Erklärung zum Zertifizierungsbetrieb
der DFN-PKI

– Sicherheitsniveau „Global“ –
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 ............................................................................ 4
1.6 Definitionen und Abkürzungen ....................................................................... 4
2 Veröffentlichungen und Informationsdienste ...................................................... 4
3 Identifizierung und Authentifizierung ................................................................. 4
4 Ablauforganisation ............................................................................................... 4
5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen ........ 5
  5.1 Infrastrukturelle Sicherheitsmaßnahmen ....................................................... 5
  5.2 Organisatorische Sicherheitsmaßnahmen ..................................................... 5
  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 .................................................................... 9
  6.3 Weitere Aspekte des Schlüsselmanagements .............................................. 9
  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 .................................................................................................. 10
7 Profile für Zertifikate, Sperrlisten und Online-Statusabfragen ......................... 10
8 Konformitätsprüfung ......................................................................................... 10
9 Rahmenvorschriften ......................................................................................... 10
10 Referenzen ...................................................................................................... 10
11 Glossar ............................................................................................................. 10
12 Änderungsverzeichnis ..................................................................................... 10
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).
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: 9
- Object Identifier (OID): 1.3.6.1.4.1.22177.300.2.1.4.9
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(9)}\}

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.

3 Identifizierung und Authentifizierung
Siehe CP.

4 Ablauforganisation
Siehe CP.
5 Infrastrukturrelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturrelle 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


- Sicherheitstechnologie, Kryptographie, elektronische Signaturen, PKI
- Internationale Standards, technische Normen
- Nationale und internationale Rechtsprechung
- Unix/Linux Betriebssysteme, TCP/IP Netzerweke 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.

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


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:
- Bootvorgänge
- fehlschlagene Login-Versuche
- Eingang und Genehmigung von Zertifikanträgen und Sperranträgen (Registrierungsdaten und -Events)
- Ausstellung und Sperrung von Zertifikaten
- Einrichtung und Änderung von Rollenzuordnungen und Berechtigungen
- Erzeugung und Sperrung von CA-Zertifikaten
- Erzeugung, Speicherung, Backup, Wiederherstellung und Vernichtung von privaten Schlüsseln von CA-Zertifikaten
- Betreten und Verlassen der Sicherheitsbereiche
- Verfügbarkeit und Auslastung von Diensten und Netzwerken


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

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

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 CD-ROM gesichert:
- inkrementelles Backup an jedem Werktag
- wöchentliches vollständiges Backup
- monatliches Archiv-Backup

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

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
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.

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. 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.

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Änderung</th>
<th>Datum</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs</td>
<td>03.04.2020</td>
</tr>
<tr>
<td>7</td>
<td>Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs</td>
<td>03.06.2020</td>
</tr>
<tr>
<td>8</td>
<td>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</td>
<td>30.09.2020</td>
</tr>
<tr>
<td>9</td>
<td>Titel und Fußzeile: Versionsnummer und Datum. 1.2: OIDs</td>
<td>30.06.2021</td>
</tr>
</tbody>
</table>