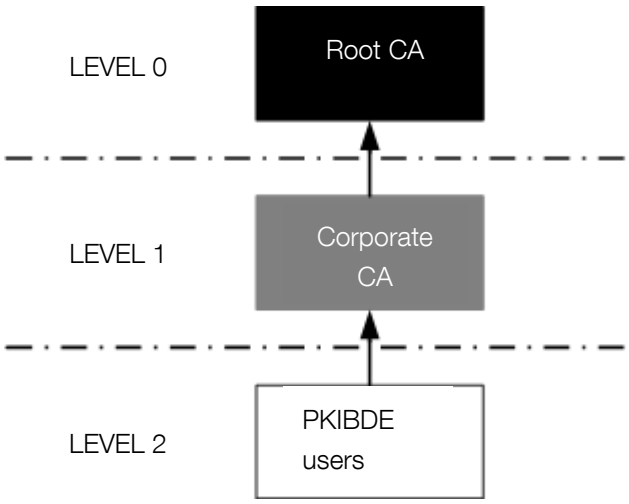
This CP details and completes the "Certification Practice Statement" (CPS) of Banco de España's PKI (PKIBDE), containing the rules to which the use of the certificates defined in this policy are subject, as well as the scope of application and the technical characteristics of this type of certificate.

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 authentication 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:



1.2 Document Name and Identification

Document name	Certificate Policy (CP) for Authentication Certificates
Document version	1.2
Document status	Approved
Date of issue	21.05.2010
OID (Object Identifier)	1.3.6.1.4.1.19484.2.2.6.1.2
CPS location	http://pki.bde.es/politicas
Related CPS	Certification Practice Statement of Banco de España's PKI OID 1.3.6.1.4.19484.2.2.1

1.3 PKI Participants

The participating entities and persons are:

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

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

1.3.2 Certification Authorities

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

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:

Unique Name	CN= BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Serial Number	F16D 7586 5D7C CF92 41AD A17A CD9A 3DE2
Unique 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. Its function is to issue certificates for PKIBDE users. This CP refers to the authentication certificates issued by said entity. Its most significant data are:

Unique Name	CN= BANCO DE ESPAÑA-AC CORPORATIVA, O=BANCO DE ESPAÑA, C=ES
Serial Number	366A 524D A5E4 4AF8 4108 A140 9B9B 76EB
Unique 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

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

Authentication Certificate issuance is carried out with the intervention of the Corporate RA, with requests managed remotely.

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 types of persons who may be subscribers of authentication certificates issued by the Corporate CA are limited to those included in the following chart:

Certification Environment	Subscribers
Corporate CA	Banco de España's employees
	Banco de España's collaborators
	Personnel in contracted companies with access to Banco de España's information systems

1.3.7 Relying Parties

Relying parties are those that make use of the certificates to identify the subscribers of authentication certificates issued by the PKIBDE Corporate CA.

1.3.8 Other affected parties

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

User Administrators: individuals within Banco de España who process the personal certificate requests and verify that they are obtained correctly.

1.4 Certificate Usage

1.4.1 Appropriate certificate use

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.

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 certificates regulated by this CP shall be used for the identification of persons as regards Banco de España's information systems.

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	+34913385000	**Fax**	+34915310059

1.5.2 Contact Person

This CP is managed by the Policy Administration Authority (PAA) of Banco de España's PKI:

Name	Banco de España's PKI Policy Administration Authority		
E-mail address	pkibde@bde.es		
Address	C/Alcala, 522. 28027 - Madrid (Spain)		
Telephone	+34913386610	**Fax**	+34913386870

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

As specified in PKIBDE's CPS.

1.5.4 Approval Procedure 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 though 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 Administration 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: Banco de España'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
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 (I&A)

3.1 Naming

3.1.1 Types of names

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

The CN (Common Name) attribute of the DN contains an ID that identifies it as an authentication certificate, '[A]', followed by the name and the two surnames.

Additionally, the following fields are used:

- SerialNumber= <Doc. Identification> (OID: 2.5.4.5)
- PS= <User Code> (OID: 2.5.4.65)

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

- For Banco de España's employees and collaborators:

  OU=PERSONAS, O=BANCO DE ESPAÑA, C=ES
- For subcontractor's employees:

  OU=PERSONAS, OU=EMPRESAS EXTERNAS, O=BANCO DE ESPAÑA, C=ES

3.1.2 The need for names to be meaningful

In all cases the distinguished names 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 user'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

Authentication certificate key pairs are generated by the Corporate CA, for which this point is not applicable.

3.2.2 Identity authentication for an entity

Issue of certificates for entities is not considered.

3.2.3 Identity authentication for an individual

Initial authentication of identity of an individual requires their physical presence. Applicants must go to their Users Administrator, duly identified by way of their identification card.

3.2.4 Non-verified applicant information

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

3.2.5 Validation of authority

No stipulation, given that the issue of certificates for entities is not considered.

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

Identity of an individual may be given in two ways:

- **In person**: for the initial issue of the certificate, in the case of renewal of a previous one, or if the previous renewal was carried out remotely. Applicants must go to their Users Administrator, duly identified by way of their identification card.
- **Remote**: for renewal of certificates due to end-of-life when the previous renewal was carried out in person and subscribers have their previous authentication certificate still in force. Applicants identify themselves remotely using their authentication certificate.

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

The individual authentication process shall be in person with the same criteria as for routine renewal.

4 Certificate Life-Cycle Operational Requirements

This chapter contains the operational requirements for the life cycle of personal authentication certificates issued by the Corporate CA. Despite the fact that these certificates will be stored on cryptographic cards, it is not the purpose of the Certificate Policy to regulate the management of said cards and, therefore, it is also assumed that the certificate applicants have previously obtained their cryptographic cards.
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?

Personal authentication certificate applications refer to two types of groups:

- Employees: the application is deemed to have been made automatically by the mere fact of joining Banco de España's staff. Employees must contact the Users Administrator assigned to them with their cryptographic card for the latter to identify them, register them in the PKI and then activate the certificate issue.
- Collaborators and subcontractors: The request must be made by the department to which they are assigned, depending on their need to access the information systems. Collaborators or subcontractors must contact the Users Administrator assigned to them with their cryptographic card for said Administrator to identify them, register them in the PKI and then activate the certificate issue.

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 authentication certificates. The PKI Administrator may request that the applicant provide the documentation it deems appropriate.

4.1.2 Enrolment process and applicants' responsibilities

This process is carried out jointly with that for obtaining the encipherment certificate, with the following procedures:

1 Once applicants have the cryptographic card, they must go to the Users Administrator assigned to them.

2 The Users Administrator identifies them and verifies that they are authorised to have an authentication certificate and that they have a valid cryptographic card.

3 In the case of new cards, applicants change, under the supervision of the Users Administrator, the card's PIN/PUK.

4 Applicants sign the Terms and Conditions Acceptance document for the Use of Personal Certificates, thus acquiring the status of certificate subscribers. This document is provided and collected, once signed, by the Users Administrator.

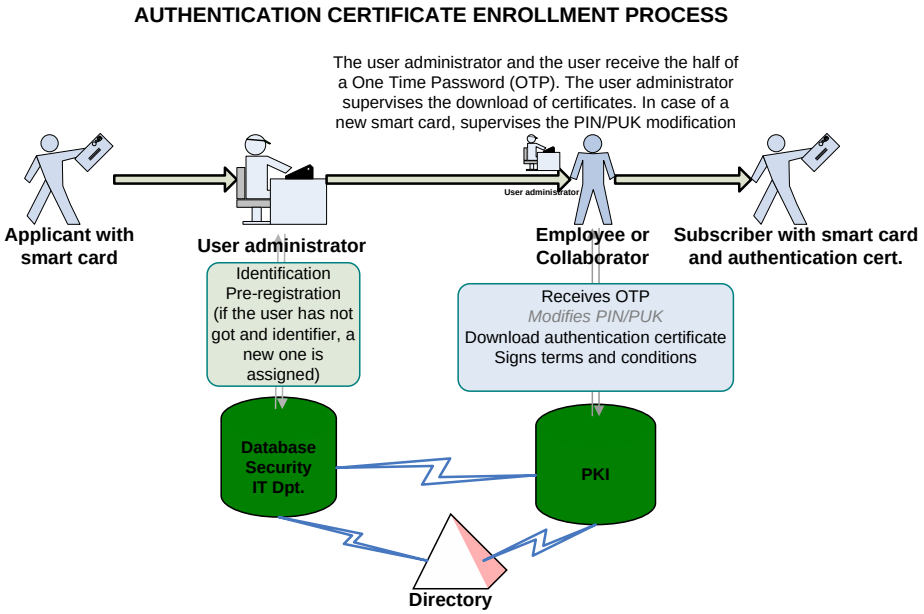
5 The Users Administrator, using the certificate issuance transaction, enters applicants' data and activates the request to the CA. The transaction generates the sending of a single-use password in two parts in order to generate the certificate. One part is sent to applicants and the other to the Users Administrator.

6 The Corporate CA, upon receipt of the requests, keeps them pending whilst waiting for the applicants to activate the process, via the web, using their password.

7 Applicants, using the two parts of the password and their user code, activate the certificate generation process in the CA.

8 The Corporate CA generates the key pair and the certificate and places the certificate and the private key in format PKCS#12 for downloading by applicants.
9 Applicants, under the supervision of the Users Administrator, download the certificate to the card.

The responsibilities of applicants not contained in this section are included in the PKIBDE CPS.
The following illustration offers a summary of the process for obtaining a personal authentication certificate.



Apart from the process described, a remote CA Administrator may enter certificate applications directly and obtain the private key and certificate in PKCS#12 format for delivery to applicants.

4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

Identification and authentication are carried out in two ways, depending on the type of application:

- Initial issue, renewal due to loss or card change or renewal after a previous online renewal: in all of these cases, identification and authentication are carried out by the Users Administrator.
- Remote renewal: identification and authentication are carried out electronically using the subscriber's valid authentication certificate. This type of renewal is alternated with the previous one.

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 Corporate CA 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.
Applications for certificates from Banco de España's employees are approved by their status as such, whilst those of collaborators and subcontractors require, for approval, prior request for certificates by the department to which they are assigned.

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.

Applicants have a limited period of 30 calendar days in which to activate the generation and downloading of the certificate. Once this period has elapsed, they will be cancelled.

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 availability of the authentication certificate via e-mail.

4.4 Certificate Acceptance

4.4.1 Form of certificate acceptance

Applicants must confirm acceptance of the authentication certificate and of its conditions by way of a hand-written signature in renewals in person or by way of an electronic signature when renewal is carried out online.

4.4.2 Publication of the certificate by the CA

The authentication 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.

Following certificate end-of-life or revocation, subscribers must discontinue use of the private key.

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

- Authentication regarding Banco de España's information systems that require verification of the identity of subscribers by way of electronic certificate.

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

Relying parties may only rely on the certificates as stipulated in this 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 the CPS and this CP. Likewise, they accept the obligations regarding the conditions of use set forth in these documents.

4.6 Certificate Renewal

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 Re-key

4.7.1 Circumstances for certificate renewal with key changeover

An authentication 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 certificate subscribers.

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 authentication certificate renewal identification and verification scenarios:

- renewals due to end-of-life of a certificate for an individual, when the previous renewal was carried out in person: in this case renewal may be carried out remotely, with identification provided by way of a current PKIBDE certificate.
- renewals due to end-of-life of a certificate for an individual when the previous renewal was carried out online, or renewal for any other reason: in this case renewal must be requested in person at the places of registration, as established for initial issuance.

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

In any case, certificate renewal is subject to:

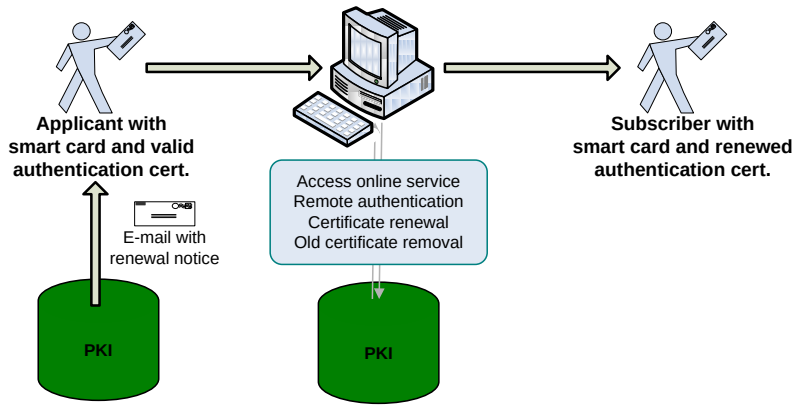
- The request being made in due time and manner, following the instructions and regulations established by PKIBDE specifically for this purpose. Renewal of a certificate may only be requested within the last 90 days of its lifetime.

- 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.

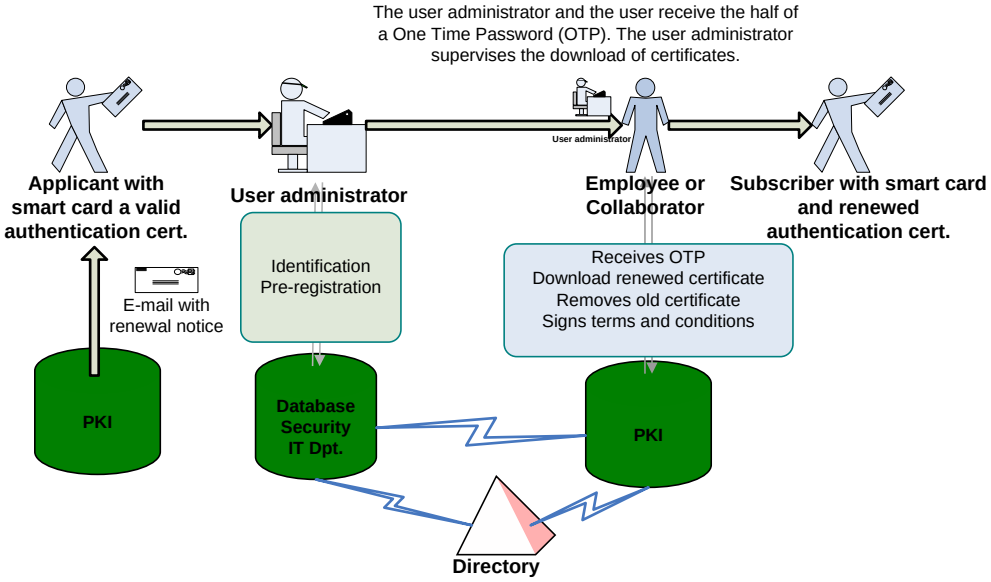
The following diagrams offer a summary of the two renewal processes for authentication certificates:

- Remote renewal (online): as described in the diagram, except for prior authorisation, the entire process is carried out by the subscribers, who receive an e-mail alert 90 days prior to the end of life of their certificate.
- Renewal in person: in this case, as with the initial issue, the Users Administrator intervenes and subscribers have to go in person. They receive an e-mail alert 90 days prior to the end of life of their certificate.

ONLINE PROCESS FOR AUTHENTICATION CERTIFICATE RENEWAL



FACE-TO-FACE PROCESS FOR AUTHENTICATION CERTIFICATE RENEWAL



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

In cases of remote renewal, subscribers confirm certificate acceptance electronically, and in the case of renewals in person, they must sign an acceptance with the Users Administrator.

4.7.6 Publication of certificates with the new keys by the CA

The authentication 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).

A personal authentication certificate may be revoked due to:

- 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 CPS or in this CP.
- The subscriber ceases to belong to the group, when said membership granted the subscriber the right to hold the certificate.
- Ceasing of PKIBDE activity.
- Defective issue of a certificate due to:
    1. Failure to comply with the material requirements for certificate issuance.
    2. Reasonable belief that basic information related to the certificate is or could be false.
    3. The existence of a data entry error or any other processing error.
- The key pair generated by the subscriber has been found to be "weak".
- The information contained in a certificate or used for the application becomes inaccurate.
- By order of the subscriber 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.
Additionally, revoked personal authentication certificates will be eliminated from the directory in which they are published.

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 factor that recommends taking such action.
Likewise, certificate subscribers may also request revocation of their certificates, which they must do in accordance with the conditions established under point 4.9.3.
The identification policy for revocation requests will be the same as that of the initial registration.
The authentication policy will accept requests for revocation signed electronically by the certificate subscribers.

4.9.3 Procedures for requesting certificate revocation

The subscribers or individuals requesting the revocation must appear before the Users Administrator, identifying themselves and indicating the reason for the request.
The Users Administrator shall always process the revocation requests submitted by its assigned subscribers. The request is made via a transaction within the Computer Security Administration application.
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 authentication certificates must be processed as quickly as possible, and in no case may said processing take more than 1 hour.

4.9.6 Requirements for revocation verification by relying parties

Verification of revocations is mandatory for each use made of an authentication certificate.
Relying parties must check the validity of the CRL prior to each use and download the new CRL from the PKIBDE repository when the one they hold expires. CRLs stored in cache[1] memory, even when not expired, do not guarantee availability of updated revocation data.
For authentication 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.

[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.

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.

4.9.9 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 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

The personal authentication certificates shall not be suspended.

4.9.14 Who can request the suspension?

Not applicable.

4.9.15 Procedure for requesting certificate suspension

Not applicable.

4.9.16 Suspension period limits

Not applicable.

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

Private authentication keys are not archived.

4.12.2 Session key protection and recovery policies and practices

No stipulation.

5 Facility, Management, and Operational 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

Not applicable.

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 Controls

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 Audit Logging 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 Archival

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 Key Changeover
As specified in PKIBDE's CPS.

5.7 Compromise 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 internal PKIBDE components, and specifically those for Root CA and Corporative CA, during certificate issue and certificate signature processes, are described in PKIBDE CPS.
In this paragraph technical security controls for the issuance of certificates under this CP are covered.

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

The keys for authentication certificates issued by the Corporate CA are generated in cryptographic hardware modules with FIPS 140-2 Level 3 certification, installed in said CA.

6.1.2 Delivery of private keys to subscribers

Delivery of the private key is carried out by subscribers downloading a file in PKCS#12 format. To guarantee delivery security, the availability of the generation and subsequent downloading of the certificate shall be notified by e-mail, and one part of the single-use password shall be provided. The rest of the password shall be notified to the Users Administrator that processed the application.
Generation of the key pair and the certificate is activated by subscribers, as well as their downloading, in the presence of their Administrator, which provides their part of the password. The downloading software forces installation of the certificate and private key in the subscriber's cryptographic card, preventing a copy of the PKCS# 12 being saved to the hard disk.

6.1.3 Delivery of the public key to the certificate issuer

The public key is generated by the Corporate CA and therefore delivery is not applicable.

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

The Corporate CA's public key is included in the certificate of said CA. The Corporate CA's certificate is not included in the certificate generated by the subscriber. The Corporate CA's certificate must be obtained from the repository specified 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 authentication certificate keys is 1024 bits.

6.1.6 Public key generation parameters and quality checks

Authentication public keys are encoded pursuant to RFC 3280 and PKCS#1. The key generation algorithm is the RSA.

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

The key defined under this policy and, therefore, the consequent linked certificate, shall be used to verify the identity of the certificate subscriber as regards Banco de España's Information Systems.
For this purpose, the 'Key Usage' and 'Extended Key Usage' fields of the certificate include the following uses:

Key Usage:

- Digital Signature.
- Key Agreement

Extended Key Usage:

- clientAuth
- smartCardLogon
- anyExtendedKeyUsage
- emailProtection[2]

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.

As regards the cryptographic cards 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

The private key, both for Root CA as for Subordinate CA, is under multi-person control; its activation is done through CA software initialization by means of a combination of CA's operators. This is the only activation method for said private key.

There is no multi-person control established for accessing the private keys of the certificates issued under this CP.

6.2.3 Escrow of private keys

The private keys of the authentication certificate are housed on cryptographic cards held by their subscribers, they are not exported under any circumstances, and access to operations with said cards is protected by a PIN.

6.2.4 Private key backup copy

The subscribers of certificates issued under this CP cannot backup their certificates because the keys cannot be exported outside of the cards and these cannot be cloned.

6.2.5 Private key archive

The Corporate CA, once the authentication certificate issuance process has finalised, does not keep a copy of its private key and, therefore, the private key can only be found on the corresponding cryptographic card held by the subscriber.

[2] This attribute is included solely in personal authentication certificates issued by PKIBDE for contracted company personnel, given that this group will not have, in general, recognised signature certificates. Its purpose is for the personnel of contracted companies to be able to use their authentication certificates to sign e-mails.

6.2.6 Private key transfer into or from a cryptographic module

No stipulated.

6.2.7 Private key storage in a cryptographic module

Private keys are created in the Corporate CA's cryptographic module, but they are not subsequently saved.

6.2.8 Private key activation method

The private key is provided in a PKCS#12 file, protected by a single-use password. Once it has been downloaded and installed on a cryptographic card, its use is controlled by the card's PIN.

6.2.9 Private key deactivation method

It can be deactivated by removing the card from the reader. Some computer applications also provide deactivation following a time-out period.

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

Authentication certificates and their linked key pair have a lifetime of 4 years, although the Corporate CA may establish a shorter period at the time of their issue.

6.4 Activation Data

6.4.1 Generation and installation of activation data

As 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 Timestamping

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.
- *bdeCertType (1.3.6.1.4.1.19484.2.3.6)*. Classified as non-critical.

FIELD	CONTENT	CRITICAL **for extensions**
Field X509v1		
1. Version	V3	
2. Serial Number	Random	
3. Signature Algorithm	SHA-1WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA, O=BANCO DE ESPAÑA, C=ES	
5. Lifetime	4 years	
6. Subject	In the case of Banco de España's employees: CN=[A] Name Surname 1 Surname 2 SerialNumber= Identity Document PS=User Code OU=PERSONAS O=BANCO DE ESPAÑA C=ES In the case of subcontractor companies' employees: CN=[A] Nombre Apellido1 Apellido 2 SerialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS OU=EMPRESAS EXTERNAS O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algorithm: RSA Encryption Minimum Key Length: 1024(big string)	
Field X509v2		
1. issuerUniqueIdentifier	Not used	

FIELD	CONTENT	CRITICAL for extensions
2. subjectUniqueIdentifier	Not used	
X509v3 extensions		
1. Subject Key Identifier	Derived from using the SHA-1 hash on the subject's public key.	NO
2. Authority Key Identifier	Derived from using the SHA-1 hash on the issuing CA's public key.	
authorityCertSerialNumber	36 6a 52 4d a5 e4 4a f8 41 08 a1 40 9b 9b 76 eb	
3. KeyUsage		YES
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	clientAuth, smartCardLogon, anyExtendedKeyUsage, emailProtection[3]	NO
5. privateKeyUsagePeriod	Not used	
6. 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. © 2004 Banco de España. Todos los derechos reservados. (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.6	
Notice Reference	Certificado personal de autenticación sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2004 Banco de España. Todos los derechos reservados	
7. Policy Mappings	Not used	
8. Subject Alternate Names	UPN (User's Principal Name in Windows 2000) E-mail address pursuant to RFC 822 1.3.6.1.4.1.19484.2.3.1 Name 1.3.6.1.4.1.19484.2.3.2 Surname1 1.3.6.1.4.1.19484.2.3.3 Surname2 1.3.6.1.4.1.19484.2.3.4 BDE employee no. 1.3.6.1.4.1.19484.2.3.5 BDE user code no. 1.3.6.1.4.1.19484.2.3.7 Identity Document 1.3.6.1.4.1.19484.2.3.15 ID for subcontractors[4]	NO
9. Issuer Alternate Names	Not used	
10. Subject Directory Attributes	Not used	
11. Basic Constraints	CA	YES
Subject Type	End Entity	

[3]This attribute shall be included solely in personal authentication certificates issued by PKIBDE for contracted company personnel.
[4]This attribute shall be included solely in personal certificates issued by PKIBDE for contracted company personnel. Enables differentiation of subscribers that belong to this group.

FIELD	CONTENT	CRITICAL for extensions
Path Length Constraint	Not used	
12. CRLDistributionPoints	(1) Active Directory: ldap:///CN=BANCO%20 DE%20ESPA%D1A%20-%20AC%20CORPORATIVA,CN=snt0053,CN=CDP, CN=Public%20Key%20Services,CN=Services,CN=Configuration, DC=BDE, DC=ES ?certificateRevocationList?base?objectclass= cRLDistributionPoint (2) LDAP: 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 (3)HTTP http://pki.bde.es/certs/ACcorporativa.crl	NO
13. Auth. Information Access	OCSP http://pkiva.bde.es CA http://pki.bde.es/certs/ACraiz.crt	NO
14. netscapeCertType	Not applicable.	
15. netscapeRevocationURL	Not applicable.	
16. netscapeCAPolicyURL	Not applicable.	
17. netscapeComment	Not applicable.	
18. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	AUTENTICACION	

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.

The CN (Common Name), serialNumber and PS (pseudonym) attributes of the DN will be what distinguish one DN from another. The letter A between brackets in the CN identifies the authentication certificate. The rest of the attributes will have the following fixed values:

- For Banco de España's employees and collaborators:

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

- For subcontractor's employees:

  OU=PERSONAS, OU=EMPRESAS EXTERNAS, O=BANCO DE ESPAÑA, C=ES

7.1.6 Certificate Policy Object Identifiers (OID)

The OID of this CP is 1.3.6.1.4.1.19484.2.2.6 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

No stipulation.

7.3 OCSP Profile

7.3.1 Version number(s)

As specified in PKIBDE's CPS.

7.3.2 OCSP Extensions

As specified in PKIBDE's CPS.

8 Compliance Audit and Other Assessment

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

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

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

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

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

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

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

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

9.1.3 Revocation or status information fees

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

9.1.4 Fees for other services, such as policy information

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

9.1.5 Refund policy

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

9.2 Confidentiality of Business Information

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 Privacy of Personal Information

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 Representations and Warranties

9.5.1 Obligations of the CA

As specified in PKIBDE's CPS.

The PKIBDE Corporate Certification Authority shall act linking a specific public key to its subscriber by way of the issue of an authentication certificate, all of this in accordance with the terms of this CP and the CPS.

The services provided by the CA in the context of this CP are the services of issue, renewal and revocation of personal authentication certificates, which are accessed by remote Administration Positions of the CA, deployed for said purpose.

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 Disclaimers of Warranties

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 Limitations of Liability

As specified in PKIBDE's CPS.

9.8 Term and Termination

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, nevertheless it will be kept 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 Amendments

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 Dispute Resolution Procedures

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.