



Certification Practice Statement

Bundesbank Email-CA externe Partner

Version 1.0

1	Introduction	4
1.1	Overview	4
1.2	Document name and identification	4
1.3	PKI participants	4
1.4	Certificate usage	5
1.5	Policy administration	5
1.6	Definitions and acronyms	5
2	Publication and repository responsibilities	6
2.1	Repositories	6
2.2	Publication of certification information	6
2.3	Time or frequency of publication	6
2.4	Access controls on repositories	6
3	Identification and authentication	7
3.1	Naming	7
3.2	Initial identity validation	8
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	10
4.1	Certificate application	10
4.2	Certificate application processing	10
4.3	Certificate issuance	10
4.4	Certificate acceptance	11
4.5	Key pair and certificate usage	11
4.6	Certificate renewal	11
4.7	Certificate re-key	11
4.8	Certificate modification	11
4.9	Certificate revocation and suspension	12
4.10	Certificate status services	14
4.11	End of subscription	14
4.12	Key escrow and recovery	14
5	Facility, management and operational controls	15
5.1	Physical controls	15
5.2	Procedural controls	17
5.3	Personnel controls	19
5.4	Audit logging procedures	19
5.5	Records archival	20
5.6	Key changeover	21
5.7	Compromise and disaster recovery	22
5.8	CA or RA termination	22

6	Technical security controls	23
6.1	Key pair generation and installation	23
6.2	Private key protection and cryptographic module engineering controls	24
6.3	Other aspects of key pair management.....	25
6.4	Activation data	25
6.5	Computer security controls.....	26
6.6	Life cycle technical controls.....	26
6.7	Network security controls	26
6.8	Time-stamping	26
7	Certificate, CRL and OCSP profiles	27
7.1	Certificate profile	27
7.2	CRL profile	28
7.3	OCSP profile	28
8	Compliance audit and other assessments	30
9	Other business and legal matters	31
10	Abbreviations	32
11	Information regarding the document	33

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 contents of the Bundesbank's security and certification concept for the live operation of the Certification Authority (CA) for Email Security Counterparties in the form of a Certification Practice Statement (CPS).

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:	Certification Practice Statement Bundesbank Email-CA externe Partner
Version:	1.0
Date:	01 April 2025
OID:	1.3.6.1.4.1.2025.590.30.1.1

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 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 counterparties of the 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, 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

Certificates issued by this CA must only be used for digital signature and encryption of emails in connection with the Bundesbank's business activities.

1.5.2 Prohibited Certificate Uses

Counterparties may not use the certificates in connection with business activities with third parties for any other purpose than specified in point 1.5.1 without the BBk-PKI's approval.

1.6 Policy Administration

1.6.1 Organisation Administering the Document

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

1.6.2 Contact person

Deutsche Bundesbank
PKI Services (Deutsche Bundesbank Trust Center)
Berliner Allee 14 Postfach 10 11 48
40212 Düsseldorf 40002 Düsseldorf
Germany Germany
Tel +49 211 874 3257/2351
Email: pki@bundesbank.de[mailto:](mailto:pki@bundesbank.de)

1.6.3 Person determining CPS suitability for the policy

See CP Bundesbank Email-CA externe Partner.

1.6.4 CPS Approval Procedures

See CP Bundesbank Email-CA externe Partner.

1.7 Definitions and Acronyms

See abbreviations in chapter 10.

2 Publication and Repository Responsibilities

2.1 Repositories

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

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

2.2 Publication of Certification Information

The Bundesbank publishes the following information:

- CA certificates with fingerprints
- CRLs
- Details of the revocation procedure
- 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

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 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	<Email address>
CN	<First name Surname>
OU	<Organisational unit>
O	<Organisation>
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 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

See CP Bundesbank Email-CA externe Partner.

3.1.4 Rules for Interpreting Various Name Forms

The DN is based on the x.509 standard.

3.1.5 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.

3.1.6 Recognition, Authentication and Role of Trademarks

See CP Bundesbank Email-CA externe Partner.

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. The BBk-PKI forwards the encrypted soft PSE and the PIN according to section 4.3.1 to the subscribers and thereby ensures that the subscribers receive the private keys.

3.2.2 Authentication of Organisation identity

Applications for a certificate for an organisation's email addresses or for people grouped according to organisation/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

When applying for a certificate for a counterparty, employees of an authorised counterparty of the Bundesbank are identified by means of a copy of their official photo ID, which is forwarded to the BBk-PKI. The copy of the ID card is destroyed by the BBk-PKI once the certificate has been delivered.

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 Bundesbank Email-CA externe Partner.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

The subscriber will be notified by the BBK-PKI about the expiry of the certificate's validity.

Certificate renewal and the associated identification and authentication process are similar to the initial application process initiated by Bundesbank employees.

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 by telephone or in writing.

The applicant's identity is documented. The BBk-PKI operating unit reserves the right to check the identity of the applicant as appropriate but is not required to do so. 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?

The process of applying for a certificate for a counterparty is initiated by Bundesbank employees via an electronic application workflow, which, after being approved by the direct supervisor of the Bundesbank employee, is sent to the BBk-PKI.

The BBk-PKI then sends an application form generated during the electronic application process to the counterparty to sign.

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 Bundesbank Email-CA externe Partner.

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 Bundesbank Email-CA externe Partner.

4.2.3 Time to Process Certificate Applications

See CP Bundesbank Email-CA externe Partner.

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 application for a certificate is made via an electronic application workflow and an application form completed by the subscriber. The certificate data are transferred to the BBk-PKI, which is operated online. The subsequent certification process runs automatically, but is started manually.

The certificate is delivered to the subscriber in the form of a software certificate only and is protected by a transport PIN. The certificate is either handed over in person against confirmation of receipt or sent by secure electronic means against confirmation of receipt. In a second step, the BBk-PKI sends the transport PIN to the applicant by secure electronic means against confirmation of receipt or by telephone.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

See 4.3.1.

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 is not published in a directory service.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.5 Key Pair and Certificate Usage

See CP Bundesbank Email-CA externe Partner.

4.6 Certificate Renewal

A certificate must 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 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.

4.8.1 Circumstance for Certificate Modification

See CP Bundesbank Email-CA externe Partner.

4.8.2 Who may request Certificate Modification

The application for certificate modification is initiated by Bundesbank employees.

See also CP Bundesbank Email-CA externe Partner.

4.8.3 Processing Certificate Modification Requests

The certificate modification process is the same as the initial application process.

4.8.4 Notification of New Certificate Issuance to Subscriber

See CP Bundesbank Email-CA externe Partner.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See CP Bundesbank Email-CA externe Partner.

4.8.6 Publication of the Modified Certificate by the CA

See CP Bundesbank Email-CA externe Partner.

4.8.7 Notification of Certificate Issuance by the CA to other Entities

See CP Bundesbank Email-CA externe Partner.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

See CP Bundesbank Email-CA externe Partner.

4.9.2 Who can request revocation

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

Those persons who confirmed the identity/authorisation of a subscriber during the certificate application process may also request revocation of his/her certificate at any time if the subscriber is no longer authorised to use the certificate.

4.9.3 Procedure for Revocation Request

A certificate can be revoked

- using the electronic application workflow
- by telephone
- by fax or
- in writing.

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

4.9.4 Revocation Request Grace Period

See CP Bundesbank Email-CA externe Partner.

4.9.5 Time within which CA must process the Revocation Request

The BBk-PKI will revoke the certificate immediately after receipt of the revocation request.

4.9.6 Revocation Checking Requirement for Relying Parties

See CP Bundesbank Email-CA externe Partner.

4.9.7 CRL Issuance Frequency

CA CRLs are issued with a validity period of 6 days. A new list is issued every day.

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 includes the information about revoked certificates until each of the certificates are expired.

4.9.8 Maximum Latency for CRLs

See CP Bundesbank Email-CA externe Partner.

4.9.9 On-line Revocation/Status Checking Availability

The BBk-PKI 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 On-line 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

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

A temporary revocation or suspension of certificates is prohibited. Once a certificate has been revoked, it cannot be reactivated.

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

See CP Bundesbank Email-CA externe Partner.

4.11 End of Subscription

See CP Bundesbank Email-CA externe Partner.

4.12 Key Escrow and Recovery

Only the subscriber can request a key recovery. The BBk-PKI forwards the encrypted soft PSE and the PIN according to section 4.3.1 to the subscribers.

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 seven 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 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. 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 Bundesbank Email-CA externe Partner.

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 Bundesbank Email-CA externe Partner.

5.4.3 Retention Period for Audit Log

The retention period for audit log data is implemented as described in the document CP Bundesbank Email-CA externe Partner. 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 Bundesbank Email-CA externe Partner.

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 256 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 Bundesbank Email-CA externe Partner.

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 Bundesbank Email-CA externe Partner.

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 parties
- Deletion of the affected key

5.7.4 Business Continuity Capabilities after a Disaster

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

5.8 CA or RA Termination

See CP Bundesbank Email-CA externe Partner.

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 is delivered via a secure channel for use by the subscriber. The subscriber receives the private key by secure electronic means. Once the subscriber has confirmed receipt, the BBk-PKI sends the transport PIN to him/her in a second step by secure electronic means against confirmation of receipt or by phone.

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 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

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 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
- 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 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 data 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 data center network the area concept for network segregation ensures only valid and secure communication.

Within Bundesbank's network the CA 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.

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

CA certificates have the following extensions.

Key Usage	cert sign, crl sign – critical
Basic Constraints	CA=true, Path Length Constraint=0 – critical
Authority Key Identifier	160-bit SHA-1 hash of issuer's key
Subject Key Identifier	160-bit SHA-1 hash of issuer's key
Certificate Issuance Policies	CP OID, CPS OID, external URL, Description

User certificates have the following non-critical extensions.

Key Usage	key encipherment, digital signature – critical
Extended Key Usage	Email protection
Basic Constraints	CA=false, no constraints on length of path – critical
Subject Alt Name	Email address
CRL Distribution Point	<a href="http://pki.bundesbank.de/BBK_EMS_EXT_CA_<year of issue>.crl">http://pki.bundesbank.de/BBK_EMS_EXT_CA_<year of issue>.crl
AIA Distribution Point	<a href="http://pki.bundesbank.de/BBK_EMS_EXT_CA_<year of issue>.crt">http://pki.bundesbank.de/BBK_EMS_EXT_CA_<year of issue>.crt
Certificate Issuance Policies	CP OID, CPS OID, external URL, Description
Authority Key Identifier	160-bit SHA-1 hash of issuer's key
Subject Key Identifier	160-bit SHA-1 hash of issuer's key

7.1.3 Algorithm Object Identifiers

The RSA (OID 1.2.840.113549.1.1.1) algorithm and SHA512 RSA (OID 1.2.840.113549.1.1.13) is used in the certificates issued by the BBk-PKI.

7.1.4 Name Forms

See 3.1.1 and 3.1.2

7.1.5 Name Constraints

See chapter 3.1.

7.1.6 Certificate Policy Object Identifier

The certificate policy OID of the CP Bundesbank Email-CA externe Partner is:
1.3.6.1.4.1.2025.590.30.1.

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

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

- Authority Key Identifier
- CRL Number
- CA Version
- CRL Distribution Point
- Reason Codes
- Revocation Date
- Certificate Serial Number.

7.3 OCSP Profile

The OCSP URL is not published as a certificate extension.

7.3.1 Version Number(s)

OCSP Responder corresponds 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

See CP Bundesbank Email-CA externe Partner.

9 Other Business and Legal Matters

See CP Bundesbank Email-CA externe Partner.

10 Abbreviations

BBk	Deutsche Bundesbank
BBk-PKI	Deutsche Bundesbank's PKI
BSI	Federal Office for Information Security (<i>Bundesamt für Sicherheit in der Informationstechnologie</i>)
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
DName	Distinguished name
EMAIL	Email address (part of the distinguished name)
HSM	Hardware Security Module
LDAP	Light Directory Access Protocol, repository service
O	Organisation (part of the distinguished name)
OCSP	Online Certificate Status Protocol
OID	Object identifier
OU	Organisational 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
RFC 3647	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 email
x.500	Protocols and services for ISO compliant repositories
x.509v1	Certification standard

11 Information Regarding the Document

See point 1.2.