BANCO DE ESPAÑA
Eurosistema

25.05.2010

OID: 1.3.6.1.4.1.19484.2.2.101.1.1

The Banco de España's Public Key Infrastructure

Policy Certificate for external entity component certificates

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

Control Sheet

Title	Policy Certificate for external entity component certificates
Author	General Secretariat Legal Department Information Systems Department
Version	1.1
Date	25.05.2010

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

TABLE OF CONTENTS

1 Introduction

1.1 Overview

This document sets out the Certificate Policy (CP) governing the component certificates issued by the Corporate Certification Authority of the Banco de España's Public Key Infrastructure (hereinafter, PKIBDE) for external entities with which the Bank exchanges data by online means.

This Certificate Policy regulates all the external entity component certificates issued by PKIBDE, and specifically:

- Generic certificates for external entity components

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.

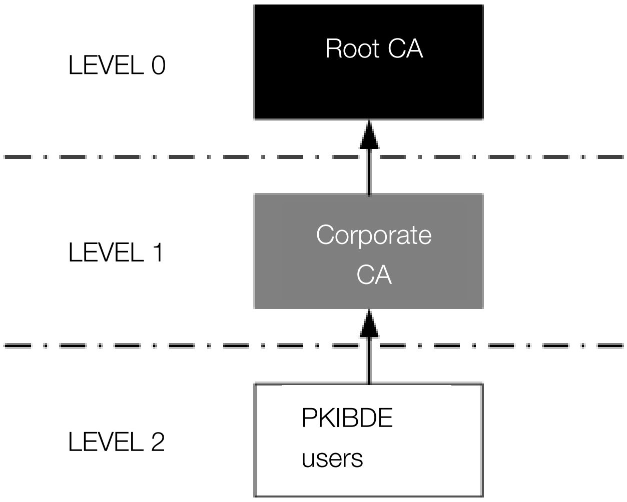
This CP details and completes the "Certification Practice Statement" (CPS) of the Banco de España's PKI, containing the rules to which the use of the certificates defined in this policy are subject, as well as the scope of application and the technical characteristics of this type of certificate.

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 external entity 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:



1.2 Document Name and Identification

Document name	Certificate Policy (CP) for External Entity Certificates
Document version	1.1
Document status	Approved
Date of issue	25.05.2010
OID (Object Identifier)	1.3.6.1.4.1.19484.2.2.101.1.1
CPS location	http://pki.bde.es/politicas
Related CPS	Certification Practice Statement of the Banco de España's PKI OID 1.3.6.1.4.19484.2.2.1

1.3 PKI Participants

The participating entities and persons are:

- The 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

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:

Distinguished Name	CN= BANCO DE ESPAÑA – AC RAIZ , O=BANCO DE ESPAÑA, C=ES
Serial Number	F16D 7586 5D7C CF92 41AD A17A CD9A 3DE2
Distinguished Name of Issuer	CN= BANCO DE ESPAÑA – AC RAIZ , O=BANCO DE ESPAÑA, C=ES
Validity Period	From 08-07-2004 11:34:12 to 08-07-2034 11:34:12

Message Digest (SHA-1)	2B60 DE7D 3337 8BF7 5B67 8B10 77BB F951 6029 D6A8

- **Corporate CA**: Certification Authority subordinate to the Root CA. 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

1.3.3 Registration Authorities

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

Issue of external entity component certificates shall be carried out using a series of remote Registration Authority positions, which will enable the CA's different Remote Administrations, designated by PKIBDE, to request and download said certificates.

These Administrators shall have authentication certificates issued by the Corporate CA. Using these certificates and the administration interface, they will act on behalf of the component managers, generating certification/revocation requests. The CA shall verify that the remote position is authorised to send the requests and, if this is the case, will process them. In the case of a certification request, it shall return the certificate for the Remote Administrator to deliver to the component manager. In the case of a request for revocation, it will return the result of the operation.

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	External entity 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
Generic certificates for external entity components	The external entity's component 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 an external entity 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
Generic certificates for external entity components	Authentication of components and encipherment of communications

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 The 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.	+34913386610	**Fax**	+34913386870

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 uses a key pair in which what is enciphered with one of these can only be deciphered by the other, and vice versa. One of these keys is "public" and includes the electronic certificate, whilst the other is "private" and is only known by the certificate subscriber and, when appropriate, by the Keys Archive.

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

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

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

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

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

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

Trust Hierarchy: set of certification authorities that maintain a relationship of trust by which a CA of a higher level guarantees the trustworthiness of one or several lower level CAs. In the case of

PKIBDE, the hierarchy has two levels, the Root CA at the top level guarantees the trustworthiness of its subordinate CAs, one of which is the Corporate CA.

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

Applicants: individuals who apply for a certificate for themselves or for a computer component.

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

Subscribers: individuals or computer components for which an electronic certificate is issued and accepted by said individuals or, in the case of component certificates, by the component manager.

1.6.2 Acronyms

PAA: Policy 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: 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 CN (Common Name) attribute of the DN must include a reference to the entity owning the computer component from which the certificate is to be used. The CN must also include information on the identification mechanism applied to issue the certificate. On the other hand, the type of computer component will be specified through a prefix to the CN.

The component certificate's CN will be as follows:

Certificate type	CN
Generic certificate for external entity components	CN=[EG] *CIF ident_method dif_num*

Where:

CIF (Código de Identificación Fiscal, Tax Identification Code) is the tax ID number assigned by the Tax Authorities to the entity responsible for the component for which the certificate is requested.

ident_method is an ID of the recognition mechanism applied to issue the certificate, with the following possible values:

- **RI-<Administrative Unit code>**, if any Banco de España internal Administrative Unit (AU) has approved the issue of the certificate, that AU shall be identified by a code within the certificate itself.
- **RE-<ID of the type of certificate used in the application[1]>**. The component certificate issued must include the information necessary to identify the PCS and the Policy Certificate linked to the certificate with which the application is signed, if it has been signed electronically using a certificate issued by a PCS external to the Banco de España.

dif_num, a number that enables the differentiation of different certificates generated by the same entity when the issue of which been approved by the same method of identification.

The following is an example of the CN field: *CN=[EG] G28000024 RI-C361A 0001*

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

- OU=COMPONENTES, O=<name of the entity>, C=ES

Where <name of the entity> is the name of the entity identified by the CIF included in the CN attribute of the certificate.

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.

[1] The list of the existing certificate type IDs is available at the address http://pki.bde.es

3.1.4 Uniqueness of names

Certificate DNs may not be repeated. The use of the component's Tax ID Code (CIF) guarantees the uniqueness of the DN. If more than one computer component is issued for one same entity, said components will be differentiated by the identification mechanism used when the certificate was issued. There may not be more than one computer component certificate of the same type for the same entity issued using the same identification mechanism.

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 entity owning 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

Certificates for external entity components are not electronic certificates for entities as defined in Section 7, Law 59/2003, dated 19 December, the Electronic Signature Act.

However, to guarantee that the computer component from which the certificate is to be used is the property of the entity indicated in the certificate, there are two alternative identification procedures:

a Electronic signature of the certificate issuance application using a certificate of an entity issued by a PCS recognised by the Banco de España for said purpose. In this case, the certificate's CN shall include an ID that identifies the PCS and the specific Certificate Policy that issued the certificate used to request the issue of the component certificate. Validation of the identity of the entity will have been carried out in accordance with the procedures established by the PCS.

b Hand-written signature of the certificate issuance application by an individual who represents the entity owning the computer component and is registered as such in the Banco de España. In this case, the certificate's CN must include the code of the Administrative Unit responsible for validating the signature.

3.2.3 Identity authentication for an individual

Not applicable.

3.2.4 Non-verified applicant information

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

3.2.5 Validation of authority

When the certificate is applied for using an electronic signature generated through the certificate of an entity issued by a PCS recognised by the Banco de España, it shall be assumed that the individual using said entity certificate has the authority to do so.

In all other cases, the authority to represent must be registered beforehand with the Banco de España.

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 external entity 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?

Request for a component certificate must be carried out by the person designated as the manager for said component by the external entity.

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 external entity component certificates.

4.1.2 Enrolment process and applicants' responsibilities

There are two types of processes, depending on the application mechanism used.

Application signed electronically via an entity certificate issued by a PCS

In this case the procedure is as follows:

1 The application is sent electronically by e-mail signed using an entity certificate issued by a PCS recognised by the Banco de España for said purpose. As regards the application content, there are two possibilities:

> **a** If the entity chooses to generate the key pair, the application must include the certificate signing request (CSR) with the public key, as well as the information necessary for the CA to generate the certificate.
>
> **b** If the entity decides that the Banco de España shall generate the public and private key pair, the application shall only include the information necessary to generate the certificate.

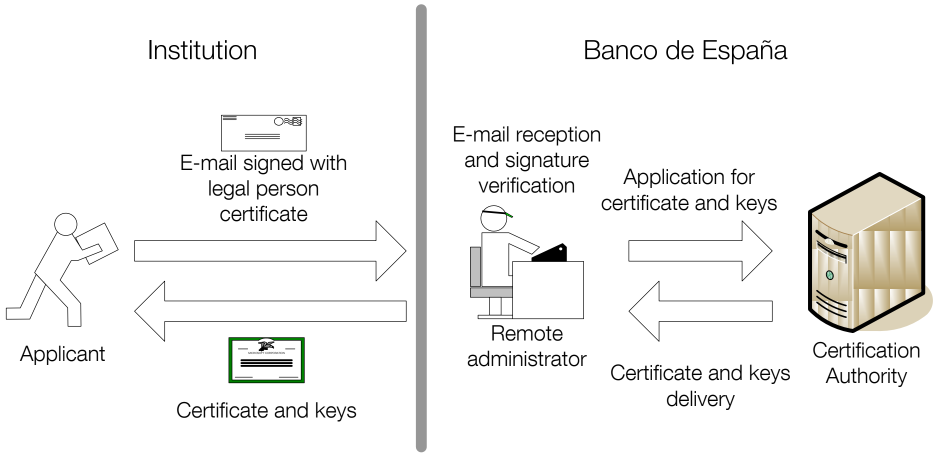
2 The Remote Administrator receives the message and verifies the electronic signature. If the signature is verified as correct, it shall request the Certification Authority to:

> **a** Issue the certificate, if the entity has sent the certificate signing request (CSR) with the public key.
>
> **b** Generate a key pair and issue the certificate linked to the public key, if the entity chose this option.

3 The CA issues the certificate and, when appropriate, generates the key pair, and the Remote Administrator downloads the corresponding file with the certificate or a file with the private key and the certificate, encrypted with a password known to the RA.

4 The Banco de España sends the applicant the certificate or file with the keys by e-mail. In this latter case, it sends the password via an e-mail message encrypted using the entity certificate that the entity used to sign the application.

The following illustration offers a summary of the process described:


Institution
Banco de España
E-mail signed with legal person certificate
Applicant
Certificate and keys
E-mail reception and signature verification
Remote administrator
Application for certificate and keys
Certificate and keys delivery
Certification Authority

Hand-written signed applications

In this case, the steps are as follows:

1 The application must include the contact telephone number and information necessary to generate the certificate, as well as the name or code of the Banco de España's Administrative Unit (department) that is to validate the request. On the other hand:

> **a** If the entity chooses to generate the key pair, the application must include a CD-ROM with the certificate signing request (CSR), which must contain the public key.
>
> **b** If the entity decides that the Banco de España should generate the key pair, this option must be indicated in the application.

2 The Administrative Unit of the Bank indicated in the request will verity its signature.

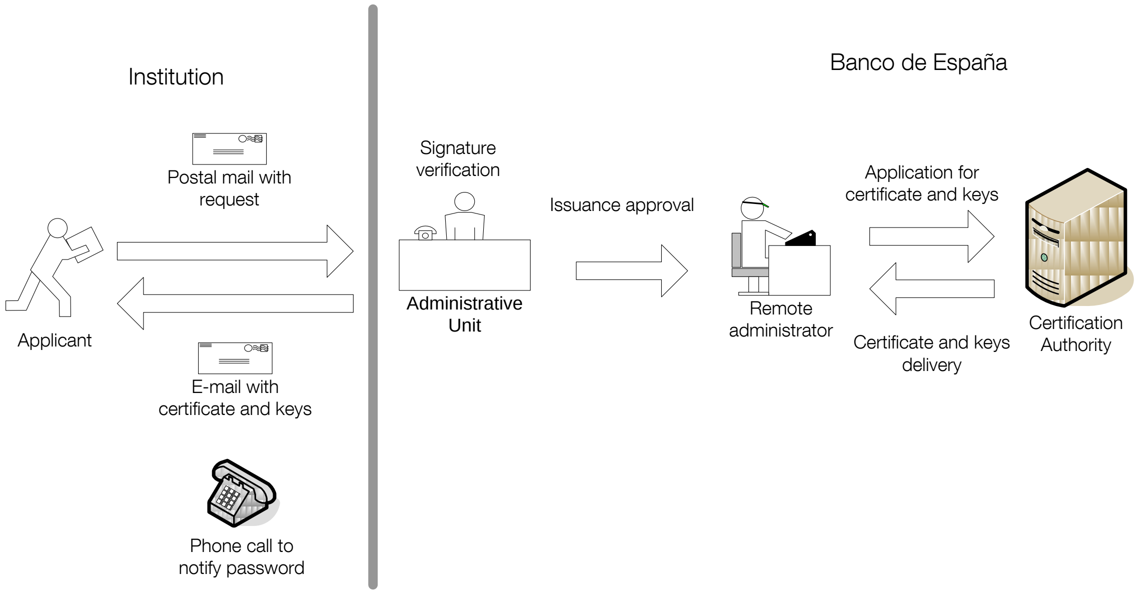
3 If the corresponding Administrative Unit approves the issuance of the certificate, a Remote Administrator of the CA will request it to:

> **a** Issue the certificate, if the entity has sent the certificate signing request (CSR) with the public key.
>
> **b** Generate a key pair and issue the certificate linked to the public key, if the entity chose this option.

4 The CA issues the certificate and, when appropriate, generates the key pair, and the Remote Administrator downloads the corresponding file with the certificate or a file with the private key and the certificate, encrypted with a password known to the RA.

5 The Banco de España sends the applicant the certificate or an encrypted file with the private key and the certificate by e-mail. In this latter case, the password with which said file has been encrypted will be notified by telephone.

The following illustration offers a summary of the process described:



4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

The way in which identification and authentication are carried out depends on the manner in which the request was made:

- If the request was made via e-mail signed using a certificate of an entity issued by a PCS recognised by the Banco de España for said purpose, identification and authentication shall be carried out by the Remote Administrator using the electronic signature.
- If the request has been signed by hand, identification and authentication of the applicant shall be carried out by the Administrative Unit indicated in the request.

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. The Corporate CA will process the requests as quickly as possible.

4.3 Certificate Issuance

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

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

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

All certificates will become effective upon issue, unless the certificate indicates a later date and time of 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

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

4.4.2 Publication of the certificate by the CA

The 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
Generic certificates for external entity components	Authentication of components and encipherment of communications

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.

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.

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).

A component 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 in the CPS or in this CP.
- The component ceases to be in service.
- Ceasing of PKIBDE activity.
- Defective issue of a certificate due to:
  1. Failure to comply with the material requirements for certificate issuance.
  2. Reasonable belief that basic information related to the certificate is or could be false.
  3. The existence of a data entry error or any other processing error.
- The key pair generated by the subscriber has been found to be "weak".
- The information contained in a certificate or used for the application becomes inaccurate.
- By order given from the component manager or an authorised third party or the individual applicant representing an entity.
- 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 CA's Remote Administrator.

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 must be processed as quickly as possible, and in no case may said processing take more than 24 hours.

4.9.6 Requirements for revocation verification by relying parties

Verification of revocations is mandatory for each use made of a 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. CRLs stored in cache[1] memory, even when not expired, do not guarantee availability of updated revocation data.

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.

4.9.9 Online certificate revocation status checking availability

There are no online systems for verification of certificate status accessible by external entities.

The addresses for web access to the CRLs are indicated under point *2.1 Repositories*.

4.9.10 Online revocation checking requirements

Not applicable, as there are no online mechanisms for revocation verification accessible by external entities.

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 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.

[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.

4.10 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 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

Key generation for external entity component certificates, when carried out by the Banco de España's Corporate CA, is carried out in cryptographic hardware modules with FIPS 140-2 Level 3 certification.
If this is performed by the entity, the cryptographic libraries shall be used on the browser from which the request is submitted.

6.1.2 Delivery of private keys to subscribers

In the event of delivery of the private key when generated by the CA, it will be carried out by e-mail to the component manager attaching a file in PKCS#12 format, encrypted with a password.
The password is delivered as follows:

- If the application was made via e-mail signed using an entity certificate issued by a PCS recognised by the Banco de España, the password shall be sent by encrypted e-mail using said certificate.
- If the certificate application was made with a hand-written signature validated by an internal Banco de España Administrative Unit, the password shall be notified by telephone to the component manager.

In those cases in which the keys have been generated by the entity, no private key is provided.

6.1.3 Delivery of the public key to the certificate issuer

When the key pair has been generated by the entity, 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).
In those cases in which the pair of keys has been generated by the Corporate CA itself, the public key will be delivered within the PKCS#12 file indicated in the previous section.

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 for legal entities is 1024 bits.

6.1.6 Public key generation parameters and quality checks

Component 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 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
Generic certificates for external entity components	digitalSignature. dataEncipherment. keyEncipherment. keyAgreement	emailProtection clientAuth anyExtendedKeyUsage

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 it is the owner entities that are responsible for the safekeeping of the certificates issued under this CP, said entities are recommended to make back-up copies to avoid their loss or deterioration.

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.

This CP does not stipulate storage in a cryptographic module if it is the entity that generates private keys.

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. The entity must import the key on the computer component from which it shall be used, therefore it will subsequently be activated according to the specification of said component.

When it is generated by the entity, it will be activated once the certificate has been obtained according to the specifications of the computer component from which the entity uses the private key and the certificate.

6.2.9 Private key deactivation method

No stipulation.

6.2.10 Private key destruction method

No stipulation.

6.2.11 Cryptographic module classification

When it is the Certification Authority that generates the keys, the cryptographic modules used comply with FIPS 140-2 standard, level 3.

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 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 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 external entities 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 external entities:

Generic certificate for external entity components

FIELD	CONTENT	CRITICAL 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	CN=[EG] CIF_Entity RI-<Administrative Unit Code>[1]
	or
	CN=[EG] CIF_Entity RE-<ID cert. used in the application>[2]-<Sequence ID>
	OU=COMPONENTES
	O=<Name of Entity>
	C=ES	

7. Subject Public Key Info	Algorithm: RSA Encryption, key length: 1024 to 2048	
Field X509v2		
1. issuerUniqueIdentifier	Not used	

[1] <Administrative Unit Code>: Code of the Banco de España internal Administrative Unit that approved the certificate application

[2] <ID cert. used in the application>: ID of the Provider of Certification Services and the Policy Certificate used to issue the entity certificate used to apply for the component certificate. The list of possible IDs is available at http://pki.bde.es

Generic certificate for external entity components		
FIELD	**CONTENT**	**CRITICAL 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		NO
keyIdentifier	Result of using the hash SHA-1 function on the public key of the issuing CA (AC CORPORATIVA) (c2 45 2b f4 f9 92 ee 33 59 98 e1 82 75 6b 8c bc d0 b6 e5 c1)	
authorityCertIssuer	CN=BANCO DE ESPAÑA – AC RAIZ, O=BANCO DE ESPAÑA C=ES	
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	1	
Data Encipherment	1	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	clientAuth, emailProtection, anyExtendedKeyUsage	NO
5. privateKeyUsagePeriod	Not used	
6. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1 (CPS)	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. ©2004 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.101 (PC)	
Notice Reference	Certificado de componente informático para Entidades externas 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	E-mail address pursuant to RFC 822 (optional) 1.3.6.1.4.1.19484.2.3.8 Name of entity (required) 1.3.6.1.4.1.19484.2.3.9 CIF of entity (required) 1.3.6.1.4.1.19484.2.3.10 Validation type. (required)[1] 1.3.6.1.4.1.19484.2.3.11 Id. Validation (mandatory)[2] 1.3.6.1.4.1.19484.2.3.12 BdE code type (optional)[1]	NO

[1] Validation type: *RI*, approval of the certificate application by an internal BdE Administrative Unit; *RE*, certificate application in accordance with an entity certificate issued by an external PCS

[2] ID of the validation mechanism: code of the Administrative Unit that approved the certificate application or ID of the entity certificate type used to apply for the certificate

Generic certificate for external entity components

FIELD	CONTENT	CRITICAL extensions
	1.3.6.1.4.1.19484.2.3.13 BdE code (optional)[2] 1.3.6.1.4.1.19484.2.3.14 Differentiating No. (required)[3]	
9. Issuer Alternate Names	Not used	
10. Subject Directory Attributes	Not used	
11. Basic Constraints		YES
Subject Type	End Entity	
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	SSL_Client, SMIME_Client	
15. netscapeRevocationURL	Not used	
16. netscapeCAPolicyURL	Not used	
17. netscapeComment	Not used	
18. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	EXTER_COMPONENTE_GENERICO	

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) attributes of the DN will be what distinguish one DN from another. The rest of the attributes will have the following values:
OU=COMPONENTE, O=<NAME OF THE ENTITY>, C=ES

[1] Banco de España entity code type. It may be REN or SIC

[2] Banco de España entity code value. There may be cases in which the entity has a code assigned by the BdE.

[3] Differentiating No.: Number used to differentiate certificates of the same entity.

7.1.6 Certificate Policy Object Identifiers (OID)

The OID of this CP is 1.3.6.1.4.1.19484. 2.2.101. An extension in X.Y format is added that indicates the CP 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 two information elements, 'Policy Information':

- Element with identifier '1.3.6.1.4.1.19484.2.2.1', which corresponds with the CPS. It includes the qualifiers: 'URL CPS' with the web address to access the CPS and this CP; 'Notice Reference' with a text note on the applicable CPS.
- Element with identifier '1.3.6.1.4.1.19484.2.2.101', which corresponds with this CP. It includes the 'Notice Reference' qualifier, with a text note on this CP.

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

7.1.9 Processing semantics for the critical "CertificatePolicy" extension

No stipulation.

7.2 CRL Profile

7.2.1 Version number

As specified in PKIBDE's CPS.

7.2.2 CRL and extensions

As specified in PKIBDE's CPS.

7.3 OCSP Profile

7.3.1 Version number(s)

As specified in PKIBDE's CPS.

7.3.2 OCSP Extensions

As specified in PKIBDE's CPS.

8 Compliance Audit and Other Controls

8.1 Frequency or Circumstances of Controls for each Authority

As specified in PKIBDE's CPS.

8.2 Identity/Qualifications of the Auditor

As specified in PKIBDE's CPS.

8.3 Relationship between the Assessor and the Entity being Assessed

As specified in PKIBDE's CPS.

8.4 Aspects Covered by Controls

As specified in PKIBDE's CPS.

8.5 Actions Taken as a Result of Deficiencies Found

As specified in PKIBDE's CPS.

8.6 Notification of the Results

As specified in PKIBDE's CPS.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

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

9.1.3 Revocation or status information fees

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

9.1.4 Fees for other services, such as policy information

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

9.1.5 Refund policy

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

9.2 Information Confidentiality

9.2.1 Scope of confidential information

As specified in PKIBDE's CPS.

9.2.2 Non-confidential information

As specified in PKIBDE's CPS.

9.2.3 Duty to maintain professional secrecy

As specified in PKIBDE's CPS.

9.3 Personal Data Protection

9.3.1 Personal data protection policy

As specified in PKIBDE's CPS.

9.3.2 Information considered private

As specified in PKIBDE's CPS.

9.3.3 Information not classified as private

As specified in PKIBDE's CPS.

9.3.4 Responsibility to protect personal data

As specified in PKIBDE's CPS.

9.3.5 Notification of and consent to the use of personal data

As specified in PKIBDE's CPS.

9.3.6 Disclosure within legal proceedings

As specified in PKIBDE's CPS.

9.3.7 Other circumstances in which data may be made public

As specified in PKIBDE's CPS.

9.4 Intellectual Property Rights

As specified in PKIBDE's CPS.

9.5 Obligations

9.5.1 Obligations of the CA

As specified in PKIBDE's CPS.

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.