



# **Certificate Policy**

## **Bundesbank Email-CA externe Partner**

Version 1.0

1	Introduction.....	4
1.1	Overview .....	4
1.2	Convention/Naming.....	4
1.3	Document Name and Identification .....	4
1.4	PKI Participants .....	4
1.5	Certificate Usage .....	5
1.6	Policy Administration.....	5
1.7	Definitions and Acronyms.....	5
2	Publication and Repository Responsibilities.....	6
2.1	Repositories .....	6
2.2	Publication of Certification Information .....	6
2.3	Time and Frequency of Publication .....	6
2.4	Access Controls on Repositories.....	6
3	Identification and Authentication .....	7
3.1	Names .....	7
3.2	Initial Identity Validation .....	7
3.3	Identification and Authentication for Re-key Requests .....	8
3.4	Identification and Authentication for Revocation Request.....	8
4	Certificate Life Cycle Operational Requirements.....	9
4.1	Certificate Application .....	9
4.2	Certificate Application Processing .....	9
4.3	Certificate Issuance.....	9
4.4	Certificate Acceptance .....	10
4.5	Key Pair and Certificate Usage .....	10
4.6	Certificate Renewal.....	10
4.7	Certificate Re-key .....	10
4.8	Certificate Modification.....	10
4.9	Certificate Revocation and Suspension.....	11
4.10	Certificate Status Service .....	13
4.11	End of Subscription .....	13
4.12	Key Escrow and Recovery .....	13
5	Facility, Management and Operational Controls .....	14
5.1	Physical Controls .....	14
5.2	Procedural Controls .....	14
5.3	Personnel Controls.....	15
5.4	Audit Logging Procedures .....	16
5.5	Records Archival.....	18
5.6	Key changeover .....	18
5.7	Compromise and Disaster Recovery .....	18
5.8	CA or RA Termination .....	19
6	Technical Security Controls .....	20
6.1	Key Pair Generation and Installation .....	20
6.2	Private Key Protection and Cryptographic Module Engineering Controls .....	21

6.3	Other Aspects of Key Pair Management .....	22
6.4	Activation Data.....	22
6.5	Computer Security Controls .....	23
6.6	Life Cycle Technical Controls.....	23
6.7	Network Security Controls.....	23
6.8	Time-Stamping.....	23
7	Certificate, CRL and OCSP Profiles.....	24
7.1	Certificate Profile.....	24
7.2	CRL Profile .....	24
7.3	OCSP Profile.....	25
8	Compliance Audit and Other Assessments.....	26
8.1	Frequency or Circumstances of Assessment .....	26
8.2	Identity/Qualifications of Assessor.....	26
8.3	Assessor's Relationship to Assessed Entity .....	26
8.4	Topics Covered by Assessment .....	26
8.5	Actions Taken as a Result of Deficiency .....	26
8.6	Communication of Results .....	26
9	Other Business and Legal Matters.....	27
9.1	Fees.....	27
9.2	Financial Responsibility.....	27
9.3	Confidentiality of Business Information.....	27
9.4	Privacy of Personal Information.....	27
9.5	Intellectual Property Rights .....	28
9.6	Representations and Warranties .....	28
9.7	Disclaimer of Warranties .....	28
9.8	Limitations of Liability .....	28
9.9	Indemnities .....	29
9.10	Term and Termination.....	29
9.11	Individual Notices and Communications with participants.....	29
9.12	Amendments.....	29
9.13	Dispute resolution Provisions .....	29
9.14	Governing Law.....	30
9.15	Compliance with Applicable Law .....	30
9.16	Miscellaneous Provisions .....	30
9.17	Other Provisions .....	30
10	Abbreviations.....	31

# 1 Introduction

## 1.1 Overview

This document provides both users and the Deutsche Bundesbank – as the Public Key Infrastructure (PKI) operator – with a summary of the binding certification guidelines of the Deutsche Bundesbank for the issuance of Email Security Certificates (to be used for encryption and signature) for counterparties in the form of a Certificate Policy (CP).

The structure of this document follows the template specified in the RFC 3647 standard.

## 1.2 Convention/Naming

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

## 1.3 Document Name and Identification

Name: Certificate Policy  
Bundesbank Email-CA externe Partner  
Version: 1.0  
Date: 01 April 2025  
OID: 1.3.6.1.4.1.2025.590.30.1

## 1.4 PKI Participants

### 1.4.1 Certification Authorities

The Bundesbank's PKI (BBk-PKI) uses a certification structure with a self-signed root certificate. The root CA certificate certifies only user certificates for the encryption and signing of emails from counterparties.

### 1.4.2 Registration Authorities

The registration authorities (RA) are responsible for:

- The verification of the identity and authenticity of subscribers,
- The operation of registration procedure,
- The documentation of registration procedure
- The operation and documentation of suspension and revocation of certificates

The authentication procedure is described in point 3.2.3.

### 1.4.3 Subscribers

Subscribers are counterparties of the Bundesbank.

### 1.4.4 Relying Parties

Relying parties are communication partners (persons, organisations or systems) that take part in the certificate-based procedure for secure email communication with the Bundesbank.

#### **1.4.5 Other Participants**

Other participants may be service providers (eg directory service operators) appointed by the BBk-PKI.

### **1.5 Certificate Usage**

#### **1.5.1 Appropriate Certificate Uses**

The appropriate certificate use must be documented in the relevant CAs CPS.

#### **1.5.2 Prohibited Certificate Uses**

All certificate uses, not listed in 1.5.1, are prohibited.

### **1.6 Policy Administration**

#### **1.6.1 Organization Administering the Document**

This CP is maintained by the operator of the BBk-PKI and the responsible IT-unit. CPs are always verified by the Deutsche Bundesbank's IT security management.

#### **1.6.2 Contact Person**

Deutsche Bundesbank

PKI Services

Berliner Allee 14      Postfach 10 11 48

40212 Düsseldorf      40002 Düsseldorf

Germany              Germany

Tel:    +49 211 874 3257/2351

E-mail: pki@bundesbank.de

#### **1.6.3 Person Determining CPS Suitability for the Policy**

CPs are always verified by the Deutsche Bundesbank's IT security management. The IT security management department is a high-level management body within the PKI.

The responsible unit verifies that each CPS complies with the guidelines in the respective CP.

#### **1.6.4 CPS Approval Procedures**

CPS documents are reviewed and approved and versioned by members of Deutsche Bundesbank's IT security management at the time of creation and after amendments.

### **1.7 Definitions and Acronyms**

See chapter 10.

## **2 Publication and Repository Responsibilities**

### **2.1 Repositories**

The Bundesbank publishes information about the BBk-PKI on its website.

- <http://www.bundesbank.de> under Service ► Banks and companies ► PKI – Public Key Infrastructure

### **2.2 Publication of Certification Information**

The Bundesbank publishes the following information:

- CA certificates with fingerprints
- CRLs
- CPs and CPSs

### **2.3 Time and Frequency of Publication**

Publication dates for CA/root CA certificates, CRLs and CP and CPS are as follows.

- CA certificates with fingerprints: as soon as they are generated
- CRLs: after revocation, otherwise on a regular schedule (see point 4.9.7)
- CPs and CPSs: after generation/update

### **2.4 Access Controls on Repositories**

Read access to the information listed under points 2.1 and 2.2 is not restricted. The BBk-PKI is responsible for write access.

## **3 Identification and Authentication**

### **3.1 Names**

#### **3.1.1 Types of Names**

The name of the certificate issued (Distinguished Name = DN) must comply with the x.509 standard. Optionally, certificates can contain Subject Alternative Names (SAN). The permitted types of names must be documented in the CPS.

#### **3.1.2 Need for Names to be meaningful**

The name of the certificate issued (DN) has to uniquely identify the subscriber. The following rules apply:

- Certificates for natural persons are to be issued in the subscriber's name.
- Certificates for people grouped according to organisation/function or for an organisation's email address have to be clearly distinguishable from certificates for natural persons.

#### **3.1.3 Anonymity or Pseudonymity of Subscribers**

Anonymity or pseudonymity in certificate names is prohibited for certificates issued to natural persons.

#### **3.1.4 Rules for Interpreting Various Name Forms**

The DN is based on the x.509 standard.

Other types of names can be entered into the "Subject Alternative Name" field. The use of "Subject Alternative Names" must be indicated by the CA.

#### **3.1.5 Uniqueness of Names**

The responsible unit ensures that the names are unique. Issuing CAs must document and technically enforce the relevant rules guaranteeing the uniqueness of names in the CPS.

#### **3.1.6 Recognition, Authentication and Role of Trademarks**

The BBK-PKI has no procedures for resolving brand disputes. Rather, such disputes are to be settled in the civil courts by the companies involved, taking into account the laws on brands and competition.

### **3.2 Initial Identity Validation**

#### **3.2.1 Method to Prove Possession of Private Key**

Key pairs of subscribers are produced in the BBk-PKI's sphere of responsibility.

#### **3.2.2 Authentication of Organisation Identity**

A natural person has to be authenticated.

#### **3.2.3 Authentication of Individual Identity**

Applicants must uniquely authenticate themselves to the respective RA when applying for a certificate.

The type of authentication and the type of proof given must be documented in the CPS.

### **3.2.4 Non-verified Subscriber Information**

Only information required to authenticate and identify the subscriber is verified. All other subscriber information is ignored.

### **3.2.5 Validation of Authority**

This procedure is described in the respective CPS.

### **3.2.6 Criteria for Interoperation**

No stipulation.

At present no cross-certification with other organizations is planned.

## **3.3 Identification and Authentication for Re-key Requests**

### **3.3.1 Identification and Authentication for Routine Re-key**

For re-key a new application is required.

### **3.3.2 Identification and Authentication for Re-key after Revocation**

If a certificate is revoked, a new application is required.

## **3.4 Identification and Authentication for Revocation Request**

Requirements for applying revocation:

- Certificate holders requesting for revocation of their own certificates must uniquely authenticate themselves to a Bundesbank Identity provider or directory system and must be authorized to proceed a revocation.
- The applicant's identity is documented in the event of a revocation request.
- The reason and the process of submitting of a revocation request is documented.

## **4 Certificate Life Cycle Operational Requirements**

### **4.1 Certificate Application**

#### **4.1.1 Who Can Submit a Certificate Application**

Only Bundesbank employees can submit a certificate application.

#### **4.1.2 Enrollment Process and Responsibilities**

An application for certificates involves a multistage registration process to the responsible unit. The following checks are made.

- Is the applicant authenticated?
- Is the applicant authorized?
- Is the application complete and correct?
- Is the DN unique?

### **4.2 Certificate Application Processing**

#### **4.2.1 Performing Identification and Authentication Functions**

Subscribers must be identified and authenticated as described in section 3.2.

#### **4.2.2 Approval or Rejection of Certificate Applications**

Meeting the formal requirements does not constitute an entitlement to issuance of a certificate.

The decision to issue certificates is entirely the decision of the responsible unit.

A certificate application must be rejected if the requirements defined in point 3.2.1 and 4.1.2 are not fulfilled.

Acceptance or rejection must be documented.

#### **4.2.3 Time to Process Certificate Applications**

As a rule, a maximum of one week is needed to process certificate applications.

### **4.3 Certificate Issuance**

#### **4.3.1 CA Actions during Certificate Issuance**

The following actions must be performed when certificates are issued:

- Verification of the certificate application
- Creation of the certificate
- Logging of relevant operations
- Informing the applicant about the creation of the certificate.

Issuing CAs must guarantee that certificates are only issued for the intended subscribers after checking their application. The issuing procedure and the tasks involved in issuing certificates must be documented in the CPS.

#### **4.3.2 Notification to Subscriber by the CA of Issuance of Certificate**

The form of notification and the applicable rules must be documented in the CAs CPS.

## **4.4 Certificate Acceptance**

### **4.4.1 Conduct Constituting Certificate Acceptance**

The certificate is deemed to have been accepted once receipt confirmation has been received or once the certificate has been used.

### **4.4.2 Publication of the Certificate by the CA**

The certificate may be published in a directory service.

### **4.4.3 Notification of Certificate Issuance by the CA to Other Entities**

No stipulation.

## **4.5 Key Pair and Certificate Usage**

### **4.5.1 Subscriber Private Key and Certificate Usage**

Only the subscriber is entitled to use the private key.

The usage of certificates is restricted to the key usage and extended key usage they are issued for.

The keys and certificates are permitted to use exclusively for communication in connection with business matters of the Deutsche Bundesbank.

### **4.5.2 Relying Party Public Key and Certificate Usage**

Relying parties are IT systems and/or IT processes which use the certificate only for the purposes stated therein. The relying party must check the trust of certificate chain and validity period of the certificate. Any limitation on the usage of certificates must be taken in account.

## **4.6 Certificate Renewal**

A certificate must not be renewed on the basis of the existing key pair. Whenever a certificate is renewed, a new key pair must always be generated. See point 4.7.

Certificate renewal must not be performed for CA certificates.

## **4.7 Certificate Re-key**

Whenever a certificate is renewed, a new key pair must be generated.

A CA certificate re-key must be handled as a new certificate application.

## **4.8 Certificate Modification**

A certificate is modified on the basis of an application and involves changing the key pair and modifying the content of the certificate as well as the technical parameters. A certificate modification must always require a re-keying.

### **4.8.1 Circumstances for certificate modification**

Certification with re-keying and modification is possible in the following cases:

- Routine re-keying
- If the validity of the certificate is about to expire or has just expired.
- Certificate application after a previous certificate has been revoked.

- The algorithms, key sizes or the validity periods of the certificate no longer provide adequate security, or the structure of the certificate urgently requires modification.
- The data on the certificate do not or no longer correspond to the facts.

The newly issued certificate replaces the existing certificate. The issuing CA and RA must guarantee that the time during which a subscriber has access to certificates with the same purpose is limited according to the use case.

#### **4.8.2 Who May Request Certificate Modification**

Application by a subscriber is governed by the rules for new applications. See point 4.1.1. If ad hoc certificate modification is required as a result of security issues relating to key sizes, validity periods or certificate structure, the responsible unit is responsible for informing PKI participants and prepare exchange of certificates. The rules for initial application apply. See point 4.1.1.

#### **4.8.3 Processing Certificate Modification Requests**

The rules for initial application apply. See point 4.2.

#### **4.8.4 Notification of new Certificate Issuance to Subscriber**

The rules for initial application apply. See point 4.3.2.

#### **4.8.5 Conduct Constituting Acceptance of a Modified Certificate**

The rules for initial application apply. See point 4.4.1.

#### **4.8.6 Publication of the Modified Certificate by the CA**

The rules for initial application apply. See point 4.4.2.

#### **4.8.7 Notification of Certificate Issuance by the CA to Other Entities**

The rules for initial application apply. See point 4.4.3.

### **4.9 Certificate Revocation and Suspension**

#### **4.9.1 Circumstances for Revocation**

- A certificate must be revoked if at least one of the following circumstances arises.
- Information in the certificate is not or no longer valid.
- The private key has been compromised.
- The subscriber is no longer authorized to use the certificate.
- The subscriber no longer requires the certificate.
- The subscriber does not comply with the obligations specified in the respective CP/CPS (see point 4.5).
- The private key of the issuing CA has been compromised. In this case, all certificates issued by this CA are revoked as well.
- The algorithms, key sizes or validity periods of the certificate no longer provide sufficient security. The responsible unit reserves the right to revoke the certificates in question.

#### **4.9.2 Who can Request Revocation**

Revocation of CA certificate

Only the Bundesbank IT security management must be entitled to process the revocation of the CA certificate, but every PKI participant may initiate a request for revocation.

Revocation of end-entity certificates

Only the subscriber for a certificate or an authenticated and authorized intermediary may request certificate revocation.

#### **4.9.3 Procedure for Revocation Request**

Prior to the revocation of a certificate, the issuing CA must verify that the revocation has been requested by the certificate's subscriber according to Section 4.9.2.

CA certificates must only be revoked as a result of a security incident on the basis of the regulations of the Incident Management processes. Any revocation of a CA certificate must be confirmed by a Risk Commission.

#### **4.9.4 Revocation Request Grace Period**

Revocation requests shall be submitted as soon as possible within a commercially reasonable time.

#### **4.9.5 Time within which CA must Process the Revocation Request**

The maximum time for processing must be defined in the CPS of the respective CA.

#### **4.9.6 Revocation Checking Requirement for Relying Parties**

Certificate status information is published using CRLs. Relying parties must use the most recent CRL to verify the validity of certificates.

#### **4.9.7 CRL Issuance Frequency**

The CRL validity period and publishing frequency is defined in the CPS of the respective CA.

If the revocation of a certificate leads to the creation of a new CRL, this is published immediately and replaces the prevailing CRL irrespective of its original duration.

A new CRL must contain the information about revoked certificates until those certificates have expired.

#### **4.9.8 Maximum Latency for CRLs**

CRLs must be published as soon as they have been created.

#### **4.9.9 Online Revocation/Status checking Availability**

CRLs from the responsible unit are published to the CRL Distribution Points. CDPs must be selected in such a way that all the designated subscribers have access to at least one of them.

Issuing CAs may additionally provide a revocation status check via OCSP.

Availability of this check, and each access to it, must be documented in the CPS.

#### **4.9.10 Online Revocation checking Requirements**

Not applicable

#### **4.9.11 Other Forms of Revocation Advertisements available**

Not applicable

#### **4.9.12 Special Requirements Re-key Compromise**

If a subscriber's private key is compromised, the corresponding certificate must be revoked immediately.

If a CA's private key is compromised, the CA certificate and all certificates that it has issued must be revoked.

#### **4.9.13 Circumstances for Suspension**

A temporary revocation or suspension of certificates is prohibited.

#### **4.9.14 Who can Request Suspension**

Not applicable

#### **4.9.15 Procedure for Suspension Request**

Not applicable

#### **4.9.16 Limits on Suspension Period**

Not applicable

### **4.10 Certificate Status Service**

The responsible unit can provide a certificate status request service.

### **4.11 End of Subscription**

A subscriber can end the subscription either by requesting for revocation of a certificate or by not applying for a new certificate once the current certificate has expired.

### **4.12 Key Escrow and Recovery**

Key escrow and recovery is not prohibited.

## **5 Facility, Management and Operational Controls**

### **5.1 Physical Controls**

#### **5.1.1 Site Location and Construction**

The central (IT) components of the SubCAs are placed in access-protected areas within the Deutsche Bundesbank's data centers (DC). The Bundesbank operates a high-availability, redundant DC across two sites. One DC is certified to TÜV IT Level 4, and the second DC site is certified to DIN EN ISO 9001 as well as DIN ISO EC 27001.

#### **5.1.2 Physical Access**

Physical access must support a multi-stage access control system.

#### **5.1.3 Power and Air Conditioning**

The power supply must meet the required standards. All online infrastructures must be installed at least in duplicate, completely separately from each other.

#### **5.1.4 Water Exposures**

The rooms must have adequate protection from exposure to water.

#### **5.1.5 Fire Prevention and Protection**

Fire prevention and fire alarm regulations must be observed.

#### **5.1.6 Media Storage**

Not applicable.

#### **5.1.7 Waste Disposal**

Waste disposal must comply with the Deutsche Bundesbank's safety regulations.

#### **5.1.8 Off-Site Backup**

An offsite backup should be implemented if the data storage is not operated in different data centers.

There is not an off-site data backup external to the data centers (e.g., at other service providers).

### **5.2 Procedural Controls**

#### **5.2.1 Trusted Roles**

Trusted roles must be established to ensure that individuals are not able to change any of the security-critical components or view, generate or manipulate certificates or private keys without being noticed.

At least these roles must be implemented:

- Head of CA Operations
- Revisor
- IT Security Officer
- System Administrator

- Access Manager
- CA Operator
- RA Operator

CAs must document established roles in their CPS.

### **5.2.2 Number of Persons Required per Task**

The implementation of a multiple-pairs-of-eyes principle when generating cryptographic keys can be found in the respective CPS.

At least these tasks must implement a multi person processing:

- HSM key ceremony
- Generation of CA keys
- RA approval processes
- Recovery of CA data

### **5.2.3 Identification and Authentication for Each Role**

The trusted roles approach is implemented using a number of technical and organizational measures. Roles must be identified and authenticated by using a smart card.

### **5.2.4 Roles Requiring Separation of Duties**

By separating certain operational and administrative roles and duties, the approach ensures that no one person alone has complete control over the solution. The respective CPS must provide more detailed information.

## **5.3 Personnel Controls**

### **5.3.1 Qualifications, Experience and Clearance Requirements**

In its operations, the responsible unit shall use experienced personnel who have the necessary IT expertise and specific knowledge of CA operations.

### **5.3.2 Background Check Procedures**

The Bundesbank subjects personnel in the responsible unit to an advanced security check with a view to sabotage protection in accordance with the Security Check Act (Sicherheitsüberprüfungsgesetz – SÜG).

### **5.3.3 Training Requirements**

Personnel operating CAs for the responsible unit receive regular and ad hoc training. They are sensitized to the security relevance of their work.

### **5.3.4 Retraining Frequency and Requirements**

Retraining is provided in particular when new or amended directives, IT systems and/or IT processes are implemented.

### **5.3.5 Job Rotation Frequency and Sequence**

Routinely job rotation shall not occur.

For new personnel or assignment of new responsibilities the requirements in point 5.3.3 apply.

### **5.3.6 Sanctions for Unauthorized Actions**

Unauthorized actions that endanger the security of the responsible unit or breach data protection requirements must be punished/prosecuted by the Human Resources Department.

### **5.3.7 Independent Contractor Requirements**

Not applicable.

### **5.3.8 Documentation Supplied to Personnel**

To ensure that they can conduct operations correctly, PKI personnel receive the following documentation.

- Certificate Policy (CP)
- Certification Practice Statement (CPS)
- Operating manuals
- User instructions
- Official rules and regulations

## **5.4 Audit Logging Procedures**

All IT systems located in the Deutsche Bundesbank infrastructure must synchronize with an internal time source. The internal time-source using a DCF77 correlation receiver.

In case of offline operation, a manual procedure must be implemented.

### **5.4.1 Types of Events Recorded**

CAs must monitor and securely store the following processes.

- System initialization
- System Login / Logoff
- CA activation
- Operator processes
- Certification applications
- User registration
- Role Management
- Key generation
- Certificate issuance
- Data backups
- Certificate publication
- Delivery of private key and certificate
- Revocation and suspension of applications
- Revocation and suspension of certificates
- CRL generation
- CRL publication

Any malfunctions or one-off operating situations must also be recorded. Retention period is documented in point 5.4.3.

#### **5.4.2 Frequency of Processing Log**

The Bundesbank's Directorate General Internal Audit verifies that certification operations are as they should be as part of its risk-oriented audits. If there is suspicion of irregularities, a more detailed audit is conducted.

#### **5.4.3 Retention Period for Audit Log**

Retention period must be based on the times stipulated in law, audit compliance provisions, and other internal rules and regulations.

Audit log retention must apply to the requirements of the DSGVO Art. 5 for CAs issuing certificates to natural persons.

The retention period is at least one year.

#### **5.4.4 Protection of Audit Log**

The logs must be protected against unauthorized access, publication, manipulation and destruction.

#### **5.4.5 Audit Log Backup Procedures**

Log data must be backed up regularly along with other relevant data. Paper logs must be stored in lockable cupboards.

#### **5.4.6 Audit Collection System (Internal vs. External)**

The audit logs shall be transferred to a central audit log collection system (Log-Appliance) for archival and central evaluation.

#### **5.4.7 Notification to Event-Causing Subject**

If a security-critical event occurs, the responsible unit must notify the IT security management incidents as well as the system owner.

#### **5.4.8 Vulnerability Assessments**

There is an active and generally accepted vulnerability and patch-management policy in place at Deutsche Bundesbank

- Information about vulnerability from the vendors of hard- and software components of the PKI system must be observed by the system owners operating staff.
- Software updates must be installed at least once a year.
- Security patches and updates must be installed immediately.
- Generally, every workplace client gets systematically planned releases including security patches twice a year

## **5.5 Records Archival**

### **5.5.1 Types of Records Archived**

All data that are relevant for the certification process (see point 5.4.1) must be archived.

### **5.5.2 Retention period for Archive**

The retention periods for archived data is at least the validity end date of the CA certificate plus one year.

### **5.5.3 Protection of Archive**

The archives must be protected against unauthorized access, publication, manipulation and destruction.

### **5.5.4 Archive Backup Procedures**

Archive and backup procedures must be defined in the respective CPS of the CA.

### **5.5.5 Requirements for Time-Stamping of Records**

Trustworthy timestamp sources may be implemented.

### **5.5.6 Archive Collection System (internal or external)**

The responsible unit is responsible for archiving. Archives must not be stored externally.

### **5.5.7 Procedures to Obtain and Verify Archive Information**

Archived Information must be stored either encrypted or signed to accomplish a verification of the integrity of data.

File names must include date information of their origin.

## **5.6 Key changeover**

When the certificate of a CA of the PKI is about to expire, a new key pair must be created and a new CA certificate must be generated. This process must be handled as a new certification application.

## **5.7 Compromise and Disaster Recovery**

### **5.7.1 Incident and Compromise Handling Procedures**

The IT security management defines the procedure to deal with security incidents and compromise of private keys.

### **5.7.2 Computing Resources, Software, and/or Data are corrupted.**

If PKI component has faulty or manipulated computing resources, software and/or data that have an impact on the processes conducted by this entity, the system in question must be stopped immediately.

The system must be reset using software and data backups, and – after checks in safe mode – it is to be put back into operation. The faulty or modified system must be analyzed. If there is a suspicion of willful action, legal steps may be taken.

If certificates have been generated using incorrect data, the subscriber or the person responsible for the IT system and/or the IT process must be informed immediately, and the certificate must be revoked by the certification authority.

### **5.7.3 Entity Private key compromise Procedures**

If a CA's private key is compromised, the corresponding certificate must be revoked immediately. All certificates issued by this certification authority must be revoked at the same time. All subscribers affected are to be notified immediately.

The entity in question is set up as a new CA with a new key pair. The certificate of the new CA is published and any subscriber certificates that were previously revoked are reissued.

### **5.7.4 Business Continuity Capabilities after a Disaster**

A disaster recovery plan must be designed, tested und implemented to mitigate the effects of any kind of natural or man-made disaster.

Relevant standards as ISO2700x and ISO 22301 Business Continuity Management should be used as source of information.

## **5.8 CA or RA Termination**

If the operations of the responsible unit or of a SubCA are terminated, the following measures must be taken:

- Notification of all subscribers as well as relying parties with a lead time of at least three months.
- Revocation of all certificates issued by the CA.
- Destruction of the CA's private keys.
- Publication of the corresponding CA and root CA CRLs.

## **6 Technical Security Controls**

### **6.1 Key Pair Generation and Installation**

#### **6.1.1 Key Pair Generation**

The key material of CAs must be generated in a Hardware Security Module. All cryptographic modules used are certified to at least Common Criteria EAL 4+ or FIPS 140-2 Level 3.

Key material for End Entities can be generated by software random key generators. Centrally generated key pairs should be generated by Hardware Security Modules

#### **6.1.2 Private Key Delivery to Subscriber**

Private keys must be delivered encrypted to subscribers when they are centrally generated.

#### **6.1.3 Public Key Delivery to Certificate Issuer**

Not applicable

#### **6.1.4 CA Public Key Delivery to Relying Parties**

Certificates of CAs must be published in the repositories named in point 2.1.

The validation of the CA certificates fingerprint must include checking the certificate's fingerprint using a second communication channel.

#### **6.1.5 Key Sizes**

Key sizes and algorithms must be chosen according to the BSI TR-02102-1 or subsequent documents.

- CA keys must have a minimum of 4096 bits for RSA or 512 bits for ECC.
- End Entity keys must have a minimum of 2048 bits for RSA or 256 bits for ECC.

For ECC only NIST curves should be used for compatibility reasons

#### **6.1.6 Public Key Parameters Generation and Quality Checking**

The following encryption algorithms are to be used.

- RSA 1.2.840.113549
- rsaEncryption 1.2.840.113549.1.1.1
- SHA256 RSA 1.2.840.113549.1.1.11
- SHA384 RSA 1.2.840.113549.1.1.12
- SHA512 RSA 1.2.840.113549.1.1.13
- ECC\_CURVE\_P256 1.2.840.10045.3.1.7
- ECC\_CURVE\_P384 1.3.132.0.34
- ECC\_CURVE\_P521 1.3.132.0.35
- ECDSA\_SHA256 1.2.840.10045.4.3.2
- ECDSA\_SHA384 1.2.840.10045.4.3.3
- ECDSA\_SHA512 1.2.840.10045.4.3.4

### **6.1.7 Key Usage Purposes (as per x.509 v3 Key Usage Field)**

For CAs, the key usage purposes are

- signing certificates 2.5.29.15.5
- signing CRLs. 2.5.29.15.6

For end entities, the key usage purposes are

- digital signature 2.5.29.15.0
- contentCommitment 2.5.29.15.1
- key encipherment 2.5.29.15.2
- data encipherment 2.5.29.15.3

See point 1.4.1.

## **6.2 Private Key Protection and Cryptographic Module Engineering Controls**

Private keys of CAs must be created inside and stored in HSMs. Private keys for end entities may be created and stored in software.

### **6.2.1 Cryptographic Module Standards and Controls**

The cryptographic modules used must be certified at least to the level of Common Criteria EAL 4+ or FIPS 140-2 Level 3.

### **6.2.2 Private Key (n out of m) Multi-Person Control**

The CAs private key must only be used in the secure environment of an HSM. The CAs private key must never leave the HSM unencrypted.

### **6.2.3 Private Key Escrow**

CA key escrow must be prohibited within or outside the Bundesbank.

### **6.2.4 Private Key Backup**

Backups of private keys for CAs must be permitted within the HSM's security system. Backups of private keys for end entities may be stored encrypted in the CA database.

### **6.2.5 Private Key Archive**

Private keys may be archived encrypted in the CA database.

### **6.2.6 Private Key Transfer into or from a Cryptographic Module**

Transfer of private keys belonging to CAs must only take place in an HSM dedicated to the same CA; the provisions of point 6.2.2 must be observed here. Transferring private keys to a new HSM must be based on processes using a multi-person control.

### **6.2.7 Private Key Storage on Cryptographic Module**

See point 6.2.1.

### **6.2.8 Method of Activating Private Key**

The activation of a CAs private keys must be described in the respective CAs CPS. Private keys belonging to end entities should be password protected depending on the particular use case.

### **6.2.9 Method of Deactivating Private Key**

The method of deactivation of a CAs private keys must be described in the respective CAs CPS.

Applications using end entities private keys must release them after the termination of the application.

### **6.2.10 Method of Destroying Private key**

Once the validity of the CA's private key has expired or this key has been revoked, the key must be deleted from the HSM environment. Private keys and further key material stored in a HSM leaving the PKI Environment must be destroyed by using a factory reset procedure, as dictated by the HSM vendor.

### **6.2.11 Cryptographic Module Rating**

See point 6.2.1.

## **6.3 Other Aspects of Key Pair Management**

### **6.3.1 Public Key Archival**

All public keys generated by the responsible unit are archived in the CA's database.

### **6.3.2 Certificate Operational Periods and Key Pair Usage Periods**

The certificates issued by the BBk-PKI have the following validity periods:

- CA certificates maximum of 6 years
- End entity certificates maximum of 3 years

## **6.4 Activation Data**

### **6.4.1 Activation Data Generation and Installation**

Activation data for CAs private keys must be generated using HSM devices. The activation smartcards for multi-person control must be PIN protected.

The PIN policies must follow Deutsche Bundesbank PIN and password regulations.

Activation data is part of the generation of the certificates for end entities.

### **6.4.2 Activation Data Protection**

Activation data of Root CA private key must be protected by two-factor authentication and multi-person control.

Activation data of Issuing CAs must be stored encrypted and transferred while start process of CA service. Decryption of activation data must only be possible using a corresponding HSM. Activation Data for centrally generated keys can be delivered to the end entities by:

- Password letter
- E-Mail

#### **6.4.3 Other Aspects of Activation Data**

Activation data of end entities locally generated keys corresponds to the relative activation method.

### **6.5 Computer Security Controls**

#### **6.5.1 Specific Computer Security Technical Requirements**

All of the responsible unit's IT systems must be run according to the applicable IT security guidelines and must be competently protected against manipulation and espionage. See point 5.4.8.

#### **6.5.2 Computer Security Rating**

The security measures must be state of the art. A threat analysis must be conducted regularly, at least every two years.

### **6.6 Life Cycle Technical Controls**

#### **6.6.1 System Development Controls**

The Deutsche Bundesbank's IT risk management process must be apply when planning and/or developing the solution.

#### **6.6.2 Security Management Controls**

See point 6.5.1.

#### **6.6.3 Life Cycle Security Controls**

Any IT systems or components that are replaced are disabled in such a way that the functions thereof and data contained therein cannot be misused.

In addition, any changes to IT systems or components must always go through the Deutsche Bundesbank's IT risk management process.

### **6.7 Network Security Controls**

See point 6.5.1.

### **6.8 Time-Stamping**

The time must be synchronous on all IT-systems (see point 5.5).

Timestamping may be implemented.

## **7 Certificate, CRL and OCSP Profiles**

### **7.1 Certificate Profile**

#### **7.1.1 Version Number(s)**

The BBk-PKI issued certificates must be conform with the x509v3 standard.

#### **7.1.2 Certificate Extensions**

CAs must document the allowed certificate extensions in the CPS

See 6.1.5, 6.1.6, 6.1.7

#### **7.1.3 Name Forms**

See points 3.1.1 and 3.1.2.

#### **7.1.4 Name Constraints**

See point 3.1.

#### **7.1.5 Certificate Policy Object Identifier (OID)**

See 1.3

#### **7.1.6 Usage of Policy Constraints Extension**

Not applicable.

#### **7.1.7 Policy Qualifiers Syntax and Semantics**

Not applicable.

#### **7.1.8 Processing Semantics for the Critical Certificate Policies Extension**

Not applicable.

### **7.2 CRL Profile**

#### **7.2.1 Version Number(s)**

The BBk-PKI must issue CRLs conforming to x.509 version 2 in accordance with RFC 5280 point 5.

#### **7.2.2 CRL and CRL Entry Extensions**

The CRLs must include the following CRL extensions and CRL entry extensions:

Authority Key Identifier

- CRL Number
- CA Version
- Reason Codes
- Revocation Date
- Certificate Serial Number

Other extensions may be used.

## **7.3 OCSP Profile**

Issuing CAs may provide OCSP services.

### **7.3.1 Version Number(s)**

OCSP Version 1 defined in RFC6960 must be supported.

### **7.3.2 OCSP Extensions**

The OCSP profiles must be defined in the CPS of the respective Issuing CA.

## **8 Compliance Audit and Other Assessments**

An audit and compliance check must be done on a regular frequently basis. The technical framework and operational processes of the PKI is part of the regular internal audit pursuant to the Bundesbank's rules for such procedures. The audit results are not published.

Initial risk management process is documented in point 6.6.

### **8.1 Frequency or Circumstances of Assessment**

As a rule, internal audits and inspections are conducted at regular intervals. Assessments will take place, among other things, with the following changes:

- change of version
- installation of new releases
- replacement of components

If there are no reasons for an earlier assessment, an assessment must take place every three years.

### **8.2 Identity/Qualifications of Assessor**

Internal audits are conducted by the Directorate General Audit and the responsible unit's management. The inspectors have sufficient knowledge and expertise in the field of public key infrastructure to be able to conduct the audits.

### **8.3 Assessor's Relationship to Assessed Entity**

Assessor's must not be involved in the responsible unit's production process. Self-assessment must be prohibited.

### **8.4 Topics Covered by Assessment**

All topics relevant to the PKI must be inspected. The topics covered in the inspection are at the discretion of the inspector.

### **8.5 Actions Taken as a Result of Deficiency**

If any deficiencies are determined, these must be rectified as quickly as possible by the CA in consultation with the inspector. The inspector must be informed once these deficiencies have been rectified.

### **8.6 Communication of Results**

The results of the assessment will not be published.

## **9 Other Business and Legal Matters**

### **9.1 Fees**

No fees will be charged.

### **9.2 Financial Responsibility**

The Deutsche Bundesbank ensures its resilience and maintain operational integrity, by proactively implementing comprehensive risk mitigation strategies. The Deutsche Bundesbank is committed to establishing robust contingency frameworks and securing necessary reserves to address potential disruptions efficiently.

### **9.3 Confidentiality of Business Information**

#### **9.3.1 Scope of Confidential Information**

All information and data about BBK-PKI subscribers and participants that are not covered by point 9.3.2 are considered confidential.

#### **9.3.2 Information not within the Scope of Confidential Information**

All information and data that are contained in published certificates and CRLs, either explicitly (e.g. e-mail addresses) or implicitly (e.g. data about certification), or that can be derived from them, are not considered confidential.

#### **9.3.3 Responsibility to Protect Confidential Information**

The responsibility to protect confidential information lies with the BBK-PKI.

### **9.4 Privacy of Personal Information**

#### **9.4.1 Privacy Plan**

Personal information is stored and processed as stipulated in legal data protection provisions.

#### **9.4.2 Information Treated as Private**

All information about the responsible unit's subscribers and participants is treated as confidential.

#### **9.4.3 Information not Deemed Private**

The provisions defined in point 9.3.2 apply.

#### **9.4.4 Responsibility to Protect Private Information**

Responsibility for protecting personal information lies with the responsible unit.

#### **9.4.5 Notice and Consent to Use Private Information**

The subscriber gives the responsible unit consent to use personal information insofar as this is required for it to render its services. In addition, all information that is not deemed confidential may be published.

#### **9.4.6 Disclosure Pursuant to Judicial or Administrative Process**

The responsible unit stores and processes personal information as stipulated in legal data protection provisions. Such information is disclosed to government entities only if corresponding rulings are presented that are in line with legal provisions.

#### **9.4.7 Other Information Disclosure Circumstances**

No other information disclosure circumstances are envisaged.

### **9.5 Intellectual Property Rights**

The Deutsche Bundesbank owns the intellectual property rights to this document. The document can be passed on to third parties as it stands.

### **9.6 Representations and Warranties**

#### **9.6.1 CA Representations and Warranties**

The BBk-PKI undertakes to follow the provisions of this CP.

#### **9.6.2 RA Representations and Warranties**

The BBk-PKI and those authorities involved in registration undertake to follow the provisions of this CP.

#### **9.6.3 Subscriber Representations and Warranties**

The subscriber undertakes to take all necessary measures to protect his/her private keys and to comply with the Bundesbank's rules for handling certificates and smart cards.

#### **9.6.4 Relying party Representations and Warranties**

The relying party's obligations are defined in point 4.5.2. S/he must also follow his/her organization's certificate guidelines.

#### **9.6.5 Representations and Warranties of other participants**

Not applicable.

### **9.7 Disclaimer of Warranties**

As a rule, no warranties are assumed. The Deutsche Bundesbank does not guarantee availability of the PKI services.

### **9.8 Limitations of Liability**

If, when implementing the agreement, the Bundesbank culpably violates an essential contractual obligation which is of major importance in an individual case, it is liable for the damages thereby caused. In the case of minor negligence, the Bundesbank's liability is limited to damages characteristic for the type of agreement in question.

The Bundesbank is only liable for renegeing on other commitments if it is culpable of gross negligence. The limitation of liability vis-à-vis merchants and government institutions specified in subsection 1, sentence 2 also applies to gross negligence committed by vicarious agents.

The exclusion or limitation of liability specified above does not apply to liability for damages resulting from injury to life, body or health; in such cases the Bundesbank is liable in accordance with the statutory provisions.

In the event that the Bundesbank is liable in accordance with the above subsections, the extent of its liability, pursuant to section 254 of the German Civil Code (Bürgerliches Gesetzbuch), shall be determined by the degree to which its own culpability, in relation to other factors, contributed to causing the damage.

## **9.9 Indemnities**

If the certificate and the corresponding private key are improperly used or if the use of key material is based on information that was incorrectly provided during the application process, the Deutsche Bundesbank is released from liability.

## **9.10 Term and Termination**

### **9.10.1 Term**

This CP comes into force on the day it is published, as defined in chapter 2.

### **9.10.2 Termination**

This document is valid until it is replaced by a new version or until the BBK-PKI operations are terminated.

### **9.10.3 Effect of Termination and survival**

The responsibility to protect confidential and personal information remains unaffected by the consequences of terminating this CP.

## **9.11 Individual Notices and Communications with participants**

No rules in this respect have been made in this CP/CPS.

## **9.12 Amendments**

### **9.12.1 Procedure for Amendment**

Amendments to the CP are published in a timely manner prior to entering into force.

### **9.12.2 Notification Mechanism and Period**

The current version of the CP published on the intranet applies to Bundesbank as well as external employees of this institution.

### **9.12.3 Circumstances under which the OID must be changed**

The OID will not be amended before the end of the CA's period of validity.

## **9.13 Dispute resolution Provisions**

It is up to the Deutsche Bundesbank to decide whether arbitration proceedings should be launched.

## **9.14 Governing Law**

The place of jurisdiction is Frankfurt am Main.

## **9.15 Compliance with Applicable Law**

This CP is governed by German law. The certificates issued by the BBk-PKI are not compliant with qualified certificates as defined in the eIDAS Regulation.

## **9.16 Miscellaneous Provisions**

### **9.16.1 Entire Agreement**

All provisions of this CP/CPS are valid between the BBK-PKI and the subscribers. If a new version is issued, this replaces all previous versions. There are no verbal or subsidiary agreements.

### **9.16.2 Assignment**

There is no provision for transfer of rights.

### **9.16.3 Severability**

If individual provisions of this CP/CPS are or become invalid, this shall not affect the remaining provisions of this CP/CPS. Likewise, if a provision is missing, this shall not affect the validity of the CP/CPS. In place of the ineffective provision, an effective provision shall be deemed to be agreed that comes closest to the original intention or that would have been determined in line with the meaning and purpose of the CP/CPS had this point been covered therein.

### **9.16.4 Enforcement**

Any legal disputes arising from the BBk-PKI operations are subject to the laws of the Federal Republic of Germany.

The place of enforcement and jurisdiction is Frankfurt am Main.

### **9.16.5 Force Majeure**

The Deutsche Bundesbank accepts no liability for the violation of an obligation, for default or for non-fulfilment under this CP if this results from an underlying event that is beyond its control (e.g., force majeure, war, network outage, fire, earthquake or other catastrophes).

## **9.17 Other Provisions**

Not applicable.

## 10 Abbreviations

2FA	Two-factor authentication
BBk	Deutsche Bundesbank
BBk-PKI	Deutsche Bundesbank PKI
BSI	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnologie)
C	Country (part of the Distinguished Name)
CA	Certification Authority
CN	Common name (part of the Distinguished Name)
CP	Certificate Policy of a PKI
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRLDP	CRL distribution point
DC	Data center
DN	Distinguished name
DName	Distinguished name
ECC	Elliptic Curve Cryptography
EMAIL	E-mail address (part of the Distinguished Name)
ESCB	European System of Central Banks
HSM	Hardware Security Module
LDAP	Light Directory Access Protocol, repository service
O	Organization (part of the Distinguished Name)
OCSP	Online Certificate Status Protocol
OID	Object identifier
OU	Organizational unit (part of the Distinguished Name)
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comment, documents for global standardization
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
CRL	Signed list belonging to a CA that contains revoked certificates.
SSL	Secure Socket Layer, protocol to ensure secure communication between a client and a server.
x.500	Protocols and services for ISO compliant repositories
x.509v3	Certification standard