deutsches forschungsnetz

Certification Policy of the

DFN-PKI

– Security Level “Global” –

DFN-Verein
CP of DFN-PKI
V7 3 June 2020
non-authoritative English translation

Contents

1 Introduction 6

1.1 Overview 6

1.2 Document Name and Identification 6

1.3 PKI Participants 6

1.4 Certificate Usage 7

1.5 Policy Administration 7

1.6 Definitions and Acronyms 8

2 Publication and Repository Responsibilities 8

2.1 Repositories 8

2.2 Publication of Certification Information 8

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 11

3.3 Identification and Authentication for Re-Key Requests 13

3.4 Identification and Authentication for Revocation Requests 13

4 Certificate Live-Cycle Operational Requirements 13

4.1 Certificate application 13

4.2 Certificate Application Processing 14

4.3 Certificate issuance 14

4.4 Certificate Acceptance 14

4.5 Key Pair and Certificate Usage 15

4.6 Certificate Renewal 15

4.7 Certificate Re-Key 15

4.8 Certificate Modification 15

4.9 Certificate Revocation and Suspension 15

4.10 Certificate Status Services 17

4.11 End of Subscription 17

4.12 Key Escrow and Recovery 17

5 Physical Controls 17

5.1 Site Location and Construction 17

5.2 Procedural Controls 17

5.3 Personnel Controls 19

5.4 Audit Logging Procedures 19

5.5 Records Archival 19

5.6 Key Changeover 19

5.7 Compromise and Disaster Recovery 19

5.8 CA or RA Termination 20

6 Technical Security Controls 20

6.1 Key Pair Generation and Installation 20

6.2 Private Key Protection and Cryptographic Module Engineering Controls 21

6.3 Other aspects of Key Pair Management 22

6.4 Activation Data 22

6.5 Computer Security Controls 22

6.6 Life Cycle Technical Controls 22

6.7 Network Security Controls 22
6.8 Time-Stamping 22
7 Certificate, CRL, and OCSP Profile 22
7.1 Certificate Profile 22
7.2 CRL Profile 24
7.3 OCSP Profile 24
8 Compliance Audit and Other Assessments 24
8.1 Audited sectors 24
8.2 Frequency and circumstances of assessment 24
8.3 Identity/Qualifications of Assessor 24
8.4 Assessor's Relationship to Assessed Entity 25
8.5 Actions Taken as a Result of Deficiency 25
8.6 Communications of Results 25
9 Other Business and Legal Matters 25
9.1 Fees 25
9.2 Financial Responsibility 25
9.3 Confidentiality of Business Information 25
9.4 Privacy of Personal Information 25
9.5 Intellectual Property rights 26
9.6 Representations and Warranties 26
9.7 Disclaimer of Warranties 26
9.8 Limitations of Liability 26
9.9 Indemnities 26
9.10 Term and Termination 27
9.11 Individual Notices and Communications with Participants 27
9.12 Amendments 27
9.13 Dispute Resolution Provisions 27
9.14 Governing Law 27
9.15 Compliance with Applicable Law 27
9.16 Miscellaneous Provisions 27
9.17 Other Provisions 28
10 References 29
11 Glossary and abbreviations 29

1 Introduction

The *Verein zur Förderung eines Deutschen Forschungsnetzes e. V.* (DFN-Verein) operates the German Research and Education Network, *Deutsches Forschungsnetz* (DFN) and ensures its further development and utilisation. This high-performance network for science and research links institutions of higher education and research institutions with one another and supports the development and testing of new applications in Germany. This is the basis on which the DFN-Verein makes services available to its users. One such service is the provision of a Public Key Infrastructure (DFN-PKI). Further information (in German) about DFN-PKI is available under http://www.pki.dfn.de.

1.1 Overview

This document contains the Certification Policy (CP) of the DFN-PKI for the Security Level “Global”. It regulates procedures and in particular specifies the conditions for the issuance of certificates in accordance with the international standard X.509 [X.509]. The regulations in this document relate exclusively to the Security Level “Global” of DFN-PKI.

The regulations in this CP and in the Certification Practice Statement (CPS) of the DFN-PCA are binding in full for all participants in the DFN-PKI. The CPS provides details of the implementation of the requirements of the CP of the DFN-PKI.

Within the framework of the DFN-PKI, the DFN-Verein organises the Policy Certification Authority (DFN-PCA) and all subordinate certification authorities (Sub-CAs) for the Security Level “Global”.

CP and CPS in the DFN-PKI are structures in accordance with RFC 3647 [RFC3647].

The DFN-PCA and all its subordinate CAs (Sub-CAs) fulfil the requirements of ETSI EN 319 411-1 [ETSI319411] in accordance with the OVCP Policy for certificates for data processing systems and the NCP policy for certificates for natural persons.

The DFN-PCA and all its subordinate CAs (Sub-CAs) comply with the requirements of the current version of the *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* [CAB-BR] published under http://www.cabforum.org. In the case of any inconsistency between this document and [CAB-BR], then the provisions of [CAB-BR] shall apply.

1.2 Document Name and Identification

This Certificate Policy document is identified as follows:

- Title: Certification Policy of the DFN-PKI - Security Level “Global” -
- Version: 7 (non-authoritative English translation)
- Object Identifier (OID): 1.3.6.1.4.1.22177.300.1.1.4.7

The OID [OID] is constituted as follows:

{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(7)}

In the certificates issued, this Object Identifier documents conformity with [ETSI319411].

1.3 PKI Participants

1.3.1 Certification Authorities

The Certification Authorities (CAs) are responsible for the issuance of certificates within the DFN-PKI.

The Policy Certification Authority of the DFN-PKI (DFN-PCA) is solely responsible for certifying certificates of directly subordinate CAs in accordance with this CP and the CPS of the DFN-PKI. The DFN-PCA and all subordinate CAs in the DFN-PKI are operated by the DFN-Verein. The public key of DFN-PCA is contained in the certificate “DFN-Verein Certification Authority 2” presented by “T-TeleSec GlobalRoot Class 2”.

Certificates for subordinate CAs can be issued in the DFN-PKI solely through the DFN-PCA. There is a subordinate CA for issuing end-entity certificates for the participants in the DFN-PKI called "DFN-Verein Global Issuing CA". In addition, DFN-Verein reserves the right to issue further subordinate issuing CAs under the DFN-PCA for participants with special requirements.

1.3.2 Registration Authorities

A Registration Authority (RA) is responsible for the scrutiny of the identity and authenticity of subscribers and subjects. These responsibilities are assumed by DFN-PCA.

In order to identify natural persons, the DFN-PCA may make use of an “Applicant Representative”. The DFN-PCA has a list of all applicant representatives.

1.3.3 Subscribers

Subscribers are organisations that subscribe to the DFN-PKI and have signed an appropriate subscriber agreement with the DFN-Verein. These organisations apply for certificates for individuals and data processing systems within their organisational realm. These persons and data processing systems are the Subjects.

The range of possible subscribers is given in the Articles of the DFN-Verein [DFN2000], in particular Article 2:

“The Association promotes the creation of the scientific and technical conditions required for establishing, operating, and using a computer-based information and communications system for publicly-supported and non-profit research in the Federal Republic of Germany [...].”

1.3.4 Relying Parties

Relying Parties are natural persons and organisations that rely on a Valid Certificate.

1.3.5 Other Participants

If a service provider is active on behalf of a Subscriber, then the commissioning subscriber is responsible for the service provider’s compliance with the CP and CPS.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued under the DFN-PKI may be used for all purposes that are enabled for the key use purposes contained in the certificate.

Depending on the profile of the certificate, these include:

- Authentication of servers with TLS
- Authentication of users (TLS-Client-Authentication)
- Digital signature and encryption of e-mails (S/Mime)
- Code signing

Subscribers or Subjects are responsible for the use in the application programs, as well as for checking whether the possible applications satisfy their security requirements.

1.4.2 Prohibited Certificate Uses

Uses of the certificate that contravene the Articles of the DFN-Verein (see Section 1.3.3), are prohibited.

The use of the certificate shall not be in contravention of key use purposes contained in the certificate, in particular the issuance of certificates and certificate revocation lists are exclusively reserved for CAs.

1.5 Policy Administration

1.5.1 Organisation Administering the document

This document is administered by the DFN-Verein.

1.5.2 Contact person

The contact person for this document is:

DFN-Verein	Tel: +49 30 884299 955
Dr Ralf Gröper	Fax: +49 30 884299 70
Alexanderplatz 1	E-mail: pki@dfn.de (no 24x7 monitoring)
10178 Berlin, Germany	www.pki.dfn.de

Contact for emergencies in which certificates from the DFN-PKI are misused or demonstrably compromised (see also Section 4.9):

- Telephone number 01805-336754 (14 €ct/min from the German landline, top inland mobile phone rate: 42 €ct/min)
- E-mail: cert-problems@dfn.de

1.5.3 Person Determining CPS Suitability for the Policy

The person named in Section 1.5.2 is responsible for the annual check of the CPS in the DFN-PKI.

1.5.4 CPS Approval Procedures

The CPS is approved by the management board of the DFN-Verein

1.6 Definitions and Acronyms

See Section 11.

2 Publication and Repository Responsibilities

2.1 Repositories

For each CA of DFN-PKI, the information listed in Section 2.2 shall be made public in accordance with Section 2.3 and Section2.4.

2.2 Publication of Certification Information

The following information shall be disclosed:

- CP of DFN-PKI
- CPS of DFN-PKI
- Certificate of “T-TeleSec GlobalRoot Class 2” and its fingerprint
- Reference to the revocation information of “T-TeleSec GlobalRoot Class 2”
- Certificates of the DFN-PCA and its Sub-CAs, with their fingerprints
- Contact information, under which revocation can be applied for
- Revocation information of DFN-PCA and its Sub-CAs
- Reference to the repository service of DFN-PKI
- Duties of the Subscribers
- Information for Subjects
- References to the test websites with a valid, a revoked and an expired certificate to test the revocation mechanisms of DFN-PKI

This information is published online under https://www.pki.dfn.de/policies/informationen and is accessible at all times (24 hours a day, 7 days a week). It will be ensured that outages and maintenance stoppages are minimised and that operations are resumed as quickly as possible.

2.3 Time or Frequency of Publication

For the up-dating of the information specified in Section 2.2 the following deadlines apply:

- Certificates: At least three working days after issuance
- CP and CPS: After a new version comes into force (after being announced, see Section 9.10.1)
- Revocation information:
- CRLs: See Section 4.9.7
- OCSP: By analogy to CRLs (see Section 4.9.7)

2.4 Access Controls on Repositories

All the information listed in Section 2.2 may be read without access control. Writing access to the information is only available to entitled individuals.

3 Identification and Authentication

3.1 Naming

3.1.1 Type of Names

In the DFN-PKI, a uniform name hierarchy is used. All Certificates issued in the DFN-PKI include a distinguished name (DN) in accordance with the X.500 standard series. A DN contains a sequence of characteristic attributes which reference each subject uniquely.

A DN has the following composition: optional attributes are set in square brackets, attribute values in angle brackets shall be replaced by the relevant value. The sequence of the attributes shall be maintained. The significance of the attributes is described in Section 3.1.2.

C=<Country>
[ST=<Federal state or province>][1]
[L=<Location>][1]
O=<Organisation>
[OU=<Organisational unit>]
CN=<Common name>
[emailAddress=<E-mail address>]

The attributes “C” and “O” shall be stated once only.

The attributes “ST” and “L” shall be described exactly once in Certificates for data processing systems (using the OIDs described in Section 7.1.6), in all other certificates single entries for the attributes “ST” and “L” are optional.

The attributes “OU”, “CN” and “emailAddress” may have multiple entries.

Further attributes (e.g. “SER” or “UID”) may be used as long as they are not in contravention of the standards used in the DFN-PKI.

Although it is possible to enter e-mail addresses in the DN, they should in preference be included in the certificate extension “subjectAlternativeName”.

Certificates for data processing systems do not contain e-mail addresses, neither in the DN nor in the subjectAlternativeName.

3.1.2 Need for Names to be Meaningful

The DN must uniquely identify the subject and it must be meaningful.

The following rules apply for the naming:

The mandatory attribute “C” shall be the 2-character code (in accordance with ISO Standard 3166-1 [ISO-3166-1]) of the country in which the Organisation named under the attribute “O” is located.

The optional attribute[1] “ST” shall contain the official name of the federal state or province in which the Organisation named under the attribute “O” is located.

The optional attribute[1] “L” shall contain the official name of the location of the Organisation named under the attribute “O”.

The mandatory attribute “O” shall contain the name of the Subscriber. The authenticity of the name is to be checked in accordance with Section 3.2.2.

If the optional attribute “OU” is described once or multiple times, it must contain in each case the name of an organisational sub-unit of the organisation named in the mandatory attribute “O”. If multiple attributes are provided for “OU”, then these shall be included in the DN directly one after the other and the sequence of the named organisational sub-units shall be from the largest to the smallest sub-unit.

The DN contains at least one attribute “CN”. Each attribute “CN” must contain an appropriate presentation of the name of the Subject. The following shall apply:

a) An attribute “CN” in a certificate for a data processing system shall contain alternatively:
   - A fully-qualified Domain Name, with a Domain registered by a Domain Name Registrar certified by ICANN. The right to use the name in a certificate is checked in accordance with Section 3.2.2.
   - An IP address registered with an Internet Registrar authorised by IANA.The right to use the IP address in a certificate is checked in accordance with Section 3.2.2.

b) An attribute “CN” in a certificate for a natural person shall contain alternatively:
   - The name of the person, consisting at least at least a first name written in full and the surname of the Subject; other first names and name suffixes of the Subject may be included in full or in an abbreviated form, or omitted entirely. All names and any supplements (e.g. “Dr”) may only be included if these are contained in the identification document used for the authentication of

[1] *Mandatory attribute in certificates for data processing systems*

the individual (see Section 3.2.3). If the subject does not belong directly to the Subscriber, then the attribute “EXT:” or “EXT – ” must precede the name, e.g. “EXT:Dr John A. Smith”.

- A pseudonym. When assigning pseudonyms, any possibility of mistaken identity must be avoided, e.g. confusion with natural persons or organisations. Nor shall a pseudonym include Domain Names, IP-addresses or other syntax elements used within the DFN-PKI (e.g. “GRP:”, “GRP – “, “EXT: “, “EXT – “). A pseudonym shall not have offensive or lewd contents. The pseudonym must be uniquely assigned to the subject (authenticated in accordance with Section 3.2.3). The pseudonym must begin with the attribute “PN:” or “PN - ”, e.g. “PN:Cover name”.

c) An attribute “CN” in a certificate for a group of people contains the Group name and must begin with the attribute “GRP:” or “GRP – ”, e.g. “GRP:Postroom”. When assigning names for groups, any possibility of mistaken identity must be avoided, e.g. confusion with existing names of natural persons or organisations. Nor shall the name include any Domain-Names, IP-Addresses or other syntax elements used within the DFN-PKI (e.g. “PN:”, “PN – ”, “EXT:”, “EXT – ”).

d) An attribute “CN” in a certificate for a Certification Authority contains the name of the CA or an unambiguous indication of the CA function.

In the event of a number of “CN” attributes, then these shall be included in the DN directly one after the other.

If the optional attribute “emailAddress” is included once or more often, then in each case it must contain an e-mail address formatted in accordance with RFC 822 [RFC822]. The right to use the e-mail address in a certificate is checked in accordance with Section 3.2.3.In the event that a number of “emailAddress” attributes are given, then these shall be included in the DN directly one after the other.

Certificates for data processing systems do not contain e-mail addresses, neither in the DN nor in the subjectAlternativeName.

The above-mentioned rules apply by analogy for e-mail addresses, IP addresses and Domain names included in the Certificate extension for alternative certificate names (“subjectAlternativeName”) under the Types “rfc822Name”, “iPAddress” or “dNSName”.

If an attribute value is longer than allowed by the relevant standard, then in its place a suitable (and where possible familiar) abbreviation shall be used.

3.1.3 Anonymity and Pseudonymity of Subscribers

For natural persons, a pseudonym may be used in the Certificate. This must be clearly shown as such in the attribute “CN” (see Section 3.1.2). The pseudonym is uniquely assigned to the subject (authenticated in accordance with Section 3.2.3). This is documented in the paperwork generated with the application for the Certificate. The Pseudonym can thus be traced back to the real identity of the Subject.

Anonymous certificates may not be issued.

3.1.4 Rules for Interpreting Various Name Forms

In the DN-attributes “ST”, “L”, “O”, “OU” and “CN”, only the following characters shall be used:

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

In the CN, an “*” may be used additionally for specific types of certificates.

The following substitutions rules exist for replacing special German characters:

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

Special symbols with accents lose the accent. Otherwise, common transliterations of relevant signs are used, generated with the characters a-z and A-Z to form the appropriate sound.

3.1.5 Uniqueness of Names

Before certification, the correctness and uniqueness of the names is checked by the DFN-PCA. The DN of a Subject must be unique and may not be given to different subjects.

In the event of a clash of names, then the principle of “First come, first served” applies. In cases of dispute, the DFN-PCA decides. The unambiguity of the DN can be achieved by using “OU”, “UID” or “SER” attributes or by the use of pseudonyms in the attribute “CN”, e.g. “PN: John Smith 2”.

3.1.6 Recognition, Authentication and Role of Trademarks

If the CN of a certificate refers to a natural person, then a recognition of trade marks or similar is not relevant. In all other cases, it is the sole responsibility of the participant to ensure that the choice of name does not infringe on trademarks or similar. The DFN-PCA is not obliged to check for such infringements. On being informed of such an infringement of rights it must revoke the certificate.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

On application it must be proved that the future subject is in possession of the private key. This is done by signing the Certificate Signing Request (CSR) contained in the certificate application using the private key and submitting this to the CA. The CA must examine the validity of the signature.

3.2.2 Authentication of Organisation and Domain Identity

Every organisation that takes part in the DFN-PKI has concluded a DFNInternet contract with the DFN-Verein. Before conclusion of the contract, the details submitted by the Organisation are verified by the DFN-Verein by checking the appropriate documents.

Alternatively, organisations are authenticated by the presentation of relevant documents such as excerpts from Registers or regional or federal legislation, or by presenting credentials (issued by lawyers, notaries public, auditors, or state institutions). Certificates are issued exclusively for the organisation named in the contract or in the submitted documentation.

If a domain name (FQDN) or an IP address is used in a certificate, then the right of the organisation to use this domain name or this IP address will be checked by the DFN-Verein as operator of the DFN-PCA.

For verification of domain names, one of the following methods is used:

1. The organisation’s right to use the FQDN by is confirmed by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value is sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact. (Method according to chapter 3.2.2.4.2 of [CAB-BR]). It is ensured that:
   - Each email, fax, SMS, or postal mail may confirm control of multiple Authorization Domain Names.
   - DFN-PCA may send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.
   - The Random Value is unique in each email, fax, SMS, or postal mail.
   - DFN-PCA may resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain un-changed.
   - The Random Value remains valid for use in a confirming response for no more than 30 days from its creation. The CPS may specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.
   - Once the FQDN has been validated using this method, also Certificates for other FQDNs that end with all the labels of the validated FQDN may be issued.
   - This method is also used for validating Wildcard Domain Names.
2. The organisation’s right to use the FQDN by is confirmed by sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at- sign ("@"), followed by an Authorization Domain Name, including a Random Value in the email, and receiving a confirming response utilizing the Random Value. (Method according to chapter 3.2.2.4.4 of [CAB-BR]). It is ensured that:
   - Each email may confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed
   - The Random Value is unique in each email.
   - The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient remain unchanged.
   - The Random Value remains valid for use in a confirming response for no more than 30 days from its creation.
   - Once the FQDN has been validated using this method, also Certificates for other FQDNs that end with all the labels of the validated FQDN may be issued.
   - This method is also used for validating Wildcard Domain Names.

For verification of IP-addresses, one of the following methods is used:

1. The Applicant's control over the IP Address is confirmed by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value is sent to an email address, fax/SMS number, or postal mail address identified as an IP Address Contact. (Method according to chapter 3.2.2.5.2 of [CAB-BR]). It is ensured that:
   - Each email, fax, SMS, or postal mail may confirm control of multiple IP Addresses.

- DFN-PCA may send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email, fax, SMS, or postal mail.
- The Random Value is unique in each email, fax, SMS, or postal mail.
- DFN-PCA may resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.
- The Random Value remains valid for use in a confirming response for no more than 30 days from its creation.

2. Confirming the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under the paragraphs above. (Method according to chapter 3.2.2.5.3 of [CAB-BR]).
3. Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the Applicant's request for validation of the IP Address. (Method according to chapter 3.2.2.5.5 of [CAB-BR]). It is ensured that:
   - DFN-PCA places the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact.
   - Each phone call is made to a single number.
   - In the event that someone other than an IP Address Contact is reached, DFN-PCA may request to be transferred to the IP Address Contact.
   - In the event of reaching voicemail, DFN-PCA may leave the Random Value and the IP Address(es) being validated.
   - The Random Value must be returned to the CA to approve the request.
   - The Random Value remains valid for use in a confirming response for no more than 30 days from its creation.

No certificates are issued for data processing systems containing internal IP addresses or local host names.[2]

3.2.3 Authentication of Individual Identity

The authentication of the identity of a natural person shall be carried out by the DFN-PCA. To this end, it may make use of a suitable service provider (e.g. PostIdent).

The authentication requires confirmation of personal identity on the basis of a valid official identity document with a photograph (ID document or passport) and shall be appropriately documented.

In the case of a change of name that has not yet been entered in the valid identification document as presented, e.g. after marriage, then in addition to the valid identification document the authentication may draw on a civil status certificate that is not more than 6 months old.

The following information shall be presented and checked:

- Name, First name(s) and supplements to the name where these are included in the identification document
- E-mail address
- Type of the identification document and the last five digits of its number, or, if this data is not available due to the chosen of identification method, other attributes which can be used to, as far as possible, distinguish the person from others with the same name.
- Name and address of the given organisation
- Proof of association with the given organisation
- This information is necessary for the issue of the certificate and will be recorded. On the basis of this data, the identification of the natural person is possible.
- E-mail addresses to be included in certificates for natural persons or groups are verified by one of the following methods:

[2] *Internal IP addresses are marked as reserved in the IANA IPv4 Address Space Registry [IANA_IP4] and in the IANA IPv6 Address Space Registry [IANA_IP6].*

Local host name: A fully-qualified domain name below a Top-Level Domain reserved for special purposes as defined in RFC 2606 [RFC2606]; or a fully-qualified Domain Name below a Top-Level Domain, that is not authorised by ICANN; or a host name without domain name components.

1. Challenge-response method where an e-mail is sent to the e-mail address to be verified. The e-mail contains a link with an individual 128-bit long random number. The link must be called by the applicant before the request can be processed.
2. Or matching against Subscriber-managed address lists if the Subscriber itself assigns the e-mail-addresses to be included in the certificate. In this procedure, the domain of the e-mail address is checked according to the rules in Chapter 3.2.2.

3.2.4 Non-verified Subscriber information

Apart from the details in Section 3.2.2 and Section 3.2.3, no further information will be checked.

3.2.5 Validation of Authority

Each Subscriber shall nominate at least one person who is empowered to apply for Certificates on their behalf.

Empowered persons give evidence of the authenticity of certificate applications to the DFN-PCA either by their manual signature (empowered person), or by a signature with a personal certificate (applicant representative). The DFN-PCA holds a complete list of the sample signatures of the empowered persons and a list of these certificates.

Every empowered person shall be authenticated in accordance with Section 3.2.3.

3.2.6 Criteria for Interoperation

Cross-certification is possible solely for the DFN-PCA.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

For routine Certificate renewal, then in addition to the method in accordance with Section 3.2.3, the identity of a natural person may be authenticated by a valid personal certificate from the DFN-PKI if the underlying identification was performed within the time limit defined in Section 4.2.1.

3.3.2 Identification and Authentication for Re-Key After Revocation

After the revocation of a certificate, an authentication can no longer be carried out with the revoked certificate.

3.4 Identification and Authentication for Revocation Requests

The authentication of a revocation (see Section 4.9) can be carried out as follows:

- Transmission of previously agreed authentication information (in writing, by telephone, or electronically)
- Transfer of a revocation application with a suitable electronic signature which authenticates the Subscriber or the Subject
- Presenting a revocation application with a manual signature

4 Certificate Live-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who Can Submit a Certificate Application

In the DFN-PKI, Subscribers can apply for certificates in accordance with Section1.3.3. If the certificate is for a natural person, the Subscriber must have an authorisation for them.

4.1.2 Enrollment Process and Responsibilities

In order to receive a certificate, an application must be submitted to a CA of DFN-PKI.

The registration process involves the following steps, which must be completed and documented:

- Check that the certificate application is complete and correct
- Check the prospective DN in accordance with Sections 3.1.2 and 3.1.5
- Check for an authentication of the Identity in accordance with Section 3.2.3 for certificates for natural persons
- Check the authentication of the Organisation in accordance with Section 3.2.2

- Examine the ownership of the private key in accordance with Section 3.2.1
- Confirm the authenticity of the certificate application by checking the clearance of the application by an empowered person, see Section 3.2.5

Accumulated paper documents must be archived and stored in a locked cabinet. Accumulated digital records must be archived and stored so as to prevent unauthorised access.

The information needed for the certification shall be passed on to the CA electronically in encrypted form and signed using the certificate of the responsible applicant representative.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Identification and authentication of subjects is carried out in accordance with Section3.2.

For authenticating organisation identity including the right to use domain names or IP addresses according to Section 3.2.2 it is possible to reuse existing documents and data if the documents or data are not older than 825 days.

If the certificate application is not intended for a data processing system: For authenticating personal identity according to Section 3.2.3 it is possible to reuse existing documents or data if they are not older than 39 months.

For validation of authority according to Section 3.2.5 it is possible to reuse existing documents or data if they are not older than 39 months.

4.2.2 Approval or Rejection of Certificate Applications

A certificate application will be accepted by the responsible CA if all steps in accordance with Section 4.1.2 have been successfully completed. Otherwise the application will be rejected and the Subscriber will be notified of this, giving reasons.When the authenticity of a certificate application for a data processing system is confirmed by an empowered person according to Section 4.1.2, it is checked for each domain name in a CN or a dnsName according to [RFC6844], whether CAA Resource Records according to [RFC6844] can be found in the DNS. If a CAA Resource Record is found, the certificate application can only be confirmed if the issue or issuewild property contain the value “pki.dfn.de” or “dfn.de”. If the certificate could not be issued in 8 hours after the check, the certificate application is discarded.

4.2.3 Time to Process Certificate Applications

Certain minimum or maximum processing times are not guaranteed.

4.3 Certificate issuance

4.3.1 CA Actions During Certificate Issuance

The formal preconditions for the issuing of a certificate will be checked by the CA in an appropriate manner. In particular, the CA checks the entitlement of the participants to receive a certificate for the name given in the DN, and the validity of the signature of the applicant representative.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

The Subscriber and if appropriate the subject will be sent the issued certificate by the CA by e-mail or they will be notified and informed about the possibility of downloading the certificate.

4.4 Certificate Acceptance

The subject is obliged to verify the correctness of their own certificate and the certificate of the issuing CA on receipt.

4.4.1 Conduct Constituting Certificate Acceptance

A certificate has been accepted if it is used or if no objection is lodged within 14 days after receipt.

4.4.2 Publication of the Certificate by the CA

The Certificates are published by DFN-PCA through the repository service of DFN-PKI and, in case of certificates for Data processing systems, via third party operated log servers of the Certificate Transparency System. Subjects of user certificates are entitled to object to the publication of their certificate.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

It is not necessary to notify other entities.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and certificate Usage

Private keys shall be suitably protected. Certificates may only be used in accordance with this CP.

4.5.2 Relying Party Public Key and Certificate Usage

If Relying Parties use Certificates from the DFN-PKI, they must ensure that these have an appropriate Security Level in the context of the application. Furthermore, Relying Parties are obliged to ensure that a certificate is correct and valid. This includes checking the signature of the certificate by the issuing CA and checking if the certificate has been revoked.

4.6 Certificate Renewal

In the case of certificate renewal without re-keying, a new certificate is issued with retention of the old key pair provided that the key pair meets the minimum cryptographic requirements of the CP, the information contained in the certificate is unchanged, and there is no suspicion that the private key has been compromised.

4.6.1 Circumstances for Certificate Renewal

An application may be made to renew a certificate if the validity of a certificate has expired.

4.6.2 Who May Request Renewal

Certificate renewal is requested by the Subscriber.

4.6.3 Processing Certificate Renewal Requests

The certificate renewal procedure corresponds to the regulations for the first application under Section 4.3; for the identification and authentication the regulations apply in accordance with Section 3.3.1.

4.6.4 Notification of New Certificate Issuance to Subscriber

The regulations apply in accordance with Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The regulations apply in accordance with Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

The regulations apply in accordance with Section 4.4.2.

4.6.7 Notifying of Certificate Issuance by the CA to Other Entities

The regulations apply in accordance with Section 4.4.3.

4.7 Certificate Re-Key

In the case of certificate renewal with re-keying, a new certificate for a new key pair is issued provided the information contained in the existing certificate remains unchanged. The procedure follows Section 4.6 by analogy.

4.8 Certificate Modification

A certificate can be modified if information contained in the certificate is to be changed (e.g. the purpose of use). The procedure follows Section 4.6 by analogy.

4.9 Certificate Revocation and Suspension

Contact information for revocation applications is published online under the address www.pki.dfn.de/policies/informationen.

- Emergency cases when certificates from the DFN-PKI have been abused, used fraudulently or demonstrably compromised can be reported 24x7 under the telephone number 01805-336754 (14 €ct/min from the German landline, top inland mobile phone rate: 42 €ct/min). Alternatively, the e-mail address cert-problems@dfn.de can be used.
- Certificates that have already expired cannot be revoked. The revocation of a certificate cannot be reversed.

4.9.1 Circumstances for Revocation

A certificate shall be revoked if any of the following apply:

- The certificate contains details that are not valid.
- The private key has been lost, stolen, disclosed, or otherwise compromised or abused.
- The subject is no longer entitled to use the certificate.
- The certificate infringes trade marks or similar in accordance with Section 3.1.6
- The use of the certificate contravenes the CP or the CPS.
- The issuing CA ceases operation.
- The subject or Subscriber has applied for a certificate revocation.

Furthermore all reasons contained in chapter 4.9.1 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [CAB-BR].

4.9.2 Who Can Request Revocation

A Subject or Subscriber may apply for a certificate revocation without giving reasons.

Third Parties may apply for a certificate revocation if they are able to provide hints that there are grounds for doing so under Section 4.9.1.

4.9.3 Procedure for Revocation Requests

If a Subject or Subscriber applies for a revocation, they must provide authentication to the issuing CA. The possibilities are presented in Section 3.4. After authentication, the issuing CA carries out the revocation.

If a third party applies for a revocation, then the issuing CA shall investigate the reasons given. If any of the grounds listed in 4.9.1 pertain, then the revocation shall be carried out.

After revocation, the Subscriber and if appropriate the Subject shall be informed electronically. The revocation information shall be made available at least until the expiry date of the revoked certificate via the revocation services.

4.9.4 Revocation Request Grace Period

If there are reasons for a revocation (see Section 4.9.1) then a revocation must be applied for immediately.

4.9.5 Time Within Which CA Must Process the Revocation Request

A CA must carry out certificate revocation immediately if grounds exist (see Section 4.9.3).

4.9.6 Revocation Checking Requirements for Relying Parties

See Section 4.5.2.

4.9.7 CRL Issuance Frequency

CAs that do not exclusively issue CA certificates shall update and reissue a CRL every 24 hours. The date in the field nextUpdate of this CRLs must not be more than 10 days after the date in the field thisUpdate.

Other CAs shall update and reissue a CRL every 180 days. The date in the field nextUpdate of this CRLs must not be more than 12 months after the date in the field thisUpdate.

If a certificate is revoked then the revoking CA shall immediately update and reissue the CRL.

4.9.8 Maximum Latency for CRLs

After CRLs are updated, they shall be reissued without delay, and at least within 24 hours.

4.9.9 On-Line Revocation/Status Checking Availability

CAs can offer OCSPs as online revocation and status checking procedures (see Section 4.10). This is obligatory for all CAs that issue certificates in accordance with [CAB-BR].

Revocation information shall be available continuously (24 hours a day, 7 days a week). It shall be ensured that unplanned outages and maintenance periods are minimised and that normal operations are restored as quickly as possible.

4.9.10 On-Line Revocation Checking Requirements

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

The correctness of the revocation and status information provided by the CA about certificates shall be ensured by the general security mechanisms of DFN-PCA (see Sections 5 and 6 and the CPS). During transmission, the revocation and status information is protected against manipulation by electronic signatures (see Sections 7.2 and 7.3).

Entries regarding revoked Certificates shall not be removed from the CRL or the OCSP service before expiry of the certificates in question.

4.9.11 Other Forms of Revocation Advertisements Available

There are no other forms of revocation advertisements available.

4.9.12 Special Requirements re Key Compromise

If a private key is compromised, the corresponding certificate is to be revoked immediately. If the private key of a CA is compromised, then all the certificates issued by the CA shall be revoked.

4.9.13 Circumstances for Suspension

Certificates cannot be suspended for a limited period.

4.9.14 Who Can Request Suspension

No entry.

4.9.15 Procedure for Suspension Request

No entry.

4.9.16 Limits on Suspension Period

No entry.

4.10 Certificate Status Services

The obligation to provide CRLs is covered in Section 2.

Certificates for which an online certificate status protocol (OCSP) is offered contain a reference to this service. Certificates in accordance with the requirements of [CAB-BR] always include a reference to the OCSP service.

The OCSP-service gives a negative report for unissued certificates.

4.11 End of Subscription

The use of a certificate ends either by revocation or if no application is received for a new certificate after the expiry of validity.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The CAs in the DFN-PKI do not offer key escrow and recovery for subscribers or subjects. Subscribers using key escrow shall follow the stipulations in the document "*Pflichten der Teilnehmer*".

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No entry.

5 Physical Controls

Suitable security measures infrastructure, organisation and personnel security measures is essential for the secure operation of a PKI. These security measures are outlined in the CPS of the DFN-PKI. Detailed information about this and about the IT-security management process is given in a security strategy. In addition, a risk analysis and evaluation is carried out regularly and documented. The results are not published, but are available for compliance audits (see Section 8). The details of the risk analysis are contained in the internal document "*Risikobewertung des PCA-Betriebs der DFN-PKI*". In the following, measures are described for the infrastructural, organisational and personal security. Details are contained in the internal operating manual "*Betriebshandbuch der DFN-PKI*".

Unless specified otherwise, security measures are based on the measures in the IT Security Guidelines - Federal Office for Information Security [IT-GSHB].

5.1 Site Location and Construction

The infrastructure security measures for all CAs are described in the CPS of DFN-PKI.

5.2 Procedural Controls

5.2.1 Trusted Roles

In Table 1, the security relevant roles are defined for the certification process. In order to ensure an orderly and audit-compliant operation of DFN-PKI, tasks must be allocated and roles separated accordingly. It is

possible to share a role between several personnel. It is also possible that one person takes on more than one role, provided that the incompatibilities listed in Section 5.2.4 are taken into account.

Role	Duties	Abb.
Applicant representative	• Transmission of certificate applications to the relevant CA • Transmission of revocation applications to the relevant CA • Giving advice to the Subject • Carrying out personal Identification in accordance with Section 3.2.3 for user certificates and archiving the relevant documents	TS
Registration Authority co-worker	• Receipt of certificate and revocation applications • Checking the authorisation of the Subscriber • Checking for completeness and correctness • Checking the authorisation of domain names • Release of certificates or revocation applications • Archiving documents	RG
CA operator	• Use and storage of electronic media on which the private keys of the CA are stored. • Knowledge of the first half of the PIN (password) for the private key of the CA.	CAO1
PIN-Contributor	• Knowledge of the second half of the PIN of the private key of CA.	CAO2
System and network administrator	• Installation, configuration, administration and maintenance of IT and communications systems. • Control of the hardware and software, but no access to or knowledge about cryptographic keys and their PINs for the certification process • Exclusive knowledge of the boot and administrator passwords for the systems	SA
System operator	• Supervision of data security and recovery for the necessary server and the CA application software.	SO
Reviser	• Carrying out internal audits • Supervising and observing data protection regulations	R
Security officer	• Defining and investigating security provisions, in particular CPS and security strategies • Allocation of roles and entitlements • Contact partner for questions relating to security	ISO

Table 1: Roles

5.2.2 Number of Persons Required per Task

In Table 2, tasks are described that require compliance with the four-eyes principle – with one representative for each of the given roles. All other activities can be carried out by one person. It shall be ensured that each role can be carried out by sufficient numbers of co-workers to ensure uninterrupted operations.

Task	Roles
Clearance and transmission of certificate and revocation applications for CA-Certificates	CAO1 & CAO2
Generation of key pairs for CA-Certificates	CAO1 & CAO2
Start of procedure for issuing certificates and CRLs	CAO1 & CAO2
Exchanging hardware and software components for the certification	SA & CAO1

Table 2: Tasks requiring the separation of duties (four-eyes principle)

5.2.3 Identification and Authentication for Each Role

The identification and authentication for the roles shall take place on the basis of the role models described in Section 5.2.1 and Section 5.2.2. The technical access to the IT systems is by login name and password or a more secure procedure. Requirements regarding the use of passwords are to be given. Physical access to the IT systems must be regulated by access control measures. The access to bank deposit boxes shall require the personal identification and authentication of the key-holder.

5.2.4 Roles Requiring Separation of Duties

Table 3 shows the tasks that are not compatible with one another.

Role	Incompatible with (X)							
	TS	RG	CAO1	CAO2	SA	SO	R	ISO
TS - Applicant representative					X	X	X	X
RG - Registration Authority co-worker					X	X	X	X
CAO1 - CA operator				X	X	X	X	X
CAO2 - PIN Contributor			X				X	X
SA – System administrator	X	X	X				X	X
SO – System operator	X	X	X				X	X
R - Reviser	X	X	X	X	X	X		
ISO – Security officer	X	X	X	X	X	X		

Table 3: Incompatibility of roles

5.3 Personnel Controls

Personnel security measures for all CAs are described in the CPS of the DFN-PKI.

5.4 Audit Logging Procedures

Measures for security monitoring for all CAs are described in the CPS of the DFN-PKI.

5.5 Records Archival

Archiving measures for all CAs are described in the CPS of the DFN-PKI.

5.6 Key Changeover

The period of validity of keys is specified in Section 6.3.2. If the key of a CA has been compromised, then the provisions of Section 5.7 shall apply. After generation of a new CA key this 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 dealing with security incidents and the compromising of private keys of a CA shall be documented in writing and handed to all personnel. The principles of the procedures are provided in the following sub-Sections. The CA addresses any critical vulnerability not previously addressed, within a period of 48 hours after its discovery. When a breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the CA will notify the natural or legal person of the breach of security or loss of integrity without undue delay.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

If faulty or manipulated computers, software and/or data are determined within a CA that could impact on the processes of the CA, then the operation of the relevant IT systems shall be stopped immediately.

The IT system must be restored on replacement hardware, with the software and the data from the security back-up, checked, and then put into service in a secure environment. Following this, the faulty or modified

IT system shall be analysed. If intentional acts are suspected then legal steps shall be taken as appropriate. In addition, security shall be reviewed in order to identify weak points. If necessary, additional defence measures shall be adopted to avoid similar incidents in the future. In such cases, the personnel of the DFN-PCA shall work together with the experts of the computer emergency team in DFN (DFN-CERT).

5.7.3 Entity Private Key Compromise Procedures

If a private key has been compromised, then the associated certificate must be revoked (see Section 4.9.1).

If the private key of a CA has been compromised, then the certificate of the CA and all certificates issued with it shall be revoked. All affected Subscribers and Subjects shall be informed.

5.7.4 Business Continuity Capabilites After a Disaster

The resumption of the certification operations after a catastrophe must be part of the emergency planning, and resumption shall be possible within a short time as soon as the certification service is secure. The assessment of the security situation is the responsibility of the security officer.

5.8 CA or RA Termination

If a CA ceases operations, then the following measures shall be taken:

- Inform Subscribers or the Subjects and the Relying Parties
- Revoke all certificates issued by the CA, including all Certificates of applicant representatives
- Destroy the private keys of the CA
- Withdraw all authorisations to act on behalf of the CA

The DFN-PCA shall ensure that the archive and the complete revocation list continue to be accessible for the assured retention period (see CPS of DFN-PKI Section 5.4.3).

6 Technical Security Controls

Suitable technical security measures are a precondition for the secure operation of a PKI. The main aspects of these security measures are described in the CPS of DFN-PKI. More detailed information is specified in a security strategy. In the following, the measures for technical security are outlined. Details are contained in the internal operating manual "*Betriebshandbuch der DFN-PKI*" (in German).

If not otherwise specified, security measures are based on the IT Security Guidelines - Federal Office for Information Security [IT-GSHB].

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The key pairs of all CAs shall be generated in a hardware security module (HSM) in accordance with the requirements of Section 6.2.1, applying the four-eyes principle (see Section 5.2.2). The number of personnel authorised for this task shall be limited to an operational minimum.

Subscribers shall generate their own key, following the regulations specified in the document "*Pflichten der Teilnehmer*".

6.1.2 Private Key Delivery to Subscriber

No entry.

6.1.3 Public Key Delivery to Certificate Issuer

The Certificate Signing Request (CSR) of the Subscriber shall be transmitted to the CA by e-mail, HTTPS or on a data medium. The correspondence of the CSR to a specific certificate application shall be confirmed by signature or electronic signature.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of all CAs of the DFN-PKI can be accessed through an information service in accordance with Section 2.

6.1.5 Key Sizes

With the use of an RSA algorithm, all keys used shall have a minimum size of 2048 Bit. Other key sizes may be used if they provide at least equivalent security.

6.1.6 Public Key Parameters Generation and Quality Checking

All cryptographic algorithms in accordance with Appendix A of [CAB-BR] are valid. All Certificates are signed with SHA-2 using the padding in accordance with PKCS#1 v2.1. Other algorithms may be used if they provide at least equivalent security.

CA-keys may not be used beyond the period of validity allowed on the basis of the algorithm.

Keys that are known to be compromised (e.g. “Debian weak keys”) or keys with weak parameters such as Value 1 RSA exponents shall not be used.

6.1.7 Key Usage Purposes

The private keys of the CAs shall only be used for issuing certificates and for signing revocation information.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The private key of every CA shall be stored in an HSM. When transported and stored, HSMs must be secure from manipulation.

6.2.1 Cryptographic Module Standards and Controls

HSMs that are used in accordance with Section 6.2 shall comply with one of the following or an equivalent standard:

- FIPS 140-1 Level 3
- CC EAL4

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

Access to the private key of a CA shall follow the four-eyes principle in accordance with Section 6.2.8 by the roles CAO1 and CAO2 jointly.

6.2.3 Private Key Escrow

DFN-PCA does not provide private key escrow.

6.2.4 Private Key Backup

CA-keys are backed-up with FIPS-140 Level 3-conformant mechanisms of the HSM, with CA-keys in encrypted form. The encryption can only be carried out by the roles CAO1 and CAO2 in the HSM in accordance with the four-eyes principle. The four-eyes principle will be implemented by a PIN in two halves, with one half each known to the roles CAO1 and CAO2. Written copies of the two PIN halves are to be placed in sealed envelopes and deposited with a public notary.

The backup of the CA-key shall be stored in a bank deposit box.

6.2.5 Private Key Archival

For archiving of private keys the regulations of Section 6.2.4 apply.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

A private key of a CA are always generated in an HSM in accordance with Section 6.1.1.

6.2.7 Private Key Storage on Cryptographic Module

Private keys of a CA shall always be stored in an encrypted form on a cryptographic module.

6.2.8 Method of Activating Private Key

The PIN of private keys of a CA must be split into two halves. One half is known only to the role CAO1 and the other half only to the role CAO2. Activation is only possible in accordance with the four-eyes principle.

6.2.9 Method of Deactivating Private Key

The deactivation of the private key of a CA shall follow automatically when the certification process has ended.

6.2.10 Method of Destroying Private Key

Before decommissioning an HSM, all the private keys stored on it must be destroyed. All copies of the private key of a CA must be destroyed after at the end of their life cycle.

When destroying the private key of a CA, the four-eyes principle shall be applied. The roles “ISO” and “CAO1” are responsible for the destruction.

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 for the following periods:

- Certificates for CAs (including for the DFN-PCA): a maximum of fifteen (15) years
- All other certificates for data processing systems: a maximum of 825 days, after 01 September 2020: 398 days.
- Certificates for natural persons and groups (user certificates): a maximum of five (5) years
- Certificates cannot be valid for longer than the issuing CA certificate.

For the period of use of key pairs, the rules from Section 6.1.6 apply. Before the key of a CA becomes invalid, a new key pair is generated in good time and made known to the relevant parties.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

For passwords or PINs to activate private keys, non-trivial combinations of alphanumeric characters and special characters shall be selected. CA-keys shall contain at least 15 characters, and other keys 8 characters.

6.4.2 Activation Data Protection

Activation data shall be kept secret and shall only be known by the personnel who need to know in accordance with Section 5.2.1 in order to carry out a specific function.

6.4.3 Other Aspects of Activation Data

No entry.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

All CAs shall be operated solely on the basis of hardened operating systems. In addition, access controls and user authentication shall be implemented as security measures.

6.5.2 Computer Security Rating

The security measures specified in Section 6.5.1 be according to the state of the art.

6.6 Life Cycle Technical Controls

For all CAs, the life-cycle of the security measures is described in the CPS of DFN-PKI.

6.7 Network Security Controls

For all CAs, the security measures for the network are described in the CPS of DFN-PKI.

6.8 Time-Stamping

No time stamping service is provided in the context of this CP.

7 Certificate, CRL, and OCSP Profile

7.1 Certificate Profile

Each certificate must be assigned to a unique serial number by the issuing CA. The serial number contains at least 64 Bit random data.

7.1.1 Version Number

Certificates are issued in accordance with the international standard X.509 in the Version 3. All Certificates include the following:

- Identification of the issuing CA and the country in which it is located
- The name of the Subject or a corresponding pseudonym
- The public key that corresponds to the private key under the control of the Subject
- The initial and final dates of the validity period of the certificate
- The series number of the certificate
- The electronic signature of the issuing CA
- If appropriate, limitations on the scope of use of the certificate

7.1.2 Certificate Extensions

All certificate extensions in accordance with [X.509], [PKIX], [PKCS] and specific manufacturer extension are permitted.

Certificates for CAs

In certificates for CAs, the extension keyUsage shall be included with the values “keyCertSign” and “cRLSign” and the extension basicConstraints with the value “CA=True”. Certificates for CAs include an extension cRLDistributionPoint with a reference to the relevant revocation list and an extension authorityInfoAccess with a reference to the signing CA certificate and the relevant OCSP service.

End-entity certificates

Certificates for all other uses are optionally marked as non-CA certificate with the extension basicConstraints with the value “CA=False” and have no CA-specific keyUsage extension, i.e. the extension keyUsage may not contain the values “keyCertSign” or “cRLSign”.

The keyUsage extension may only have the value “nonRepudiation” if the private key cannot be restored and the private key can only be accessed by the Subject due to technical and organisational measures.

End-Entity-Certificates always contain the extension cRLDistributionPoint with a reference to the associated revocation list and the extension authorityInfoAccess with a reference to the signing CA-certificate. Certificates for data processing systems and certificates for natural persons and groups also always include the extension authorityInfoAccess with a reference to the relevant OCSP service.

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.

Domain names and IP addresses that are contained in the Subject-DN are also always included in the alternative certificate name (“subjectAlternativeName”) under the attributes “dNSName” or “iPAddress”.

7.1.5 Name Constraints

See Section 3.1.

7.1.6 Certificate Policy Object identifier

The following OIDs are included in Certificates:

Certificates for data processing systems:

- 1.3.6.1.4.1.22177.300.30: Compliancy with the Baseline Requirements of CA/Browser Forum [CAB-BR] (see Section 1.1).
- CA/Browser forum reserved OID OV 2.23.140.1.2.2
- 1.3.6.1.4.1.22177.300.1.1.4: Note of the “Global” security level and conformity with [ETSI319411].
- OID of this CP in accordance with Section 1.2
- OID of the CPS valid for the issuing CA

Certificates for other End-Entity Certificates (not for data processing systems):

- 1.3.6.1.4.1.22177.300.1.1.4: Display of the “Global” security level and conformity with [ETSI319411].
- OID of this CP in accordance with Section 1.2

- OID of the valid CPS for the issuing CA CPS

Certificates for CAs:

- 1.3.6.1.4.1.22177.300.30: Compliancy with the Baseline Requirements des CA/Browser Forum [CAB-BR] (see Section 1.1).
- 1.3.6.1.4.1.22177.300.1.1.4: Note of the “Global” security level and conformity with [ETSI319411].
- Optional: 1.3.6.1.4.1.22177.300.1.1.4.2.2: OID von CP 2.2
- Optional: 1.3.6.1.4.1.22177.300.1.1.4.3.0: OID von CP 3.0
- Optional: 1.3.6.1.4.1.22177.300.1.1.4.3.1: OID von CP 3.1

7.1.7 Usage of Policy Constraints Extensions

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

For each CA in the DFN-PKI, a CRL is provided. This contains the revoked certificates of the CA. Each CRL contains the following information:

- Version number (see Section 7.2.1)
- Signature algorithm
- Identification of the issuing CA
- The date and time when issued in the field thisUpdate
- nextUpdate (see Section 4.9.7)
- Series numbers and revocation dates of the revoked certificates
- The electronic signature of the issuing CA

7.2.1 Version Number

Revocation lists shall be drawn up in accordance with the international standard X.509, Version 2.

7.2.2 CRL and CRL Entry Extensions

The extensions cRLNumber and authorityKeyIdentifer (variant keyid) are set.

7.3 OCSP Profile

The OCSP service is operated in accordance with [RFC6968].

OCSP-responses are signed with a certificate issued by the CA of the certificate to be tested.

8 Compliance Audit and Other Assessments

The procedures for all CAs of DFN-PCA are to be designed so that they comply with this CP and the CPS of the DFN-PKI.

8.1 Audited sectors

The sectors covered by an audit or assessment and the method of conformity testing shall be in accordance with ETSI EN 319 411-1 [ETSI319411].

8.2 Frequency and circumstances of assessment

Frequency and circumstances of the assessment are regulated by ETSI EN 319 411-1 [ETSI319411].

8.3 Identity/Qualifications of Assessor

The assessment shall be carried out by an accredited auditor in accordance with ETSI EN 319 411-1 [ETSI319411].

8.4 Assessor's Relationship to Assessed Entity

The relationship of the assessor to the assessed entity follows from Section 8.3.

8.5 Actions Taken as a Result of Deficiency

The repair of identified deficiencies is the responsibility of the DFN-Verein.

8.6 Communications of Results

The communication of the results is the responsibility of the DFN-Verein.

9 Other Business and Legal Matters

9.1 Fees

The DFN-Verein charges for its services at the usual rates of DFN-PKI.

9.2 Financial Responsibility

Insurance cover and guarantees for material defects and deficits of title are not provided for.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All information about subscribers to DFN-PKI or subjects that is not covered by Section 9.3.2, shall be deemed to be confidential information. Subjects are entitled to inspect the data that was archived relating to the issuance of their certificate. Within the scope of the German Data Protection Act, the same shall apply for the subscriber.

9.3.2 Information Not Within the Scope of Confidential Information

Information is classified as non-confidential if it is contained in the published certificates and revocation lists either explicitly (e.g. e-mail addresses) or implicitly (e.g. data about the certification) or if it can be derived from these.

9.3.3 Responsibility to Protect Confidential Information

The DFN-PCA is responsible for measures to protect confidential information. Data may only be passed on in the course of providing services if a confidentiality declaration has previously been signed and the personnel entrusted with the tasks have given an undertaking to comply with the legal requirements for data protection.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The DFN-PCA must electronically store and process the private data required for the provision of its services. This is done in compliance with the German Federal Data Protection Act (BDSG).

9.4.2 Information Treated as Private

For private data, the provisions of Section 9.3.1 shall apply by analogy.

9.4.3 Information Nnot Deemed Private

For private data the provisions of Section 9.3.2 shall apply by analogy.

9.4.4 Responsibility to Protect Private Information

For private data, the provisions of Section 9.3.3 shall apply by analogy.

9.4.5 Notice and Consent to Use Private Information

The DFN-PCA utilises private data to the extent that is necessary to perform the services.

9.4.6 Disclosure Pursuant to Judicial and Administrative Process

The DFN-Verein is subject to the laws of the Federal Republic of Germany and must release confidential and private information if obliged to do so under law or if a court orders the release.

9.4.7 Other Information Disclosure Circumstances

No further circumstances are envisaged for a disclosure of information.

9.5 Intellectual Property rights

The DFN-Verein is originator of this CP, and the CPS of the DFN-PKI. These documents may be distributed to third parties in an unchanged state. No further transmission is permitted. In particular, the transmission of amended versions and the dissemination in machine-readable forms or in amendable forms of electronic storage, in whole or in part, is not permitted without the agreement of the DFN-Verein.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The DFN-PKI is a service of the *Verein zur Förderung eines Deutschen Forschungsnetzes e.V.* (DFN-Verein). The DFN-PCA is operated by the DFN-CERT Services GmbH (DFN-CERT) under a service contract for data processing. The DFN-Verein carries out the resultant audit duties with regard to DFN-CERT and thus ensures that the agreed procedures can be implemented.

If further contractors carry out duties in the DFN-PKI, then it will be verified by means of suitable measures and assessments that the tasks carried out comply with the requirements in accordance with the CP and CPS of DFN-PKI. The responsibility for the operation of the CAs of DFN-PKI remains with the DFN-Verein.

The DFN-Verein has adopted adequate measures within the framework of legal requirements for the eventuality that, as a result of insolvency or for other reasons, it is itself no longer in a position to ensure the minimum continuation of services after termination of the CA operations in accordance with [ETSI319411].

The DFN-Verein has taken adequate precautions in order to be able to meet the liabilities arising from its activities with relation to the DFN-PKI.

The DFN-Verein has the financial stability and the resources to operate a CA in conformity with the requirements of [ETSI319411].

The departments of the DFN-PCA that issue and revoke certificates have a documented structure that ensures impartial execution of their duties.

The DFN-PCA undertakes to carry out conscientiously all the duties described in this CP and the CPS of the DFN-PKI.

9.6.2 RA Representations and Warranties

The DFN-PCA is obliged to carry out all the duties specified in this CP and in the CPS of DFN-conscientiously.

9.6.3 Subscriber Representations and Warranties

Each subscriber shall sign a subscriber agreement with the DFN-Verein. In this the subscriber undertakes in particular to comply with this CP.

In addition, the provisions contained in the document "*Pflichten der Teilnehmer*" shall be complied with. The Subscriber shall also inform Subjects about the provisions in the document "*Information für Zertifikatinhaber*" and obtain their undertaking to comply with these. When the certificate is sent to the Subject by e-mail, the DFN-PCA will attach this document.

9.6.4 Relying Party Representations and Warranties

The provisions of section 4.5.2 apply.

9.6.5 Representations and Warranties of Other Participants

To the extent that other participants are involved in the certification process as service-providers, then the DFN-PCA is responsible for obliging the service-provider to comply with the CP and the CPS of the DFN-PKI.

9.7 Disclaimer of Warranties

Warranty is regulated in the contracts between the participating parties.

9.8 Limitations of Liability

Limitations of liability are regulated in the contracts between the participating parties.

9.9 Indemnities

Indemnification is regulated in the contracts between the participating parties.

9.10 Term and Termination

9.10.1 Term

The CP and the CPS of DFN-PKI come into force on the date contained in them. They will be made public through the corresponding information service (see Section 2). A change to the CP or CPS of the DFN-PKI will be announced in advance by the DFN-Verein, giving a period of notice appropriate for the scope of the amendments, but at least two weeks in advance.

The management board of the DFN-Verein is responsible for the implementation of and compliance with this CP and the CPS of the DFN-PKI.

9.10.2 Termination

This document is valid until it is replaced by a new version (see section 9.10.1) or until the DFN-PCA ceases operations.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

The DFN-PCA retains the right to make other communications apart from those specified in this CP, at its discretion.

9.12 Amendments

An amendment to the CP may only be made by the management of the DFN-Verein. If amendments affect security-relevant aspects or require the Subscriber to make changes to procedures, then the OID of the CP shall be amended (see Section 1.2).

9.13 Dispute Resolution Provisions

The contact named in Section 1.5.2 is responsible for the resolution of disputes. If a dispute cannot be resolved at this level, then the management of the DFN-Verein can be called on, and if necessary the Committee of the DFN-Verein.

9.14 Governing Law

The operations of the DFN-PKI are governed by the laws of the Federal Republic of Germany.

9.15 Compliance with Applicable Law

In the DFN-PKI, the DFN-Verein issues certificates with which advanced electronic signatures can be generated in accordance with the German Digital Signature Act. These may be called on as evidence before a court of law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

All the provisions contained in this CP and the CPS of the DFN-PKI apply between the DFN-Verein and the participants. When a new version is issued it replaces all previous versions. Verbal agreements and side agreements are not valid.

9.16.2 Assignments

Rights and obligations arising from this CP can be assigned in accordance with usual legal requirements.

9.16.3 Severability

Should individual provisions of this CP or the CPS of the DFN-PKI prove to be ineffective or incomplete this shall not affect the validity of the other provisions.

Instead of the ineffective provision, an effective provision shall be deemed to be agreed which comes as close as possible to the intention of the ineffective provision. In the event of gaps, then a provision shall be deemed to be agreed that would have reasonably been agreed in accordance with the intention of this CP or the CPS if the matter had been taken into consideration from the start.

9.16.4 Legal disputes / Place of jurisdiction

Legal disputes arising from the actions of a CA operating within the DFN-PKI are subject to the laws of the Federal Republic of Germany. Place of performance and exclusive place of jurisdiction is the location of the DFN-Verein. The DFN-Verein is registered at the Local Court Berlin-Charlottenburg under the number 7729NZ.

9.17 Other Provisions

No entry.

10 References

[CAB-BR] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum, https://cabforum.org/baseline-requirements/

[DFN2000] Satzung des DFN-Vereins, July 2000, http://www.dfn.de/fileadmin/6Organisation/Geschaeftsstelle/satzungdfn.pdf

[EIDAS Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910]

[ETSI319411] Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, EN 319 411-1

[IANA_IP4] Internet Protocol version 4 (IPv4) Address Space, IANA, http://www.iana.org/assignments/ipv4-address-space

[IANA_IP6] Internet Protocol Version 6 Address Space, IANA, https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml

[ISO-3166-1] Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm

[IT-GSHB] IT Security Guidelines - Federal Office for Information Security https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITSecurityGuidelines/guidelines.html

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

[PKIX] RFCs und Spezifikationen der IETF Arbeitsgruppe Public Key Infrastructure (X.509)

[RFC2606] Reserved Top Level DNS Names, Network Working Group, IETF, 1999

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

[RFC6844] DNS Certification Authority Authorization (CAA) Resource Record, P. Hallam-Baker, R. Stradling IETF, 2013

[RFC6960] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, S. Santesson et. al., IETF, 2013

[RFC822] Standard for ARPA Internet Text Messages, David H. Crocker, 1982

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

11 Glossary and abbreviations

Term	Explanation
Applicant	The applicant is always a subscriber
Authorization Domain Name	The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Term	Explanation
Base Domain Name	The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.
CA	Certification Authority
CA certificate	Certificate from with further certificates (CA and/or End-Entity certificates) can be issued
CRL	Certificate Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
CSR	Certificate signing request
DFN-PCA	Main certification authority of the DFN-PKI (Policy Certification Authority)
Subscriber agreement	Contractual basis for subscribing to the DFN-PKI
DN	Unique name of the Subject or issuer in certificates. (Distinguished name)
End-entity certificate	All non-CA certificates
Certification Practice Statement (CPS)	Practical (technical and organisational) implementation of the certification policy
Domain Contact	The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.
EXT	Attribute in CN: external subject
GRP	Attribute in CN: Person or functional group
Subject information	Information for the Subject on handling private keys t
OCSP	Online Certificate Status Protocol
Public key	Key of a cryptographic key pair which is made public. It can be used to check electronic signatures
OID	Object identifier – unique reference to an object in a name space
PCA	Policy Certification Authority
PKCS#7	Data exchange format for the transmission of signatures and encrypted data or for the distribution of certificates [PKCS]
PKCS#10	Data exchange format for transmission of the public key and DN of a certificate request (CSR) to a CA [PKCS]
PKCS#12	Data exchange format for the storage of private and public keys which are secured with a password on the basis of a symmetrical encryption process [PKCS]
PKI	Public Key Infrastructure

Term	Explanation
PN	Attribute in CN: Pseudonym
Private key	Key of a cryptographic key pair, which is only available to the owner. A private key can be used to generate an electronic signature
RA	Registration Authority
Registration Authority	Registration authorities register subscribers of a CA and receive certificate requests for CAs
Revocation request	If a certificate is to be declared invalid before expiry, a revocation request must be submitted for this certificate
Revocation list	List of all revoked certificates of a CA
Subscriber	Subscribers are organisations that take part in the DFN-PKI and have signed a corresponding agreement with the DFN-Verein
Subscriber-service	A subscriber service carries out duties relating to the issuing of certificates that can more appropriately be done locally at the Subscriber.
Applicant Representative	The Applicant representative applies for certificates for the Subscriber, advises subjects, and can carry out personal identification on behalf of the Registration Authority
Certificate	Allocation of a cryptographic key to a name, confirmed by the signature of a CA
Certificate request	Document in paper or electronic form with which a CA applies for a certificate. It contains the name of the applicant, the DN for the certificate and the public key.
Subject	The entity described in the subject field of the certificate, i.e. a natural person, a group of individuals, or a data processing system
Certificate name	Synonyms: Subject-DN, Name
Relying party	Natural person or legal entity relying on the certificate
Public key infrastructure (PKI)	The technical equipment and associated processes and concepts necessary for asymmetrical cryptography
Certificate Policy (CP)	The Certificate Policy of a PKI specifies the provisions that all participants must comply with. Each PKI contains only one certificate policy.
Certification Authority (CA)	The main task of the certification authority is the issuing of certificates