DEUTSCHE BUNDESBANK
EUROSYSTEM

Certificate Policy

Authentication Certificates - Advanced -

Version 1.3

1 Introduction 4
1.1 Overview 4
1.2 Document Name and Identification 5
1.3 PKI Participants 5
1.4 Certificate Usage 6
1.5 Policy Administration 6
1.6 Definitions and Acronyms 7
2 Publication and Repository Responsibilities 8
2.1 Repositories 8
2.2 Publication of Certification Information 8
2.3 Time and Frequency of Publication 8
2.4 Access Controls on Repositories 8
3 Identification and Authentication 9
3.1 Names 9
3.2 Initial Identity Validation 9
3.3 Identification and Authentication for Re-key Requests 10
3.4 Identification and Authentication for Revocation Request 10
4 Certificate Life Cycle Operational Requirements 11
4.1 Certificate Application 11
4.2 Certificate Application Processing 11
4.3 Certificate Issuance 12
4.4 Certificate Acceptance 12
4.5 Key Pair and Certificate Usage 12
4.6 Certificate Renewal 12
4.7 Certificate Re-key 13
4.8 Certificate Modification 14
4.9 Certificate Revocation and Suspension 14
4.10 Certificate Status Service 16
4.11 End of Subscription 16
4.12 Key Escrow and Recovery 16
5 Facility, Management, and Operational Controls 17
5.1 Physical Controls 17
5.2 Procedural Controls 17
5.3 Personnel Controls 18
5.4 Audit Logging Procedures 19
5.5 Records Archival 21
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 ... 27
7.3 OCSP Profile ... 28
8 Compliance Audit and Other Assessments ... 29
8.1 Frequency or Circumstances of Assessment ... 29
8.2 Identity/Qualifications of Assessor ... 29
8.3 Assessor's Relationship to Assessed Entity ... 29
8.4 Topics Covered by Assessment ... 29
8.5 Actions Taken as a Result of Deficiency ... 29
8.6 Communication of Results ... 29
9 Other Business and Legal Matters ... 30
9.1 Fees ... 30
9.2 Financial Responsibility ... 30
9.3 Confidentiality of Business Information ... 30
9.4 Privacy of Personal Information ... 30
9.5 Intellectual Property Rights ... 31
9.6 Representations and Warranties ... 31
9.7 Disclaimer of Warranties ... 31
9.8 Limitations of Liability ... 32
9.9 Indemnities ... 32
9.10 Term and Termination ... 32
9.11 Individual Notices and Communications with participants ... 32
9.12 Amendments ... 33
9.13 Dispute resolution Provisions ... 33
9.14 Governing Law ... 33
9.15 Compliance with Applicable Law ... 33
9.16 Miscellaneous Provisions ... 33
9.17 Other Provisions ... 34
10 Abbreviations ... 35

1 Introduction

1.1 Overview

This document provides both users and the Deutsche Bundesbank – as the Public Key Infrastructure (PKI) operator – with a summary of the binding certification guidelines of the Deutsche Bundesbank for the issuance of authentication certificates (advanced) in the form of a Certificate Policy (CP). Figure 1 shows an overview of the CAs for the authentication solution.

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

The Bundesbank is a member of the European Bridge CA (EBCA).

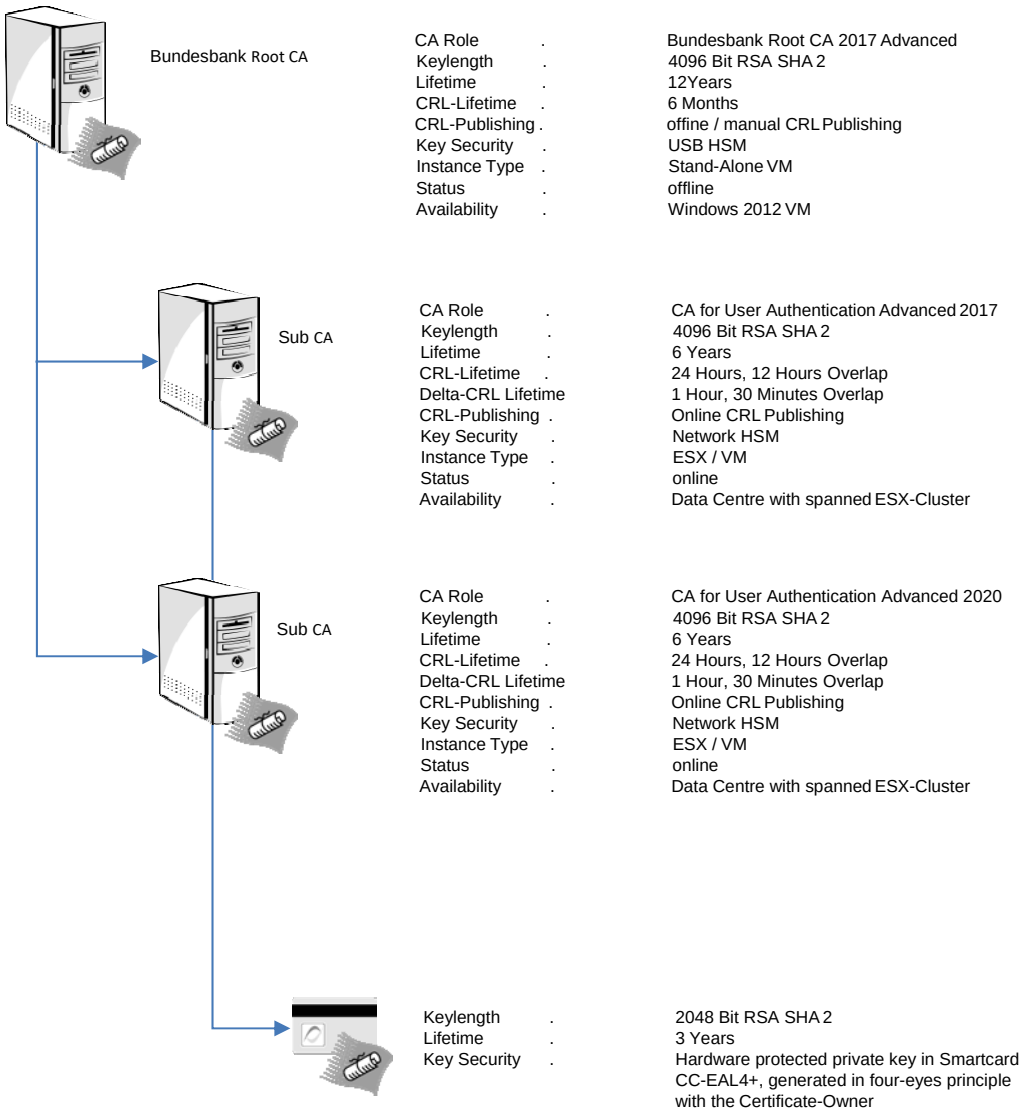

Figure 1: Overview of the 2FA CA Infrastructure of Deutsche Bundesbank

1.2 Document Name and Identification

Name: Certificate Policy
Authentication Certificates - Advanced -
Version: 1.3
Date: 10 August 2020
OID: 1.3.6.1.4.1.2025.590.10.1.1

All the detailed parts for the solution are described in the CPS “Authentication Certificates - Advanced -“ with the OID 1.3.6.1.4.1.2025.590.10.1.2

1.3 PKI Participants

1.3.1 Certification Authorities

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

1.3.2 Registration Authorities

The registration authorities (RA) are responsible for:

- verifying the identity and authenticity of subscribers,
- registration procedure,
- documentation of registration procedure and
- suspension and revocation of certificates

There are registration authorities at all Bundesbank locations. These are responsible for the employees who work within their scope.

The registration procedure is described in point 3.2.3.

1.3.3 Subscribers

Subscribers are natural persons only. SubCAs have to document in their CPS which natural persons may be subscribers.

1.3.4 Relying Parties

Relying parties are IT systems and/or IT processes that use a certificate issued by the BBK-PKI-Advanced to verify authorisation or authenticity of subscribers named in point 1.3.3.

The systems to be authenticated must be documented in the CPS.

1.3.5 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Appropriate certificate use must be documented in the relevant SubCAs CPS. The certificates are exclusively used for Deutsche Bundesbank internal business purposes by subscribers listed in 1.3.3.

1.4.2 Prohibited Certificate Uses

Private use of certificates is prohibited.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

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

1.5.2 Contact person

Deutsche Bundesbank
PKI Services

Berliner Allee 14	Postfach 10 11 48
40212 Düsseldorf	40002 Düsseldorf
Germany	Germany

Tel: +49 211 874 3815/3257/2351
Fax: +49 69 709094 9922
E-mail: pki@bundesbank.de

1.5.3 Person determining CPS Suitability for the Policy

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

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

1.5.4 CPS Approval Procedures

This CP will be published on the Deutsche Bundesbank's intranet site and website.

The documents (CP and CPS) will be independently reviewed by the ESCB's PKI Assessment Body. The documents will not be passed on to any other organisations for validation.

1.6 Definitions and Acronyms

See chapter 10.

2 Publication and Repository Responsibilities

2.1 Repositories

The Bundesbank publishes 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 restricted to Bundesbank employees as well as external employees of this institution).

2.2 Publication of Certification Information

The Bundesbank publishes the following information.

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

2.3 Time and Frequency of Publication

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

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

2.4 Access Controls on Repositories

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

3 Identification and Authentication

3.1 Names

3.1.1 Types of Names

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

3.1.2 Need for Names to be Meaningful

The name of the certificate issued (DN) must uniquely identify the subscriber within the BBk-PKI-Advanced. The following rule applies.

- Certificates for natural persons must be issued in the subscriber's name.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymity or pseudonymity in certificate names is prohibited.

3.1.4 Rules for Interpreting Various Name Forms

The DN is based on the x.509 standard.

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

3.1.5 Uniqueness of Names

The responsible unit ensures that the names are unique. SubCAs must document the relevant rules guaranteeing the uniqueness of names in the CPS.

3.1.6 Recognition, Authentication and Role of Trademarks

As the names of the issued certificates (DN) refer to natural persons in the Deutsche Bundesbank, the recognition of brands and trademarks is not relevant.

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

If the key material is generated by the applicant, the subscriber must furnish proof that he/she is in possession of the private key. Proof is normally furnished by submitting a Certificate Signing Request in the PKCS#10 format.

3.2.2 Authentication of Organisation Identity

Given that the names of the issued certificates (DN) refer to natural persons in Deutsche Bundesbank, authentication of an organisation identity is not required.

3.2.3 Authentication of Individual Identity

Applicants (natural persons) must uniquely authenticate themselves to the respective RA when applying for a certificate.

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

3.2.4 Non-verified Subscriber Information

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

3.2.5 Validation of Authority

This procedure is described in the respective CPS.

3.2.6 Criteria for Interoperation

Not applicable. No cross-certification with other organisations is planned at present.

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 must be identical to the initial application process, or processed in case of self-service renewal Workflow.

3.3.2 Identification and Authentication for Re-key after Revocation

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

3.4 Identification and Authentication for Revocation Request

Requirements for applying revocation:

- Applicants (natural persons) must uniquely authenticate themselves when requesting revocation of a certificate. This can be done by ID card (passwort) or Bundesbank ID Card.
- If a uniquely authentication of the applicant is not possible certificate will be suspended.
- The applicant's identity is documented in the event of a revocation request.
- Reason and way of submitting of revocation request is documented.

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Those subscribers listed in point 1.3.3 can submit a certificate application. The following natural persons are eligible to apply for certificates.

- Bundesbank employees,
- External employees of this institution, where applicable.

4.1.2 Enrollment Process and Responsibilities

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

- Is the applicant authorised?
- Is the application complete and correct?
- Is the DN unique?
- Has the person been authenticated?

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

Meeting the formal requirements does not constitute an entitlement to issuance of a certificate. The decision to issue certificates is entirely at the discretion of the responsible unit.

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

Acceptance or rejection must be documented.

4.2.3 Time to Process Certificate Applications

The issuance of a certificate must be realized online without a delay.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

The certificate may be published in a directory service.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No other entities require notification.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Only the subscriber is entitled to use the private key.

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 trust of certificate chain and validity period of the certificate. Any limitation on the usage of certifiates must be taken account.

4.6 Certificate Renewal

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

4.7 Certificate Re-key

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

4.7.1 Circumstances for Certificate Re-key

Certification with re-keying is possible in the following cases.

- Routine re-keying
  - if the validity of the certificate is about to expire or
  - has just expired.
- Certificate application after a previous certificate has been revoked.
- The algorithms, key sizes or the validity periods of the certificate no longer provide adequate security, or the structure of the certificate urgently requires modification.

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

4.7.2 Who May Request Certification of a New Public Key

Application by a subscriber is governed by the rules for new applications. See point 4.1.1.

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

4.7.3 Processing Certificate Re-keying Requests

The rules for initial application apply. See point 4.2.

4.7.4 Notification of New Certificate Issuance to Subscriber

The rules for initial application apply. See point 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

The rules for initial application apply. See point 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

The rules for initial application apply. See point 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The rules for initial application apply. See point 4.4.3.

4.8 Certificate Modification

Within the BBk-PKI-Advanced, a certificate is modified on the basis of an application and involves changing the key pair and modifying the content of the certificate as well as the technical parameters. A certificate modification always requires re-keying.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A certificate must be revoked if at least one of the following circumstances arises.

- Information in the certificate is not or is no longer valid.
- The private key has been compromised.
- Loss of the Deutsche Bundesbank identity card.
- The subscriber is no longer authorised to use the certificate.
- The subscriber no longer requires the certificate.
- The subscriber does not comply with the obligations specified in the respectivet CP/CPS (see point 4.5).
- The private key of the issuing CA or of the RootCA has been compromised. In this case, all certificates issued by this CA are revoked as well.
- The algorithms, key sizes or validity periods of the certificate no longer provide sufficient security. The responsible unit reserves the right to revoke the certificates in question.

4.9.2 Who can Request Revocation

A revocation request for a natural person can be made by the subscriber, someone appointed by the subscriber, or by his/her superior.

4.9.3 Procedure for Revocation Request

The revocation process is documented in the RA systems of the individual CA. More detailed information is entered in the CPS of the SubCAs.

4.9.4 Revocation Request Grace Period

As soon as a circumstance for revocation arises, subscribers must immediately arrange for the certificate to be revoked.

If special events occurs which require the revocation of a Sub-CA, the assessment by a security officer and revocation of the Sub-CA must take place within 24 hours after the event has been recognized.

4.9.5 Time within Which CA Must Process the Revocation Request

The rules governing revoked and suspended certificates can be found in the CPS of the respective CA.

4.9.6 Revocation Checking Requirement for Relying Parties

Information about revocation is published using CRLs. Relying parties must use the most recent CRL to verify the validity of certificates.

4.9.7 CRL Issuance Frequency

Root CA CRLs are issued with a validity period of 180 days. A new list is issued one week prior to expiry of the most recent CRL. Rules governing the publication of CRLs of SubCAs can be found in the respective CA's CPS.

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 contains the information about revoked certificates until those certificates have expired.

4.9.8 Maximum Latency for CRLs

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

4.9.9 Online revocation/status checking availability

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

SubCAs can additionally provide a revocation status check via OCSP.

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

4.9.10 Online Revocation checking Requirements

Not applicable.

4.9.11 Other Forms of Revocation Advertisements available

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

4.9.12 Special Requirements Re-key Compromise

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

4.9.13 Circumstances for Suspension

Temporary revocation, called suspension, of certificates is only possible in the following case:

- Short-term loss of a smartcard.

4.9.14 Who can Request Suspension

A suspension request can be made by the subscriber, someone appointed by the subscriber, or his/her superior.

4.9.15 Procedure for Suspension Request

The suspension process is documented in the RA systems of the individual CA. More detailed information is entered in the SubCAs CPS.

4.9.16 Limits on Suspension Period

Whenever suspensions are imposed, SubCAs must document the rules governing the maximum duration of a suspension.

4.10 Certificate Status Service

The responsible unit can provide a certificate status request service.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

Key escrow and recovery by the responsible unit is prohibited.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

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

The root CA is operating offline (without connection to a LAN). Outside the operating hours, all components (used to run the root CA) are stored in a vault. The access to the components is protected by mechanisms that enforce a four-eyes principle. The provision in a vault is designed in such a way that the necessary components are also available in the event of a disaster due to separate fire protection sections

5.1.2 Physical Access

Physical access must be via a multi-stage access control system.

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposures

The rooms must have adequate protection from exposure to water.

5.1.5 Fire Prevention and Protection

Fire prevention and fire alarm regulations must be observed.

5.1.6 Media Storage

Not applicable.

5.1.7 Waste Disposal

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

5.1.8 Off-Site Backup

There is not an off-site data backup external to the data centres (eg at other service providers).

5.2 Procedural Controls

5.2.1 Trusted Roles

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

SubCAs must document established roles in their CPS.

5.2.2 Number of Persons Required per Task

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

The key ceremony for launching Hardware Security Modules (HSM) is generally subject to a multiple-pairs-of-eyes principle with at least three persons from different IT units.

5.2.3 Identification and Authentication for Each Role

The trusted roles approach is implemented using a number of technical and organisational measures. Roles are identified and authenticated by using smart cards, user IDs and passwords.

5.2.4 Roles Requiring Separation of Duties

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

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

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

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

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

Routinely job rotation does not occur.
For new personnel or assignment of new responsibilities the requirements in point 5.3.3 apply.

5.3.6 Sanctions for Unauthorised Actions

Unauthorised actions that endanger the security of the responsible unit or breach data protection requirements are punished/prosecuted by HR.

5.3.7 Independent Contractor Requirements

Not applicable.

5.3.8 Documentation Supplied to Personnel

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

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

5.4 Audit Logging Procedures

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

5.4.1 Types of Events Recorded

SubCAs must monitor and document the following processes.

- System initialisation
- Certification applications
- User registration
  The following information is collected
  - Unique personell identifier [UPN] of issued certificates. UPN is a internal identifier, owned by HR-Department. UPN is as well the e-mail address of a subscriber.
  - Serialnumber of the Smartcard’s chip
    Using the Serialnumber of the SC-Chip the id-card is also matched to the id-card itself (represented by an unique id-card-identifier).
- Key generation for the CA and users
- Certificate issuance for the CA and users
- Data backups for the CA
- Certificate publication by the CA
- Delivery of private key and certificate
- Revocation and suspension applications
- Revocation and suspension of a certificate
- Drawing up of a CRL

- Publication of a CRL

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

The audit logging procedure is invoked during startup of the Logappliance. This is done and ensored by a system daemon.

In case of system failures, maintenance or reboots of the Logappliance all logs are being cashed and resubmitted to the Logappliance when it is available again.

5.4.2 Frequency of Processing Log

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

5.4.3 Retention Period for Audit Log

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

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

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

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

There is an active and generally acceptet vulnerability and patch-management policy in place at Deutsche Bundebank

- Generally every workplace client gets systematically planned releases including security patches twice a year
- For critical vulnerabilities ad-hoc updates are in place

- Generally the Card Management as well as the HSM also gets systematically planned releases including security patches twice a year

5.5 Records Archival

All IT systems located in the Deutsche Bundesbank infrastructure are synchronized with an internal time source. The internal time-source gets it's time by using a DCF77 correlation receiver.

5.5.1 Types of Records Archived

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

5.5.2 Retention period for Archive

The retention periods are defined in point 5.4.3.

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

Data backups are made every day. The data backups must be stored in different fire sections of the building.

5.5.5 Requirements for Time-Stamping of Records

No trustworthy timestamp sources are supported at present.

5.5.6 Archive Collection System (internal or external)

The responsible unit is responsible for archiving. Archives are not stored externally.

5.5.7 Procedures to Obtain and Verify Archive Information

There is no standardised procedure for obtaining and verifying archived information.

5.6 Key changeover

The CA shall change the key whenever the validity of a user certificate to be issued would exceed the remaining term of the CA.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

5.7.2 Computing Resources, Software, and/or Data are corrupted

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

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

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

5.7.3 Entity Private key compromise Procedures

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

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

5.7.4 Business Continuity Capabilities after a Disaster

See CPS of the SubCAs.

5.8 CA or RA Termination

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

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

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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

Key material for natural persons must be generated on a smartcard certified to, at least, Common Criteria EAL 4+.

6.1.2 Private Key Delivery to Subscriber

No private keys are delivered. See point 6.1.1.

6.1.3 Public Key Delivery to Certificate Issuer

The subscriber delivers the public key in a Certificate Signing Request. The technical process of delivery must be described in the CPS.

6.1.4 CA Public Key Delivery to Relying Parties

The public keys of SubCAs are published in the repositories named in point 2.1.

6.1.5 Key Sizes

Only those combinations of key algorithms and sizes are used that the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway and the Federal Office for Information Security consider to be secure.

The CA key of the SubCAs has a minimum size of 4096 bits.

For subscribers, keys have a minimum size of 2048 bits.

6.1.6 Public Key Parameters Generation and Quality Checking

The following encryption algorithms are to be used.

- RSA with OID 1.2.840.113549.1.1.1
- SHA256 RSA 1.2.840.113549.1.1.11

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

For SubCAs, the key usage purposes are

- signing certificates and
- signing CRLs.

For natural persons, the key usage purposes are

- digital signature and
- key encryption.

See point 1.4.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Private keys of Root-CA and SubCAs are created inside and stored in HSMs.

Private keys of natural persons are securely stored on smart cards.

6.2.1 Cryptographic Module Standards and Controls

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

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

The SubCAs private key may only be used in the secure environment of an HSM. The SubCAs private key never leaves the HSM. For the Root CA a processing of the private key uses a 2 out of 4 multi-person control.

6.2.3 Private Key Escrow

Key escrow is prohibited within or outside the Bundesbank.

6.2.4 Private Key Backup

Backups of private keys for RootCA and/or SubCAs are only permitted within the HSM's security system. Backups of private keys for natural persons are not permitted.

6.2.5 Private Key Archive

There is no archive of private keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Transfer of private keys belonging to Root-CA or SubCAs can only take place in an HSM of the same CA; the provisions of point 6.2.2 must be observed here.

Transfering private keys to a new HSM is based on process using a 3 out of 8 multi-person control

The private keys stored on the smart card are used for natural persons. Export is not possible.

6.2.7 Private Key Storage on Cryptographic Module

See point 6.2.1.

6.2.8 Method of Activating Private Key

Private keys belonging to natural persons must be activated by entering a PIN.

6.2.9 Method of Deactivating Private Key

If private keys of a certification authority are compromised, they must be deactivated.

Smartcards with key materials of natural persons are suspended after an incorrect PIN has been entered three times. The re-activation (unlock) of the smartcard after suspension must be realized by the challenge and response technique. A workflow is needed to inform the service desk of the smartcard lock. After that the service desk contacts the affected employee and starts the challenge and response technique.

6.2.10 Method of Destroying Private key

Once the validity of the CA's private key has expired or this key has been revoked, it is keept for 10 years. After this period it is deleted from the HSM environment. Storage devices are destroyed or securely deleted. Private keys and further key material stored in the HSM leaving the HSM Environment are destroyed by using a factory reset procedure, as dictated by the HSM vendor.

6.2.11 Cryptographic Module Rating

See point 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

- Root CA certificates maximum of 12 years
- 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 CA private keys (root and sub) is generated using HSM devices. The activation smartcards for multi-person control are PIN protected.

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

Activation data are a by-product of the generation of the certificates for natural persons. The subscriber creates his/her own PIN during the issuance process.

6.4.2 Activation Data Protection

Natural persons sign a confidentiality agreement with regard to activation data by initial allocation of the Deusche Bundesbank identity card.

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

Activation data of Sub-CA is transferred while start of CA service in form of an encrypted data file with private key. Decryption of data file is only possible by corresponding HSM.

6.4.3 Other Aspects of Activation Data

Not applicable.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

6.5.2 Computer Security Rating

The security measures are state of the art. A threat analysis is conducted regularly (at least every two years).

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

For every IT-system or application in Bundesbank an internal risk assesment is made (IT-Risk Management Process). This rule also applies to the procedures for which this policy applies.

6.6.2 Security Management Controls

See point 6.5.1.

6.6.3 Life Cycle Security Controls

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

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

6.7 Network Security Controls

See point 6.5.1.

6.8 Time-Stamping

It is guaranteed that the time is synchronous on all IT-systems (see point 5.5).

Time-stamping is currently not available.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

The BBk-PKI-Advanced and the authentication solution issue certificates issued are in line with the X509v3 standard.

7.1.2 Certificate Extensions

SubCAs must document the certificate extensions used in the CPS and store the intended use of certificates in the respective certificates' Key Usage and Extended Key Usage.

7.1.3 Algorithm Object Identifiers

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

7.1.4 Name Forms

See points 3.1.1 and 3.1.2.

7.1.5 Name Constraints

See point 3.1.

7.1.6 Certificate Policy Object Identifier (OID)

The Certificate policy OID of the CP Authentication Certificates – Advanced – is 1.3.6.1.4.1.2025.590.10.1.1

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-Advanced issues CRLs in line with the x.509 norm, version 2.

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

SubCAs can provide OCSPs.

7.3.1 Version Number(s)

OCSP Version 1 should be used.

7.3.2 OCSP Extensions

Any extensions used must be documented when providing the OCSP status check.

8 Compliance Audit and Other Assessments

The working processes of the CA and other entities involved in registration are subject to regular and ad hoc inspections.

The technical framework and operational processes of the PKI undergo a 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. Assemments will take place, among other things, with the following changes:

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

If there are no grounds for an earlier assesment, an assesment will take place no later than three years

8.2 Identity/Qualifications of Assessor

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

8.3 Assessor’s Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

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

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication of Results

The results of the assessment will not be published.

9 Other Business and Legal Matters

9.1 Fees

No fees will be charged.

9.2 Financial Responsibility

Risks which may arise from liability for a CA are covered by the Deutsche Bundesbank.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

9.3.2 Information not within the Scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

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

9.4.3 Information not Deemed Private

The provisions defined in point 9.3.2 apply.

9.4.4 Responsibility to Protect Private Information

Responsibility for protecting personal information lies with the responsible unit.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

No other information disclosure circumstances are envisaged.

9.5 Intellectual Property Rights

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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

9.6.2 RA Representations and Warranties

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

9.6.3 Subscriber Representations and Warranties

The subscriber’s obligations are defined in point 4.5.1.

9.6.4 Relying party Representations and Warranties

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

9.6.5 Representations and Warranties of other participants

Not applicable.

9.7 Disclaimer of Warranties

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

9.8 Limitations of Liability

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

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

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

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

9.9 Indemnities

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

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and survival

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

9.11 Individual Notices and Communications with participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances under which the OID must be Changed

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

9.13 Dispute resolution Provisions

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

9.14 Governing Law

The place of jurisdiction is Frankfurt am Main.

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

There is no provision for transfer of rights.

9.16.3 Severability

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

9.16.4 Enforcement

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

The place of enforcement and jurisdiction is Frankfurt am Main.

9.16.5 Force Majeure

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

9.17 Other Provisions

Not applicable.

10 Abbreviations

2FA	Two-factor authentication
BBk	Deutsche Bundesbank
BBk-PKI-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
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
CRLDP	CRL distribution point
DC	Data centre
DN	Distinguished name
DName	Distinguished name
EMAIL	E-mail address (part of the Distinguished Name)
EBCA	European Bridge CA, link between individual organisations' public key infrastructures
Hardwaretoken	Hardware to store private keys
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
PSE	Personal Secure Environment
RA	Registration Authority
RFC	Request for Comment, documents for global standardisation
RFC3647	This RFC describes documents that outline PKI operations
Root CA	Highest CA of a PKI
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm

SigG	Electronic Signature Act (*Gesetz über Rahmenbedingungen für elektronische Signaturen*)
S/MIME	Secure Multipurpose Internet Mail Extensions, standard for secure e-mail
CRL	Signed list belonging to a CA that contains revoked certificates
SSL	Secure Socket Layer, protocol to ensure secure communication between a client and a server
SÜG	Security Clearance Act (*Sicherheitsüberprüfungsgesetz*)
x.500	Protocols and services for ISO compliant repositories
x.509v3	Certification standard