DEUTSCHE BUNDESBANK
EUROSYSTEM

Certification Practice Statement

Bundesbank Issuing CA for Email-Security

Version 2.0

1 Introduction

1.1 Overview

This document provides the Certification Practice Statement for the “Bundesbank Issuing CA for Email-Security”

It stands for a binding guideline for the issuance, use and management of certificates in their life cycle and is aimed at security management, operators and subscribers.

This CPS complies with the requirements and regulations set of the document "Bundesbank CP for PKI certificate class -standard-" with the policy identifier 1.3.6.1.4.1.2025.590.20.1.

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

1.1.1 Certificate Acceptance Framework of the ESCB

The BBk-Email-Security CA issues certificates for the following CAF defined certificate classes:

- standard encryption

1.2 Document name and identification

Name:	Certification Practice Statement for Email-Security CA (CPS)
Version:	2.0
Date:	2026-08-20
OID:	1.3.6.1.4.1.2025.590.20.1.4

1.3 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.

1.4 PKI participants

1.4.1 Certification authorities

The Deutsche Bundesbank PKI Standard (BBk-PKI-Standard) uses a two-tier certification structure with a self-signed root certificate.

The Root CA certifies only (business area) SubCAs. SubCAs are used to create certificates for the subscribers named in point 1.4.3.

The Bundesbank Issuing CA for Email-Security is signed by the Bundesbank Root CA -Standard-.

1.4.2 Registration authorities

The registration authorities are responsible for checking the identity and authenticity of subscribers. The registration procedure is described in point 3.2.3.

1.4.3 Subscribers

Subscribers are

- Bundesbank employees and
- external employees of Bundesbank.

Subscribers can be persons with a personal email address, persons responsible for (postmasters) or other users of (subscribers) a functional email address (non-personal email address).

1.4.4 Relying parties

Relying parties are communication partners (persons, organizations 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 certificates issued may only be used for the encryption and signing of emails in connection with the Bundesbank's business activities.].

1.5.2 Prohibited certificate uses

See [CP-BBk-PKI-Standard].

1.6 Policy administration

1.6.1 Organization administering the document

This CPS is maintained by the operator of the BBk-PKI.

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
Email: pki@bundesbank.de

1.6.3 Person determining CPS suitability for the policy

See [CP-BBk-PKI-Standard].

1.6.4 CPS approval procedures

See [CP-BBk-PKI-Standard].

1.7 Definitions and acronyms

See abbreviations in chapter 10.

2 Publication and repository responsibilities

2.1 Repositories

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

- https://www.bundesbank.de under Service ► Services for banks and companies ► PKI
- or at this direct link https://www.bundesbank.de/en/service/banks-and-companies/pki/cp-cps

It is also available on the intranet (access restricted to Bundesbank employees as well as their external employees).

2.2 Publication of certification information

The Bundesbank publishes the following information.

- CA certificates with fingerprints
- Root CA certificates with fingerprints
- CRLs
- CPs and CPSs

2.3 Time or frequency of publication

Publication dates for CA/root CA certificates, CRLs and CPs and CPSs are as follows.

– CA/root CA certificates with fingerprints	as soon as they are generated
– CRLs	after revocation, otherwise according to standard frequency (see point 4.9.7)
– CPs and CPSs	after generation/update

2.4 Access controls on repositories

See [CP-BBk-PKI-Standard].

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The names of the certificates issued (distinguished name = DN) are based on the x.509 standard.

The DN generally follows the structure below.

EMAIL	<E-mail address>
CN	<First name Surname>
OU	<Organizational unit>
O	<Organization>
C	DE

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 organization/function or for an organization's email address have to be clearly distinguishable from certificates for natural persons.

3.1.3 Anonymity or pseudonymity of subscribers

See [CP-BBk-PKI-Standard].

3.1.4 Rules for interpreting various name forms

The DN is based on the x.509 standard. Furthermore, the Bundesbank's Lotus Notes/Domino naming conventions apply.

3.1.5 Uniqueness of names

The uniqueness of names is tecnicaly enforced through the configuration of policies in the CA Solution.

3.1.6 Recognition, authentication and role of trademarks

See [CP-BBk-PKI-Standard].

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

See [CP-BBk-PKI-Standard].

3.2.2 Authentication of organization identity

Applications for a certificate for an organization's email addresses or for people grouped according to organization/function are always submitted by a natural person who is authenticated using a multi-stage registration process pursuant to point 3.2.3.

3.2.3 Authentication of individual identity

As a rule, all Bundesbank employees as well as their external employees are registered personally (face-to-face) by the respective HR departments.

See also [CP-BBk-PKI-Standard].

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of authority

The application process for certificates entails a number of stages and is conducted by means of an electronic application workflow, which is approved by the relevant business unit.

3.2.6 Criteria for interoperation

See [CP-BBk-PKI-Standard].

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Before the validity of a certificate expires, the subscriber receives several requests for a certificate renewal that involves a re-keying process.

The identification and authentication process entails a number of stages and is conducted by means of an electronic application workflow that is largely identical to the initial application process.

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

A revocation request can be made by the subscriber, someone appointed by the subscriber as well as his/her superior using the electronic application workflow.

The applicant's identity is documented. The subscriber is informed that the certificate has been revoked.

4 Certificate life cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application?

Those subscribers listed in point 1.4.3 can submit a certificate application.

4.1.2 Enrolment process and responsibilities

The certificate application process entails a number of stages and is conducted by means of an electronic application workflow, which is approved by the relevant department and sent to the BBk-PKI.

When applying for a certificate, the applicant explicitly recognises the validity of the CPS of the issuing CA.

See also [CP-BBk-PKI-Standard].

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Subscribers are identified and authenticated as described in chapter 3.2.

4.2.2 Approval or rejection of certificate applications

See [CP-BBk-PKI-Standard].

4.2.3 Time to process certificate applications

Certificate applications are proceeded in the PKI-Services department during their opening hours. 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

Once the certificate application has been processed, the key pair is created in the BBk-PKI's secure area in line with the dual control principle and the certificate is generated.

The subscription of a certificate is arranged by an electronic workflow. This information will be manually transferred via secure token into the PKI. The following generation of the certificates is realized automaticly, manually started.

The delivery occurs as a software certificate only. The certificate is thereby protected by a transport PIN and is filed by the BBk-PKI in line with the dual control principle directly on secure way to the Email-Security-Gateway.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The subscribers are notified by the workflow system. This notification is made via email.

4.4 Certificate acceptance

See [CP-BBk-PKI-Standard].

4.5 Key pair and certificate usage

See [CP-BBk-PKI-Standard].

4.6 Certificate renewal

A certificate may not be renewed on the basis of the existing key pair. When a certificate is renewed, a new key pair is always generated.

4.7 Certificate re-key

When a certificate is renewed, a new key pair is always generated. The certificate is always modified (see chapter 4.8).

4.8 Certificate modification

A certificate modification always requires re-keying and the revocation of the old certificate.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

See [CP-BBk-PKI-Standard].

4.9.2 Who can request revocation?

See [CP-BBk-PKI-Standard].

4.9.3 Procedure for revocation request

A certificate can be revoked using the electronic application workflow.

The BBk-PKI revokes the certificate at the CA in question and publishes the corresponding CRL. The subject and the subscriber are informed that the certificate has been revoked.

The published CRLs contain all the certificates that were revoked up until the validation end date of the respective CA.

4.9.4 Revocation request grace period

See [CP-BBk-PKI-Standard].

4.9.5 Time within which CA must process the revocation request

The BBk-PKI revokes the certificate as soon as it has received the revocation request. After the revocation request is started, the revocation itself is done in 24 hours. On business days (Monday to Friday) the PKI Services division is responsible for the requests. During weekend the manager on duty is able to request the revocation during the same time (24 hours).

4.9.6 Revocation checking requirement for relying parties

See [CP-BBk-PKI-Standard].

4.9.7 CRL issuance frequency

A CRL is generated every day with a validity period of 6 days.

4.9.8 Maximum latency for CRLs

See [CP-BBk-PKI-Standard].

4.9.9 On-line revocation/status checking availability

Not applicable. On-line revocation and status checking is currently not available.

4.9.10 On-line revocation checking requirements

Not applicable

4.9.11 Other forms of revocation advertisements available

Not applicable. Other forms of revocation advertisements are not available.

4.9.12 Special requirements re-key compromise

If a subscriber's private key is compromised, the corresponding certificate has to be revoked immediately. If a CA's private key is compromised, the CA certificate and all certificates that it has issued have to be revoked.

4.9.13 Circumstances for suspension

Not applicable.

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 services

The BBk-PKI currently does not provide any services to check the status of certificates. See chapter 2 for information about the publication of CRLs.

4.11 End of subscription

See [CP-BBk-PKI-Standard].

4.12 Key escrow and recovery

Key escrow and recovery services are not provided.

5 Facility, management and operational controls

5.1 Physical controls

The CA is operated on a hardware PKI cluster of three separate instances. They 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.
The components of the RA are operated by the Deutsche Bundesbank IT department under the terms of its general regulations and policies.

DC Certifications

One DC is certified to TÜV IT Level 4 and EN 50600 Level 4, the second DC site is certified to DIN EN ISO 9001 as well as DIN ISO EC 27001. Both certificates confirm in areas with high protection and maximum availability requirements the following security mechanisms:

- Availability,
- Access Security,
- minimizing risks and downtime,
- protection against financial and reputational losses.

The TSI.STANDARD criteria catalog certifies and tests

- Environment, Construction,
- Fire Protection,
- Extinguishing Systems,
- Security Systems,
- Cabling,
- Power Supply,
- Air Conditioning,
- Organization
- and Documentation.

5.1.1 Site location and construction

The hosting locations are in secure DC conforming to the general Deutsche Bundesbank standards for physical and environmental security. Further details may be available on request. The facilities meet the following physical requirements:

- They are distant from smoke ventilation points to avoid possible damage from fires on other floors.
- Absence of windows to the outside of the building.
- Surveillance cameras in restricted access areas.
- Access control based on card and PIN code.
- Fire protection and prevention systems: detectors, extinguishers, personnel training on what steps to take in the event of fire, etc.

- Transparent partitions that delimit the different zones and enable observation of the rooms from the access passageways, in order to detect intrusions or illicit activity inside.
- Cabling, both for data transmission and telephony, protected against damage and interception.

5.1.2 Physical access

The operational activities related to the lifecycle of the certification process occur within the premises, with physical protection against intrusion through alarms, controls on access through the security perimeter. It can only be accessed by authorized personnel, with restrictive physical tiers. The access is regulated by a control system for premises logs accesses. Employee smartcards are used as proximity readers to grant access.

5.1.3 Power and air conditioning

Systems have permanent power supply units as well as a generator. The DC has redundant systems. The air-conditioning regulate/controls 24/7 temperature and humidity, by a supervision system.

5.1.4 Water exposures

Appropriate measures have been taken to prevent exposure of the equipment and cables to water.

5.1.5 Fire prevention and protection

The fire prevention and protection system is composed by a smoke detection system and a fire suppression system.

5.1.6 Media storage

All media storage containing software and data, audit logs, archives, or backup information are stored within the DC with adequate physical and logical access controls designed to limit access only to authorized personnel and protect such media from accidental damage.

5.1.7 Waste disposal

Waste management measures has been adopted that guarantee destruction of any material that could contain information, as well as management measures for removable media.

5.1.8 Off-site backup

Backups of critical system data, audit logs and other information necessary to recovery data correctly are implemented in two of its own premises, which have the necessary security measures in place and are suitably physically separated.

5.2 Procedural controls

5.2.1 Trusted roles

Generally, the CA and card issuing authority system supports eight trusted roles:

a) Head of CA Operations
a role of responsibility, supervision and controlling which is accompanied by the IT security management

b) IT Security Officer
planning and monitoring the implementation of security measures concerning the whole CA operations, including technical, organizational and physical measures.

c) System Administrator
Responsible for the configuration of system properties like networking, backup, cluster, database and system certificates.

d) Access Manager
Responsible for the CAs role- and access management

e) CA Operator
Authorized to install, configure and maintain the CA trustworthy systems for registration, certificate generation and revocation management.
Configuration of templates
Configuration of policies
Generation of CA requests

f) RA Operator
Operation of certificate revocation and certificate request approval

g) Revisor
Audit of all PKI Components

h) Agent for Registration
Registration of certificates and revocation requests.

5.2.2 Number of persons required per task

All cryptographic operations of the CA are protected by the HSM. In live operations, the BBk-PKI applies a dual control principle as standard for the use of highly security-critical access media, cryptographic key materials and certificates.

This ensures that the storage, access to and use of highly secure access media by PKI operating staff is always subject to the dual control principle. In addition, the entire process of generating cryptographic key material and certificates up to the stage where they are passed on is also subject to the dual control principle. Using the dual control principle as standard requires the roles

of those people involved in the generation process to be documented in various logs that are to be created or generated by the system (see point 5.2.1).

5.2.3 Identification and authentication for each role

Without exception, smart cards are used for the authentication process of natural persons. Connected services store their keys on HSMs.

5.2.4 Roles requiring separation of duties

The CA cryptographic operations are protected by HSMs. As written in 5.2.1, there is always just one trusted role to be used by a dedicated operator at a time or must be accompanied by a four-eye principle.
An RA operator cannot approve his/her own request.

5.3 Personnel controls

See [CP-BBk-PKI-Standard].

5.4 Audit logging procedures

The PKI system uses a chain-signed audit database. Access to the database is restricted to the assigned roles. System logging is constituted as a separate service to the syslog daemon.

5.4.1 Types of events recorded

The audit database covers at least the following types of entries:

- System initialization
- System Login / Logoff
- CA activation
- Operator processes
- Certification applications
- User registration
- 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.

5.4.2 Frequency of processing log

The frequency of processing log data is implemented as described in the document [CP-BBk-PKI-Standard].

5.4.3 Retention period for audit log

The retention period for audit log data is implemented as described in the document [CP-BBk-PKI-Standard]. Due to the size of the data volume a rollover of audit data will happen every two years.

5.4.4 Protection of audit log

Audit logs can be evaluated by authorized persons only.
Audit logs are protected for integrity by a chained signature and stored in the PKIs system database.

5.4.5 Audit log backup procedures

Audit Log data is backed up regularly along with PKI system database.
The database backups are encrypted.

5.4.6 Audit collection system (internal vs external)

Audit Logs are not stored in a central audit log collection system.

5.4.7 Notification to event-causing subject

Some events of the operator workflow are sent out to the persons involved by email. Other notifications are implemented as described in the document [CP-BBk-PKI-Standard].

5.4.8 Vulnerability assessments

The vendor of the PKI system informs customers about vulnerabilities of the system in the internet and for subscribed customers by e-mail. Vulnerabilities are documented in CVEs together with the information in which version the vulnerability is fixed.
Regular system updates are proceeded immediately in case a relevant vulnerability is fixed in a subsequent version, other updates are installed within the vendors regular update sequence, but at least once a year.

5.5 Records archival

Backups are stored in encrypted form on an NFS drive on a daily basis to guarantee the recoverability of the system.
In case data is deleted from the PKI database the file of the regular backup is archived and stored for at least one year.

5.5.1 Types of records archived

Archiving takes place in the form of a system backup. The system backup contains all data records and is the only form for archiving them.

5.5.2 Retention period for archive

The retention periods is at least one year.

5.5.3 Protection of archive

The archives are protected by encryption using an AES 265 key.

5.5.4 Archive backup procedures

Backups are stored automatically in encrypted form on an NFS drive on a daily basis to guarantee the recoverability of the system. Archives are copies of backups to be generated in the rare event that data is deleted in the PKI database.
Cases for archival are:

- Deletion of CA properties.
- Deletion of expired end entity properties or certificates.

The deletion of audit data is not possible and therefore not needed to be archived in an external process.

5.5.5 Requirements for time-stamping of records

The system is using a trusted NTP time source.

5.5.6 Archive collection system (internal or external)

Archiving takes place on internal NFS file systems.

5.5.7 Procedures to obtain and verify archive information

Archived backup files are encrypted. The name of the file contains the date of storage.

5.6 Key changeover

The Key changeover for the CA key pairs is timed according to the maximum key lifetimes and renewal periods set out in the [CP-BBk-PKI-Standard].
The CA key changeover process is designed that:

- It is guaranteed at all times that the CA’s certificate lifetime encompasses all lifetimes of certificates, which issued by it.
- A new key pair of the CA is generated before the point in time where its remaining lifetime equals the subordinate certificate’s validity period to avoid lifetime cuts in the respective certificate chain.

- All certificates are issued by the next generation CA at the latest from the moment at which the certificate expiration date of an issued certificate exceeds the expiration date of the issuing CA certificate
- However, a CA continues to issue CRLs signed with the original CA private key until the expiration date of the last issued certificate using the original key pair has been reached

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

See [CP-BBk-PKI-Standard].

5.7.2 Computing resources, software and/or data are corrupted

In case of corruption of system resources software or data the PKI system can be recovered by the import of the latest backup.
Backup and recovery procedures are defined in the operating manual for the PKI system.

5.7.3 Entity private key compromise procedures

In case a key compromise is detected the certificate is revoked by the issuing CA.
The assessment of whether keys are insufficient for the corresponding application is based on BSI-TR-02102-1.
For **end entity** certificates the revocation is carried out by the issuing departments following the revocation procedures handled in the relevant RA management system by the processing department or business unit e.g. smartcard management system. The subscriber is informed about the revocation of the certificate.
Key compromise of an **issuing CA** private key operating under this CPS must be reported to the Bundesbank security management. The security management body of the Deutsche Bundesbank triggers the procedure for revocation of a CA certificate described in the CA management handbook.

- Revocation of the CA certificate by CA the certificate is issued from.
- Information for all subscribers holding active certificates.
- Information for all relying parities.
- Deletion of the affected key.

5.7.4 Business continuity capabilities after a disaster

The general disaster recovers procedures are defined as part of the general Deutsche Bundesbank Business Continuity Plans.

5.8 CA or RA termination

See [CP-BBk-PKI-Standard].

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key material is generated on a HSM in a four-eye principle. The generation of the key pair is recorded in the audit database.

6.1.2 Private key delivery to subscriber

The private key of the subscriber is imported in the BBk-PKI's secure area in line with the dual control principle to the Email-Security-Gateway. A later export of the private keys is not possible from there.

6.1.3 Public key delivery to certificate issuer

Not applicable. There are no provisions for a subscriber to generate his/her own key.

6.1.4 CA public key delivery to relying parties

CA certificates containing correspondent public keys are stored in the AIA URLs defined in the issued certificates.
http://pki.bundesbank.de/<IssuingCA>.crt
Relying parties have to check the CA certificates fingerprint using a second communication channel.
The CA's public keys can also be called up via the certificate service outlined in chapter 2.

6.1.5 Key sizes

The key size for end entity certificates is at least 4096 bit RSA .

6.1.6 Public key parameters generation and quality checking

Quality checking is part of the certificate policy validation in the issuing process.
Allowed key parameters are:

- 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

6.1.7 Key usage purposes

The CA's private key is used only to sign certificates and CRLs.

For end entities, the key usage purposes are:

- digital signature 2.5.29.15.0
- key encipherment 2.5.29.15.2

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

The CAs private keys are generated in the HSM. The access is protected by a random generated PIN code. For automatic activation reasons of the online CAs the PIN code is stored encrypted in the database.
The HSMs are certified to FIPS 140-2 Level 3.

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

In the CA environment only in the case of restoring a HSM a workflow enabling a four-eye principle using cards is realized.

6.2.3 Private key escrow

The CA's private key is not stored with third parties.

6.2.4 Private key backup

A private key backup is realized by a synchronization between the PKI clusters members.
To back up a key from an HSM outside the HSM environment a number of backup smart cards have to be used. The key is encrypted with a Master Backup Key (MBK) that only exists in the HSM environment. (on the HSMs of the cluster).

Backups of private keys for end entities are stored encrypted in the CA database.

6.2.5 Private key archival

No archival of private keys is implemented.

6.2.6 Private key transfer into or from a cryptographic module

See 6.2.4.

6.2.7 Private key storage on cryptographic module

See 6.2.1.

6.2.8 Method of activating private key

See 6.2.1.

6.2.9 Method of deactivating private key

If private keys of a certification authority are compromised, they must be deactivated. Along with the fact that Issuing CAs are autoactivated, the autoactivation is cleared from the CA and a new PIN code for the key is set.

6.2.10 Method of destroying private key

For CA keys a key can be destroyed using the CAs interface. The process is regulated by a role-based control and framed by a four-eye principle.

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 BBk-PKI are archived in the CA's database.

6.3.2 Certificate operational periods and key pair usage periods

The certificates issued under this CPS have the following validity periods:

- Root CA certificates maximum of 12 years
- CA certificates maximum of 6 years
- User certificates maximum of 2 years

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data for CAs private keys is generated using HSM devices. The activation smart cards for multi-person control are PIN protected.

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

Activation data is generated at the same time as the certificates. Non-trivial combinations of upper case, lower case, numbers and special characters are used for passwords and PINs. These must be at least ten characters long.

6.4.2 Activation data protection

Activation data are suitably protected from loss, theft, modification, unauthorised publication and unauthorised use.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Certification Authorities and HSM are operated in the data center.

Physically access to the data center is limited to trusted roles and persons only. In order to enter the date center, biometric features must be presented. Every access is documented. The DC is video monitored. Only persons with a dedicated security clearance are allowed to enter.

Within the Datacenter network the Area concept for network segregation ensures only valid and secure commination.

Within Bundesbank’s network the SubCA is placed inside a dedicated DMZ. The RA and VA systems residing in lower secure network areas are connected by the CA system.

An authorization concept ensures the need-to-know principle, which means that every role is only allowed to access information, which is necessary (e.g., the card issuer is allowed to undertake request, but nobody else).

6.5.2 Computer security rating

The CA cluster contains a hardened Linux system with limited access.

A threat analysis is conducted every two years.

6.6 Life cycle technical controls

6.6.1 System development controls

The Deutsche Bundesbank’s IT risk management process is involved in planning and 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 security concerning changes to the PKI system or components are going through the Deutsche Bundesbank's IT risk management process.

6.7 Network security controls

See point 6.5.1.

6.8 Time-stamping

See point 5.5.5.

7 Certificate, CRL and OCSP profiles

7.1 Certificate profile

7.1.1 Version number(s)

Certificates issued by CAs operating under this CPS are using X.509v3 extensions.
Version: 3 (0x02)
CRLs signed by CAs operating under this CPS are using version 2 extensions.
Version: 2 (0x01)**.**

7.1.2 Certificate extensions

Issuing CA certificates have the following extensions.

Extension	Possible Values	Critical Flag
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing	yes
Basic Constraints	Subject Type=CA Path Length Constraint=0	yes
Subject Key Identifies	160-bit SHA-1 hash of subject's public key	no
Authority Key Identifier	160-bit SHA-1 hash of issuer's public key	no
CRL Distribution Point	Contains HTTP URLs to obtain the current CRL	no
Certificate Issuance Policies	CP OID CPS OID of the issuing CA CPS OID of this CA An external URL Description	no
Authority Information Access	Contains HTTP URL to obtain the Root CA certificate	no

The CA-certificates are provided on the website referred to in Chapter 2.1 of related CP. The selected values can be found here.

User certificates can have the following extensions. (marked are required)

Extension	Possible Values	Critical Flag
Key Usage	Key Encipherment Digital Signature,	yes
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	yes
Extended Key Usage	Email protection (1.3.6.1.5.5.7.3.4)	no
Subject Key Identifier	160-bit SHA-1 hash of subject's public key	no
Authority Key Identifier	160-bit SHA-1 hash of issuer's public key	no
CRL Distribution Point	Contains a HTTP URL to obtain the current CRL	no
AIA Distribution Point	Contains a HTTP URL to obtain the issuer certificate	no
Certificate Issuance Policies	CP OID CPS OID of the issuing CA An internal and external URL Description	no
Subject Alternative Name	E-mail address	no

7.1.3 Algorithm object identifiers

The RSA (OID 1.2.840.113549.1.1.1) algorithm is used in the certificates issued by the BBk-PKI.

7.1.4 Name forms

The CA certificates issued by the Root CA contain the entire distinguished name (DN) in the subject name and issuer name fields.

The names of the CA certificates issued are based on the x.509 standard and are in line with the following structure.

EMAIL	pki@bundesbank.de
CN	Bundesbank Issuing CA for Email-Security <year of issue>
OU	Bundesbank PKI
O	Bundesbank
C	DE

The names of the user certificates issued are based on the x.509 standard and are in line with the following structure.

	Employee	External employee
EMAIL	<Firstname.Surname> or <Email address>	
	@bundesbank.de	@externe-mitarbeiter.bundesbank.de @bundespolizei.bundesbank.de
CN	<Firstname Surname> or <local part of Email address>	
OU	SMIME-Certificates	
O	Bundesbank	
C	DE	

7.1.5 Name constraints

See chapter 3.1.

7.1.6 Certificate policy object identifier

The certificate policy OID of the [CP-BBk-PKI-Standard] is: 1.3.6.1.4.1.2025.590.20.1

7.1.7 Usage of policy constraints extension

Not applicable

7.1.8 Policy qualifiers syntax and semantics

Not applicable

7.1.9 Processing semantics for the critical certificate policies extension

Not applicable

7.2 CRL profile

7.2.1 Version number(s)

The BBk-PKI issues CRLs in line with the x.509 norm, version 2.

7.2.2 CRL and CRL entry extensions

A CRL distribution point (CRLDP) is contained in the user certificates.

7.3 OCSP profile

Not applicable. The certificates currently do not support OSCP.

8 Compliance audit and other assessments

An audit and compliance check is scheduled on a regular frequently basis every **3 years**.
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 is carried out every 3 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 are not be involved in the responsible unit's production process. Self-assessment is prohibited.

8.4 Topics Covered by Assessment

All topics relevant to the PKI are 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 are be rectified as quickly as possible by the CA in consultation with the inspector. The inspector is 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

See [CP-BBk-PKI-Standard].

10 Abbreviations

BBk	Deutsche Bundesbank
BBk-PKI	Deutsche Bundesbank's PKI
BSI	Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnologie*)
C	Country (part of the distinguished name)
CA	Certification Authority
Certificate	Secure assignment of public keys to a subscriber
CN	Common name (part of the distinguished name)
CP	Certificate Policy of a PKI
CPS	Certification Practice Statement
CRL	Certificate Revocation List; signed list belonging to a CA that contains revoked certificates
CRLDP	CRL distribution point
DN	Distinguished name
EMAIL	E-mail address (part of the distinguished name)
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 standardisation
RFC3647	This RFC describes documents that outline PKI operations
Root CA	Highest CA of a PKI
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions, standard for secure e-mail
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.509v1	Certification standard

11 Information regarding the document

See point 1.2.