DEUTSCHE BUNDESBANK EUROSYSTEM

Certification Practice Statement

CA for Email Security

Version 2.1

1 Introduction

1.1 Overview

This document provides both users and the Deutsche Bundesbank – as the Public Key Infrastructure (PKI) operator – with a summary of the binding contents of the Bundesbank's security and certification concept for the live operation of the Certification Authority (CA) for Email Security in the form of a Certification Practice Statement (CPS).

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:	Certification Practice Statement (CPS) CA for Email Security
Version:	2.1
Date:	1 April 2014
OID:	1.3.6.1.4.1.2025.590.2.2

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 CAs for different purposes. The sub CA for Email Security is 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

- Bundesbank employees,
- Employees of the Financial Market Stabilisation Agency (FMSA),
- External employees of these institutions, where applicable, as well as
- Counterparties, where applicable.

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

See CP for Email Security Certificates.

1.4.2 Prohibited certificate uses

See CP for Email Security Certificates.

1.5 Policy administration

1.5.1 Organisation administering the document

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

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 +49 211 874 2874
Email: pki@bundesbank.de

1.5.3 Person determining CPS suitability for the policy

This CPS 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 CP for Email Security Certificates.

1.5.4 CPS approval procedures

This CPS 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 CA for Email Security for 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 CA for Email Security on its website [German only]

- http://www.bundesbank.de under Service ► Service für Banken und Unternehmen ► PKI
- or at this direct link http://www.bundesbank.de/Navigation/DE/Service/Services_Banken_und_Unternehmen/PKI/pki.html

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 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

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

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

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

The DN generally follows the structure below.

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

3.1.2 Need for names to be meaningful

The name of the certificate issued (DN) has to uniquely identify the subscriber. The following rules apply.

- Certificates for natural persons are to be issued in the subscriber's name.
- Certificates for people grouped according to organisation/function or for an organisation's email address have to be clearly distinguishable from certificates for natural persons.

3.1.3 Anonymity or pseudonymity of subscribers

See CP for Email Security Certificates.

3.1.4 Rules for interpreting various name forms

The DN is based on the x.509 standard. Furthermore, the Bundesbank's Lotus Notes/Domino naming conventions apply.

3.1.5 Uniqueness of names

See CP for Email Security Certificates.

3.1.6 Recognition, authentication and role of trademarks

See CP for Email Security Certificates.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

See CP for Email Security Certificates.

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

As a rule, all Bundesbank and FMSA employees as well as the external employees of these institutions are registered personally (face-to-face) by the respective HR departments.

The registration process to use certificates for the Email Security entails a number of stages and is conducted by means of an electronic application workflow, which is approved by the relevant department and sent to the BBk-PKI.

When applying for a certificate for a counterparty, employees of an authorised counterparty of the Bundesbank or the FMSA are identified personally (face-to-face) in accordance with the process agreed on with the counterparty and by means of a copy of the counterparty's official photo ID, which is passed on to the BBk-PKI.

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of authority

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

3.2.6 Criteria for interoperation

See CP for Email Security Certificates.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Before the validity of a certificate expires, the subscriber receives several re-key requests.

The identification and authentication process entails a number of stages and is conducted by means of an electronic application workflow that is largely identical to the initial application process.

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

A revocation request can be made by the subscriber, someone appointed by the subscriber as well as his/her superior either using the electronic application workflow, by telephone as well as by fax or in writing.

The applicant’s identity is documented. The BBk-PKI operating unit reserves the right to check the identity of the applicant as appropriate but is not required to do so. The subscriber is informed that the certificate has been revoked.

4 Certificate life cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application?

Those subscribers listed in point 1.3.3 can submit a certificate application.

4.1.2 Enrolment process and responsibilities

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

When applying for a certificate, the applicant explicitly recognises the validity of the CPS of the issuing CA.

See also CP for Email Security Certificates.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Subscribers are identified and authenticated as described in chapter 3.2.

4.2.2 Approval or rejection of certificate applications

See CP for Email Security Certificates.

4.2.3 Time to process certificate applications

See CP for Email Security Certificates.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

The delivery occurs as a software certificate. For the Bundesbank and FMSA employees as well as the external employees of these institutions the certificates are hosted in a secure way on the Email Security Gateway System of the Bundesbank. For employees of an authorised counterparty of the Bundesbank or the FMSA, delivery is effected on a hand-delivered basis with confirmation of receipt or via a secure electronic procedure.

4.3.2 Notification to subscriber by the CA of issuance of certificate

See CP for Email Security Certificates.

4.4 Certificate acceptance

See CP for Email Security Certificates.

4.5 Key pair and certificate usage

See CP for Email Security Certificates.

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.

4.7 Certificate re-key

When a certificate is renewed, a new key pair is always generated. The certificate is always modified (see chapter 4.8).

4.8 Certificate modification

In the case of the CA for Email Security, a certificate is modified on the basis of an application and involves changing the key pair and modifying the content of the certificate as well as the technical parameters.

4.8.1 Circumstance for certificate modification

See CP for Email Security Certificates.

4.8.2 Who may request certificate modification?

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

See CP for Email Security Certificates.

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

See CP for Email Security Certificates.

4.8.5 Conduct constituting acceptance of modified certificate

See CP for Email Security Certificates.

4.8.6 Publication of the modified certificate by the CA

See CP for Email Security Certificates.

4.8.7 Notification of certificate issuance by the CA to other entities

See CP for Email Security Certificates.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

See CP for Email Security Certificates.

4.9.2 Who can request revocation?

See CP for Email Security Certificates.

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.

The published CRLs contain all the certificates that were revoked up until the validation end date of the respective CA.

4.9.4 Revocation request grace period

See CP for Email Security Certificates.

4.9.5 Time within which CA must process the revocation request

See CP for Email Security Certificates.

4.9.6 Revocation checking requirement for relying parties

See CP for Email Security 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.

4.9.8 Maximum latency for CRLs

See CP for Email Security Certificates.

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

See CP for Email Security Certificates.

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

5.1 Physical controls

5.1.1 Site location and construction

The CA for Email Security is operated from within an access-protected area and has a separate secure area. In addition, it has a number of vaults to store production and backup systems and media.

Both the secure area and the vaults are connected to the building's central master alarm terminal. In addition, the secure area is connected to a local optical and acoustic alarm system.

5.1.2 Physical access

Physical access is via a multi-stage access control system. Only the PKI operating personnel that work in the BBk-PKI’s secure area have access. Access is via an ID-based login.

5.1.3 Power and air conditioning

The power supply meets the required standards. An emergency power supply via diesel generators is in place. The secure area is air conditioned.

5.1.4 Water exposures

The rooms have adequate protection from exposure to water.

5.1.5 Fire prevention and protection

Fire prevention and protection regulations have been met. The rooms are connected to the fire alarm system via smoke alarms. There is an adequate number of hand-held fire extinguishers. An INERGEN fire suppression system is installed in the floor.

5.1.6 Media storage

All data media with software and all daily backups are kept in multiple copies as original and backup versions and are stored securely in different sections of the building. In addition, all software no longer in use as well as old data backups are stored in an archive.

All data media are kept in multi-level, application-specific steel boxes which are securely stored in safes which are placed in vaults.

5.1.7 Waste disposal

Electronic data media are destroyed and disposed of on site in an appropriate manner. Paper data media are shredded and disposed of on site in an appropriate manner.

5.1.8 Off-site backup

There is no off-site data backup at service providers external to the BBk-PKI.

5.2 Procedural controls

5.2.1 Trusted roles

Trusted roles are established to ensure that individuals are not able to change any of the BBk-PKI's security-critical components or view, generate or manipulate certificates or private keys without being noticed. The names of the people involved in generating and delivering keys and certificates are logged.

5.2.2 Number of persons required per task

In live operations, the BBk-PKI applies a dual control principle as standard for the use of highly security-critical access media, cryptographic key materials and certificates.

This ensures that the storage, access to and use of highly secure access media by PKI operating staff is always subject to the dual control principle. In addition, the entire process of generating cryptographic key material and certificates up to the stage where they are passed on is also subject to the dual control principle. Using the dual control principle as standard requires the roles of those people involved in the generation process to be documented in various logs that are to be created or generated by the system (see point 5.2.1).

5.2.3 Identification and authentication for each role

The role concept is implemented using a number of technical and organisational measures. Roles are identified and authenticated when accessing

- the secure areas and vaults
- secure storage or security-critical systems and applications

by using SmartCards, hardware tokens, user IDs and passwords.

The roles are documented in various logs that are to be created or generated by the system (see point 5.2.1).

5.2.4 Roles requiring separation of duties

By separating certain roles and duties, the concept ensures that no one person alone can generate a key or issue and pass on a certificate.

5.3 Personnel controls

5.3.1 Qualifications, experience and clearance requirements

In its operations, the BBk-PKI ensures that it uses experienced staff who have the necessary IT expertise and specific knowledge of CA operations.

5.3.2 Background check procedures

The Bundesbank subjects BBk-PKI staff to an advanced security check regarding sabotage protection in accordance with the Security Check Act (*Sicherheitsüberprüfungsgesetz* – SÜG).

5.3.3 Training requirements

Staff undertaking BBk-PKI operations receive regular and ad hoc training. They are made aware of the security relevance of their work.

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

PKI operations staff are deployed in all areas of CA operations.

5.3.6 Sanctions for unauthorised actions

Unauthorised actions that endanger the security of the BBk-PKI or breach data protection requirements are sanctioned/prosecuted via the HR department.

5.3.7 Independent contractor requirements

Not applicable

5.3.8 Documentation supplied to personnel

In order to ensure that they can conduct operations correctly, PKI staff receive the following documentation.

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

The following events are logged and recorded.

- System initialisation
- Certification applications
- User registration
- Key generation for the CA, root CA and users
- Certificate issuance for the CA, root CA and users
- Data backups for the CA and root CA
- Certification publication for the CA and root CA
- Delivery of private key and certificate
- Revocation requests
- Revocation of a certificate
- Drawing up of a CRL
- Publication of a CRL

Any malfunctions or one-off operating situations are also recorded.

5.4.2 Frequency of processing log

The Bundesbank's Controlling Department checks that certification operations are as they should be as part of its risk-oriented checks. If there is suspicion of irregularities, a more detailed check is scheduled.

5.4.3 Retention period for audit log

Retention periods are based on the times stipulated in law, audit compliance provisions as well as other internal rules and regulations.

5.4.4 Protection of audit log

The logs are protected against unauthorised access, manipulation and destruction.

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)

Not applicable

5.4.7 Notification to event-causing subject

If a security-critical event arises, the BBk-PKI notifies those responsible for IT security incidents as well as the system owner.

5.4.8 Vulnerability assessments

A vulnerability assessment can be conducted at any time if so required.

5.5 Records archival

5.5.1 Types of records archived

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

5.5.2 Retention period for archive

The retention periods are defined in point 5.3.4.

5.5.3 Protection of archive

The archives are protected against unauthorised access, manipulation and destruction.

5.5.4 Archive backup procedures

Data backups are made every day after the following have been completed.

- Keys issued
- Certificates revoked
- CRLs drawn up

They are kept as originals and backups and stored securely 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 BBk-PKI operating unit is responsible for the archive collection system.

5.5.7 Procedures to obtain and verify archive information

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

5.6 Key changeover

The CA changes the key at the latest when the validity of the 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 incident and compromise handling procedure.

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 is stopped immediately.

The system is reset using software and data backups, and – after checks to ensure that operations are secure – it is put back in operation. The faulty or modified system is analysed. If there is a suspicion of wilful action, legal action may be taken.

If certificates are generated with incorrect information, the subscriber is informed immediately and the CA revokes the certificate.

5.7.3 Entity private key compromise procedures

If an entity's private key is compromised, the corresponding certificate has to be revoked immediately. At the same time, all certificates issued by this entity are to be revoked. All subscribers affected are 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

After a disaster, reinstating a CA's operations is part of contingency planning and this can happen at short notice providing the BBk-PKI's operations are secure.

5.8 CA or RA termination

If the CA for Email Security operations is terminated, the following measures are taken.

- Notification of all subscribers as well as relying parties with a notice period 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 CA key pairs are generated in a cryptographically secure module in line with the dual control principle. The IT system runs offline without a network connection.

Subscribers' key pairs are generated centrally in the BBk-PKI's secure area offline using IT systems without a network connection and in line with the dual control principle.

6.1.2 Private key delivery to subscriber

The private key is delivered to the subscriber for use in a secure way.

6.1.3 Public key delivery to certificate issuer

Not applicable. There are no provisions for a subscriber to generate his/her own key.

6.1.4 CA public key delivery to relying parties

When a key pair is delivered, a certificate chain is also provided. The CA's public keys can also be called up via the certificate service outlined in chapter 2.

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 considers to be secure for a qualified electronic signature in accordance with the Signature Act.

The CA key of the CA/root CA 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 used.

- RSA with OID 1.2.840.113549.1.1.1
- SHA1 RSA 1.2.840.113549.1.1.5

6.1.7 Key usage purposes

The CA's private key is used only to sign certificates and CRLs.

6.2 Private key protection and cryptographic module engineering controls

Private keys are stored in a cryptographically secure manner.

6.2.1 Cryptographic module standards and controls

Cryptographic protection measures are based on international standards. Furthermore, the IT system is operated offline without a network connection and is stored in a vault out of office hours.

6.2.2 Private key (n out of m) multi-person control

The CA's private key is protected by the dual control principle.

6.2.3 Private key escrow

The CA's private key is not stored with third parties.

6.2.4 Private key backup

A cryptographically secure backup of the CA's private key is available. This backup is subject to the same protection measures as the production system. The dual control principle applies for access to this backup.

There is no backup for a subscriber's private key.

6.2.5 Private key archival

After a CA has expired or been revoked, the CA's private key is kept for ten years. This archive is subject to the same protection measures as the production system. The dual control principle applies for access to this archive.

6.2.6 Private key transfer into or from a cryptographic module

The CA's private key is transferred only for backup or restoration purposes. This process is subject to the same protection measures as the production system. The dual control principle applies for access to this process.

6.2.7 Private key storage on cryptographic module

The CA's key pair is stored in a cryptographically secure module.

6.2.8 Method of activating private key

The CA's private key can only be activated by means of the dual control principle.

The subscriber's private key is activated once receipt confirmation has been received or once the certificate is used for the first time.

6.2.9 Method of deactivating private key

A CA's private key is automatically deactivated once the certification process has come to an end.

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 kept for ten years and then destroyed. Storage media are destroyed or securely deleted.

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 BBk-PKI are archived in the CA's database.

6.3.2 Certificate operational periods and key pair usage periods

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

- Root CA certificates 8 years
- CA certificates 4 years
- User certificates 2 years

6.4 Activation data

The BBk-PKI protects access to the CA's and user's private key cryptographically and by means of the dual control principle.

6.4.1 Activation data generation and installation

Activation data are generated at the same time as the certificates. Non-trivial combinations of upper case, lower case, numbers and special characters are used for passwords and PINs. These must be at least ten characters long.

6.4.2 Activation data protection

Activation data are suitably protected from loss, theft, modification, unauthorised publication and unauthorised use.

6.4.3 Other aspects of activation data

Not applicable

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All of the BBk-PKI's IT systems must have an operating system with current security patches and a virus scanner. The BBk-PKI is operated offline. The operating system is on a read-only medium. Access control is deployed as a security measure.

6.5.2 Computer security rating

The security measures are in line with the latest technology. A threat analysis has been conducted and a security concept has been compiled.

6.6 Life cycle technical controls

6.6.1 System development controls

The system owner is involved in the system development of the BBk-PKI components. The software in use can withstand those threat scenarios that are commonly known.

6.6.2 Security management controls

The BBk-PKI operating staff have been informed of the application's high security requirements.

There are measures in place to ensure that system developers have no access to live operations and data.

All changes to the BBk-PKI are subject to an acceptance test.

6.6.3 Life cycle security controls

Any IT systems or components that are replaced are taken out of operation in such a way that the functions thereof and data contained therein cannot be misused. In addition, any changes to IT systems or components are logged in paper records.

6.7 Network security controls

The BBk-PKI is operated offline. Not applicable.

6.8 Time-stamping

Time-stamping is currently not available. Not applicable.

7 Certificate, CRL and OCSP profiles

7.1 Certificate profile

7.1.1 Version number(s)

The BBk-PKI issues certificates in line with the X509v3 standard.

7.1.2 Certificate extensions

CA certificates have the following extensions.

Key Usage	cert sign, crl sign – critical
Basic Constraints	CA=true, no constraints on length of path – critical
Subject Alt Name	Email address – not critical
Authority Key Identifier	160-bit SHA-1 hash of issuer's key
Subject Key Identifier	160-bit SHA-1 hash of issuer's key

User certificates have the following non-critical extensions.

Key Usage	key encipherment, digital signature
Extended Key Usage	Email protection
Basic Constraints	CA=false, no constraints on length of path
Subject Alt Name	Email address
Issuer Alt Name	Email address
Netscape Certificate Type	SMIME, signature
Netscape Comments	Bundesbank PKI Generated Certificate
CRL Distribution Points	http://www.bundesbank.de/Redaktion/DE/Downloads/Service/Services_Banken_Unternehmen/PKI/CA_for_Email-Security_<year of issue>-crl.crl?__blob=publicationFile
Authority Key Identifier	160-bit SHA-1 hash of issuer's key
Subject Key Identifier	160-bit SHA-1 hash of issuer's key

Serial numbers are not issued more than once by the issuing CA and are thus unique.

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.

7.1.4 Name forms

The CA certificates issued by the root CA contain the entire distinguished name (DN) in the subject name and issuer name fields.

The names of the CA certificates issued are based on the x.509 standard and are in line with the following structure.

EMAIL	ems.pki@bundesbank.de
CN	CA for Email-Security <year of issue>
OU	SMIME-Certificates
O	Bundesbank
C	de

The names of the user certificates issued are based on the x.509 standard and are in line with the following structures.

DN – Deutsche Bundesbank

	Employee	**External employee**	**Counterparty**
EMAIL	<Firstname.Surname> or <Email address>		
	@bundesbank.de	@externe-mitarbeiter.bundesbank.de @bafin.bundesbank.de	@<domain>
CN	<Firstname Surname> or <Email address>		
OU	<YYYYMMDD>		
OU	CA for Email-Security <year of issue>		
O	Bundesbank		<company>
C	de		

DN – Financial Market Stabilisation Agency (FMSA)

	Employee	**External employee**	**Counterparty**
EMAIL	<Firstname.Surname> or <Email address>		
	@fmsa.de	@fmsa.de	@<domain>
CN	<Firstname Surname> or <Email address>		
OU	<YYYYMMDD>		
OU	CA for Email-Security <year of issue>		
O	FMSA		<company>
C	de		

7.1.5 Name constraints

See chapter 3.1.

7.1.6 Certificate policy object identifier

The certificate policy OID of the CP for Email Security Certificates is:
1.3.6.1.4.1.2025.590.1.5.

7.1.7 Usage of policy constraints extension

Not applicable

7.1.8 Policy qualifiers syntax and semantics

Not applicable

7.1.9 Processing semantics for the critical certificate policies extension

Not applicable

7.2 CRL profile

7.2.1 Version number(s)

The BBk-PKI issues CRLs in line with the x.509 norm, version 1.

7.2.2 CRL and CRL entry extensions

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

7.3 OCSP profile

Not applicable. The BBk-PKI currently does not support OSCP.

8 Compliance audit and other assessments

See CP for Email Security Certificates.

9 Other business and legal matters

See CP for Email Security Certificates.

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)
EMS	Email security
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.