DEUTSCHE BUNDESBANK
EUROSYSTEM

Certificate Policy

Email Security Certificates

- Counterparties -

Version 1.0

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 Email Security Certificates (to be used for encryption and signature) for counterparties in the form of a Certificate Policy (CP).

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). The certificates issued by the Bundesbank's PKI meet the advanced signature requirements stipulated in the German electronic signature law (*Gesetz über Rahmenbedingungen für elektronische Signaturen* – SigG).

1.2 Document name and identification

Name:	Certificate Policy Email Security Certificates - Counterparties -
Version:	1.0
Date:	15 June 2016
OID:	1.3.6.1.4.1.2025.590.1.14

1.3 PKI participants

1.3.1 Certification authorities

The Bundesbank's PKI (BBk-PKI) uses a two-stage certification structure with a self-signed root certificate.

The root CA certificate certifies only subordinate specialist CAs. The CAs that are subordinate to the root CA are used to create user certificates.

1.3.2 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.

1.3.3 Subscribers

Subscribers are

- Counterparties of the Bundesbank, as well as
- Counterparties of the Financial Market Stabilisation Agency (FMSA).

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).

1.3.4 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 and/or the FMSA.

1.3.5 Other participants

Other participants may be service providers (eg directory service operators) appointed by the BBk-PKI.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The certificates issued may only be used for the encryption and signing of emails in connection with the Bundesbank's/FMSA's business activities.

1.4.2 Prohibited certificate uses

The private use of certificates is prohibited.

Counterparties may not use the certificates in connection with business activities with third parties for any other purpose than specified in point 1.4.1 without the BBk-PKI's approval.

1.5 Policy administration

1.5.1 Organisation administering the document

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

1.5.2 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 3815/3257/2351
Fax +49 69 709094 9922
Email: pki@bundesbank.de

1.5.3 Person determining CPS suitability for the policy

This CP is checked by the system owner of the BBk-PKI.

The BBk-PKI system owner checks that each CPS complies with the provisions of the respective CP.

1.5.4 CPS approval procedures

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

It is possible to pass on this documentation to other organisations to allow an independent review of the functioning of the BBk-PKI.

1.6 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 ► Services for banks an companies ► PKI
- or at this direct link http://www.bundesbank.de/Navigation/EN/Service/Services_for_banks_and_companies/PKI/pki.html?nsc=true

It is also available on the intranet (access limited to Bundesbank and FMSA employees as well as external employees of these institutions).

2.2 Publication of certification information

The Bundesbank publishes the following information.

- CA certificates with fingerprints
- Root 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 CP and CPS 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

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

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.

3.1.5 Uniqueness of names

The BBk-PKI ensures that the names and email attributes are unique. Furthermore, each certificate is given a unique serial number enabling it to be uniquely and permanently allocated to a subscriber.

3.1.6 Recognition, authentication and role of trademarks

When applying for certificates for counterparties, only those brands or trademarks may be used as part of the certificate entry for the company or authority given on the application form which the company or authority is authorised to use. However, this authorisation is not verified at the registration stage.

Generally speaking, the BBk-PKI 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. If the BBk-PKI is presented with a legally binding judgement declaring the wrongful use of a brand or trademark, the certificate will be revoked.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The key pairs for the CAs and the subscribers are generated exclusively by the BBk-PKI.

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 or of the FMSA 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

This check 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 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/FMSA 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

The applicant's identity is documented in the event of a revocation request. 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/FMSA employees via an electronic application workflow, which, after being approved by the direct supervisor of the Bundesbank/FMSA 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 occurs as part of a multistage registration process and is sent to the BBk-PKI. The following checks are made.

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

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

The issuance of a certificate does not constitute an entitlement even if the formal requirements have been met. The decision to issue certificates is entirely at the BBk-PKI's discretion.

4.2.3 Time to process certificate applications

As a rule, a maximum of one week is needed to process certificate applications.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

4.3.2 Notification to subscriber by the CA of issuance of certificate

After the certificate has been created, the BBk-PKI sends it to the subscriber in a secure manner.

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

It is possible that the certificate will 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.

The subscriber is responsible for the following actions.

- To give immediate notification if the information in the certificate is not or is no longer correct.
- To adhere to the restrictions with regard to use of the private key (see point 1.4.1).
- To arrange for immediate revocation of the certificate if the private key is compromised or if the certificate is no longer required (see chapter 4.9).

4.5.2 Relying party public key and certificate usage

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

4.6 Certificate renewal

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

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). Thus the following points are not applicable.

4.8 Certificate modification

In the case of the BBk-PKI, 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

The following circumstances require certificate modification with a new key pair and data modification.

- Routine certificate modification
  - if the validity of the certificate is about to expire or
  - has just expired.
- Certificate application after a previous certificate has been revoked.
- Information on the certificate is no longer correct.
- 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.

4.8.2 Who may request certificate modification?

In case of certificates for counterparties, the application for certificate modification is initiated by Bundesbank/FMSA employees.

If a certificate modification is required ad hoc as a result of security issues relating to key sizes, validity periods or certificate structure, the BBk-PKI modifies the certificate without having received an application. The subscriber is notified of any ad hoc certificate modifications.

4.8.3 Processing certificate modification requests

The certificate modification process is the same as the initial application process. The key pair is created in the BBk-PKI's secure area in line with the dual control principle and the certificate is generated.

4.8.4 Notification of new certificate issuance to subscriber

After the certificate has been created, the BBk-PKI sends it to the subscriber in a secure manner.

4.8.5 Conduct constituting acceptance of modified certificate

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

4.8.6 Publication of the modified certificate by the CA

It is possible that the certificate will be published in a directory service.

4.8.7 Notification of certificate issuance by the CA to other entities

No other entities require notification.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate has to 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.
- 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 this CP / CPS (see point 4.5).
- The BBk-PKI ceases to be a CA. In this case, all certificates issued by the BBk-PKI would be revoked.
- The private key of the issuing or of a superordinated root CA has been compromised. In this case, all certificates issued by this CA would be revoked.
- The algorithms, key sizes or validity periods of the certificate no longer provide sufficient security. The BBk-PKI reserves the right to revoke the certificates in question.

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 that 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.

A user may request revocation at any time, even if none of the circumstances specified in section 4.9.1 apply.

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

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

4.9.5 Time within which CA must process the revocation request

The BBk-PKI revokes the certificate as soon as it has received the revocation request.

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 check the validity of certificates.

4.9.7 CRL issuance frequency

CA CRLs are issued with a validity period of 30 days; root CA CRLs with a validity period of 180 days. A new list is issued one week prior to expiry of the most recent CRL.

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

CRLs are published as soon as they have been created.

4.9.9 On-line revocation/status checking availability

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

4.9.10 On-line revocation checking requirements

Not applicable

4.9.11 Other forms of revocation advertisements available

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

4.9.12 Special requirements re-key compromise

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

4.9.13 Circumstances for suspension

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

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

4.11 End of subscription

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

4.12 Key escrow and recovery

It is technically possible for the BBk-PKI to provide key escrow and recovery services, however, it does not currently do so.

5 Facility, management and operational controls

Detailed information can be found in the respective CPSs.

6 Technical security controls

Detailed information can be found in the respective CPSs.

7 Certificate, CRL and OCSP profiles

Detailed Information can be found in the respective CPSs.

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 checks.

The technical framework and operational processes of the PKI undergo a regular internal audit pursuant to the Bundesbank's regulations for such procedures. The audit results are not published.

8.1 Frequency or circumstances of assessment

As a rule, internal audits and assessments are conducted at regular intervals.

8.2 Identity/qualifications of assessor

Internal audits are conducted by the Audit Department, the system owner and BBk-PKI's management. The assessors 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

Assessors may not be involved in the BBk-PKI's production process. Self-assessment is prohibited.

8.4 Topics covered by assessment

All topics relevant to the PKI can be assessed. The topics covered in the assessment are at the discretion of the assessor.

8.5 Actions taken as a result of deficiency

If any deficiencies are determined, these have to be corrected as quickly as possible by the CA in consultation with the assessor. The assessor has to be informed when these deficiencies have been corrected.

8.6 Communication of results

It is not planned to communicate the results of the assessment.

9 Other business and legal matters

9.1 Fees

No fees will be charged.

9.2 Financial responsibility

Risks that may incur the liability of the CA are covered by Deutsche Bundesbank.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All information and data about BBk-PKI 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 explicitly (eg email addresses) or implicitly (eg data about certification) contained in or that can be derived from certificates and CRLs that are published are not considered confidential.

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of personal information

9.4.1 Privacy plan

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

9.4.2 Information treated as private

All information about BBk-PKI subscribers and participants is treated as private.

9.4.3 Information not deemed private

The provisions defined in point 9.3.2 apply.

9.4.4 Responsibility to protect private information

The responsibility to protect private information lies with the BBk-PKI.

9.4.5 Notice and consent to use private information

The subscriber gives the BBk-PKI consent to use private information as far as this is required for it to render its services. In addition, all information that is not deemed private may be published.

9.4.6 Disclosure pursuant to judicial or administrative process

The BBk-PKI stores and processes private information as stipulated in legal data protection provisions. Such information is disclosed to government entities only if corresponding decisions 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 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 undertakes to follow the provisions of this CP.

9.6.2 RA representations and warranties

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

9.6.3 Subscriber representations and warranties

The subscriber’s representations and warranties are defined in point 4.5.1.

9.6.4 Relying party representations and warranties

The relying party’s representations and warranties are defined in point 4.5.2. s/he also has to follow his/her organisation’s certificate guidelines.

9.6.5 Representations and warranties of other participants

Any service providers (eg providers of directory services) appointed by the BBk-PKI must undertake to comply with this CP.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

If, when implementing the agreement, the Bundesbank violates through fault of its own 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 shall be limited to damages characteristic for the type of agreement in question.

The Bundesbank shall only be 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 shall also apply to gross negligence committed by vicarious agents.

The exclusion or limitation of liability specified above shall not apply to liability for damages resulting from injury to life, body or health; in such cases the Bundesbank shall be 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 Bundesbank is released from liability.

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

This document is valid until it is replaced with a new version or until BBk-PKI operations are terminated.

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

No regulations in this respect have been made in this CP.

9.12 Amendments

9.12.1 Procedure for amendment

Changes to the CP are published in good time before they enter into force.

9.12.2 Notification mechanism and period

Subscribers receive a signed email notifying them of changes to the CP in good time before they enter into force.

The consent of employees of authorised Bundesbank and FMSA counterparties to the changes will be assumed unless the BBk-PKI receives declaration to the contrary in a digitally signed email before they enter into force. The BBk-PKI will draw special attention to this consequence when announcing changes.

9.12.3 Circumstances under which OID must be changed

The OID does not change before the end of the CA’s period of validity.

9.13 Dispute resolution provisions

It is at the Bundesbank’s discretion whether an affair is submitted to arbitration.

9.14 Governing law

The place of jurisdiction is Frankfurt am Main.

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

All regulations in this CP are valid between the BBk-PKI 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

It is not planned to assign 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 (attorneys' fees and waiver of rights)

Any legal disputes arising from the BBk-PKI'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 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

BBk	Deutsche Bundesbank
BBk-PKI	Deutsche Bundesbank's PKI
BSI	Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnologie*)
C	Country (part of the distinguished name)
CA	Certification Authority
Certificate	Secure assignment of public keys to a subscriber
CN	Common name (part of the distinguished name)
CP	Certificate Policy of a PKI
CPS	Certification Practice Statement
CRL	Certificate Revocation List; signed list belonging to a CA that contains revoked certificates
CRLDP	CRL distribution point
DN	Distinguished name
DName	Distinguished name
EBCA	*European Bridge CA*, link between individual organisations' public key infrastructures
EMAIL	Email 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-1	Secure Hash Algorithm No 1

SigG	Signature Act – Electronic signature law (*Gesetz über Rahmenbedingungen für elektronische Signaturen*)
S/MIME	Secure Multipurpose Internet Mail Extensions, standard for secure email
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

11 Information regarding the document

See point 1.2.