DEUTSCHE BUNDESBANK
EUROSYSTEM

Certification Practice Statement

Authentication Certificates - Advanced -

Version 1.3

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 User Authentication - Advanced - in the form of a Certification Practice Statement (CPS). 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 standard.

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

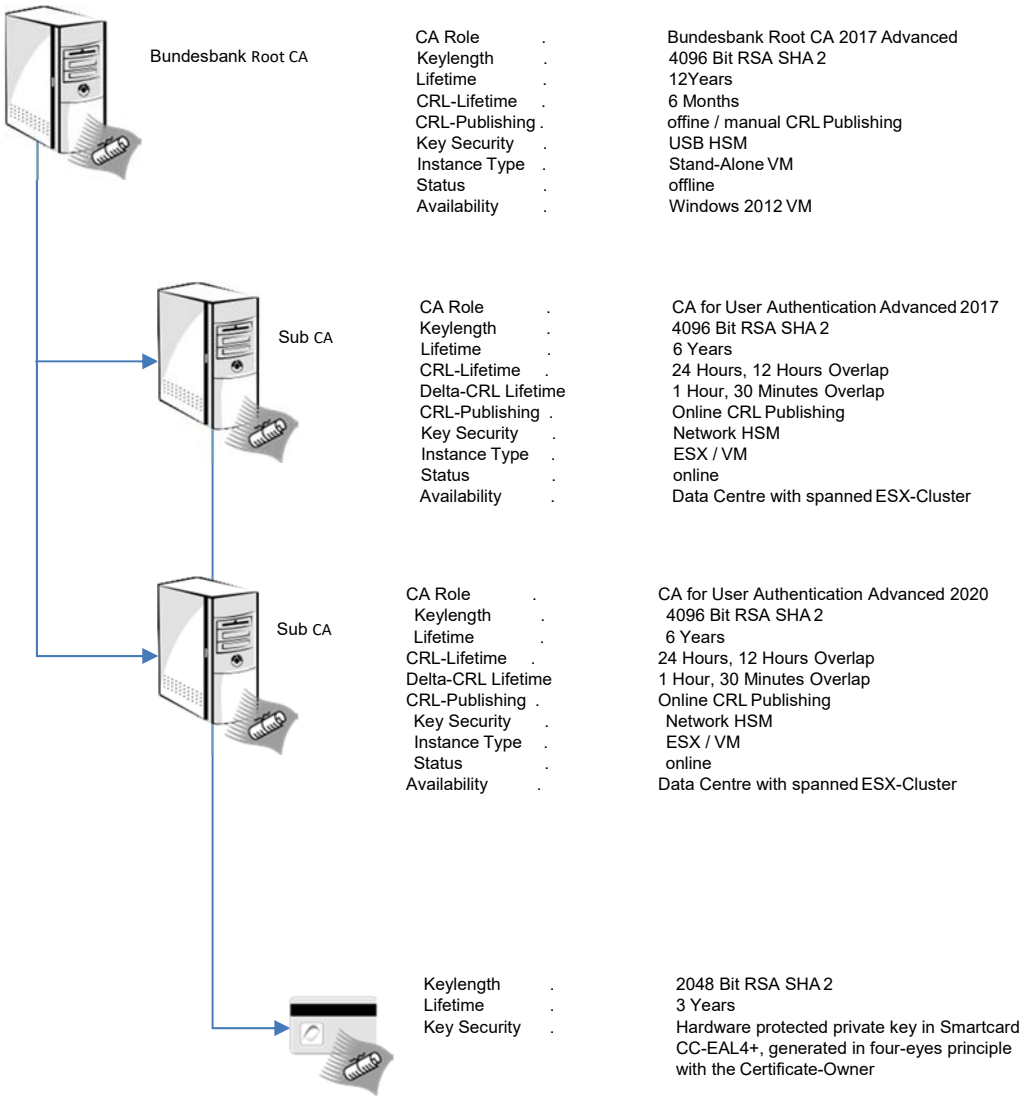

Figure 1: Overview of the 2FA CA Infrastructure of Deutsche Bundesbank

1.2 Document Name and Identification

Name:	Certification Practice Statement Authentication Certificates - Advanced -
Version:	1.3
Date:	10 August 2020
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 exists 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

- Employees of the Deutsche Bundesbank,
- External Employees with contract of employment with Deutsche Bundesbank

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

1.3.4 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 to are both internal IT-systems and IT-processes of Deutsche Bundesbank and IT-systems and IT-processes of ESCB.

1.3.5 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The certificates are issued to the subscribers' listed in 1.3.3 for authentication purpose only.

1.4.2 Prohibited Certificate Uses

See CP for Authentication Certificates - Advanced -.

1.5 Policy Administration

1.5.1 Organization Administering the Document

See CP for Authentication Certificates - Advanced -.

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

See CP for Authentication Certificates - Advanced -.

1.5.4 CPS Approval Procedures

See CP for Authentication Certificates - Advanced -.

1.6 Definitions and Acronyms

See abbreviations in chapter 10.

2 Publication and Repository Responsibilities

2.1 Repositories

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

- http://www.bundesbank.de under Service ► Services for banks and companies ► PKI
- or at this direct link

  https://www.bundesbank.de/en/service/banks-and-companies/pki/cp-cps

It is also available on the intranet (access limited to Bundesbank employees as well as external employees of this institution).

2.2 Publication of Certification Information

The Bundesbank publishes the following information.

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

2.3 Time or Frequency of Publication

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

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

2.4 Access Controls on Repositories

See CP for Authentication Certificates - Advanced -.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

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

The DN generally follows the structure below:

Certificates of Root-CA

CN	**Bundesbank Root CA 2017 Advanced**
E	pki@bundesbank.de
OU	Bundesbank PKI
O	Bundesbank
C	DE

Certificates of Sub-CAs

CN	**CA for User Authentication Advanced 2017**
E	pki@Bundesbank.de
OU	Bundesbank PKI
O	Bundesbank
C	DE
CN	**CA for User Authentication Advanced 2020**
E	pki@Bundesbank.de
OU	Bundesbank PKI
O	Bundesbank
C	DE

Certificates for advanced authentication

CN	<First name Surname>
OU	<Organisational unit>
DC	<Domain Component>

Based on the Active Directory it is not possible that the same CN is used several times.

The DN does not contain organization (O) or country (C) attributes because the certificates will be for internal employees only.

3.1.2 Need for Names to be Meaningful

See CP for Authentication Certificates - Advanced -.

3.1.3 Anonymity or Pseudonymity of Subscribers

See CP for Authentication Certificates - Advanced -.

3.1.4 Rules for Interpreting Various Name Forms

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

Certificates for advanced authentication contain the User Principal Name of subscriber in subjekt alternative name field.

3.1.5 Uniqueness of Names

Any Names (CNs and UPN) are unique within the Active Directory of the Deutsche Bundesbank.

3.1.6 Recognition, Authentication, and Role of Trademarks

See CP for Authentication Certificates - Advanced -.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

When the subscriber receives a secure smartcard, the Deutsche Bundesbank identity card, a certificate request is generated. This has to be done in presence of the user (and his id-card). Within this procedure the private key is generated in the chip of the smartcard and the user set his PIN. The user gives evidence to be the owner of the secure smartcard by the valid PKCS#10 request which is only possible by knowing the PIN.

3.2.2 Authentication of Organization Identity

See CP for Authentication Certificates - Advanced -.

3.2.3 Authentication of Individual Identity

Authentication of identity of subscibers (listet in point 1.3.3) is always a face-to-face process to get a Deutsche Bundesbank identity card with an user-based certificate for user authentication:

- Any (new) employee has to identifiy himself at the HR department by ID card (passport) to get a new Deutsche Bundesbank identity card. The process is undertaken by natural persons only.
    - Photo will be taken
    - Bundesbank id-card will be printed, including photo using an internal IT-System, handled by natural persons
    - The new employee (see point 1.3.3) has to write an acknowledgement for receiving his id-card
- The responsible person at the business area of the new employee requests a unique user-id. For doing so, a personalised workflow is used, involving natural persons only
- IT department creates unique user-information (CN and UPN) in Active Directory (User Provisioning Group); without an identity within the AD no certificate will be created. The user information are created by natural persons only

- The card issuing authority, represented by natural persons as well is cross checking the identity of the empolyee using the Bundesbank id-card (face-to-face).
- Officers of the card issuing authority can only access the system in their assigned roles using their own id-card.
- The card issuing authority is generating the certificate in presence of the employee
- The employee has to assign his PIN personally
- The employee receives an internal E-Mail to get proof of the act
- The Bundesbank ID-card is being activated checking that there will only exist one valid ID-card per employee
- Handover of the Bundesbank ID-Card is documented in an acknowledgement-paper, which finalises the whole workflow and guarantees the activation of card and certificate. The handling of the Bundesbank id-card (usage, how to handle with lost or stolen cards, etc.) is regulated in internal terms and conditions. This ruleset has the nature of a policy and, therefore is mandatory for all subscriber (see point 1.3.3).
- Employees address is stored as private data in the HR application only.
- Employees department and work phone numbers are stored in the active directory and collaboration services and can be accessed by every operator.

3.2.4 Non-verified Subscriber Information

See CP for Authentication Certificates - Advanced -.

3.2.5 Validation of Authority

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

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

a) The person is determined by the HR system and
b) The person possesses an AD-account.

3.2.6 Criteria for Interoperation

See CP for Authentication Certificates - Advanced -.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

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

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

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

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

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

3.3.2 Identification and Authentication for Re-key after Revocation

See CP for Authentication Certificates - Advanced-.

3.4 Identification and Authentication for Revocation Request

In order to avoid delay in disabling compromised credentials a suspension request can be made by the subscriber, someone appointed by the subscriber as well as his/her superior either using the electronic application workflow, by telephone as well as by fax or in writing. If an employee is not longer working for Deutsche Bundesbank, the revocation is mandated by HR.

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

The issuance of a temporary Deutsche Bundesbank identity card (with temporary certificate) by a subscriber leads to a suspension of the original (standard) identity card (respectively the certificate). The subscriber has to identify himself by showing an official document containing a photo. The photo is shown to issuer while picking the identity of the requesting user as well by the card issuing authority software. The subscriber gets information via e-mail that a temporary identity card is issued and the standard identity card (respectively the certificate) is suspended.

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

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

All certificate applications are issued through registration authorites and cannot be requested directly by an end-entity.

4.1.2 Enrollment Process and Responsibilities

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

Enduser certificates will be generated on a secure smartcard, the Deutsche Bundesbank identity card, in a four-eye principle with the presence of the subscriber. The management of the identity cards is realized by the human resources department. The name and the photo of the subscriber is printed on the card.

The initialisation of the crypto chip and the generation of key material are controlled by the Card Management System. To perform these actions it is necessary that the Production Officer is logged on the Card Management System with its own identity card.

Responsibilities of subscribers were part of general instruction for safe and correct use of the standard Deutsche Bundesbank standard IT equipment, they were published in the intranet of BBk.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Subscribers are identified and authenticated as described in section 3.2.

The interface between the Card Managament System and the CA (on the HSM) is authenticated with certificates.

4.2.2 Approval or Rejection of Certificate Applications

The formal attestations for a subscriber to get a certificate:

a) Preparation of the identity card (with photo on it)
b) Optical identification (by HR) of the subscriber, or processed in case of self-service renewal Workflow.
c) Electronic workflow in the Card Management System

Without these three points it is not possible to get a certificate.

4.2.3 Time to Process Certificate Applications

The issuance of a certificate is realized online without a delay.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The subscribers will be notified by the Card Managament System. This notification will be done via email.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Receiving the certificate is integrated into a workflow which:

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

Completion of this workflow by the user constitutes acceptance of the certificate(s).

4.4.2 Publication of the Certificate by the CA

See CP for Authentication Certificates - Advanced -.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

See CP for Authentication Certificates - Advanced -.

4.5 Key Pair and Certificate Usage

The crypto-API of Bundesbank identity card is MS-CAPI and PKCS#11.

4.5.1 Subscriber Private Key and Certificate Usage

See CP for Authentication Certificates - Advanced -.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties are IT systems and/or IT processes which use the certificate only for the purposes stated therein. The relying party also checks the validity period of the certificate.

Applications in which certificates are to be used must be compatible with the interfaces specified in point 4.5.

4.6 Certificate Renewal

See CP for Authentication Certificates - Advanced -.

4.7 Certificate Re-key

See CP for Authentication Certificates - Advanced -.

4.8 Certificate Modification

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

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

See CP for Authentication Certificates - Advanced -.

4.9.2 Who Can Request Revocation

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

4.9.3 Procedure for Revocation Request

The suspensions and revocations are realized as automatic processes in the Card Management System.

The suspension process can be triggerd by on of the folloing actions:

- Loss or damage of identity card. In this case, the certificates will be taken out of service by suspension, but a final blocking will only take place during the creation of a new card.
- Identity card is temporarily unavailable.

In both cases employee user is provided with a time-limited ID-Card after authenticating against an operator of the card issuing authorty.

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

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

4.9.4 Revocation Request Grace Period

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

4.9.5 Time within Which CA Must Process the Revocation Request

The CA must process the revocation request within one hour. In this interval a new CRL will be published. Of course, the same time is guilty for the suspension request.

4.9.6 Revocation Checking Requirement for Relying Parties

See CP for Authentication Certificates - Advanced -.

4.9.7 CRL Issuance Frequency

The basic CRL will be generated every 12 hours with a lifetime of 24 hours. The delta CRL will be generated every 30 minutes.

4.9.8 Maximum Latency for CRLs

See CP for Authentication Certificates - Advanced -.

4.9.9 Online revocation/status checking availability

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

4.9.10 Online Revocation checking Requirements

See CP for Authentication Certificates - Advanced -.

4.9.11 Other Forms of Revocation Advertisements available

See CP for Authentication Certificates - Advanced -.

4.9.12 Special Requirements Re-key Compromise

See CP for Authentication Certificates - Advanced -.

4.9.13 Circumstances for Suspension

See CP for Authentication Certificates - Advanced -.

4.9.14 Who can Request Suspension

See CP for Authentication Certificates - Advanced -.

4.9.15 Procedure for Suspension Request

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

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

4.9.16 Limits on Suspension Period

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

4.10 Certificate Status Services

See CP for Authentication Certificates - Advanced -.

4.11 End of Subscription

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

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

4.12 Key Escrow and Recovery

See CP for Authentication Certificates - Advanced -.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

The CA has implemented appropriate physical security controls to restrict access to CA hardware and software, including the servers, workstations, and any cryptographic hardware modules, used in connection with providing CA services.

The CA limits access to hardware and software to those personnel performing in a trusted role.

The CA components are operated in a secure environment, only trusted and authorized staff can access these components.

The components of the RA are operated by the Deutsche Bundesbank IT department under the terms of its general regulations and policies.

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.

5.1.2 Physical Access

See 5.1.1 and CP for Authentication Certificates - Advanced -.

5.1.3 Power and Air Conditioning

See 5.1.1 and CP for Authentication Certificates - Advanced -.

5.1.4 Water Exposures

See 5.1.1 and CP for Authentication Certificates - Advanced -.

5.1.5 Fire Prevention and Protection

See 5.1.1 and CP for Authentication Certificates - Advanced -.

5.1.6 Media Storage

See 5.1.1 and CP for Authentication Certificates - Advanced -.

5.1.7 Waste Disposal

See 5.1.1 and CP for Authentication Certificates - Advanced -.

5.1.8 Off-Site Backup

See 5.1.1 and CP for Authentication Certificates - Advanced -.

5.2 Procedural Controls

5.2.1 Trusted Roles

Generally, the CA and Card Management System support five trusted roles:

1. PKI Administrator authorized to install, configure and maintain the CA trustworthy systems for registration, certificate generation and revocation management.
2. CA Certificate-Manager
   Operation of certificate revocation and certificate request approval. Certificate and CRL issuance on offline certificate authorities.
3. HSM Adminstrator
   Responsible for HSM Administration, Backup, Recovery, Clustermanagemt
4. (System-) Auditor
   Audit of all PKI Components
5. Agent for Registration
   Registration of certificates and revocation requests as a service of the card issuing authority. The card issuing authority is always the HR department.

It is not possible for a person to be a member of more than one trusted role.

5.2.2 Number of Persons Required per Task

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

5.2.3 Identification and Authentication for Each Role

See CP for Authentication Certificates - Advanced -.

5.2.4 Roles Requiring Separation of Duties

The CA cryptographic operations are protected by HSMs. For sensitive key operations at least three employees of different IT-departments are necessary. As written in 5.2.1, there is always just one trusted role to a dedicated employee.

5.3 Personnel Controls

See CP for Authentication Certificates - Advanced -.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

See CP for Authentication Certificates - Advanced -.

5.4.2 Frequency of Processing Log

See CP for Authentication Certificates - Advanced -.

5.4.3 Retention Period for Audit Log

See CP for Authentication Certificates - Advanced -.

5.4.4 Protection of Audit Log

Audit logs are protected in such a way that confidentiality and integrity is guaranteed and unauthorized access is prevented.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

See CP for Authentication Certificates - Advanced -.

5.4.7 Notification to Event-Causing Subject

See CP for Authentication Certificates - Advanced -.

5.4.8 Vulnerability Assessments

See CP for Authentication Certificates - Advanced -.

5.5 Records Archival

See CP for Authentication Certificates - Advanced -.

5.6 Key Changeover

The Key changeover for the CA key pairs are timed according to the maximum key lifetimes and renewal periods set out in the CP for Authentication Certificates – Advanced - .

The CA key changeover process is designed that:

- It is guaranteed at all times that the CA’s certificate lifetime encompasses all lifetimes of certificates, which are subordinate to it in the hierarchy.
- 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.
- At the latest from the point in time where the CA’s key pair remaining lifetime equals the subordinate certificate’s validity period will all vertificates be signed by the new CA key pair.
- 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 for Authentication Certificates - Advanced -.

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

See CP for Authentication Certificates - Advanced -.

5.7.3 Entity Private key compromise Procedures

See CP for Authentication Certificates - Advanced -.

5.7.4 Business Continuity capabilities after a Disaster

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

5.8 CA or RA Termination

See CP for Authentication Certificates - Advanced -.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Subscribers' private key will be generated on the crypto module in the smartcard (Deutsche Bundesbank identity card).

6.1.2 Private Key Delivery to Subscriber

The private key never leaves the Deutsche Bundesbank identity card.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

See CP for Authentication Certificates - Advanced -.

6.1.5 Key Sizes

See CP for Authentication Certificates - Advanced -.

6.1.6 Public Key Parameters Generation and Quality Checking

See CP for Authentication Certificates - Advanced -.

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

See CP for Authentication Certificates - Advanced -.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

See CP for Authentication Certificates - Advanced -.

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

See CP for Authentication Certificates - Advanced -.

6.2.3 Private Key Escrow

See CP for Authentication Certificates - Advanced -.

6.2.4 Private Key Backup

See CP for Authentication Certificates - Advanced -.

6.2.5 Private Key Archive

See CP for Authentication Certificates - Advanced -.

6.2.6 Private Key Transfer into or from a Cryptographic Module

See CP for Authentication Certificates - Advanced -.

6.2.7 Private Key Storage on Cryptographic Module

See CP for Authentication Certificates - Advanced -.

6.2.8 Method of Activating Private Key

See CP for Authentication Certificates - Advanced -.

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 of the smartcard after suspension because of wrong PIN is realized by the challenge and response technique. The process is as follows:

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

6.2.10 Method of Destroying Private key

See CP for Authentication Certificates - Advanced -.

6.2.11 Cryptographic Module Rating

See CP for Authentication Certificates - Advanced -.

6.3 Other Aspects of Key Pair Management

See CP for Authentication Certificates - Advanced -.

6.4 Activation Data

See CP for Authentication Certificates - Advanced -.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Certification Authorities and HSM were operated in the data center.

Access is limited physically to Data Center, limited to trusted Roles and Persons. For accessing the datacenter biometrics are used as well as video surveillance. Every access is documented. Only persons with a dedicated security clearance are allowed to enter.
Within the Datacenter network the Area concept for network segregation ensures only valid and secure commincation.
Within Bundesbank's network the SubCA is placed inside a dedicated DMZ. Only CMS (Card Management System) and RA-Systems are allowed to connect to it using safe and encrypted protocols ensuring high level encrytion algorythms and ciphers.
Authentication of each stakeholder is done by certificate, presented to CMS. Every event is logged.
An authorisation concept ensures the need-to-know principle, which means that every role is only allowed to access information, which is necessary (e.g. the card issuer are allowed to undertake request, but nobody else).

6.5.2 Computer Security Rating

See CP for Authentication Certificates - Advanced -.

6.6 Life Cycle Technical Controls

See CP for Authentication Certificates - Advanced -.

6.7 Network Security Controls

See CP for Authentication Certificates - Advanced -.

6.8 Time-Stamping

See CP for Authentication Certificates - Advanced -.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

See CP for Authentication Certificates - Advanced -.

7.1.2 Certificate Extensions

CA certificates have the following extensions.

Extension	Possible Values	Critical Flag
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing	yes
Basic Constraints	Subject Type=CA Path Length Constraint=0	yes
Subject Key Identifies	Unique number corresponding to the subject's public key.	no
Authority Key Identifier	Unique number corresponding to the authority`s public key.	no
CRL Distribution Point	Contains a HTTP URL to obtain the current CRL	no
Certificate Issuance Policies	OID + internal and external URL link	no

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

User certificates have the following extensions.

Extension	Possible Values	Critical Flag
Key Usage	Digital Signature, Key Encipherment	yes
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	yes
Extended Key Usage	Smart Card Logon Client Authentication	no
Subject Key Identifies	Unique number corresponding to the end-entities public key.	no
Authority Key Identifier	Unique number corresponding to the authority`s public key.	no
CRL Distribution Point	Contains a HTTP URL to obtain the current CRL	no
Certificate Issuance Policies	OID + external URL link	no
Subject Alternative Name	E-mail address	no

7.1.3 Algorithm Object Identifiers

See CP for Authentication Certificates - Advanced -.

7.1.4 Name Forms

See 3.1.1 and CP for Authentication Certificates - Advanced -.

7.1.5 Name Constraints

See CP for Authentication Certificates - Advanced -.

7.1.6 Certificate Policy Object Identifier

The certificate policy OID of the CP for Authentication Certificates - Advanced - is:
1.3.6.1.4.1.2025.590.10.1.1

7.1.7 Usage of Policy Constraints Extension

See CP for Authentication Certificates - Advanced -.

7.1.8 Policy Qualifiers Syntax and Semantics

See CP for Authentication Certificates - Advanced -.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

See CP for Authentication Certificates - Advanced -.

7.2 CRL Profile

See CP for Authentication Certificates - Advanced -.

7.2.1 Version Number(s)

Version 2

7.2.2 Signature Algorithm

sha256RSA
(OID: 1.2.840.113549.1.1.11)

7.2.3 Issuer

DN of Issuer Certificate

7.2.4 This Update

Date of creation

7.2.5 NextUpdate

Date of expirrary

7.2.6 CRL Entries

List of revoked certifcates (serialnumbers)

7.2.7 Extensions

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

7.3 OCSP Profile

The OCSP URL is not published as a certifcate extension.

7.3.1 Version Number(s)

OCSP Version 1 is used. OCSP Responder correspondents to RFC 5019.

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	
nextUpdate	Time OCSP response ends to be valid	

8 Compliance Audit and Other Assessments

See CP for Authentication Certificates - Advanced -.

9 Other Business and Legal Matters

See CP for Authentication Certificates - Advanced -.

.

10 Abbreviations

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
CMS	Card Management System
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
DC	Data centre
DN	Distinguished name
DName	Distinguished name
EBCA	European Bridge CA, link between individual organisations' public key infrastructures
EMAIL	E-mail address (part of the distinguished name)
FMSA	Financial Market Stabilisation Agency
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	Signature Act – Electronic signature law (Gesetz über Rahmenbedingungen für elektronische Signaturen)
S/MIME	Secure Multipurpose Internet Mail Extensions, standard for secure e-mail
SSL	Secure Socket Layer, protocol to ensure secure communication between a client and a server
SÜG	Security Clearance Act (Sicherheitsüberprüfungsgesetz)
x.500	Protocols and services for ISO compliant repositories
x.509v1	Certification standard