

28.03.2023

OID: 1.3.6.1.4.1.19484.2.2.2

The Banco de España's Public Key Infrastructure

Basic Statement: PKI characteristics and requirements

OVERVIEW This text is merely an extract of the characteristics and requirements of the Banco de España's PKI, which are described fully in the Certification Practice Statement (CPS) and in the corresponding Certificate Policies (CP) applicable to the certificate being applied for or used.

It is recommended that the CPS be read, as well as the applicable CPs, in order to have a clear idea of the purposes, specifications, regulations, rights, obligations and responsibilities governing the provision of the certification service.

This Basic Statement has been drawn up in accordance with "ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates", specifically pursuant to the recommendations in Annex B for the "PKI Disclosure Statement".

Control Sheet

| | |
|----------------|---------------------------------------------------------------------------|
| Title | Basic Statement: PKI characteristics and requirements |
| Author | General Secretariat Legal Department Information Systems Department |
| Version | 1.6 |
| Date | 28.03.2023 |

Change Log

| Version | Date | Reason for the change |
|----------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 1.0 | 5.04.2006 | Initial Version |
| 1.1 | 25.10.2006 | Review of version 1. |
| 1.2 | 25.05.2010 | Review following introduction of electronic dating services Renaming of the Policy Approval Authority to Policy Management Authority |
| 1.3 | 07.07.2011 | Changes following review of electronic signature certification policy |
| 1.4 | 20.10.2014 | Consolidation in a single document of the certificate policies for all the certificates issued for Banco de España's internal users |
| 1.5 | 11.05.2015 | Update due to the renewal of the Certification Authorities |
| 1.6 | 28.03.2023 | Personal data protection legal texts update. |

TABLE OF CONTENTS

| | | |
|----|---------------------------------------------------------------------------------|---|
| 1 | Glossary | 4 |
| 2 | CA Contact Data | 4 |
| 3 | Types of certificates, validation procedures and use | 4 |
| 4 | Constraints | 6 |
| 5 | Subscribers' Obligations | 6 |
| 6 | Obligations of relying parties | 7 |
| 7 | Liability limitations | 7 |
| 8 | Applicable agreements, Certification Practice Statement and Policy Certificates | 8 |
| 9 | Personal Data Protection | 8 |
| 10 | Provision of certification services free of charge | 8 |
| 11 | Governing Law | 9 |
| 12 | Disputes and Jurisdiction | 9 |
| 13 | CA and repository audits, certifications and security standards | 9 |

1 Glossary

CA: Certification Authority.

PAA: Banco de España's Policy Management Authority

CRL: Certificate Revocation List.

CPS: Certification Practice Statement.

LDAP: Lightweight Directory Access Protocol.

CP: Certificate Policy.

PIN: Password that protects the use of the cryptographic card.

PKI: Public Key Infrastructure.

PUK: Password to unblock the card, if it has been blocked due to repeatedly entering the wrong PIN.

2 CA Contact Data

This PKI is managed by the Policy Management Authority (AAP) of Banco de España's PKI:

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

3 Types of certificates, validation procedures and use

The Banco de España's PKI issues the following types of personal certificates:

- **Personal certificates.** This is a package of certificates stored in the same cryptographic device (typically a smartcard) intended for general use of any Banco de España's internal user. This comprises the following certificates:

- Authentication certificate, used to authenticate the subscriber to IT systems that accept this mechanism.
- Electronic signature certificate, used to sign electronic documents, e-mail and electronic transactions.
- Encryption certificate (deprecated¹) or software recoverable encryption certificate, used to encrypt electronic documents and e-mail.

- **Administrator certificate.** This is a certificate stored in a cryptographic device (typically a smartcard) used to authenticate subscribers that have got an administration account to IT systems that accept this mechanism.

- **Provisional personal certificates.** This is a package of certificates stored in the same cryptographic device (typically a smartcard) intended for the case that the subscriber has forgotten his smartcard with personal certificates.

These certificates have a maximum expiration period of 7 days, although User Administrators can request a lower period.

This package comprises the following certificates:

¹ This certificate type is not issued by the Corporate CA any more, but it is still possible to recover the key pairs corresponding to old encryption certificate from the Key Archive

- Authentication certificate, used to authenticate the subscriber to IT systems that accept this mechanism.
- Electronic signature certificate, used to sign electronic documents, e-mail and electronic transactions.
- **Provisional administrator certificate.** This is a certificate stored in a cryptographic device (typically a smartcard) intended for the case that the subscriber has forgotten his smartcard with an administrator certificate. This certificate has a maximum expiration period of 7 days, although User Administrators can request a lower period.

The certificates are issued for Banco de España employees and for personal not belonging to the Banco de España who, due to their relationship with the Bank, need to interoperate with the Banco de España's Information Systems.

All internal user certificates use cryptographic cards. The only exception is for encryption certificates recoverable in software that can be used in mobile devices. Their subscribers may not export their private keys from the cryptographic card.

Verification of the status of the certificates may be made by consulting the latest CRL at:

- LDAP: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
- WEB: <http://pki.bde.es/crls/ACcorporativav2.crl>
- WEB: <http://pki.redbde.es/crls/ACcorporativav2.crl>

4 Constraints

Reliability constraints

The certificates must be used for the functions and purposes established in the corresponding Certificate Policy.

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

Unless other uses are authorised in the corresponding CP, certificates issued by the Banco de España's PKI are valid only for use in relation to the Bank itself (authentication of its systems, signature and encipherment of e-mails to or from the Bank, signature and encipherment of Bank information).

Loss Limits

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

Data Storage

Registration and certification management data shall be stored for 15 years.

5 Subscribers' Obligations

Subscribers of certificates issued by the Banco de España's PKI have the obligation to:

- 1 Provide accurate, full and truthful information regarding the data requested by those entrusted with their verification in order to carry out the registration process.
- 2 Inform PKI management of any modification to said data.
- 3 Understand and accept the terms and conditions for use of the certificates and, specifically, those contained in the applicable CPS and CPs, as well as any modifications thereto.
- 4 Restrict and condition the use of the certificates to the scope of their labour relationship with the Banco de España and pursuant to that permitted under the corresponding Certificate Policy and the CPS.
- 5 Take the necessary care and measures to guarantee the safekeeping of their card, preventing its loss, disclosure, modification or unauthorised use.
- 6 The process to obtain the certificates requires the personal selection of a control PIN for the cryptographic card and activation of the private keys and a PUK for unlocking. The holder is responsible for keeping the PIN and PUK numbers secret.
- 7 Immediately request the revocation of a certificate upon detecting any inaccuracy in the information contained therein or upon becoming aware of or suspecting any loss of reliability of the private key corresponding to the public key contained in the certificate due, among other causes, to: loss, theft, potential compromise, knowledge by third parties of the PIN and/or PUK.
- 8 Not monitor, manipulate or carry out any reverse engineering on the technical implementation (hardware and software) of the certification services.
- 9 Not transfer or delegate to third parties the obligations pertaining to a certificate assigned to them.
- 10 Fulfil any other obligation derived from the applicable legislation, the CPS or the Certificate Policies.

6 Obligations of relying parties

Third parties who accept and rely on certificates issued by the Banco de España's PKI shall have the following obligations:

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

7 Liability limitations

PKIBDE shall be held liable in the case of breach of the obligations contained in Law 59/2003, dated 19 December, the Electronic Signature Act, and its implementation regulations, in the CPS and in the specific Certificate Policies.

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

The PKI of the Banco de España, as a Certification Service Provider, does not accept responsibility for the content of the documents signed using its certificates, such as message or communication encrypting processes.

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

8 Applicable agreements, Certification Practice Statement and Policy Certificates

All the applicable agreements, Certification Practice Statement and Policy Certificates are available on the web page set up for this purpose: <http://pki.bde.es>

In particular, the following documents can be highlighted:

| Document Name | File Name | Electronic Address |
|------------------------------------------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------------------------|
| Certification Practice Statement | PKIBdE_DPC-vX.Y.pdf | http://pki.bde.es/politicas |
| Certificate Policy for internal user certificates | PKIBdE_PC_CertUsuarioInterno-vX.Y.pdf | http://pki.bde.es/politicas |
| Certificate Policy for personal authentication certificates for mobile devices | PKIBdE_PC_CertAutenticacionMovil-vX.Y.pdf | http://pki.bde.es/politicas |
| Certificate Policy for Internal Use Component Certificates | PKIBdE_PC_CertComponentes-vX.Y.pdf | http://pki.bde.es/politicas |
| Certificate Policy for External Entity Component Certificates | PKIBdE_PC_CertComponentesEntidadesExternas-vX.Y.pdf | http://pki.bde.es/politicas |
| Certificate Policy for Time-stamping Authority Certificates | PKIBdE_PC_CertTSA_vX.Y.pdf | http://pki.bde.es/politicas |
| Time-stamping Authority of Banco de España Time Stamping Policies and Practices | PKIBdE_PST_y_DPST-vX.Y.pdf | http://pki.bde.es/politicas |

X.Y indicates the version at any given time

9 Personal Data Protection

The processing of personal data shall comply with the provisions set out in the applicable regulations on the subject and, in particular, with the following:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- Organic Law 3/2018 of 5 December 2018 on the protection of personal data and digital rights.
- Banco de España Internal Instruction 5/2020 of 30 July on the protection of personal data.

In addition, personal data shall be processed in compliance with the instructions set out in the processing report applicable to "Electronic Certificates", including all its annexes.

10 Provision of certification services free of charge

No charge is made for obtaining and using internal user certificates issued by the Banco de España's PKI

11 Governing Law

The operations and functioning of Banco de España's PKI, as well as this Certification Practice Statement and the applicable Certificate Policies for each type of certificate shall be subject to the regulations applicable to them and, specifically:

- European Parliament and Council Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures (OJ, 19 January 2000).
- Spanish Law 59/2003, of 19 December, on Electronic Signature (Spanish Official Gazette, 20 December).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and Organic Law 3/2018.
- Organic Law 3/2018 of 5 December 2018 on the protection of personal data and digital rights.
- Banco de España Internal Instruction 5/2020 of 30 July on the protection of personal data.
- Royal Legislative Decree 1/1996, of 12 April, approving the Revised Intellectual Property Act (Spanish Official Gazette, 22 April).

Likewise, where applicable, the internal rules and procedures established by Banco de España and designed to guarantee the level of security required by Royal Legislative Decree 311/2022, dated May 3, which regulates the National Security Framework (ENS).

12 Disputes and Jurisdiction

All disputes between users or third parties and PKIBDE shall be notified by the disputing party to the Banco de España's PAA, endeavouring to resolve said disputes between the parties themselves. In the event that agreement cannot be reached between the parties, resolution of any dispute that may arise shall be submitted to the courts and tribunals of the city of Madrid, the parties waiving any other jurisdiction to which they may have a right.

13 CA and repository audits, certifications and security standards

Audits

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

As established in article 31 of Royal Legislative Decree 311/2022, dated May 3, which regulates the National Security Framework (ENS), an ordinary regular audit will be performed, at least every two years, to verify compliance with the National Security Framework requirements, and on an extraordinary basis, the previously mentioned audit must be performed whenever there are substantial modifications that may affect the required security measures.

Standards

The personal electronic signature certificates issued by the Banco de España PKI fulfil all the technical and organisational requirements established for recognised certificates in:

- Spanish Law 59/2003, of 19 December, the Electronic Signature Act (Official State Gazette, 20 December).
- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.