deutsches forschungsnetz

Erklärung zum Zertifizierungsbetrieb der DFN-PKI

– Sicherheitsniveau „Global“ –

DFN-Verein
CPS der DFN-PKI
V13 29.09.2023

Inhaltsverzeichnis

1 Einleitung

1.1 Überblick

Im Rahmen der DFN-PKI betreibt der DFN-Verein für das Sicherheitsniveau Global die oberste Zertifizierungsstelle (Policy Certification Authority, DFN-PCA) und alle nachgeordneten Zertifizierungsstellen (Sub-CAs).

Dieses Dokument ist die *Erklärung zum Zertifizierungsbetrieb der DFN-PKI – Sicherheitsniveau Global* – (CPS) der DFN-PCA sowie aller Sub-CAs für das Sicherheitsniveau Global. Es beschreibt Spezifikationen, Prozesse und technische Sicherheitsmaßnahmen der DFN-PCA und aller Sub-CAs für die Ausstellung von Zertifikaten.

Diesem Dokument zugehörig ist die Zertifizierungsrichtlinie (CP) der DFN-PKI in der jeweils aktuellen Version: „Zertifizierungsrichtlinie der DFN-PKI – Sicherheitsniveau Global –".

Im Folgenden werden die Begriffe DFN-PKI und DFN-PCA ausschließlich im Kontext des Sicherheitsniveaus Global verwendet.

Der Betrieb der DFN-PCA sowie aller Sub-CAs 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 DFN-PKI – Sicherheitsniveau Global –
- Version: 13
- Object Identifier (OID): 1.3.6.1.4.1.22177.300.2.1.4.13

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) global (4) major-version(13)}

1.3 Teilnehmer der Zertifizierungsinfrastruktur

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

Siehe CP.

CP und CPS werden in deutscher und englischer Sprache veröffentlicht. Die deutschen und englischen Versionen haben immer die gleiche Versionsnummer und werden inhaltlich synchronisiert. Die englische Version ist maßgeblich.

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 aller CAs befinden sich in den Betriebsräumen der DFN-PCA. Die Betriebsräume bieten hinsichtlich der infrastrukturellen Sicherheitsmaßnahmen einen ausreichenden Schutz.

Es ist eine Gefahrenmeldeanlage mit Aufschaltung auf eine Alarmzentrale installiert.

5.1.2 Zutrittskontrolle

Der Zutritt zu den Betriebsräumen der DFN-PCA 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, Handfeuerlöscher 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 Backup-Medien 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 Backup-Medien 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

Siehe CP.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an die Mitarbeiter

Die Mitarbeiter der DFN-PCA werden von der Geschäftsführung benannt und eingesetzt. Die Benennung wird erst wirksam, wenn der Mitarbeiter sie akzeptiert. Mitarbeiter 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 Rechtsprechung
- Unix/Linux Betriebssysteme, TCP/IP Netzwerke und relationale Datenbanken

Die Arbeitgeber der Mitarbeiter mit sicherheitskritischen Rollen halten diese von mit der Policy der DFN-PKI in Konflikt stehenden Interessen, die ihre Unbefangenheit beeinträchtigen können, frei.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Von allen Mitarbeitern der DFN-PCA liegt ein maximal drei Jahre altes polizeiliches Führungszeugnis vor. Vor Ablauf der drei Jahre wird ein Mitarbeiter rechtzeitig aufgefordert, ein neues Führungszeugnis vorzulegen. Eine Ernennung eines neuen Mitarbeiters wird erst nach Vorliegen eines Führungszeugnisses wirksam.

5.3.3 Anforderungen an die Schulung

In der DFN-PCA werden ausschließlich qualifizierte Mitarbeiter eingesetzt, für die regelmäßig geeignete Schulungen durchgeführt werden. Die Nachweise über die Schulungen werden gemäß der Regelungen aus Abschnitt 5.5 archiviert. 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 DFN-PCA, in der Regel werden Schulungen jährlich wiederholt. Schulungen werden darüber hinaus nach der Einführung neuer Richtlinien, IT-Systeme und Sicherheitstechnik durchgeführt.

5.3.5 Ablauf und Sequenz der Job Rotation

Es gibt keine Vorgaben für regelmäßige Job Rotation.

5.3.6 Sanktionen für unautorisierte Handlungen

Unautorisierte Handlungen, die die Sicherheit der IT-Systeme der DFN-PCA gefährden oder gegen Datenschutzbestimmungen verstoßen, werden disziplinarisch geahndet und der Mitarbeiter wird ggf. von seinen Funktionen entbunden. Bei strafrechtlicher Relevanz werden die zuständigen Behörden informiert.

Teilnehmerservice-Mitarbeiter, die gegen ihre Pflichten verstoßen, werden nachgeschult. Bei wiederholtem Verstoß werden sie von ihrer Rolle entbunden und das entsprechende Zertifikat gesperrt.

5.3.7 Anforderungen an die Arbeitsverträge

Für die Arbeitsverträge der Mitarbeiter der DFN-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 DFN-PCA steht neben CP und diesem CPS das Betriebshandbuch der DFN-PCA zur Verfügung.

5.4 Sicherheitsüberwachung

5.4.1 Überwachte Ereignisse

Zur Abwehr von Angriffen und zur Kontrolle der ordnungsgemäßen Funktion der DFN-PCA werden u. a. nachfolgende Ereignisse mit Zeitpunkt des Auftretens erfasst:

1. Ereignisse im Lebenszyklus von CA-Zertifikaten und Schlüsseln:

- 1. die Schlüsselerzeugung, -sicherung, -speicherung, -wiederherstellung, -archivierung und -vernichtung;
- 2. die Beantragung von Zertifikaten, deren Erneuerung, die Beantragung von neuen Schlüsseln und die Sperrung;
- 3. die Genehmigung und Ablehnung von Zertifikatsanträgen;
- 4. Lifecycle-Ereignisse von HSMs;
- 5. Erstellung von CRLs;
- 6. Signieren von OCSP-Antworten und
- 7. Einführung neuer und Stilllegung bestehender Zertifikatsprofile.

2. Ereignisse im Lebenszyklus von End-User-Zertifikaten:

- 1. die Beantragung von Zertifikaten, deren Erneuerung, die Beantragung von neuen Schlüsseln und die Sperrung;
- 2. alle Verifizierungstätigkeiten;
- 3. die Genehmigung und Ablehnung von Zertifikatsanträgen;
- 4. die Ausstellung von Zertifikaten;
- 5. Erstellung von Zertifikatswiderrufslisten; und
- 6. Signieren von OCSP-Antworten
- 7. sowie Anfrage nach unbekannten Zertifikatseriennummern im OCSP

3. Sicherheitsereignisse:

- 1. erfolgreiche und erfolglose Zugriffsversuche auf das PKI-System
- 2. durchgeführte PKI- und Sicherheitssystem-Aktionen;
- 3. Änderungen an sicherheitsrelevanten Konfigurationen
- 4. die Installation, Aktualisierung und Entfernung von Software;
- 5. Systemabstürze, Hardwareausfälle und andere Anomalien;
- 6. Firewall- und Router-Aktivitäten; und
- 7. Betreten und Verlassen des Rechenzentrums.

4. Weitere Ereignisse:

- 1. Verfügbarkeit und Auslastung von Diensten und Netzwerken
- 2. Start und Beendigung der Log-Funktion

Die Systemzeit wird kontinuierlich, spätestens alle 24 Stunden mit der Referenzzeit UTC synchronisiert, z. B. über GPS oder DCF77. Durch Einsatz geeigneter Maßnahmen wird die Genauigkeit und Monotonität der Zeit im Rahmen des Standes der Technik sichergestellt.

Die Protokolldaten werden entsprechend der jeweiligen Anforderungen archiviert (siehe Abschnitt 5.5).

Mit der Überwachung der Ereignisse wird die Rechenschaftspflicht individueller Mitarbeiter sichergestellt.

Die Protokolldaten werden im Rahmen von Konformitätsprüfungen den Auditoren zur Verfügung gestellt.

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

Protokolldaten werden frühestens sieben Jahre nach Ablauf aller mit dem Protokoll in Beziehung stehenden Zertifikate gelöscht.

5.4.4 Schutz der Protokolldaten

Elektronische Log-Dateien 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 DFN-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 Geschäftsführung informiert.

5.4.8 Schwachstellenuntersuchung

Alle drei Monate oder nach größeren Systemänderungen wird ein Vulnerability Scan auf die PCA-Systeme durchgeführt. Fordert das CA/Browser Forum zu einem Vulnerability Scan auf, so wird dieser innerhalb von einer Woche durchgeführt.

Zusätzlich wird einmal jährlich oder nach größeren Systemänderungen ein umfangreicher Penetration Test durchgeführt.

Vulnerability Scans und Penetration Tests werden nur von fachkundigen, unabhängigen Personen durchgeführt. Die Fachkunde wird dokumentiert.

5.5 Archivierung

5.5.1 Archivierte Daten

Dokumente und Daten aus Zertifikatanträgen, Dokumente und Daten aus der Verifikation der Angaben in Zertifikatanträgen, ausgestellte Zertifikate und Sperrinformationen zu Zertifikaten werden archiviert.

5.5.2 Aufbewahrungszeitraum für archivierte Daten

Die in 5.5.1 spezifizierten Daten werden nach Ablauf aller auf diesen Daten basierender Zertifikate mindestens sieben Jahre aufbewahrt.

5.5.3 Schutz der Archive

Es wird durch geeignete Maßnahmen sichergestellt, dass die Daten nicht verändert, gelöscht, unbefugt gelesen oder kopiert werden können. Darüber hinaus wird sicher gestellt, dass für jedes Zertifikat eindeutig der zugehörige Antrag identifiziert werden kann.

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 auf Band oder anderen Medien gesichert:

- inkrementelles Backup an jedem Werktag
- wöchentliches vollständiges Backup

- monatliches Archiv-Backup
- Backup-Medien werden in den Büroräumen außerhalb des Server-Raums aufbewahrt
- Regelmäßige Restore-Tests inkl.Dokumentation

5.5.5 Anforderungen für Zeitstempel

Die Systemzeit für Zeitstempel wird mit einer DCF77-Uhr synchronisiert.

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. Details der Softwareentwicklung sind im internen Dokument „Betriebshandbuch der DFN-PKI“ enthalten.

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
- Mindestens wöchentliche Überprüfung der Konfigurationen nach Kapitel 3h) der Network and Certificate System Security Requirements des CA/Browserforums
- Einspielung von Upgrades und Patches sofern erforderlich
- Account Management und zeitnahe Modifikation oder Entfernung von Zugriffsberechtigungen

Die Integrität der Systeme und Informationen ist gegen Viren, bösartigen und unauthorisierte Software geschützt. Updates und Patches, die vom Hersteller zur Verfügung gestellt werden, werden zunächst in einer Testumgebung installiert. Wenn festgestellt wird, dass die Updates oder Patches Instabilitäten oder Schwachstellen bewirken, die den Nutzen übersteigen, werden diese nicht auf Produktionssystemen installiert. Andernfalls erfolgt die Installation auf den Produktionssystemen. Die Installation wird dokumentiert. Eine Entscheidung über eine nicht erfolgte Installation wird ebenfalls dokumentiert.

Änderungen an Systemen oder Konfigurationen erfolgen sowohl für reguläre Veränderungen als auch für Notfall-Maßnahmen im Rahmen von Change Control Prozeduren. Diese Änderungen werden dokumentiert.

6.6.3 Lebenszyklus Sicherheitsmaßnahmen

Hardware und Software der CA Systeme werden kontinuierlich gewartet. Lebenszyklus-Controls von evaluierten Systemen wie z.B. HSMs werden strikt befolgt.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Das Netzwerk der DFN-PCA ist in verschiedene Sicherheitszonen unterteilt, die jeweils durch ein Firewall-System voneinander abgeschottet sind. Alle Sicherheitsmaßnahmen werden auf alle Systeme in derselben Zone angewandt. Das Netzwerk zur Administration ist vom operativen Netzwerk getrennt. Die Systeme, mit denen die Implementierung der Sicherheitsmaßnahmen administriert werden, werden nicht für andere Zwecke verwendet. Es werden zwei Rechenzentren mit redundanten Netzwerkanbindungen betrieben.

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 Firewall-Systemen ist ein Regelwerk aktiviert, das nur den in einer definierten Kommunikationsmatrix erlaubten Netzwerkverkehr zulässt.

Ungenutzte Accounts, Anwendungen, Services, Protokolle und Ports werden auf den Systemen der DFN-PCA entfernt bzw. deaktiviert.

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.

12 Änderungsverzeichnis

Für weiter zurückliegende Änderungen siehe https://www.pki.dfn.de/policies/policyarchiv

Version	Änderung	Datum
6	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs	03.04.2020
7	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs	03.06.2020
8	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs 5.1.1: Beschreibung der Gefahrenmeldeanlage ergänzt 5.4.1: Entry/Exit und Verfügbarkeit+Auslastung 5.4.8: Beschreibung Vulnerability Scan und Penetration Tests 6.6.2: Change Control 6.7: Netzwerktrennung	30.09.2020
9	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs	30.06.2021
10	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs	01.10.2021
11	Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs 5.3.1: Akzeptanz einer Benennung 5.3.2: Ernennung erst nach Vorliegen wirksam 5.4.1: Überwachte Ereignisse ausführlicher beschrieben, Zeitsynchronisation präziser dokumentiert 5.5.4: Restore-Tests auch hier beschrieben 6.6.2: Integrität der Systeme 6.7: Netzwerksicherheitsmaßnahmen ergänzt	14.11.2022
12	Titel und Fußzeile: Versionsnummer und Datum, Referenz auf CC BY-ND 1.2: OIDs 5.4.1 Einblick in Protokolldaten während eines Audits; Dokumentation der Ereignisse angepasst.	01.09.2023
13	Titel: Englische Version maßgeblich 1.2: OIDs 2: Englische Versionen von CP und CPS maßgeblich 5.4.1: Ereignisse erweitert.	29.09.2023