DEUTSCHE BUNDESBANK
EUROSYSTEM

Bundesbank CPS Issuing CA for Users -Advanced- 2024

Version 1.1

Stand: 11. September 2024

Changehistory

Version	Kapitel	Änderungshinweis	Datum	Name und Ordnungsmerkmal
0.1	alle	Erstellung	01.01.2023	Benedict Stopfkuchen
1.1	Alle	Reformat of all chapters	14.08.2024	Clemens Härtling
1.1	Alle	Reformat and Rephrasing	10.09.2024	Benedict Stopfkuchen

Table of Contents

1 Introduction

1.1 Overview

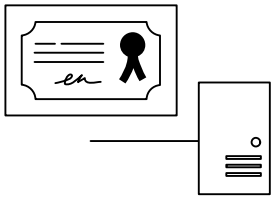
This document provides the Certification Practice Statement for the “Bundesbank Issuing CA for Users -Advanced- 2024”

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 -advanced" with the policy identifier 1.3.6.1.4.1.2025.590.21.1.

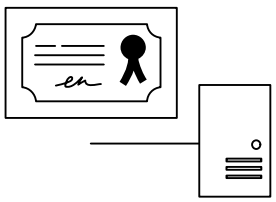
The structure of this document follows the template specified in the RFC 3647 standard.

Root CAs



CA Role	Root CA certificate class -advanced-
CA Name	Bundesbank Root CA -Advanced- 2023
CPS Identifier	1.3.6.1.4.1.2025.590.21.1.1
Lifetime	12 years
CRL-Lifetime	8 mounth
CRL-Publishing	offline / manual
OCSP	none
Key Security	HSM
Location	Root CA appliance
Status	offline
Availability	PKI appliance

Subordinate CAs



CA Role	Issuing CA certificate class -advanced-
CA Name	Bundesbank Issuing CA for Users -Advanced- 2024
CPS Identifier	1.3.6.1.4.1.2025.590.21.1.2
Lifetime	6 years
CRL-Lifetime	6 days
CRL-Publishing	online / automatic
OCSP	yes / private
Key Security	HSM
Location	Sub CA appliance
Status	online
Availability	PKI appliance cluster

Figure 1: Overview of Deutsche Bundesbank certificate class -advanced-

1.1.1 Certificate Accptance Framework of the ESCB

The BBk-UserCA-Advanced issues certificates for the following CAF defined certificate classes:

- advanced authentication

1.2 Document Name and Identification

Name:	Bundesbank CPS Issuing CA for Users -Advanced- 2024
Version:	1.1
Date:	11.09.2024
OID:	1.3.6.1.4.1.2025.590.21.1.2

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

All components of the PKI System are operated in accordance to the “Certificate Policy PKI for certificate class -advanced-“ (CP- BBk-PKI-Advanced)

1.4.1 Certification Authorities

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

The two tier certification structure exists independently to any other certification structure operated by Deutsche Bundesbank. The Root CA is not cross-signed.

The Root CA certifies only (business area) SubCAs. SubCAs are used to create certificates for the subscribers named in point 1.3.3.

The Bundesbank Issuing CA for Users -Advanced- 2024 (BBk-UserCA-Advanced) is signed by the “Bundesbank Root CA -Advanced- 2023” (BBk-RootCA-Advanced).

At the time of publication of this version of this document, no further CAs have been issued by the BBk-PKI-Advanced (see figure 1)

1.4.2 Registration Authorities

The registration authorities (RA) are responsible for:

- verifying the identity and authenticity of subscribers,
- adherence to the registration process,
- documentation of registration process and
- suspension and revocation of certificates

Registration authorities are operated in Bundesbank networks and locations only.

There are smart card issuing authority systems in all Bundesbank locations. These are responsible for the employees who work within their scope.

The Bundesbank operates a high availability cluster of two RAs that are served by a transparent load balancer system.

The registration of subscribers and the issuance of smart cards is upstream of the registration authorities through a smart card issuing authority system.

The BBk-UserCA-Advanced accepts requests from this system only. There are no other sources allowed.

The registration procedure and processes are described in point 3.2.3.

1.4.3 Subscribers

Subscribers are

- Employees of the Deutsche Bundesbank,
- Persons with a contractual relationship with the Deutsche Bundesbank

The application process is identical for the employees listed above. Both types of subscribers use the same Deutsche Bundesbank IT equipment (no difference in technical environment).

1.4.4 Relying Parties

Relying parties are IT systems and/or IT processes that use a certificate issued by the BBK-PKI- Advanced to verify authorization or authenticity of subscribers named in point 1.3.3. The systems to be authenticated to are both internal IT-systems or IT-processes of Deutsche Bundesbank and IT-systems or IT-processes of ESCB.

1.4.5 Other Participants

Not applicable.

1.5 Certificate Usage

1.5.1 Appropriate Certificate Uses

The certificates are issued to natural persons as listed in 1.3.3 only.

Certificates issued by this CA must only be used for the following uses.

- Authentication

Other applications that may arise from future use cases must be included in this document in a later version, communicated to the relying parties and, in particular, verified by the CAF Approval Board.

1.5.2 Prohibited Certificate Uses

All certificate uses, not listed in 1.4.1, are prohibited.

1.6 Policy Administration

1.6.1 Organization Administering the Document

See [CP-BBk-PKI-Advanced]

1.6.2 Contact Person

Deutsche Bundesbank PKI Services

Berliner Allee 14 Postfach 10 11 48

40212 Düsseldorf 40002 Düsseldorf Germany

Tel: +49 211 874 3257/2351

E-mail: pki@bundesbank.de

1.6.3 Person Determining CPS Suitability for the Policy

See [CP-BBk-PKI-Advanced]

1.6.4 CPS Approval Procedures

See [CP-BBk-PKI-Advanced].

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-Advanced on its website

- http://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 limited to Bundesbank employees as well as external employees of this institution).

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 as soon as they are generated with fingerprints
- 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-Advanced].

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:

3.1.2 Certificate of the CA

CN	**Bundesbank Issuing CA for Users -Advanced- 2024**
OU	Bundesbank PKI
O	Bundesbank
C	DE

3.1.3 Certificates for subscribers

Subject attributes	
CN	<mandatory>
O	Bundesbank
OU	<optional>
C	DE
Email	<optional>
Serial	<optional>
DC	<optional>

Subject alternative name attributes	
UPN	<optional>
RFC822 name	<optional>

3.1.4 Need for Names to be Meaningful

- Certificates for end entities are issued in the subscriber's name.

3.1.5 Anonymity or Pseudonymity of Subscribers

- Anonymity or pseudonymity in certificate names are not used in certificates issued by this CA

3.1.6 Rules for Interpreting Various Name Forms

Distinguished Names represent the LDAP naming context referring to RFC 2247.

Certificates **may** contain the User Principal Name or E-Mail address of the subscriber in subject alternative name field.

3.1.7 Uniqueness of Names

The subject (DN) in the certificate request is unique for an end entity subscribing to the CA and is enforced by technical policy settings of the CA.

3.1.8 Recognition, Authentication, and Role of Trademarks

See [CP-BBk-PKI-Advanced].

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Private keys are generated on hardware cryptographical devices with a proven key generation mechanism and a sufficient entropy. Private keys never leave the hardware crypto system.

The Deutsche Bundesbank issues smart cards for this purpose (Dienstausweis).

Within the issuance process an asymmetric keypair is generated. The certificate request is composed of subscriber information and the public key and is signed by the private key in a predetermined format like PKCS#10 to be send to the registration authority.

The individual smart card PIN must be known in order to generate a signature.

The CAs technical policy settings are set to verify the signature of every request.

3.2.2 Authentication of Organization Identity

See [CP-BBk-PKI-Advanced].

3.2.3 Authentication of Individual Identity

Authentication of identity of subscribers (listed in point 1.3.3) is always a face-to-face process to get a Deutsche Bundesbank smart card (Dienstausweis):

- Any (new) employee has to identify himself at the HR department by ID card (passport) to get a new Deutsche Bundesbank smart card. The process is always carried out by natural persons:
    - Photos are taken.
    - The Bundesbank smart card is printed, including the photo, using an internal IT-System, handled by natural persons.
    - The new employee (see point 1.3.3) has to sign an acknowledgement for receiving his smart card.
- Responsible persons processing requests of new employees at a dedicated business area are using a personalized workflow, involving natural persons only.
- The IT department creates a unique user object (DN and UPN) in the central Active Directory (User Provisioning Group). Without an user object in the Active Directory it is not possible to request for a certificate. The user creation process is not automated and is processed by natural persons only.
- The card issuing authority, represented by natural persons, cross checks the identity of the employee using the smart cards visual features (face-to-face).
- Officers of the card issuing authority can access the system in their assigned roles using their own personalized smart card only.
- The card issuing authority requests the certificate in presence of the employee.
- The employee must assign his/her PIN personally.
- The employee receives an internal E-Mail to be informed about the process.
- When activating the smart card, it is ensured that only one smart card is assigned to the Bundesbank account.
- The issuance of the Bundesbank smart card is documented in an acknowledgement-paper, which finalizes the whole workflow and guarantees the activation of smart card and certificate. The handling of the Bundesbank smart card (usage,

how to handle with lost or stolen cards, etc.) is regulated in internal terms and conditions. This ruleset has the nature of a policy and, therefore is mandatory for all subscriber and is acknowledged in this rollout process (see point 1.3.3).

- Employees address data is stored as private data in the HR application only.
- Employees department and work phone numbers are stored in the active directory and collaboration services and can be accessed by every operator.

3.2.4 Non-verified Subscriber Information

See [CP-BBk-PKI-Advanced].

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.

For a natural person it is possible to request a certificate only if

a) The person is determined by the HR system

and

b) The person possesses an AD-account.

3.2.6 Criteria for Interoperation

See [CP-BBk-PKI-Advanced].

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

The identification and authentication process for natural persons is identical to the initial application process, or processed in case of self-service renewal Workflow.

The self-service renewal and rekeying have always to be based on a two-factor authentication using cryptographical processor devices. The Bundesbank smart card can be used for the identification and authentication to the self-service registration authority workflow. Other two factor authenticators are not permitted until stated differently in this document.

The workflow ensures the identity and the validity of authentication of the subscriber within the process. The renewal request is automatically approved based on the authentication and authorization given in the self-service workflow.

The self-service renewal workflow is only be reachable in the Bundesbank trusted internal network.

A subscriber who cannot present valid information to the process has to use the initial application process for renewal.

Re-Key Requests for the same subject (DN) for the CAs certificate will not be approved by the Root CA and therefore will generate a new CA.

3.3.2 Identification and Authentication for Re-key after Revocation

See [CP-BBk-PKI-Advanced].

CA Certificates are always processed as a new application.

3.4 Identification and Authentication for Revocation Request

In order to avoid delay in disabling compromised credentials a suspension request can be made by the subscriber, someone appointed by the subscriber as well as his/her superior either using the electronic application workflow, by telephone as well as by fax or in writing. If an employee is no longer working for Deutsche Bundesbank, the revocation is mandated by HR.

The superior or HR requests revocation by an electronic workflow, which can only be used by authenticated users. Through the use of the workflow the traceability is ensured.

The issuance of a temporary Deutsche Bundesbank smart card (with temporary certificate) by a subscriber leads to a suspension of the original (standard) smart card (respectively the certificate). The subscriber has to identify himself by showing an official document containing a photo. The operator generates a temporary smart card using the card issuing authority software. The process suspends the subscriber's original card automatically. The subscriber is informed by e-mail that a temporary smart card has been issued and the standard identity card (respectively the certificate) is suspended for their person.

All necessary information of revocation and suspension requests, the time they are proceeded as well as the operators involved are (securely) logged in the database of the card issuing authority system.

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

All certificate applications are issued through registration authorities and cannot be requested directly by the subscriber.

4.1.2 Enrollment 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-Advanced.

End-user certificates will be generated on a cryptographic enabled smart card, the Deutsche Bundesbank smart card (Dienstausweis), in a four-eye principle with the presence of the subscriber. The management of the smart cards is operated by the human resources department. The name and the photo of the subscriber is printed on the card.

The initialization of the crypto chip and the generation of key material are controlled by the card issuing authority system. To perform these actions, it is necessary that the Production Officer is logged on the card issuing authority system with its own identity card.

The responsibilities of subscribers in dealing with their certificates and smart cards is part of the general instruction for safe and correct use of the Deutsche Bundesbank standard IT equipment, which are published in the intranet of the Bundesbank.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Subscribers are identified and authenticated as described in section 3.2.

4.2.2 Approval or Rejection of Certificate Applications

The formal attestations for a subscriber to get a certificate:

a) Preparation of the smart card (with photo on it)

b) Optical identification (by HR) of the subscriber, or processed in case of self-service renewal Workflow.

c) Electronic workflow in the card issuing authority system

All three processes must be completed to request for a certificate.

4.2.3 Time to Process Certificate Applications

Certificate applications are proceeded in the HR department during their opening hours.

In the self-service renewal process certificates are issued online, without a delay.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The CA validates signature of the submitted request for prove of possession of the private key (3.2.1).

Validation of the names and their uniqueness is processed. (3.1)

Validation of key sizes is processed (6.1.5)

Validation of Public Key parameters and quality checking is processed (6.1.5)

The CA verifies the certificate signing request and answers with the signed public key of the subscriber.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The subscribers are notified by the card issuing authority system. This notification is made via email.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Receiving the certificate is integrated into a workflow which:

- Generates new key pairs on the smart card
- Requests the user to set a PIN for the protection of the private key against unauthorized use
- Requests the actual issuance of the certificate
- Handover of the Bundesbank smart card is documented in an acknowledgement-paper, which finalizes the whole workflow and guarantees the activation of card and certificate. The handling of the Bundesbank smart card (usage, how to handle with lost or stolen cards, etc.) is regulated in internal terms and conditions. This ruleset has the nature of a policy and, therefore is mandatory for all subscribers (see 1.3.3). The acknowledgement-paper must be signed and archived.

The completion of this workflow by the user and the subsequent usage of the smart card constitutes acceptance of the certificate(s).

4.4.2 Publication of the Certificate by the CA

See [CP-BBk-PKI-Advanced].

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

See [CP-BBk-PKI-Advanced].

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The private key can only be used in the cryptographical environment of the smart card by presenting the PIN. The Bundesbank uses Minidriver and PKCS#11 as application interfaces to the smart card's crypto system.

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

Certificates are bound to the Bundesbank environment and are only accepted by relying parties.

A private use of Bundesbank certificates is prohibited.

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 also checks the validity period of the certificate.

Applications in which certificates are to be used must be compatible with the interfaces specified in point 4.5.1

4.6 Certificate Renewal

See [CP-BBk-PKI-Advanced].

4.7 Certificate Re-key

See [CP-BBk-PKI-Advanced].

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-Advanced].

4.9.2 Who Can Request Revocation

A revocation request can be made by the subscriber, someone appointed by the subscriber, or by his/her superior. In the event of the end of the employment relationship, the request for revocation can by initiated by HR.

4.9.3 Procedure for Revocation Request

The suspensions and revocations are realized as automatic processes in the card issuing authority system.

The suspension process can be triggered by one of the following actions:

- Loss or damage of the smart card. In this case, the certificates will be taken out of service by suspension. A final revocation of the certificates will take place during the creation of a newsmart card.
- smart card is temporarily unavailable.

In both cases the employee is provided with a time-limited smart card after authenticating against an operator of the card issuing authority.

The revocation process can be triggered by one of the following actions:

- Destruction of the Deutsche Bundesbank smart card after return to HR
- Creation of a new Deutsche Bundesbank smart card for the same employee
- Suspended certificates will be definitively revoked as part of the issuance of a new certificate and smart card.
- End of employment relationship. The supervisor or HR must inform the subscriber about the revocation of the certificate, also in the case of an extraordinary termination.

4.9.4 Revocation Request Grace Period

All revocation requests are considered effective with the request reaching the Bundesbank staff. The consequence of a revocation needs to be fulfilled completely within one hour (see 4.9.5).

4.9.5 Time within Which CA Must Process the Revocation Request

The CA must process the revocation request within one hour. In this interval a new CRL will be published. The same time frame applies to the suspension request.

4.9.6 Revocation Checking Requirement for Relying Parties

See [CP-BBk-PKI-Advanced].

4.9.7 CRL Issuance Frequency

A CRL is generated every hour with a lifetime of 6 days. No delta CRL is generated.

4.9.8 Maximum Latency for CRLs

The CRL is published automatically at time of it’s generation.

4.9.9 Online revocation/status checking availability

The BBk-PKI-Advanced does only provide OCSP Information for internal usage in the Deutsche Bundesbank network. The OCSP responder information is not reachable from other networks. The certificates do not contain a reference to the OCSP responder.

The OCSP Responder works in a real-time manner with the possibility to configure caches.

4.9.10 Online Revocation checking Requirements

The requesting applications must be able to process responses in accordance with RFC 6960

4.9.11 Other Forms of Revocation Advertisements available

See [CP-BBk-PKI-Advanced].

4.9.12 Special Requirements Re-key Compromise

See [CP-BBk-PKI-Advanced].

4.9.13 Circumstances for Suspension

See [CP-BBk-PKI-Advanced].

4.9.14 Who can Request Suspension

See [CP-BBk-PKI-Advanced].

4.9.15 Procedure for Suspension Request

The notification of a (short-term) loss of an smart card will lead to a suspension of the certificate.

The issuance of a temporary Deutsche Bundesbank smart card (including a temporary certificate) results in a (automatic) suspension of the certificate on the original smart card. The subscriber will get a notification via e-mail that a temporary smart card is issued.

4.9.16 Limits on Suspension Period

Generally, the limitation of the suspension period is restricted by the validity of a temporary identity card (max. 21 days**)** or/and the issuance of a new identity card.

4.10 Certificate Status Services

See [CP-BBk-PKI-Advanced].

4.11 End of Subscription

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

The operator is obliged to provide an equivalent substitute at the end of a service of CA or RA. Security management is always involved in the decision-making process.

4.12 Key Escrow and Recovery

See [CP-BBk-PKI-Advanced].

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

- Enviorment, 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 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.

5.1.8 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.

5.2 Procedural Controls

5.2.1 Trusted Roles

Generally, the CA and Card issuing authority system support seven trusted roles:

a) Head of CA Operations
   as 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 as a service of the card issuing authority

5.2.2 Number of Persons Required per Task

All cryptographic operations of the CA are protected by the HSM. For sensitive key operations like Root CA activation at least multi person control / multi-eye principle is performed and required on the HSM. The generation of key pairs on the smart card is realized in multi-eye principle.

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. For sensitive key operations like Root CA activation at least two operators are necessary. 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 own request.

5.3 Personnel Controls

See [CP-BBk-PKI-Advanced].

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-Advanced].

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-Advanced].[CP-BBk-PKI-Advanced]. 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-Advanced].

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 period 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-Advanced].

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-Advanced].

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-Advanced].

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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

Subscribers' private key is generated on the crypto module of the smart card (Deutsche Bundesbank Dienstausweis).

6.1.2 Private Key Delivery to Subscriber

The private key never leaves the Deutsche Bundesbank smart card. For there is no centralized key generation for subscribers a delivery to the subscriber is not necessary.

6.1.3 Public Key Delivery to Certificate Issuer

The public key (signed with the private key) of the subscriber will be transferred in a secure way to the CA as a PKCS#10 request.

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

http://cdp-pcauaa.de.escb.eu/<IssuingCA>.crt

Relying parties have to check the CA certificates fingerprint using a second communication channel.

6.1.5 Key Sizes

The key size for End Entity certificates is at least 2048 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 (as per X.509 v3 Key Usage Field)

For natural persons, the key usage purposes are.

- digital signature 2.5.29.15.0

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.

For Bundesbank smart cards keys are generated in the cryptographic controller of the device.
The access to key operations is protected by a personal PIN which is only known by the employee.

The smart cards are certified to Common Criteria EAL 4+

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

In the Sub 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

Private key escrow is not used.

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).

For smart cards a centralized backup of private keys is not permitted and is prevented by technical controls.

6.2.5 Private Key Archive

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.

No key deactivation method is defined for smart cards. The access to cryptographical operations with the key can be prevented by blocking the smart cards PIN. There is no centralized process defined to block a employees smart cards PIN.

Smart cards with key materials of natural persons are suspended after an incorrect PIN has been entered three times. The re-activation of the smart card after suspension because of wrong PIN is realized by the challenge and response technique. The process is as follows:

-
- The affected employee asks a colleague to send an order to reset his PIN to the help desk.
- A help desk employee calls the affected user under the stored telephone number
- There is a check of the reason for the support call.
- In the case of the PIN reset, a reset is carried out via the smart card management tool. The rescue operation is initiated in form of a challenge / response process between the employee and the user provisioning service
- At the end, User sets his personal PIN

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.

Smart cards are wiped in all initialization processes. The keys are destroyed by the initialization. During update, renewal and migration processes, keypairs and certificates that are not defined in the smart card management profile or are superseded are wiped from the card automatically.

6.2.11 Cryptographic Module Rating

See [CP-BBk-PKI-Advanced].

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 under this CPS have the following validity periods.

- CA certificates maximum of 6 years
- User certificates maximum of 3 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 in the process of activating the smart card. The subscriber creates his/her own PIN during the issuance process.

6.4.2 Activation Data Protection

Natural persons are signing a confidentiality agreement with regard to activation data within the smart card initialization process of the Deutsche Bundesbank smart card.

Activation data of Issuing CAs is stored encrypted and transferred in the start process of CA service. Decryption of activation data is only be possible using a corresponding HSM.

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. The CMS (Card issuing authority system) connects to the RA using safe and encrypted protocols ensuring high level encryption algorithms and ciphers.

Authentication of each stakeholder is done by certificate, presented to CMS. Every event is logged.

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

A thread 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.

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	Unique number corresponding to the subject's public key.	no
Authority Key Identifier	Unique number corresponding to the authority`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 internal and external URL Description	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	Digital Signature,	yes
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	yes
Extended Key Usage	Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2)	no
Subject Key Identifier	Unique number corresponding to the end-entities public key.	no
Authority Key Identifier	Unique number corresponding to the authority`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 and OCSP information.	
Certificate Issuance Policies	CP OID CPS OID of the issuing CA An internal and external URL Description	no
Subject Alternative Name	UPN E-mail address	No
Certificate template information (1.3.6.1.4.1.311.21.7)	Template OID	No
szOID_NTDS_CA_SECURITY_EXT (1.3.6.1.4.1.311.25.2)	SID	

7.1.3 Name Forms

See 3.1.1 and 3.1.2.

7.1.4 Name Constraints

See point 3.1.

7.1.5 Certificate Policy Object Identifier

Certificate Policy Bundesbank PKI for certificate class -advanced-
1.3.6.1.4.1.2025.590.21.1

CPS der Bundesbank Issuing CA for Users -Advanced-
1.3.6.1.4.1.2025.590.21.1.2

7.1.6 Usage of Policy Constraints Extension

See [CP-BBk-PKI-Advanced].

7.1.7 Policy Qualifiers Syntax and Semantics

See [CP-BBk-PKI-Advanced].

7.1.8 Processing Semantics for the Critical Certificate Policies Extension

See [CP-BBk-PKI-Advanced].

7.2 CRL Profile

7.2.1 Version Number(s)

Version 2

7.2.2 Signature Algorithm

Sha512RSA

(OID: 1.2.840.113549.1.1.13)

7.2.3 Issuer

DN of Issuer Certificate

7.2.4 This Update

Date of creation

7.2.5 Next Update

Date of expiry

7.2.6 CRL Entries

List of revoked certificates (serial numbers)

7.2.7 Extensions

Extension	Possible Values	Critical Flag
Authority Key Identifier	Unique number corresponding to the authority`s public key.	no
CRL Number	CRL Number=<Number of the CRL>	no
Next CRL Publish	Date of next CRL publish	no
Issuing Distribution Point	Distribution point of the CRL	yes

7.3 OCSP Profile

The OCSP URL is not published as a certificate extension.

7.3.1 Version Number(s)

OCSP Responder correspondents to RFC6960.

7.3.2 OCSP Extensions

Profile of OCSP response signing certificate

Extension	Possible Values	Critical Flag
Key Usage	Digital Signature	yes
Extended Key Usage	OCSP Signing (OID: 1.3.6.1.5.5.7.3.9)	no
Subject Key Identifies	Unique number corresponding to the subject’s public key.	no
Authority Key Identifier	Unique number corresponding to the authority`s public key.	no
Subject Alternative Name	DNS-Name= <DNS-Name of OCSP-Responder>	no
CRL Distribution Point	Contains a HTTP URL to obtain the current CRL	no
1.3.6.1.5.5.7.48.1.5	No Check	no

Profile of OCSP response

Extension	Possible Values	Critical Flag
Version	1	yes
Extended Key Usage	OCSP Signing (OID: 1.3.6.1.5.5.7.3.9)	no
Authority Name Identifies	Unique number corresponding to the subject's public key.	no
Authority Key Identifies	Unique number corresponding to the subject's public key.	no
Serial number	Serial number requested for	
Status	good or revoked	
this update	Time OCSP response starts to be valid	

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-Advanced].

10 Abbreviations

AIA	Authority Information Access
BBk	Deutsche Bundesbank
BBk-PKI-Advanced	Deutsche Bundesbank PKI Advanced
BSI	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnologie)
C	Country (part of the distinguished name)
CA	Certification Authority
CMS	Card issuing authority system
CN	Common name (part of the distinguished name)
CP	Certificate Policy of a PKI
CPS	Certificate Practice Statement
CRL	Certificate Revocation List; signed list belonging to a CA that contains revoked certificates
CRLDP	CRL distribution point
DC	Data Center
DC	Domain Component
DN	Distinguished name
EBCA	European Bridge CA, link between individual organizations' public key infrastructures
EMAIL	E-mail address (part of the distinguished name)
Smart card	Hardware to store private keys
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
Root CA	Highest CA of a PKI
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer, protocol to ensure secure communication between a client and a server
VA	Validation Authority
x.500	Protocols and services for ISO compliant repositories
x.509 v3	Certification standard

11 Related Documents

[CP-BBk-PKI-Advanced]	Certificate Policy Bundesbank PKI for certificate class -advanced- (1.3.6.1.4.1.2025.590.21.1)