

Erklärung zum Zertifizierungsbetrieb der obersten Zertifizierungsstelle der DFN-PKI

- Sicherheitsniveaus: Classic und Basic -

Dieses Dokument einschließlich aller Teile ist urheberrechtlich geschützt.
Die unveränderte Weitergabe (Vervielfältigung) ist ausdrücklich erlaubt.
Die Überführung in maschinenlesbare oder andere veränderbare Formen der elektronischen Speicherung, auch auszugsweise, ist ohne Zustimmung des DFN-Vereins unzulässig.

Kontakt: pki@dfn.de

© DFN-Verein

Inhaltsverzeichnis

1 Einleitung	4
1.1 Überblick	4
1.2 Identifikation des Dokuments	4
1.3 Teilnehmer der Zertifizierungsinfrastruktur	4
1.4 Zertifikatnutzung	4
1.5 Verwaltung des Dokuments	5
1.6 Definitionen und Abkürzungen	5
2 Veröffentlichungen und Informationsdienste	5
2.1 Informationsdienste	5
2.2 Veröffentlichung von Informationen	5
2.3 Aktualisierung von Informationen	5
2.4 Zugriff auf Informationsdienste	5
3 Identifizierung und Authentifizierung	5
4 Ablauforganisation	5
5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen ..	5
5.1 Infrastrukturelle Sicherheitsmaßnahmen	5
5.2 Organisatorische Sicherheitsmaßnahmen	6
5.3 Personelle Sicherheitsmaßnahmen	6
5.4 Sicherheitsüberwachung	7
5.5 Archivierung	8
5.6 Schlüsselwechsel	8
5.7 Kompromittierung und Wiederherstellung	8
5.8 Einstellung des Betriebs	8
6 Technische Sicherheitsmaßnahmen	8
6.1 Schlüsselerzeugung und Installation	8
6.2 Schutz des privaten Schlüssels	8
6.3 Weitere Aspekte des Schlüsselmanagements	8
6.4 Aktivierungsdaten	9
6.5 Sicherheitsmaßnahmen für Computer	9
6.6 Lebenszyklus der Sicherheitsmaßnahmen	9
6.7 Sicherheitsmaßnahmen für das Netzwerk	9
6.8 Zeitstempel	9
7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen	9
8 Konformitätsprüfung	9
9 Rahmenvorschriften	9
10 Referenzen	9
11 Glossar	9

1 Einleitung

Im Rahmen der DFN-PKI betreibt der DFN-Verein für die Sicherheitsniveaus Classic und Basic jeweils die oberste Zertifizierungsstelle (CA), die sogenannte PCA (Policy Certification Authority).

1.1 Überblick

Innerhalb der DFN-PKI werden verschiedene Sicherheitsniveaus unterstützt. Alle Regelungen in dieser Erklärung zum Zertifizierungsbetrieb (CPS) gelten für die drei Sicherheitsniveaus "Classic" und "Basic".

Dieses Dokument ist die CPS der PCA der DFN-PKI. Es beschreibt Spezifikationen, Prozesse und technische Sicherheitsmaßnahmen der PCA für die Ausstellung von Zertifikaten.

Diesem Dokument zugehörig ist die Zertifizierungsrichtlinie (CP) der DFN-PKI in der jeweils aktuellen Version: "Zertifizierungsrichtlinie der DFN-PKI – Sicherheitsniveaus: Classic und Basic –".

Der Betrieb der PCA, der Betrieb von CAs für DFN-Anwender und der Betrieb zentraler CAs für einzelne Nutzer, deren Organisationen bisher keine eigenen Zertifizierungsdienstleistungen anbieten, erfolgt im Auftrag des DFN-Vereins durch die DFN-CERT Services GmbH.

1.2 Identifikation des Dokuments

Dieses Dokument ist durch folgende Angaben identifiziert.

- Titel: Erklärung zum Zertifizierungsbetrieb der obersten Zertifizierungsstelle der DFN-PKI – Sicherheitsniveaus: Classic und Basic -
- Version: 2.3
- Object Identifier (OID): 1.3.6.1.4.1.22177.300.2.1.6.2.3

Der OID [OID] ist wie folgt zusammengesetzt:

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

OID zur Aufnahme in Zertifikate finden sich in Abschnitt 7.1.6 im CP.

1.3 Teilnehmer der Zertifizierungsinfrastruktur

1.3.1 Zertifizierungsstellen

Siehe CP.

1.3.2 Registrierungsstellen

Für die PCA gibt es folgende ausgezeichnete Registrierungsstellen (RAs):

- DFN-Verein, Geschäftsstelle Berlin
- DFN-Verein, Geschäftsstelle Stuttgart
- DFN-CERT Services GmbH, Hamburg

1.3.3 Zertifikatnehmer

Siehe CP.

1.3.4 Zertifikatprüfer

Siehe CP.

1.3.5 Weitere Teilnehmer

Siehe CP.

1.4 Zertifikatnutzung

Siehe CP.

1.5 Verwaltung des Dokuments

Siehe CP.

1.6 Definitionen und Abkürzungen

Siehe CP.

2 Veröffentlichungen und Informationsdienste

2.1 Informationsdienste

Siehe CP.

2.2 Veröffentlichung von Informationen

Alle gemäß CP erforderlichen Informationen werden bereitgestellt unter:

<http://www.pki.dfn.de/policies/informationen>

2.3 Aktualisierung von Informationen

Siehe CP.

2.4 Zugriff auf Informationsdienste

Siehe CP.

3 Identifizierung und Authentifizierung

Siehe CP.

4 Ablauforganisation

Siehe CP.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

5.1.1 Lage und Konstruktion

Die technischen Systeme der PCA befinden sich in den Betriebsräumen der PCA bei der DFN-CERT Services GmbH oder an DFN-Kernnetzknotten. Die Betriebsräume bieten hinsichtlich der infrastrukturellen Sicherheitsmaßnahmen einen ausreichenden Schutz.

5.1.2 Zutrittskontrolle

Der Zutritt zu den Betriebsräumen der PCA und zu den DFN-Kernnetzknotten ist durch geeignete technische und infrastrukturelle Maßnahmen gesichert und wird nur autorisierten Mitarbeitern gestattet. Der Zutritt durch betriebsfremde Personen wird durch eine Besucherregelung festgelegt.

5.1.3 Stromversorgung und Klimatisierung

Die Installation zur Stromversorgung entspricht den erforderlichen Normen, eine Klimatisierung der Betriebsräume für die technische Infrastruktur ist vorhanden.

5.1.4 Abwehr von Wasserschäden

Die Betriebsräume für die technische Infrastruktur verfügen über einen angemessenen Schutz vor Wasserschäden.

5.1.5 Feuer

Die Brandschutzvorschriften werden eingehalten, Handfeuerlöcher sind in ausreichender Anzahl vorhanden.

5.1.6 Lagerung der Datenträger

Die Zertifizierung betreffende Papierunterlagen werden in einem verschlossenen Stahlschrank aufbewahrt. Datenträger mit Schlüsselmaterial von CAs sowie Backupmedien werden in einem Tresor aufbewahrt, der der VdS-Schutzklasse I oder höher entspricht.

5.1.7 Abfallentsorgung

Informationen auf elektronischen Datenträgern und auf Papierdatenträgern werden sachgemäß vernichtet und anschließend durch einen Dienstleister sachgerecht entsorgt.

5.1.8 Externes Backup

Ausgelagerte Backupmedien werden in einem Bankschließfach verwahrt.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Sicherheitsrelevante Rollen

Siehe CP.

5.2.2 Erforderliche Anzahl von Personen je Tätigkeit

Siehe CP.

5.2.3 Identifizierung und Authentifizierung der Rollen

Siehe CP.

5.2.4 Trennung von Rollen

Die PCA wählt für ihren Betrieb die in Tabelle 1 angegebene Aufteilung der Rollen auf Personengruppen. Keine Person gehört mehr als einer Personengruppe an.

Personengruppe	Rollen
1	R, ISO
2	TS, RG, CAO1
3	CAO2, SA, SO

Tabelle 1: Aufteilung der Rollen auf Personengruppen bei der PCA

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an die Mitarbeiter

Die Mitarbeiter der PCA erfüllen alle notwendigen Anforderungen an Vertrauenswürdigkeit, Integrität, Zuverlässigkeit und Fachkunde. Neben einer Ausbildung auf dem Gebiet Informationstechnik verfügen sie über angemessene Fachkenntnisse in den Bereichen:

- Sicherheitstechnologie, Kryptographie, elektronische Signaturen, PKI
- Internationale Standards, technische Normen
- Nationale und internationale Rechtssprechung
- Unix/Linux Betriebssysteme, TCP/IP Netzwerke und relationale Datenbanken

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Von allen Mitarbeitern der PCA liegt ein maximal zwei Jahre altes polizeiliches Führungszeugnis vor.

5.3.3 Anforderungen an die Schulung

In der PCA werden ausschließlich qualifizierte Mitarbeiter eingesetzt, für die regelmäßig geeignete Schulungen durchgeführt werden. Mitarbeiter erhalten erst nach Nachweis der notwendigen Fachkunde die Berechtigung, spezifische Rollen auszuführen.

5.3.4 Frequenz von Schulungen

Die Frequenz der Schulungen orientiert sich an den Anforderungen der PCA. Schulungen werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt.

5.3.5 Ablauf und Sequenz der Job Rotation

Keine Angaben.

5.3.6 Sanktionen für unautorisierte Handlungen

Unautorisierte Handlungen, die die Sicherheit der IT-Systeme der PCA gefährden oder gegen Datenschutzbestimmungen verstoßen, werden disziplinarisch geahndet. Bei strafrechtlicher Relevanz werden die zuständigen Behörden informiert.

5.3.7 Anforderungen an die Arbeitsverträge

Für die Arbeitsverträge der Mitarbeiter der PCA gilt das Recht der Bundesrepublik Deutschland. Alle Mitarbeiter sind gemäß den gesetzlichen Datenschutzbestimmungen zur Geheimhaltung verpflichtet.

5.3.8 Dokumente für die Mitarbeiter

Den Mitarbeitern der PCA steht neben CP und diesem CPS das Betriebshandbuch der PCA zur Verfügung.

5.4 Sicherheitsüberwachung

5.4.1 Überwachte Ereignisse

Zur Abwehr von Angriffen und zur Kontrolle der ordnungsgemäßen Funktion der PCA werden u.a. nachfolgende Ereignisse in Form von Log-Dateien oder Papierprotokollen erfasst:

- Bootvorgänge
- fehlgeschlagene Login-Versuche
- Eingang und Genehmigung von Zertifikatanträgen und Sperranträgen
- Ausstellung und Sperrung von Zertifikaten
- Einrichtung und Änderung von Rollenzuordnungen und Berechtigungen

5.4.2 Frequenz der Protokollanalyse

Eine Überprüfung der Protokolldaten findet regelmäßig mindestens einmal pro Monat statt. Bei Verdacht auf außergewöhnliche Ereignisse werden Sonderprüfungen vorgenommen.

5.4.3 Aufbewahrungszeitraum für Protokolldaten

Die Aufbewahrungsdauer von Dokumenten und Zertifikaten entspricht mindestens der Gültigkeitsdauer des Zertifikats der CA, mit dem das Zertifikat des Zertifikatnehmers erstellt wurde, zuzüglich eines Jahres.

5.4.4 Schutz der Protokolldaten

Elektronische Logdateien werden mit Mitteln des Betriebssystems gegen Zugriff, Löschung und Manipulation geschützt und sind nur den System- und Netzwerkadministratoren zugänglich.

5.4.5 Backup der Protokolldaten

Die Protokolldaten werden zusammen mit anderen relevanten Daten der PCA einem regelmäßigen Backup unterzogen.

5.4.6 Überwachungssystem

Es wird ein internes Überwachungssystem verwendet.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Bei schwerwiegenden Ereignissen wird unverzüglich der Sicherheitsbeauftragte informiert. In Zusammenarbeit mit den Systemadministratoren werden notwendige Aktionen festgelegt, um auf die Ereignisse adäquat reagieren zu können, ggf. wird die Geschäftsleitung informiert.

5.4.8 Schwachstellenuntersuchung

Eine Schwachstellenuntersuchung findet durch die PCA selbst bzw. durch den Hersteller der verwendeten Software statt.

5.5 Archivierung

5.5.1 Archivierte Daten

Im Rahmen des Zertifizierungsprozesses angefallene Daten wie Zertifikatanträge, ausgestellte Zertifikate, Sperranträge und CRLs werden archiviert.

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Es gelten die Regelungen aus Abschnitt 5.4.3.

5.5.3 Schutz der Archive

Es wird durch geeignete Maßnahmen sichergestellt, dass die Daten nicht verändert, gelöscht, unbefugt gelesen oder kopiert werden können.

5.5.4 Datensicherungskonzept

Die in Abschnitt 5.4.1 und Abschnitt 5.5.1 aufgeführten Daten werden auf Grundlage eines Datensicherungskonzepts mit folgenden Eckwerten einem Backup auf Band oder CD-ROM unterzogen:

- inkrementelles Backup an jedem Werktag
- wöchentliches vollständiges Backup
- monatliches Archivbackup
- Die Backupmedien werden in den Büroräumen außerhalb des Serverraums sowie in einem Bankschließfach außerhalb der Büroräume aufbewahrt.

5.5.5 Anforderungen für Zeitstempel

Keine Angaben.

5.5.6 Archivierungssystem

Es wird ein internes Archivierungssystem verwendet.

5.5.7 Prozeduren zum Abrufen und Überprüfen von archivierten Daten

Der Sicherheitsbeauftragte kann den Abruf und die Prüfung der archivierten Daten autorisieren.

5.6 Schlüsselwechsel

Siehe CP.

5.7 Kompromittierung und Wiederherstellung

Siehe CP.

5.8 Einstellung des Betriebs

Siehe CP.

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselerzeugung und Installation

Siehe CP.

6.2 Schutz des privaten Schlüssels

Siehe CP.

6.3 Weitere Aspekte des Schlüsselmanagements

Siehe CP.

6.4 Aktivierungsdaten

Siehe CP.

6.5 Sicherheitsmaßnahmen für Computer

Siehe CP.

6.6 Lebenszyklus der Sicherheitsmaßnahmen

6.6.1 Softwareentwicklung

Die Erstellung von Software erfolgt durch qualifizierte Mitarbeiter in einer gesicherten Entwicklungsumgebung. Der Einsatz von Software (Eigen- oder Fremdentwicklung) auf einem Produktivsystem erfolgt erst nach Abnahme und Freigabe.

6.6.2 Sicherheitsmanagement

Das Sicherheitsmanagement umfasst folgende Aspekte:

- jährliches Audit (Konformitätsprüfung)
- regelmäßige Evaluierung und Weiterentwicklung des Sicherheitskonzepts
- Überprüfung der Sicherheit im laufenden Betrieb (siehe Abschnitt 5.4)
- regelmäßige Integritätsprüfungen der eingesetzten Anwendungen und Betriebssysteme
- zentrales Logging aller sicherheitsrelevanten Vorgänge
- Zusammenarbeit mit dem DFN-CERT
- Einspielung von Upgrades und Patches sofern erforderlich

6.6.3 Sicherheitseinstufung

Keine Angaben.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Das Netzwerk der PCA ist in verschiedene Sicherheitszonen unterteilt, die jeweils durch ein Firewallsystem voneinander abgeschottet sind. Darüber hinaus werden zur Abwehr von Angriffen aus dem Internet, wie auch aus dem Intranet, Intrusion Prevention bzw. Detection Systeme eingesetzt. Kritische Sicherheitsvorfälle werden unverzüglich in Zusammenarbeit mit dem DFN-CERT verfolgt und bearbeitet. Auf allen Firewalls ist ein Regelwerk aktiviert, das nur den in einer definierten Kommunikationsmatrix erlaubten Netzwerkverkehr zulässt.

6.8 Zeitstempel

Siehe CP.

7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen

Siehe CP.

8 Konformitätsprüfung

Siehe CP.

9 Rahmenvorschriften

Siehe CP.

10 Referenzen

Siehe CP.

11 Glossar

Siehe CP.