DFN-PKI

DFN
Deutsches
Forschungsnetz

DFN-PKI Certificate Policy

- Security levels: Global, Classic and Basic -

DFN-Verein

DFN-PKI CP

V2.1

December 2006

Contents

1 Introduction ... 5

1.1 Overview ... 5

1.2 Document name and identification ... 5

1.3 PKI participants ... 6

1.4 Certificate usage ... 7

1.5 Policy administration ... 7

1.6 Definitions and acronyms ... 7

2 Publications and repository responsibilities ... 7

2.1 Repositories ... 7

2.2 Publication of certification information ... 7

2.3 Time or frequency of publication ... 8

2.4 Access controls on repositories ... 8

3 Identification and authentication ... 8

3.1 Naming ... 8

3.2 Initial identity validation ... 10

3.3 Identification and authentication for re-key requests ... 11

3.4 Identification and authentication for revocation request ... 11

4 Certificate life-cycle operational requirements ... 12

4.1 Certificate application ... 12

4.2 Certificate application processing ... 12

4.3 Certificate issuance ... 12

4.4 Certificate acceptance ... 12

4.5 Key pair and certificate usage ... 13

4.6 Certificate renewal ... 13

4.7 Certificate re-key ... 14

4.8 Certificate modification ... 14

4.9 Certificate revocation and suspension ... 14

4.10 Certificate status services ... 15

4.11 End of subscription ... 15

4.12 Key escrow and recovery ... 15

5 Facility, management, and operational controls ... 16

5.1 Physical controls ... 16

5.2 Procedural controls ... 16

5.3 Personnel controls ... 17

5.4 Audit logging procedures ... 17

5.5 Records archival ... 17

5.6 Key changeover ... 18

5.7 Compromise and disaster recovery ... 18

5.8 CA or RA termination ... 18

6 Technical security controls 18

6.1 Key generation and installation 19

6.2 Private Key Protection and Cryptographic Module Engineering Controls.............20

6.3 Other aspects of key pair management 21

6.4 Activation data 21

6.5 Computer security controls..21

6.6 Life cycle technical controls 21

6.7 Network security controls..21

6.8 Time-stamping 21

7 Certificate, CRL, and OCSP profiles 22

7.1 Certificate profile 22

7.2 CRL profile..23

7.3 OCSP profile..23

8 Compliance audit and other assessments 23

8.1 Frequency and circumstances of assessment 23

8.2 Identity/qualifications of assessor 23

8.3 Assessor's relationship to assessed entity...23

8.4 Topics covered by assessment 23

8.5 Actions taken as a result of deficiency..23

8.6 Communication of results..23

9 Other business and legal manners..23

9.1 Fees 23

9.2 Financial responsibility..23

9.3 Confidentiality of business information...24

9.4 Privacy of personal information...24

9.5 Intellectual property rights..24

9.6 Representations and warranties 25

9.7 Disclaimers of warranties 25

9.8 Limitations of liability 25

9.9 Indemnities 25

9.10 Term and termination...25

9.11 Individual notices and communications with participants 25

9.12 Amendments...25

9.13 Dispute resolution provisions..26

9.14 Governing law 26

9.15 Compliance with applicable law..26

9.16 Miscellaneous provisions 26

9.17 Other provisions 26

10 References...27

11 Glossary...28

1 Introduction

The “Verein zur Förderung eines Deutschen Forschungsnetzes e.V.” (DFN-Verein – the association for the promotion of a German research network) operates Germany‘s National Research and Education Network “Deutsches Forschungsnetz” (DFN), and ensures its further development and usage. This high performance network for science and research links universities and research establishments and supports the development and testing of new applications in Germany. On this basis, the DFN-Verein provides its sites with services, one of which involves the provision of a public key infrastructure in Germany's National Research and Education Network (DFN-PKI). Information on the DFN-PKI is available under http://www.pki.dfn.de.

1.1 Overview

A number of security levels are supported within the DFN-PKI. All regulations in this Certificate Policy (CP) apply equally to the “Global”, “Classic” and “Basic” security levels apart from cases where this is explicitly identified otherwise in the text. An overview of the security levels is shown in table 1.

Security level	Identification	Root certificate	CA operator
Global	Personal	Anchored within standard browsers	DFN-Verein
Classic	Personal	Self-signed	DFN-Verein, DFN-sites, third parties
Basic	Also weaker than personal	Self-signed	DFN-Verein, DFN-sites, third parties

Table 1: Overview of the security levels of the DFN-PKI

This document is the CP of the DFN-PKI for the “Global”, “Classic” and “Basic” security levels. It regulates the processes within the DFN-PKI and defines, in particular, the general conditions for issuing certificates in accordance with the international X.509 [X.509] standard.

There is only this one CP for the “Global”, “Classic” and “Basic” security levels in the entire DFN-PKI. All regulations specified in this CP are binding for all participants of the DFN-PKI and may not be toned down.

In addition, there must be a separate Certification Practice Statement (CPS) for each certification authority (CA) in the DFN-PKI. Each CA covers in its CPS how it implements the requirements of the DFN-PKI CP in detail and at which security level the CA is operated.

This CP and all CPSs in the DFN-PKI must meet the requirements of RFC 3647 [RFC3647], in particular with regard to the standard structure of the documents.

1.2 Document name and identification

This CP is identified as follows:

- Title: DFN-PKI Certificate Policy - Security levels: Global, Classic and Basic -
- Version: 2.1
- Object Identifier (OID): 1.3.6.1.4.1.22177.300.1.1.5.2.1

The OID [OID] has the following structure:

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) dfn-verein(22177) pki(300) cp(1) x.509(1) global/classic/basic(5) major-version(2) minor-version(1)}

This OID is not directly included in certificates. Instead, the OIDs from Section 7.1.6 are used depending on the security level.

1.3 PKI participants

1.3.1 Certification authorities

CAs are responsible for issuing certificates within the DFN-PKI.

The Policy CA (PCA) of the DFN-PKI certifies only certificates of directly subordinated CAs in accordance with this CP and the CPS of the PCA.

The PCA and all CAs at the Global security level are operated by the DFN-Verein. CAs at the Classic and Basic security levels can also be operated by the users themselves or by appointed third parties.

Each certificate is clearly mapped to one of the three security levels (Global, Classic, or Basic). Depending on the security level, the certificates issued can be traced to different root certificates (see Table 2).

Security level	Root certificate
Global	The public key of the PCA is included in a certificate (“DFN-Verein PCA Global - G01”), which was issued by the “Deutsche Telekom Root CA 2”.
Classic and Basic	The public key of the PCA is included in a self-signed root certificate (“DFN-Verein PCA Classic – G01” or “DFN-Verein PCA Basic – G01”).

Table 2: Security level and root certificate

All subordinate CAs of the PCA operating within the DFN-PKI can issue certificates for natural persons and organizations.

1.3.2 Registration authorities

Registration authorities (RAs) are responsible for checking the identity and authenticity of subscribers.

At least one primary RA which is to be appointed in the CPS is assigned to each CA within the DFN-PKI. Only these RAs may be used to register directly subordinated CAs and RAs. Other subscribers can also be registered.

All CAs within the DFN-PKI are able to appoint further RAs for locally checking the identity and authenticity of the subscribers. However, these non-primary RAs may not be used to register further subordinated CAs and RAs.

Compliance with the CP must be assured in writing to the relevant CA responsible. Similarly, the appointment and dismissal of RAs must be documented and communicated.

1.3.3 Subscribers

Subscribers are natural persons and organizations who/which are granted certificates based on their eligibility stated in the charter of the DFN-Verein.

1.3.4 Relying parties

Relying parties are natural persons or organizations who/which check the identity of a subscriber by using a certificate that was issued in the DFN-PKI.

1.3.5 Other participants

Other participants can be natural persons or organizations who/which are involved in the certification process as service providers. For service providers who operate in the name and on behalf of a DFN-site, the commissioning DFN-site is responsible for complying with the CP and CPS.

1.4 Certificate usage

1.4.1 Appropriate certificate usage

Certificates issued as part of the DFN-PKI can be used for authentication, electronic signature and encryption, etc. Subscribers are responsible themselves for usage in the application programs and for checking whether these applications meet the security requirements appropriately.

1.4.2 Prohibited certificate usage

Basically no certificate usage is prohibited, but certificates and revocation lists may only be issued by CAs.

1.5 Policy administration

1.5.1 Organization administering the document

This document is administrated by the DFN-Verein. Please see Section 1.5.2 for contact information.

1.5.2 Contact person

The contact for this document is:

DFN-Verein
Dr. Marcus Pattloch
Stresemannstr. 78
10963 Berlin, Germany

Telephone: +49 30 884299-24
Fax: +49 30 884299-70
E-mail: pki@dfn.de
WWW: http://www.pki.dfn.de

1.5.3 Person determining CPS suitability for the policy

The person named in Section 1.5.2 is responsible for checking all CPSs in the DFN-PKI.

1.5.4 CPS approval procedures

CPSs are authorized by the DFN-Verein or by a service provider commissioned by it.

1.6 Definitions and acronyms

See Section 11.

2 Publications and repository responsibilities

2.1 Repositories

Each CA within the DFN-PKI must hold the information named in Section 2.2 in accordance with Sections 2.3 and 2.4.

2.2 Publication of certification information

Each CA within the DFN-PKI must publish the following up-to-date information and specify the addresses of the relevant information services in its CPS:

- DFN-PKI CP
- CA security level (Global, Classic or Basic)
- Certificate of the associated PCA and its fingerprint
- Root certificate and its fingerprint (only at the Global security level)
- CPS of the CA
- Certificate of the CA and its fingerprint
- List of the RAs belonging to the CA
- Reference to a directory service for the certificates issued, if such a service is operated

- Reference to the CRL of the CA and the PCA
- Contact information under which a revocation can be requested.

Furthermore, the subscribers should be provided with information on the DFN-PKI, for checking the validity of certificates, on the correct implementation of cryptography and on the use of certificates.

2.3 Time or frequency of publication

The following deadlines apply with regard to updating the information named in Section 2.2:

• Certificates:	within three working days after issuing
• CP and CPS:	within one week after generation of a new version
• List of RAs:	within three working days following a change
• CRLs:	see Section 4.9.7.

2.4 Access controls on repositories

Read access to all information listed in Section 2.2 must be possible without access controls. Write access to this information may only be granted to the persons authorized. The information services should be available without time restrictions.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

A standard naming hierarchy is used in the DFN-PKI. All certificates issued within the DFN-PKI include distinguished names (DNs) in accordance with the X.500 series of standards. A DN contains a unique sequence of naming attributes ensuring a unique reference to each subscriber. Variations of this must be agreed with the DFN-Verein and explained in the CPS.

A DN always complies with the following scheme, where optional attributes appear in square brackets and attributes in angle brackets must be replaced with the relevant values. The sequence of the attributes must be adhered to.

C=DE,

[ST=<Federal state>,]

[L=<Location>,]

O=<Organization>,

[OU=<Organizational unit>,]

[CN=<Common name>,]

[emailAddress=<e-mail address>]

The attribute “O=” contains the name of the organization which the subscriber is part of.

“OU=” is the only attribute that may be specified several times.

The “CN=” attribute is mandatory for natural persons, and should be used for reasons of interoperability (e.g., for data processing systems) otherwise.

Even though it is possible to specify e-mail addresses in the DN, they should rather be included in the “subjectAlternativeName” certificate extension.

Each CA agrees a unique namespace with its higher-level CA. When issuing certificates, a CA may only use DNs that are located in its agreed namespace. The issuing CA is responsible for the uniqueness of the names.

Each CA must publish its namespace in its CPS. There are no namespace restrictions for the PCA.

3.1.2 Need for names to be meaningful

The DN must clearly identify the subscriber. The following rules apply in relation to issuing names in DNs:

- Certificates for natural persons may only be issued for a permitted name of the subscriber. Name extensions may only be used if they are included in official identification documents with photo, e.g., “CN=Susan Sample, Dr.”.
- Certificates for groups of persons must start with the “GRP:” tag, e.g., “CN=GRP:Mail office”. This may be dispensed with for CAs and RAs, if the function is clear from the CN. When issuing names for groups of persons, any confusion with existing names (e.g., with natural persons or organizations) must be excluded. It is also not possible to use DNS names, IP addresses or other syntax elements that are used within the DFN-PKI.
- When issuing certificates for data processing systems, the fully qualified domain name must be used for the name, e.g., “CN=pki.pca.dfn.de”. “Wildcard certificates” (e.g., “CN=*.pca.dfn.de” are not permitted, in particular.
- When issuing names for pseudonyms, any confusion with existing names (e.g., with natural persons or organizations) must be excluded. It is also not possible to use DNS names, IP addresses or other syntax elements that are used within the DFN-PKI. A pseudonym must not have any offensive or suggestive content. The CN of a pseudonym must start with the “PN:” tag, e.g., “CN=PN:pseudonym”.
- The CN for external subscribers who do not belong to a DFN user and who do not act in the name or on behalf of a DFN-site, must start with the “EXT:” tag, e.g., “CN=EXT:Sam Sample”.

3.1.3 Anonymity or pseudonymity of subscribers

For natural persons, the certificate may list a pseudonym instead of the name. This must be clearly shown in the CN (see Section 3.1.2).

The PCA does not offer to issue pseudonym certificates. If a subordinate CA permits pseudonyms, details on the permitted pseudonyms must be covered in a corresponding CPS.

It is prohibited to issue anonymous certificates.

3.1.4 Rules for interpreting various name forms

Only the following characters may be used in names:

a-z A-Z 0-9 ' ( ) + , - . / : = ? space

The following substitution rules apply with regard to the substitution of German special characters:

Ä -> Ae, Ö ->Oe, Ü -> Ue, ä -> ae, ö -> oe, ü -> ue, ß -> ss

Special characters with accents lose their accents. In all other cases, generally used spelling rules are applied to generate the relevant character by concatenating the characters a-z and A-Z in such manner that the relevant sound is created.

3.1.5 Uniqueness of names

Before certification, the correctness and uniqueness of the name specified must be checked by the CA responsible. The DN of a subscriber must be unique and must not be issued to different subscribers.

In the event of identical names, the “First come, first served” principle generally applies. In the event of disputes, the CA responsible will decide.

In addition, the issuing CA must assign a unique serial number to each certificate, thus enabling a unique and unchangeable mapping to the subscriber.

3.1.6 Recognition, authentication, and role of trademarks

If the DN of a certificate relates to a natural person, trademarks do not need to be recognized. In all other cases it is solely the subscriber's responsibility that their choice of name does not violate any trademark and trademark rights etc. The CAs are not obligated to check such rights. If a CA is notified of a violation of such rights, it must revoke the certificate.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

If the key is not generated by a CA, the subscriber must assure during the certificate request process that he owns the private key.

This is done by transferring the subscriber's public key to the RA in a certificate signing request (CSR) that is electronically signed by the associated private key. The RA must check the validity of the signature and, in addition, the authenticity of the CSR must be confirmed, e.g., by a hand-written signature of the subscriber.

3.2.2 Authentication of an organization identity

Certificates for organizations are always requested by natural persons who must be authenticated in accordance with Section 3.2.3. In addition, an organization is authenticated by presenting relevant documentation as part of the registration process.

3.2.3 Authentication of individual identity

The following procedures are in place for authenticating the identity of a natural person.

a) The subscriber turns up in person at an RA responsible. An employee of the RA checks the identity based on the official identity document with photo (identity card or passport).

b) A natural person is authenticated by a suitable service provider who carries out and then documents a personal identity check based on an official identity document with photo (identity card or passport). The service used must either have a confirmation of conformity for the implementation of security measures by a review and confirmation office that is recognized by the Federal Network Agency [BNA, Bundesnetzagentur] or such conformity must be made mandatory by means of contractual regulations.

c) A natural person can be authenticated based on the postal address (principal place of residence). The correctness of the address must be verified by suitable measures. It is not permitted to anonymize the postal address, e.g. to use post boxes or "in care of" general delivery ("poste restante").

The procedures permitted depending on the security level are illustrated in table 3. Please note in particular that procedure c) is only permitted for the Basic security level. If the subscriber is a CA or RA, the identity and authenticity must always be checked in accordance with procedure a).

Security level	Type of certificate		Procedure		
	RA/CA	Other	a)	b)	c)
Global	X		permitted	---------	---------
Global		X	permitted	permitted	---------
Classic	X		permitted	---------	---------
Classic		X	permitted	permitted	---------

Security level	Type of certificate		Procedure		
	RA / CA	Other	a)	b)	c)
Basic	X		permitted	---------	---------
Basic		X	permitted	permitted	permitted

Table 3: Permitted procedures for authenticating a natural person

The following information must be available and checked for all procedures:

- Last name, first name(s) and name extensions, if included on the identity document
- E-mail address
- Type and last five digits of the number of the identity document
- Name and address of the associated organization
- Proof for belonging to the organization specified

3.2.4 Non-verified subscriber information

Apart from the details in Sections 3.2.2 and 3.2.3, no other information is checked.

3.2.5 Validation of authority

The request of an organization to accredit a person to manage its DFN-PKI matters must be made in writing or in a suitable electronically signed format by a person authorized to sign. Accredited persons may issue other authorizations and further accreditations to persons to manage DFN-PKI matters for the organization.

Every person who has been accredited must be authenticated in accordance with Section 3.2.3 a).

3.2.6 Criteria for interoperation

Cross-certification is only possible for the PCA.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

If the requestor has a valid certificate, the identification and authentication procedure for re-certification may be carried out by using this certificate. It is also permitted to authenticate certificate requests on the basis of the handwritten signature of the subscriber.

3.3.2 Identification and authentication for re-key after revocation

Once a certificate has been revoked, the subscriber can no longer be authenticated on the basis of the revoked certificate.

3.4 Identification and authentication for revocation request

Revocations can be authenticated as follows

Transfer of previously agreed authentication information (in writing, by telephone or electronically)

Presentation of a revocation request with a handwritten signature

Handover of a revocation request with a suitable electronic signature which authenticates the subscriber.

4 Certificate life-cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application?

In the DFN-PKI, subscribers can request certificates in accordance with Section 1.3.3. CAs can further restrict the group of authorized subscribers in their CPS.

4.1.2 Enrollment process and responsibilities

In order to receive a certificate, a request must be submitted to the registration authority responsible.

The following procedure must be followed and documented at the registration authority:

- Check of the certificate application regarding completeness and correctness
- Check of the uniqueness of the requested DN
- Check of the availability or performance of an identity authentication pursuant to Section 3.2.3
- Possibly review of the authentication of an organization pursuant to Section 3.2.2
- Review of ownership of the private key pursuant to Section 3.2.1
- Secure archiving of the documentation incurred during the certification process – paper documentation must be stored in a locked filing cabinet

Information required for certification is transferred to the CA responsible either electronically in an encrypted format and signed using the certificate of the RA responsible or via postal letter.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Subscribers are identified and authenticated in accordance with Section 3.2.

4.2.2 Approval or rejection of certificate applications

A certificate request is accepted by the RA responsible, if all work steps in accordance with Section 4.1.2 have been successfully completed. Otherwise the certificate request is rejected and the requestor is notified of this and the reasons for the rejection.

4.2.3 Time to process certificate applications

Basically it takes a maximum of one week to process a certificate request.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA checks the formal requirements for issuing a certificate in a suitable manner. In particular, the CA checks the authorization of the RA to approve a certificate for the name specified in the DN and also the validity of the signature of the RA which approves the certificate application.

4.3.2 Notification to subscriber by the CA of issuance of certificate

After the certificate has been issued, the certificate is transferred to the subscriber in a suitable manner by the CA or the subscriber is notified about it having been issued. If personal details or authorization information that is not included in the certificate are transferred, they must be protected in a suitable manner.

4.4 Certificate acceptance

The subscriber is obligated to verify the correctness of his own certificate and the certificate of the issuing CA on receipt of his certificate.

4.4.1 Conduct constituting certificate acceptance

A certificate is accepted by the subscriber, if the certificate is used or if no objection is raised within 14 days of receipt of the certificate. By accepting the certificate, the subscriber assures that all details and explanations regarding the information contained in the certificate are valid.

4.4.2 Publication of the certificate by the CA

If no objections were raised against the publication of the certificate, it is published by the CA via an information service (see Section 2).

4.4.3 Notification of certificate issuance by the CA to other entities

There is no need to notify other entities.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscriber must ensure that his private key is protected appropriately and that the certificate is used in compliance with this CP.

The certificate must be revoked without delay, if the details of the certificate are no longer correct or if the private key was lost, stolen or possibly compromised.

If a CA does not offer any way of private key escrow or if an optionally offered private key escrow opportunity at the CA is not taken up by the subscriber, the subscriber is responsible for safeguarding private keys in such a manner that he is able to decrypt any data that may be encrypted.

4.5.2 Relying party public key and certificate usage

Before a certificate is used, relying parties should check its validity and then use the certificate solely in compliance with this CP.

4.6 Certificate renewal

If a certificate is renewed without changing the key, the CA responsible issues a new certificate for the subscriber by keeping the old key pair, if the key pair meets the cryptographic minimum requirements of the current CP, the information contained in the certificate remains unchanged and there is no suspicion that the private key may have been compromised.

4.6.1 Circumstance for certificate renewal

Certificate renewal may be requested, if a certificate expires.

4.6.2 Who may request renewal?

Certificate renewal is generally requested by the subscriber. It is incumbent on the CA responsible whether it actively supports certificate renewal.

4.6.3 Processing certificate renewal requests

The certificate renewal process is subject to the regulations in Section 4.3, while the regulations in Section 3.3.1 apply to identification and authentication.

4.6.4 Notification of new certificate issuance to subscriber

The regulations in Section 4.3.2 apply.

4.6.5 Conduct constituting acceptance of a renewal certificate

The regulations in Section 4.4.1 apply.

4.6.6 Publication of the renewal certificate by the CA

The regulations in Section 4.4.2 apply.

4.6.7 Notification of certificate issuance by the CA to other entities

The regulations in Section 4.4.3 apply.

4.7 Certificate re-key

In the event of re-certification with key change, the CA responsible issues a new certificate for a new key pair for a subscriber who already holds a certificate, if the information contained in the certificate remains the same. The procedure is the same as explained in Section 4.6.

4.8 Certificate modification

A certificate can be modified, if the information contained in the certificate (e.g., the intended certificate usages) changes. The meaning of the regulations in Section 4.6 applies. If the identity of the subscriber has changed, the procedure is the same as for a first time certificate application. The old certificate must be revoked once a new certificate has been issued.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate must be revoked, if at least one of the following reasons applies:

- The certificate contains invalid information.
- The private key of the subscriber was lost, stolen, disclosed or compromised/misused otherwise.
- The subscriber is no longer authorized to use the certificate (see Section 1.3.3).
- The subscriber does not comply with the CP.
- The subscriber demands that the certificate is revoked.
- The CA or RA responsible does not comply with the CP or CPS.
- The CA terminates its operation.

4.9.2 Who can request revocation?

Revocations can be requested by the subscriber or the RA responsible. Third parties can request revocations, if they present evidence that one of the revocation reasons named in Section 4.9.1 applies.

4.9.3 Procedure for revocation request

If subscribers request a certificate to be revoked, they must authenticate themselves to the RA responsible. Possible procedures are illustrated in Section 3.4.

If the RA has successfully authenticated the subscriber or itself requested the certificate to be revoked, it authorizes this request and forwards it to the CA.

The CA revokes the certificate after it has checked the RA’s authorization for revoking the certificate and the request approving signature of the RA.

4.9.4 Revocation request grace period

If reasons for revoking a certificate (see Section 4.9.1) apply, a revocation request must be submitted without delay.

4.9.5 Time within which CA must process the revocation request

A CA must revoke a certificate without delay if the necessary prerequisites apply) see Section 4.9.3).

4.9.6 Revocation checking requirement for relying parties

See Section 4.5.2.

4.9.7 CRL issuance frequency (if applicable)

CRLs must be generated and published at least once a month. If a certificate is revoked, a new CRL must be generated and published without delay.

4.9.8 Maximum latency for CRLs (if applicable)

Once new CRLs have been generated, they must be published without delay.

4.9.9 On-line revocation/status checking availability

If an online revocation and status review procedure (e.g., OCSP) is offered, the details on this must be specified in the CPS.

4.9.10 On-line revocation checking requirements

The requirements for the protection of the private key in accordance with Section 6.2 apply.

4.9.11 Other forms of revocation advertisements available

No information

4.9.12 Special requirements re key compromise

If the private key is compromised, the relevant certificate must be revoked without delay. If the private key of a CA is compromised, all certificates that were issued by it are revoked.

4.9.13 Circumstances for suspension

Suspension (temporary deferment) of certificates is not permitted. Revoked certificates cannot be renewed or extended.

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 obligation of each CA to provide a CRL is covered in Section 2.

If other services for querying the status of certificates (e.g., OCSP) are offered by a CA, the features of the procedure, the availability of the service and the optional features must be listed in the associated CPS.

4.11 End of subscription

Certificate usage is terminated by the subscriber either by means of revocation or by not requesting a new certificate once the old one has expired.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

If the key escrow and recovery services are offered by a CA, the guidelines and practices must be described in the associated CPS in detail. The PCA does not offer key escrow and recovery for subscribers.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 Facility, management, and operational controls

Guaranteeing suitable infrastructure-related, organizational and staff-related security measures is a prerequisite for securely operating a PKI. Each CA must describe the essential basic features of these security measures in its CPS. Detailed information should be specified in a security concept. This does not need to be published but should be available as part of the conformity check (see Section 8).

If individual security measures are not specified, they must always be based on the action catalogs of the 'IT Grundschutzhandbuch' [IT-GSHB].

5.1 Physical controls

Each CA must describe in its CPS the infrastructure-related security measures.

5.2 Procedural controls

5.2.1 Trusted roles

Table 4 defines the security-relevant roles that are required as part of the certification process. In order to guarantee proper and audit-proof operation of a CA, tasks must be distributed and functions must be separated accordingly. It is possible to split a role amongst several employees. Similarly, an employee may have more than one role, but the role incompatibilities listed in Section 5.2.4 must be observed.

It is possible to expand the role model, but such expansions must be described in the CPS.

Role	Task of the role	Code
Participant service	Acceptance of certificate and revocation requests. Authentication of the identity and check of the authorization of subscribers. Document verification. Helpdesk and support services for subscribers.	TS
Registrator	Review of certificate applications and revocation requests with regard to completeness and correctness. Document archiving. Approval, transfer of certificate and revocation requests to the CA responsible.	RG
CA employee	Responsible for using and storing electronic data media on which the private keys of the CA are stored. Knowledge of the first half of the PINs (passwords) of the private keys of the CA.	CAO1
PIN issuer	Knowledge of the second half of the PINs (passwords) of the private keys of the CA.	CAO2
System and network administrator	Installation, configuration, administration and maintenance of the IT and communication systems. Control of the hardware and software used, but no access to and no knowledge of cryptographic keys and their PINs for the certification process. Exclusive knowledge of the boot and administrator passwords of the systems.	SA
System operator	Support of backup and restore of the servers required and the CA application software.	SO
Audit	Performance of internal audits and audits of sub-CAs, monitoring and compliance with data protection provisions.	R
Security officer	Definition and review of compliance with the security provisions, in particular the CPS and the security concept. Assignment of persons to roles and authorizations. Contact for security-relevant questions.	ISO

Table 4: Roles

5.2.2 Number of persons required per task

Table 5 describes the activities which require the dual control principle to be adhered to – implemented by one representative of each of the roles specified. All other activities can be performed by one person.

Activity	**Roles**
Approval and transfer of certificate and revocation requests for CA certificates	RG & TS
Generation of key pairs for CA certificates	CAO1 & CAO2
Start of processes for issuing certificates and revocation lists	CAO1 & CAO2
Replacement of hardware and software components for certification	SA & CAO1

Table 5: Activities requiring the dual-control principle

5.2.3 Identification and authentication for each role

The roles must be identified and authenticated based on the role model described in Sections 5.2.1 and 5.2.2. Technical access to the IT systems requires a user ID and password or a stronger authentication method, and rules on password usage must be specified. Physical access to the IT systems must be regulated by means of admittance control measures. Access to safe deposit boxes requires ownership of the associated key as well as personal identification and authentication.

5.2.4 Roles requiring separation of duties

Table 6 lists which roles are incompatible.

Role	**Incompatible with**							
	TS	RG	CAO1	CAO2	SA	SO	R	ISO
TS – Participant service					X	X	X	X
RG – Registrator					X	X	X	X
CAO1 - CA employee				X	X	X	X	X
CAO2 - PIN issue			X				X	X
SA – System administrator	X	X	X				X	X
SO – System operator	X	X	X				X	X
R - Audit	X	X	X	X	X	X		
ISO – Security officer	X	X	X	X	X	X		

Table 6: Incompatibility of roles

Each CA must show in its CPS how the roles are split amongst groups of persons. A person must not be assigned incompatible roles.

5.3 Personnel controls

Each CA must describe the staff-related security procedures in its CPS.

5.4 Audit logging procedures

Each CA must describe the audit logging procedures in its CPS.

5.5 Records archival

Each CA must describe the archiving procedures in its CPS.

5.6 Key changeover

The validity of keys is defined in Section 6.3.2. If a key of the CA was compromised, the rules listed in Section 5.7 apply. Once a new CA key has been generated, it must be published in accordance with Section 2.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The procedures for handling security incidents and the compromise of private keys of a CA must be documented in writing and handed out to all employees. The basic features of the procedures are listed in the following sub-sections.

5.7.2 Computing resources, software, and/or data are corrupted

If faulty or manipulated computers, software and/or data affecting the processes of the CA are detected within a CA, operation of the corresponding IT system must be stopped without delay.

The IT system must be re-installed, checked and commissioned in a secure state on a replacement hardware, with the software and the data from the data backup being restored. The faulty or modified IT system must then be analyzed. If deliberate action is suspected, legal steps may have to be initiated. In addition, security must be assessed and an audit must be performed in order to detect any deficiencies. It may be necessary to take up additional defense measures in order to prevent similar incidents. In such cases, employees of the CA will collaborate with the experts of the computer emergency response team in the DFN (DFN-CERT).

5.7.3 Entity private key compromise procedures

If a private key of a subscriber was compromised, the associated certificate must be revoked (see Section 4.9.1).

If the private key of a CA was compromised, the certificate of the CA and all certificates issued with it must be revoked. In addition, all subscribers affected must be notified.

5.7.4 Business continuity capabilities after a disaster

A restart of certification practice following a disaster must be part of emergency planning and be able to take place within a short amount of time, if the security of the certification service is guaranteed. The assessment of the security situation is the responsibility of the security officer.

5.8 CA or RA termination

If a CA discontinues its operation, the following measures must be taken:

- Notification of all subscribers, RAs affected and the contact person listed in Section 1.5.2 at least three months before operation is discontinued
- Revocation of all certificates issued by the CA
- Secure destruction of the private keys of the CA

The operator of the CA must ensure that the archives and the opportunity to retrieve a complete revocation list continue for the retention period that was assured (see Section 5.5).

6 Technical security controls

Guaranteeing suitable technical security controls is a condition for securely operating a PKI. Each CA must describe the essential basic features of these security measures in its CPS. Detailed information should be recorded in a security concept. This does not need to be published but should be available as part of the conformity check (see Section 8).

If individual security measures are not specified, they must always be based on the action catalogs of the ‘IT Grundschutzhandbuch’ [IT-GSHB].

6.1 Key generation and installation

6.1.1 Key pair generation

The key pairs of all CAs must be generated either in an IT system without network connection or in a hardware security module (HSM) which meets the requirements in Section 6.2.1.

For RAs, keys can be generated by the RA or CA responsible. If the key is generated in the CA, the procedure must be illustrated in the CPS.

With regard to subscribers, the key can be generated by the subscriber himself or in the associated RA or CA. If the key is generated by the RA or CA responsible, the procedure must be illustrated in the CPS.

6.1.2 Private key delivery to subscriber

If it is necessary to transfer the private key to a subscriber or an RA, the private key must be sufficiently secured during the transfer and the procedure must be illustrated in the CPS.

6.1.3 Public key delivery to certificate issuer

The CSR of the subscriber is transferred to the CA by e-mail, HTTPS or on data media. Affiliation of the CSR to a specific certificate application is confirmed by signature or electronic signature.

6.1.4 CA public key delivery to relying parties

All participants in the DFN-PKI download the public key of every CA via an information service in accordance with Section 2.

6.1.5 Key sizes

At the Global security level, all keys used must have a minimum length of 2048 bits when using the RSA algorithm.

At the Classic and Basic security levels, the key length for CAs must be at least 2048 bits and for all other keys at least 1024 bits when using the RSA algorithm. To ensure a long-term security level, however, using at least 2048 bits is strongly recommended.

Security level	RSA key length for CAs	RSA key length – Other
Global	2048 bits	2048 bits
Classic, Basic	2048 bits	1024 bits, 2048 bits (recommended)

Table 7: Overview of the key lengths in the DFN-PKI

Furthermore, all cryptographic algorithms are always permitted in accordance with the current “Overview of suitable algorithms” of the Federal Network Agency [BNA, Bundesnetzagentur], if their security is at least equivalent to RSA with 2048 bits. When using other algorithms, they must be described in the CPS.

6.1.6 Public key parameters generation and quality checking

Not applicable.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Not applicable.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

If the private key of the CA is used in a networked IT system, the private key must be stored in a hardware security module (HSM) in such a way that it cannot be exported. This requirement does not apply if the key is used on a dedicated IT system that is not networked. However, it must be ensured that no keys remain on the IT system after the private key has been used.

6.2.1 Cryptographic module standards and controls

HSMs, which are used in accordance with Section 6.2, must meet one of the following or equivalent standards

- FIPS 140-1 level 3
- CC EAL4
- ITSEC E3 security level “high”

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

Access to the private key of a CA must always follow the dual control principle in accordance with Section 6.2.8 and involve the CAO1 and CAO2 roles.

6.2.3 Private key escrow

If private key escrow is provided, this must be described in the CPS. The PCA does not provide for private key escrow.

6.2.4 Private key backup

If the private key of a CA is backup-ed, the private keys must be stored on data media in a secure environment, e.g., a safe deposit box. The private keys must be secured by a PIN where each half is known to the CAO1 and CAO2 roles respectively. Written copies of the two PIN halves are stored in sealed envelopes in a second safe deposit box or with a notary. Access to these safe deposit boxes is strictly regulated. If there are deviations from this procedure, they must be described in the CPS.

If backup of private keys of subscribers is provided by the RA or CA responsible, this must be described in the CPS.

6.2.5 Private key archival

The process of archiving private keys is governed by the rules in Section 6.2.4.

6.2.6 Private key transfer into or from a cryptographic module

Private keys of a CA which were generated in an IT system without network connection in accordance with Section 6.1.1 can be subsequently imported into an HSM.

6.2.7 Private key storage on cryptographic module

In cryptographic modules, private keys of a CA must always be stored in an encrypted format.

6.2.8 Method of activating private key

For private keys of a CA, the PIN must be split into two halves. Only the CAO1 and CAO2 roles know one of the halves, respectively. Activation is only possible based on the dual-control principle.

6.2.9 Method of deactivating private key

Private keys of a CA must be deactivated automatically once the certification process has ended.

6.2.10 Method of destroying private key

When destroying the private keys of a CA, the dual-control principle must be applied. Destroying the private keys is the responsibility of the “ISO” and “CAO1” roles.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

See Section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

The certificates issued in the DFN-PKI are valid as follows:

Certificates for CAs (also for the PCA): a maximum of twelve years

Certificates for data processing systems (server certificates): a maximum of five years

Certificates for natural persons (user certificates): a maximum of three years

Certificates cannot be valid longer than the issuing CA certificate.

The useful life of private keys is governed by the rules in Section 6.1.5.

6.4 Activation data

6.4.1 Activation data generation and installation

Passwords or PINs to activate private keys require non-trivial combinations of alpha-numerical characters and special characters to be selected. They must be at least 15 characters long for the PCA, and 8 characters otherwise.

6.4.2 Activation data protection

Activation data must be kept secret and must only be known to the employees who require it in accordance with Section 5.2.1 in order to perform a specific function. A written copy of the activation data is at best permitted for key escrow in accordance with Section 6.2.4.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All applications within a CA must only be operated on the basis of hardened operating systems. In addition, access control and user authentication must be implemented as security measures.

6.5.2 Computer security rating

The security measures named in Section 6.5.1 must be up-to-date in terms of technology.

6.6 Life cycle technical controls

Each CA must describe the life cycle of the security controls in its CPS.

6.7 Network security controls

Each CA must describe the security measures for the network in its CPS.

6.8 Time-stamping

No information

7 Certificate, CRL, and OCSP profiles

7.1 Certificate profile

7.1.1 Version number(s)

Certificates are issued in accordance with the international X.509 standard (version 3).

7.1.2 Certificate extensions

As a rule, all certificate extensions in accordance with [X.509], [NETS], [PKIX], [PKCS] as well as manufacturer-specific extensions are permitted.

Certificates for CAs must include the “keyUsage” extension with the “keyCertSign” and “cRLSign” values as well as the “basicConstraints” extension with the “CA=True” value.

Certificates for all other intended purposes are optionally tagged as a non-CA certificate with the “basicConstraints” extension with the “CA=False” value and do not have a CA-specific “keyUsage” extension, i.e., the “keyUsage” extension must not have the “keyCertSign” or “cRLSign” values.

The “keyUsage” extension may only be given the “nonRepudiation” value if it is not possible to restore the private key and if – as a result of technical and organizational measures – the private key can only be accessed by the subscriber

7.1.3 Algorithm object identifiers

Object identifiers for algorithms are used in accordance with PKIX.

7.1.4 Name forms

See Section 3.1.

7.1.5 Name constraints

See Section 3.1.

7.1.6 Certificate object identifier

The following OIDs can be included in certificates depending on the security level.

Global: Object Identifier (OID): 1.3.6.1.4.1.22177.300.1.1.4.2.1

The OID [OID] has the following structure: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) dfn-verein(22177) pki(300) cp(1) x.509(1) global(4) major-version(2) minor-version(1)}

Classic: Object Identifier (OID): 1.3.6.1.4.1.22177.300.1.1.1.2.1

The OID [OID] has the following structure: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) dfn-verein(22177) pki(300) cp(1) x.509(1) classic(1) major-version(2) minor-version(1)}

Basic: Object Identifier (OID): 1.3.6.1.4.1.22177.300.1.1.2.2.1

The OID [OID] has the following structure: {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) dfn-verein(22177) pki(300) cp(1) x.509(1) basic(2) major-version(2) minor-version(1)}

If other OIDs than the ones presented here are used, they must be described in the corresponding CPS.

7.1.7 Usage of Policy Constraints extension

None

7.1.8 Policy qualifiers syntax and semantics

See Section 1.2.

7.1.9 Processing semantics for the critical Certificate Policies extension

None

7.2 CRL profile

7.2.1 Version number(s)

Revocation lists must be created in accordance with the international X.509 standard, version 1 or 2.

7.2.2 CRL and CRL entry extensions

No information

7.3 OCSP profile

No information

8 Compliance audit and other assessments

Each CA within the DFN-PKI must design its processes in such a manner that they comply with this CP and its CPS. Each CA is entitled to review all its downstream CAs and RAs for compliance with the corresponding CP and CPS. The PCA is reviewed by the DFN-Verein.

8.1 Frequency and circumstances of assessment

The frequency or circumstances of a review are defined by the CA responsible.

8.2 Identity/qualifications of assessor

The CA responsible can review compliance with the policies of its downstream CAs and RAs itself. A conformity review can also be carried out by third parties.

8.3 Assessor's relationship to assessed entity

The relationship between the assessor and the assessed entity results from Section 8.2. Self-reviews are not permitted.

8.4 Topics covered by assessment

The areas affected by an assessment are defined by the relevant CA responsible. For circumstances that mandatorily require assessment, specific areas can be defined in advance.

8.5 Actions taken as a result of deficiency

Defects detected must be eliminated in consultation between the reviewing CA and the reviewed CA or RA.

8.6 Communication of results

Review results are not published as a rule.

9 Other business and legal manners

9.1 Fees

If a CA collects fees for its services, this must be specified in its CPS.

9.2 Financial responsibility

Insurance protection and a guarantee for physical and legal defects are not envisaged.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All information about participants in the DFN-PKI which is not covered by Section 9.3.2 is classified as confidential information.

9.3.2 Information not within the scope of confidential information

All information that is contained explicitly (e.g., e-mail address) or implicitly (e.g., data on the certification) in the certificates and revocation lists issued or which can be derived therefrom is classified as non-confidential.

9.3.3 Responsibility to protect confidential information

Every CA operating within the DFN-PKI is responsible for taking measures to protect confidential information. As part of the provision of services, data may only be passed on if a confidentiality agreement was signed beforehand and the employees entrusted with the tasks were obligated to comply with the legal data protection provisions.

9.4 Privacy of personal information

9.4.1 Privacy plan

The CAs and RAs operating within the DFN-PKI must electronically store and process personal data for the provision of services. This must take place in compliance with the applicable laws.

9.4.2 Information treated as private

The regulations in Section 9.3.1 also apply to personal data.

9.4.3 Information not deemed private

The regulations in Section 9.3.2 also apply to personal data.

9.4.4 Responsibility to protect private information

The regulations in Section 9.3.3 also apply to personal data.

9.4.5 Notice and consent to use private information

The subscriber agrees to personal data being used by a CA, if this is required to provide the service. In addition, all information that was not treated as confidential (see Section 9.4.3) and whose publication was not objected to may be published.

9.4.6 Disclosure pursuant to judicial or administrative process

All CAs operating within the DFN-PKI are subject to the law of the Federal Republic of Germany and must release confidential and personal information to government bodies in compliance with the applicable laws if corresponding decisions have been made.

9.4.7 Other information disclosure circumstances

No other circumstances for publication are defined.

9.5 Intellectual property rights

The DFN-Verein is the originator of this CP and of the CPS of the PCA. The documents named may be passed on to third parties unchanged. Further rights will not be granted. In particular, it is not permitted to transfer amended versions and to transfer the policy or extracts thereof into machine-readable or other changeable electronic formats without approval by the DFN-Verein.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Each CA operating within the DFN-PKI undertakes to perform all tasks described as part of this CP and its CPS in all conscience and with due care.

9.6.2 RA representations and warranties

Each RA operating within the DFN-PKI undertakes to perform all tasks described in this CP and the CPS of its associated CA in all conscience and with due care.

9.6.3 Subscriber representations and warranties

The provisions in Section 4.5.1 apply.

9.6.4 Relying party representations and warranties

The provisions in Section 4.5.2 apply.

9.6.5 Representations and warranties of other participants

If other participants are involved as service providers in the certification process, the commissioning CA is responsible to obligate the service provider to comply with the CP and its CPS.

9.7 Disclaimers of warranties

Warranty is regulated in the contracts between the parties involved.

9.8 Limitations of liability

Limitations of liability is regulated in the contracts between the parties involved.

9.9 Indemnities

Indemnification from liability is regulated in the contracts between the parties involved.

9.10 Term and termination

9.10.1 Term

The CP and all CPSs become effective on the day on which they are published by the relevant information service (see Section 2). Any change to the CP or CPS of the PCA will be announced by the DFN-Verein, changes to other CPSs will be announced by the relevant CA.

9.10.2 Termination

This document shall apply until it is replaced by a new version (see Section 9.10.1) or until operation of the CAs operated by the DFN-Verein is discontinued.

9.10.3 Effect of termination and survival

Termination of the CP or a CPS does not affect the responsibility to protect confidential information and personal data.

9.11 Individual notices and communications with participants

Notifications other than those defined in this CP shall be at the discretion of the CAs.

9.12 Amendments

The CP can only be changed by the DFN-Verein. If changes are made which concern security-relevant aspects or required processes to be carried out at the subscriber, the OID of the corresponding document (see Section 1.2) and possibly the OID of the CP in certificates (see Section 7.1.6) must be changed.

9.13 Dispute resolution provisions

As a rule, the authority named in Section 1.5.2 shall be responsible for settling conflicts.

9.14 Governing law

Operation of the DFN-PKI is governed by the laws of the Federal Republic of Germany.

9.15 Compliance with applicable law

DFN-Verein issues certificates which can be used to generate advanced electronic signatures in accordance with the German Digital Signature Act (*Signaturgesetz*). These may become eligible as evidence in court as part of free consideration of evidence.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

All regulations contained in this CP or a CPS apply between a CA that operates within the DFN-PKI and its subscribers. The publication of a new version replaces all previous versions. Verbal agreement or side agreements are not permitted.

9.16.2 Assignment

No information

9.16.3 Severability

If individual provisions of this CP or a CPS are invalid or incomplete, this shall not affect the validity of the other provisions.

In place of the invalid provisions the valid provision that approximates as closely as possible the intent and purpose of the invalid provision shall apply. In the event of any incompleteness, the provision that approximates what would have reasonably be agreed in accordance with the intent and purpose of this CP or a CPS if the affair had been taken into consideration from the start shall be deemed to be agreed.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Legal disputes resulting from the operation of a CA that operates within the DFN-PKI are subject to the laws of the Federal Republic of Germany. The place of performance and the exclusive place of jurisdiction shall be the headquarters of the relevant operator.

9.17 Other provisions

Not applicable.

10 References

[BNA] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen [*Federal Network Agency for Electricity, Gas, Telecommunications, Posts and Railways*], http://www.bundesnetzagentur.de

[IT-GSHB] IT-Grundschutzhandbuch [*basic IT protection*] – the basis for IT security, http://www.bsi.bund.de/gshb/

[NETS] Netscape Certificate Extensions, Communicator 4.0 Version, http://wp.netscape.com/eng/security/comm4-cert-exts.html

[PKCS] RSA Security Inc., RSA Laboratories "Public Key Cryptography Standards", http://www.rsasecurity.com/rsalabs

[PKIX] RFCs and specifications by the Public Key Infrastructure (X.509) IETF working group

[RFC3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003

[SigG] Digital Signature Act [*Gesetz über Rahmenbedingungen für elektronische Signaturen*], Federal Law Gazette I 2001, p. 876

[X.509] Information technology - Open Systems Interconnection - The Directory: authentication framework, Version 3, ITU, 1997

11 Glossary

Term	Explanatory notes
CA	Certification Authority – the most important task of certification authorities is issuing certificates
Certificate	Mapping of a cryptographic key to a name, where the mapping is confirmed by the signature of a CA
CN	Common Name
CP	Certificate Policy – the certificate policy of a PKI specifies the rules that all participants have to comply with. There is exactly one certificate policy in every PKI
CPS	Certification Practice Statement, practical implementation (in terms of technology and organization) of the certificate policy
CRL	Certificate Revocation List - list of all certificates that were revoked by a CA
CSR	Certificate Signing Request – document in paper form or electronic format which is used to request a CA to issue a certificate. A certificate signing request includes the name of the requestor, the desired DN in the certificate and always the public key
DC	Domain Component
DN	Distinguished name – unique name of the subscriber or issuer in certificates. A DN consists of several elements such as C, O, OU and CN.
EXT	Flat in the CN: External subscribers
GRP	Tag in the CN: Groups of persons or functions
HSM	Hardware Security Module – a device which securely saves and processes cryptographic keys
Identification	Persons requesting certificates in the DFN-PKI must have their identity ascertained. This process is referred to as identification.
Key Escrow	See Section 4.12
Key Recovery	See Section 4.12
LDAP	Lightweight Directory Access Protocol – protocol for the use of directory services
O	Element in the DN: Organization
OCSP	Online Certification Status Protocol
OID	Object Identifier – unique reference to an object in a namespace
OU	Element of the DN: Organizational Unit
PCA	Policy Certification Authority – top-level CA of a PKI
PKCS	Public Key Cryptography Standard) [PKCS] – series of cryptographic specifications
PKCS#7	Data exchange format for the transfer of signatures and encrypted data or for the distribution of certificates [PKCS]

Term	Explanatory notes
PKCS#10	Data exchange format for the transfer of the public key and DN of a certificate request to a CA [PKCS]
PKCS#12	Data exchange format for saving private and public keys who are secured with a password based on a symmetrical encryption process [PKCS]
PKI	Public Key Infrastructure – name for the necessary technical equipment and the associated processes and concepts for asymmetrical cryptography
PKIX	A series of specifications of the IETF in the environment of digital certificates in accordance with X.509 specifications [PKIX]
PN	Tag in the CN: Pseudonyms
Private key	Key of a cryptographic key pair which is only available to the owner. A private key can be used, for example to generate electronic signatures.
Public key	Key of a cryptographic key pair which is made public. A public key can be used, for example to check electronic signatures.
RA	Registration Authority – the most important task of registration authorities is reviewing the identity and authenticity of subscribers
Re-certification	Issue of a new certificate while keeping the corresponding key pair (e.g., on expiry of a certificate)
Registration	Process during which an RA checks a certificate request and forwards it to the CA responsible (see Section 4.1.2)
Revocation request	If a certificate is to be declared invalid before expiry, a revocation request must be submitted for this certificate
SigG	German Digital Signature Act [*Signaturgesetz*] [SigG]
X.509v3	International Standard for the definition of certificates (Version 3) [X.509]