deutsches forschungsnetz

Certification Practice Statement of the DFN-PKI

– Security Level “Global” –

DFN-Verein
CPS of DFN-PKI
V16 26 November 2025

1 Introduction

1.1 Overview

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

This document is the *Certification Practice Statement of the DFN-PKI – Security Level "Global"* – (CPS) of DFN-PCA and all Sub-CAs for the Global Security Level. It covers specifications, processes, and technical security measures of the DFN-PCA and all Sub-CAs for the issuing of certificates.

This document belongs together with the Certificate Policy (CP) of the DFN-PKI in the currently valid version: "Certificate Policy der DFN-PKI – Global Security Level – ".

In the following, reference is made to DFN-PKI and DFN-PCA solely in the context of the Global Security Level.

The work of the DFN-PCA and all sub-CAs is carried out on behalf of the DFN-Verein by the DFN-CERT Services GmbH.

1.2 Document Name and Identification

This document is identified as follows.

Title: Certification Practice Statement der DFN-PKI – Security Level "Global" –

Version: 16

Object Identifier (OID): 1.3.6.1.4.1.22177.300.2.1.4.16

The OID [OID] consists of the following:

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) dfn-verein(22177) pki(300) cps(2) x.509(1) global (4) major-version(16)}

1.3 PKI Participants

See CP.

1.4 Certificate Usage

See CP.

1.5 Policy Administration

See CP.

1.6 Definitions and Acronyms

See CP.

2 Publication and Repository Responsibilities

See CP.

CP and CPS are published in German and English. The German and English versions always have the same version number and are synchronised in terms of content. The English version is authoritative.

3 Identification and Authentication

See CP.

4 Certificate Life-Cycle Operational Requirements

See CP.

5 Facility, Management and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The technical systems of all CAs are located in the operational premises of the DFN-PCA. The premises provide sufficient protection in terms of infrastructure security measures. There is an alarm system with a connection to a security service.

5.1.2 Physical Access

Access to the operational premises of the DFN-PCA secured by suitable technical and infrastructure measures and is only permitted for authorised personnel. Access by third parties is governed by visitor regulations.

5.1.3 Power and Air Conditioning

The power supply is installed in accordance with the relevant standards; air conditioning is provided for the operational rooms for the technical infrastructure.

5.1.4 Water Exposures

The operational rooms for the technical infrastructure are appropriately protected against damage by water.

5.1.5 Fire Prevention and Protection

The fire protection regulations are complied with; sufficient numbers of hand-held fire extinguishers are available.

5.1.6 Media Storage

Paper documents relating to certification are stored in a locked steel cabinet. Date storage media with key material of CAs and backup media are stored in a safe of VdS Class I or higher.

5.1.7 Waste Disposal

Information on electronic data storage media and on paper shall be destroyed in a qualified manner and then suitably disposed of by a service provider.

5.1.8 Off-Site Backup

External backup media are stored in a bank deposit box.

5.2 Procedural Controls

5.2.1 Trusted Roles

See CP.

5.2.2 Number of Persons Required per Task

See CP.

5.2.3 Identification and Authentication for Each Role

See CP.

5.2.4 Roles Requiring Separation of Duties

See CP.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

The personnel of the DFN-PCA are appointed by the management. The appointment will not take effect until the employee accepts it. Employees meet all the necessary requirements regarding trustworthiness, integrity, reliability and expertise. In addition to qualifications in the field of computer sciences they have appropriate expertise in the fields of:

- Security technology, cryptography, electronic signatures, PKI

- International standards, technical codes of practice
- National and international jurisdiction
- Unix/Linux operating systems, TCP/IP networks and relational databases

The employers of personnel with security-critical roles shall keep them free from conflicts of interests with the policy of DFN-PKI which could impair their impartiality.

5.3.2 Background Check Procedures

For all personnel of the DFN-PCA, a police certificate of good conduct shall be held that is not more than three years old. Before their certificate exceeds the three year period, a co-worker shall be called on to present a new certificate of good conduct. Appointment of a new employee will not be effective until a certificate of good conduct is available.

5.3.3 Training Requirements

In the DFN-PCA, only qualified personnel shall be employed for whom suitable training is provided at regular intervals. Records of the training shall be archived in accordance with the provisions of Section 5.5. Personnel shall require documentation that they possess the required skills before being allowed to carry out a specific task.

5.3.4 Retraining Frequency and Requirements

The frequency of training is oriented on the requirements of the DFN-PCA; as a rule, retraining shall be provided annually. Training sessions shall also be provided after the introduction of new regulations, IT systems and security technology.

5.3.5 Job Rotation Frequency and Sequence

There are no requirements on job rotation.

5.3.6 Sanctions for Unauthorised Actions

Unauthorised actions that endanger the security of the IT systems of DFN-PCA or that breach data protection regulations shall meet with disciplinary sanctions and the individual shall be released form their duty if appropriate. In cases of criminal relevance, the responsible authorities shall be informed.

Applicant representatives who breach their obligations shall be retrained. In the event of repeated breaches they shall be relieved of their duty and the corresponding certificate revoked.

5.3.7 Independent Contractor Requirements

The employment contracts of the personnel of DFN-PCA are governed by the laws of the Federal Republic of Germany. All personnel are bound to confidentiality in accordance with the legal provisions for data protection.

5.3.8 Documentation Supplied to the personnel

In addition to the CP and this CPS, the personnel of DFN-PCA also have access to the operating manual of DFN-PCA.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

To defend against attacks, on the technical systems of the DFN-PCA, and to confirm the orderly functioning of the DFN-PCA, among other things the following events shall be recorded in the form of audit logs together with the time when the event occurred:

1. CA certificate and key lifecycle events:
    1. Key generation, backup, storage, recovery, archival, and destruction;
    2. Certificate requests, renewal, and re-key requests, and revocation;
    3. Approval and rejection of certificate requests;
    4. Cryptographic device lifecycle management events;
    5. Generation of Certificate Revocation Lists;
    6. Signing of OCSP Responses and
    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

2. Subscriber Certificate lifecycle management events:

1. Certificate requests, renewal, and re-key requests, and revocation;
2. All verification activities;
3. Approval and rejection of certificate requests;
4. Issuance of Certificates;
5. Generation of Certificate Revocation Lists; and
6. Signing of OCSP Responses
7. Multi-Perspective Issuance Corroboration attempts from each Network Perspective, minimally recording the following information:
   - an identifier that uniquely identifies the Network Perspective used;
   - the attempted domain name and/or IP address; and
   - the result of the attempt (e.g., "domain validation pass/fail", "CAA permission/prohibition").
8. Multi-Perspective Issuance Corroboration quorum results for each attempted domain name or IP address represented in a Certificate request (i.e., "3/4" which should be interpreted as "Three (3) out of four (4) attempted Network Perspectives corroborated the determinations made by the Primary Network Perspective).
9. as well as request for unknown certificate serial numbers in OCSP.

3. Security events, including:

1. Successful and unsuccessful PKI system access attempts;
2. PKI and security system actions performed;
3. Security profile changes;
4. Installation, update and removal of software on a Certificate System;
5. System crashes, hardware failures, and other anomalies;
6. Firewall and router activities (as described in Section 5.4.1.1); and
7. Entries to and exits from the CA facility.

4. other events:

1. availability and utilization of services and networks
2. start and termination of the log function

The system time shall be continuously synchronised with a reference time UTC, e.g. via GPS or DCF77 at least every 24 hours. Suitable measures shall be used to ensure the precision and monotony of the time in accordance with the state of the art.

The audit log data shall be archived in accordance with the relevant requirements (See Section 5.5).

Monitoring events ensures accountability of individual employees.

The log data is made available to auditors as part of conformity audits.

5.4.1.1 Router and firewall activities logs

Logging of router and firewall activities includes the following:

1. Successful and unsuccessful login attempts to routers and firewalls; and

2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and

3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and

4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2 Frequency of Processing Log

The audit logs shall be checked at regular intervals, at least one a month. If unusual events are suspected then special checks shall be carried out.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained for at least seven years after termination of all certificates related to the audit.

5.4.4 Protection of Audit Log

Electronic log-files shall be protected against access, deletion and manipulation by means of the operating system, and shall only be accessible by the system and network administrators.

5.4.5 Audit Log Backup Procedures

The audit logs shall be backed up regularly together with other relevant data of DFN-PCA.

5.4.6 Audit Collection System

An internal monitoring system is used.

5.4.7 Notification to Event-Causing Subject

Serious events shall be immediately reported to the security officer. Necessary steps shall be taken in cooperation with the system administrators in order to respond adequately, if appropriate the management shall be informed.

5.4.8 Vulnerability Assessment

Every three months or after major system changes, a vulnerability scan is performed on the systems of the PCA. If the CA/Browser Forum requests a vulnerability scan, it will be performed within one week. Once a year or after major system changes a comprehensive penetration test is performed.

Vulnerability scans and penetration tests are performed by competent, independent experts. Their qualification is recorded.

5.5 Records Archival

5.5.1 Types of Records Archived

Documents and data from certificate applications, documents and data from the verification of the entries in certificate applications, issued certificates, as well as revocation information concerning certificates are archived.

5.5.2 Retention Period for Archive

The data specified in 5.5.1 shall be retained for at least seven years after all Certificates based on the documentation cease to be valid.

5.5.3 Protection of Archive

Suitable measures will be taken to ensure that the data cannot be changed, deleted, read without authorisation or copied. Furthermore its will be ensured that the relevant application for each certificate can be uniquely identified.

5.5.4 Archive Backup Procedures

The data listed in Section 5.4.1 and Section 5.5.1 are backed up on tape or other media on the basis of a data security strategy as follows:

Incremental backup on every working day

Complete weekly backup

Monthly archive backup

The backup media are stored in the premises outside the server room

Regular restore tests incl. documentation

5.5.5 Requirements for Time-Stamping of Records

System time used for time-stamping is synchronized with a DCF77 clock.

5.5.6 Archive Collection System

An internal archiving system is used.

5.5.7 Procedures to Obtain and Verify Archive Information

The security officer is entitled to authorise the obtaining and verifying of archived data.

5.6 Key Changeover

See CP.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The DFN-PCA maintains a comprehensive and actionable plan for mass revocation events. The mass revocation plan is tested annually. Lessons learned are incorporated.

5.8 CA or RA Termination

See CP.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

See CP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

See CP.

6.3 Other Aspects of Key Pair Management

See CP.

6.4 Activation Data

See CP.

6.5 Computer Security Controls

See CP.

6.6 Life Cycle Security Controls

6.6.1 System Development

Software is developed by qualified personnel in a secure development environment. Software (whether produced internally or by third parties) is only used on a productive system after checking and release. Details of the software development are contained in the internal operating manual (*Betriebshandbuch der DFN-PKI*).

6.6.2 Security Management

The security management covers the following aspects:

- Annual audit (compliance testing)
- Regular evaluation and further development of the security strategy
- Checking security for on-going operations (See Section 5.4)
- Regular integrity testing of the applications and operating systems
- Central logging of all security-relevant events
- Cooperation with DFN-CERT
- At least weekly check of the configurations according to chapter 3h) of the Network and Certificate System Security Requirements of the CA/Browser Forum
- Upgrading or patching as necessary

- Account management and timely modification or removal of access permissions
- The integrity of the systems and information is protected against viruses, malicious and unauthorized software.

Updates or vendor provided patches are first installed in a test environment. If it is found that the updates or patches introduce instabilities or vulnerabilities that outweigh the benefits, they are not installed on production systems. Otherwise, they are installed. The installation is documented. Decisions about not installing updates or patches is also documented.

Changes to systems or configurations, for regular changes and for emergency measures, are performed through change control procedures. Changes are documented.

6.6.3 Life Cycle Security Controls

Hardware and software for issuance systems are continuously maintained. Life cycle procedures for evaluated systems, e.g. HSMs, are strictly followed.

6.7 Network Security Controls

The network of the DFN-PCA is divided into various security zones which are separated from one another by a firewall system. All security measures are applied to all systems in the same zone. The network used for administration is separated from the operational network. Systems which are used to administrate the implementation of the security policy are not used for other purposes. Two distinct data centers with redundant network connections are used.

Intrusion Prevention and Detection Systems are used to defend against attacks from the Internet and from the Intranet. Critical security incidents are immediately followed up and investigated in cooperation with DFN-CERT. For all Firewall Systems, a regulatory system is activated that only permits the network traffic that is allowed in a defined communications matrix.

Unused accounts, applications, services, protocols and ports are removed or deactivated on the DFN-PCA systems.

6.8 Time-Stamping

See CP.

7 Certificate, CRL and OCSP Profiles

See CP.

8 Compliance Audit and Other Assessments

See CP.

9 Other Business and Legal Matters

See CP.

10 References

See CP.

11 Glossary

See CP.

12 Change history

For changes further in the past refer to https://doku.tid.dfn.de/de:dfnpki:policyarchiv

Version	Change	Date
6	Title and footer: Version number and date 1.2: OIDs	03.04.2020

7	Title and footer: Version number and date 1.2: OIDs	03.06.2020
8	Title and footer: Version number and date 1.2: OIDs 5.1.1: Description of alarms 5.4.1: Entry/Exit and availabilty/capacity 5.4.8: Description of vulnerability scans and penetration tests 6.6.2: Change Control 6.7: Description of separation of networks	30.09.2020
9	Title and footer: Version number and date 1.2: OIDs	30.06.2021
10	Title and footer: Version number and date 1.2: OIDs	01.10.2021
11	Title and footer: Version number and date. 1.2: OIDs 5.3.1: Acceptance of a appointment 5.3.2: Appointment not effective until present 5.4.1: Monitored events described in more detail, time synchronization documented more precisely 5.5.4: Restore tests also described here 6.6.2: Integrity of systems 6.7: Network security measures added	14.11.2022
12	Title and footer: Version number and date, reference to CC-BY-ND. 1.2: OIDs 5.4.1 Insight into log data during an audit; documentation of events adapted.	01.09.2023
13	Title: English version is authoritative 1.2: OIDs 2: English version of CP/CPS is authoritative 5.3.1: Events expanded.	29.09.2023
14	Title and footer: Version number and date, reference to CC-BY-ND. 1.2: OIDs 5.4.1 and 5.4.1.1: Requirements on router and firewall logging refined 12: URL to policy archive changed	22.08.2024
15	Title and footer: Version number and date 1.2: OIDs	29.07.2025
16	Title and footer: Version number and date 1.2: OIDs 5.4.1 MPIC events 5.7.1 Mass revocation plan	26.11.2025