Certification Practice Statement
of the Policy Certification Authority
of the DFN-PKI

- Security levels: Global, Classic and Basic -
1 Introduction
As part of the DFN-PKI, the DFN-Verein operates the top-level certification authority (CA), the so-called PCA (Policy Certification Authority) for the Global, Classic and Basic security levels.

1.1 Overview
A variety of security levels are supported within the DFN-PKI. All regulations in this Certificate Practice Statement (CPS) apply to the three security levels “Global”, “Classic” and “Basic”.

This document is the CPS of the PCA of the DFN-PKI. It describes specifications, processes and technical security measures of the PCA for the certificate issuing process.

This document is accompanied by the Certificate Policy (CP) of the DFN-PKI in the relevant current version: “DFN-PKI Certificate Policy - Security levels: Global, Classic and Basic -”.

The PCA, the CAs for DFN-sites and CAs for individual users whose organizations do not offer their own certification services at present are centrally operated by DFN-CERT Services GmbH on behalf of the DFN-Verein.

1.2 Document name and identification
This document is identified by the following details.
- Title: Certificate Practice Statement of the Certificate Policy Authority of the DFN-PKI - Security levels: Global, Classic and Basic -
- Version: 2.1
- Object Identifier (OID): 1.3.6.1.4.1.22177.300.2.1.5.2.1

The OID [OID] has the following structure:

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

Please refer to Section 7.1.6 in the CP for OIDs to be included in certificates.

1.3 PKI participants

1.3.1 Certification authorities
See CP.

1.3.2 Registration authorities
The following primary registration authorities (RAs) are available for the PCA:
- DFN-Verein, Berlin office
- DFN-Verein, Stuttgart office
- DFN-CERT Services GmbH, Hamburg

1.3.3 Subscribers
See CP.

1.3.4 Relying parties
See CP.

1.3.5 Other participants
See CP.
1.4 Certificate usage
See CP.

1.5 Policy administration
See CP.

1.6 Definitions and acronyms
See CP.

2 Publications and repository responsibilities

2.1 Repositories
See CP.

2.2 Publication of certification information
All information required in accordance with the CP is provided under:
http://www.pki.dfn.de/policies/informationen

2.3 Time or frequency of publication
See CP.

2.4 Access controls on repositories
See CP.

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 the PCA are located in the operating rooms of the PCA at DFN-CERT Services GmbH or at the DFN core nodes. The operating rooms offer sufficient protection with regard to infrastructure-related security measures.

5.1.2 Physical access
Admittance to the operating rooms of the PCA and the DFN core network nodes is protected by means of suitable technical and infrastructure-related measures and is only granted to authorized employees. Admittance for external parties is defined by visitor regulations.

5.1.3 Power and air conditioning
The installation for power supply fulfils the necessary standards, and operating rooms are air conditioned for the technical infrastructure.

5.1.4 Water exposures
The operating rooms for the technical infrastructure are suitably protected against water damage.
5.1.5 Fire prevention and protection
Fire protection regulations are complied with, a sufficient amount of hand-operated fire extinguishers is available.

5.1.6 Media storage
Paper documents relating to certification is stored in a locked steel filing cabinet. Data media with key materials for CAs as well as backup media is stored in a safe that corresponds to Protection Class I or higher of the VdS [German Association of Indemnity Insurers].

5.1.7 Waste disposal
Information on electronic data media and paper-based data media is destroyed properly and then disposed of properly by a service provider.

5.1.8 Off-site backup
Externally-stored backup media is held in a safe 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
For its operation, the PCA splits the roles amongst the groups of persons as specified in table 1. No person may belong to more than one group.

<table>
<thead>
<tr>
<th>Group of persons</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>R, ISO</td>
</tr>
<tr>
<td>2</td>
<td>TS, RG, CAO1</td>
</tr>
<tr>
<td>3</td>
<td>CAO2, SA, SO</td>
</tr>
</tbody>
</table>

Table 1: Split of roles amongst groups of persons at the PCA

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements
The employees of the PCA meet all necessary requirements regarding trustworthiness, integrity, reliability and expert knowledge. Apart from being trained in the area of information technology, they have appropriate expert knowledge in the following areas:
- Security technology, cryptography, electronic signatures, PKI
- International and technical standards
- National and international legislation
- Unix/Linux operating systems, TCP/IP networks and relational databases

5.3.2 Background check procedures
For all employees, PCA holds police clearance certificates that are no older than two years.
5.3.3 Training requirements
The PCA exclusively deploys qualified employees who are given appropriate training on a regular basis. Only after they are able to produce evidence of the expert knowledge required, employees will be authorized to perform specific roles.

5.3.4 Retraining frequency and requirements
The frequency of training courses is based on the requirements of the PCA. Training is given in particular, when introducing new policies, IT systems and security technology.

5.3.5 Job rotation frequency and sequence
No information

5.3.6 Sanctions for unauthorized actions
Unauthorized actions that put the security of the IT systems of the PCA at risk or which violate data protection provisions are punished with disciplinary action. In the event of criminal relevance, the relevant authorities will be notified.

5.3.7 Independent contractor requirements
The law of the Federal Republic of Germany applies in relation to the employment contracts of the employees of the PCA. All employees are obligated to maintain secrecy in accordance with the legal data protection provisions.

5.3.8 Documentation supplied to personnel
Apart from the CP and this CPS, the operating manual of the PCA is available to the employees of the PCA.

5.4 Audit logging procedures
5.4.1 Types of events recorded
To prevent attacks and to control proper functioning of the PCA, among others, the following events are recorded in the form of log files or paper logs:
- boot processes
- failed login attempts
- receipt and approval of certificate requests and revocation requests
- issue and revocation of certificates
- setup and change of role mappings and authorizations

5.4.2 Frequency of processing log
The log data is reviewed on a regular basis at least once a month. On suspicion of extraordinary events, special checks will be carried out.

5.4.3 Retention period for audit log
The retention period for documents and certificates corresponds at least to the period of validity of the certificate of the CA with which the subscriber’s certificate was generated plus one year.

5.4.4 Protection of audit log
Using tools of the operating system, electronic log files will be protected against access, deletion and manipulation and can only be accessed by the system and network administrators.

5.4.5 Audit log backup procedures
The log data and other relevant data of the PCA are subjected to regular backups.
5.4.6 Audit collection system (internal vs. external)

An internal monitoring system is used.

5.4.7 Notification to event-causing subject

In the case of serious events, the security officer will be notified without delay. Necessary actions are defined in collaboration with the system administrators in order to be able to respond adequately to the events, and the Board of Management will be informed if necessary.

5.4.8 Vulnerability assessments

Defects are investigated by the PCA itself or by the manufacturer of the software used.

5.5 Records archival

5.5.1 Types of records archived

Data incurred as part of the certification process (e.g., certificate requests, certificates issued, revocation requests and CRLs) is archived.

5.5.2 Retention period for archive

The regulations in Section 5.4.3 apply.

5.5.3 Protection of archive

Appropriate measures are used to ensure that the data cannot be amended, deleted, read without authorization or copied.

5.5.4 Archive backup procedures

On the basis of a data backup concept, the data listed in Sections 5.4.1 and 5.5.1 is backed up to tape or CD-ROM with the following key values:

- incremental backup on every working day
- weekly full backup
- monthly archive backup
- The backup media is stored in the office premises outside the server room as well as in a safe deposit box outside the office premises.

5.5.5 Requirements for time-stamping of records

No details.

5.5.6 Archive collection system (internal or external)

An internal archiving system is used.

5.5.7 Procedures to obtain and verify archive information

The security officer can authorize archived data to be called up and reviewed.

5.6 Key changeover

See CP.

5.7 Compromise and disaster recovery

See CP.

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 technical controls

6.6.1 System development controls
Software is developed by qualified employees in a secure development environment. Software (in-house or third-party development) is only used on a live system after it has been accepted and approved.

6.6.2 Security management controls
Security management covers the following aspects:

- annual audit (conformity check)
- regular evaluation and further development of the security concept
- security audit during live operation (see Section 5.4)
- regular integrity reviews of the applications and operating systems used
- central logging of all security-relevant processes
- collaboration with the DFN-CERT
- import of upgrades and patches, if required

6.6.3 Life cycle security controls
No details.

6.7 Network security controls
The network of the PCA is split into various security zones which are partitioned by means of a firewall system. In addition, intrusion prevention or detection systems are used to prevent attacks from the Internet and intranet. Critical security incidents will be tracked and processed without delay in collaboration with the DFN-CERT. On all firewalls rules are activated which only permit network traffic that is permitted in a defined communication matrix.

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 manners
See CP.

10 References
See CP.

11 Glossary
See CP.